亚马逊云科技

Developer Guide

Amazon Config



Amazon Config: Developer Guide

Table of Contents

What Is Amazon Config? 1
Considerations 1
Ways to Use Amazon Config 1
Resource Administration 1
Auditing and Compliance 2
Managing and Troubleshooting Configuration Changes 2
Security Analysis 2
Partner Solutions 3
Features 3
How Amazon Config Works 4
Resource Discovery 5
Resource Tracking 5
Delivery of Configuration Items 6
Control Access to Amazon Config 9
Terminology and concepts 9
Amazon Config Interfaces 10
Resource Management 11
Configuration Recorder 11
Delivery Channel 6
Amazon Config Rules 13
Amazon Service Integrations 17
Amazon Organizations 17
Amazon Control Tower 17
Amazon CloudTrail 17
Amazon Security Hub 18
Amazon Trusted Advisor 18
Amazon Audit Manager 19
Amazon Systems Manager 19
Amazon Firewall Manager 19
Amazon EC2 Dedicated Hosts 20
Application Load Balancers 20
Amazon CodeBuild 20
Amazon X-Ray 21
Amazon Service Management Connector 21

Amazon API Gateway ... 21
Region Support ... 21
Considerations ... 21
List of Supported Regions ... 22
Service Limits ... 26
Supplemental Information ... 28
Amazon Software Development Kits for Amazon Config ... 29
Getting Started ... 31
Signing up for Amazon ... 31
Sign up for an Amazon Web Services account ... 31
Secure IAM users ... 31
Ways to Get Started with Amazon Config ... 32
Setting Up (Console) ... 32
Setting up ... 32
1-click setup ... 33
Manual setup ... 36
Setting Up (Amazon CLI) ... 43
Setting up ... 43
Prerequisites ... 44
Starting Amazon Config ... 110
Verifying setup ... 113
Working with Amazon SDKs ... 115
Configuration Recorder ... 117
Considerations for the customer managed configuration recorder ... 118
Considerations for service-linked configuration recorders ... 119
Supported services ... 119
Drift detection for the configuration recorder ... 120
Starting the customer managed configuration recorder ... 120
Stopping the customer managed configuration recorder ... 121
Changing the recording frequency for the customer managed configuration recorder ... 122
Renaming the customer managed configuration recorder ... 125
Viewing your configuration recorders ... 126
Deleting your configuration recorders ... 127
Delivery Channel ... 129
Considerations ... 129
Terminology ... 130

Components of a Configuration Item ... 131
Viewing the Delivery Channel ... 133
Updating the Delivery Channel ... 134
Renaming the Delivery Channel ... 139
Delivering Configuration Snapshots ... 140
Delivering Configuration Snapshots ... 141
Verifying Delivery Status ... 141
Viewing Configuration Snapshots ... 142
Viewing Configuration Snapshots ... 142
Example Configuration Snapshot ... 143
Example Notifications ... 148
Example Configuration Item Change Notifications ... 149
Example Configuration History Delivery Notification ... 164
Example Configuration Snapshot Delivery Started Notification ... 165
Example Configuration Snapshot Delivery Notification ... 166
Example Compliance Change Notification ... 167
Example Rules Evaluation Started Notification ... 170
Example Oversized Configuration Item Change Notification ... 171
Example Delivery Failed Notification ... 174
Amazon Config Dashboard ... 176
Compliance and Resource Inventory ... 176
Amazon Config Usage and Success Metrics ... 178
Resource Management ... 181
Supported Resource Types ... 182
Amazon AppStream ... 183
Amazon AppFlow ... 183
... 184
Amazon API Gateway ... 184
Amazon Athena ... 185
Amazon Bedrock ... 185
Amazon CloudFront ... 185
Amazon CloudWatch ... 186
Amazon CodeGuru ... 187
Amazon Cognito ... 187
Amazon Connect ... 188
Amazon Detective ... 188

Amazon DynamoDB ... 189
Amazon EC2 ... 189
Amazon ECR ... 198
Amazon ECS ... 198
Amazon EFS ... 199
Amazon EKS ... 199
Amazon EMR ... 200
Amazon EventBridge ... 200
Amazon Forecast ... 201
Amazon Fraud Detector ... 202
Amazon GuardDuty ... 202
Amazon Inspector ... 203
Amazon IVS ... 203
Amazon Keyspaces ... 203
Amazon OpenSearch Service ... 204
Amazon Personalize ... 205
Amazon Pinpoint ... 205
Amazon QLDB ... 206
Amazon Kendra ... 206
Amazon Kinesis ... 207
Amazon Lex ... 207
Amazon Lightsail ... 208
Amazon Lookout for Metrics ... 208
Amazon Lookout for Vision ... 209
Amazon Macie ... 209
Amazon Managed Grafana ... 209
Amazon Managed Service for Prometheus ... 209
Amazon MemoryDB ... 210
Amazon MQ ... 210
Amazon MSK ... 210
Amazon QuickSight ... 211
Amazon Redshift ... 211
Amazon RDS ... 213
Amazon Route 53 ... 214
Amazon SageMaker AI ... 215
Amazon SES ... 217

Amazon SNS ... 217
Amazon SQS ... 217
Amazon S3 ... 218
Amazon WorkSpaces ... 220
Amazon Amplify ... 220
Amazon AppConfig ... 220
Amazon App Runner ... 221
Amazon App Mesh ... 222
Amazon AppSync ... 222
Amazon Audit Manager ... 223
Amazon Auto Scaling ... 223
Amazon Backup ... 224
Amazon Batch ... 225
Amazon Budgets ... 225
Amazon Certificate Manager ... 225
Amazon CloudFormation ... 226
Amazon CloudTrail ... 226
Amazon Cloud9 ... 226
Amazon Cloud Map ... 227
Amazon CodeArtifact ... 227
Amazon CodeBuild ... 228
Amazon CodeDeploy ... 228
Amazon CodePipeline ... 229
Amazon Config ... 229
Amazon DMS ... 230
Amazon DataSync ... 231
Amazon Device Farm ... 232
Amazon Elastic Beanstalk ... 233
Amazon FIS ... 233
Amazon Global Accelerator ... 234
Amazon Glue ... 234
Amazon Ground Station ... 235
Amazon HealthLake ... 235
Amazon IAM ... 235
Amazon IoT ... 237
Amazon KMS ... 240

Amazon Lambda ... 241
Amazon Mainframe Modernization ... 241
Amazon Network Firewall ... 241
Amazon Network Manager ... 242
Amazon Panorama ... 243
Amazon Private CA ... 244
Amazon Resilience Hub ... 244
Amazon Resource Explorer ... 244
Amazon RoboMaker ... 245
Amazon Signer ... 245
Amazon Secrets Manager ... 245
Amazon Security Hub ... 246
Amazon Service Catalog ... 246
Amazon Shield ... 246
Amazon Step Functions ... 247
Amazon Systems Manager ... 247
Amazon Transfer Family ... 248
Amazon WAF ... 249
Amazon X-Ray ... 251
Elastic Load Balancing ... 251
MediaConnect ... 252
MediaPackage ... 252
MediaTailor ... 253
Resource Coverage by Region Availability ... 253
North and South America ... 253
Europe ... 318
Asia Pacific ... 370
China ... 417
Africa and Middle East ... 454
GovCloud ... 506
Recording Amazon Resources ... 553
Considerations ... 554
Regional and global Resources ... 555
Amazon Config Rules and global resource types ... 558
Recording frequency ... 560
Non-recorded resources ... 561

Recording resources (Console) ... 561
Recording resources (Amazon CLI) ... 565
Excluding resources ... 573
Stopping recording ... 574
Recording Third-Party Resources (Amazon CLI) ... 574
Adding Resources ... 575
Recording Configuration Items ... 578
Reading Configuration Items ... 579
Deleting Resources ... 580
Recording Software Configurations ... 581
Prerequisites ... 581
Recording Software Configurations ... 582
Looking up Resources ... 584
Viewing Resources ... 585
Viewing compliance (Console) ... 586
Viewing compliance (Amazon SDKs) ... 586
Viewing Compliance History ... 594
Viewing Compliance History (Console) ... 594
Viewing Compliance History (Amazon CLI) ... 595
For Resources and Rules ... 600
Querying Compliance History ... 602
Tagging Your Resources ... 603
Restrictions Related to Tagging ... 603
Managing Tags with Amazon Config API Actions ... 604
Amazon Config Rules ... 605
Considerations ... 605
Region Support ... 608
Components of a Rule ... 615
How Amazon Config Rules Work ... 616
Trigger Types ... 617
Evaluation Modes ... 618
Rule Metadata ... 619
Managed Rules ... 621
List of Managed Rules ... 621
List of Managed Rules by Evaluation Mode ... 830
List of Managed Rules by Trigger Type ... 853

List of Managed Rules by Region Availability 875
Creating Managed Rules With Amazon CloudFormation Templates 1429
Custom Rules 1431
Custom Policy Rules 1431
Custom Lambda Rules 1431
Format differences for Amazon Config Custom Rules 1432
Creating Custom Policy Rules 1432
Creating Custom Lambda Rules 1439
Managing Deleted Resources for Custom Lambda Rules 1461
Service-Linked Rules 1463
Adding Rules 1464
Using the console 1464
Using the Amazon SDKs 1467
Updating Rules 1470
Using the console 1471
Using the Amazon SDKs 1471
Deleting Rules 1475
Considerations 1475
Using the console 1476
Using the Amazon SDKs 1477
Viewing Rules 1478
Using the console 1478
Using the Amazon SDKs 1479
Turning on Proactive Evaluation 1491
Using the console 1491
Using the Amazon SDKs 1494
Sending Evaluations to Security Hub 1498
Send Rule Evaluations to Security Hub 1498
Evaluating Resources with Rules 1498
Deleting Evaluation Results 1503
Troubleshooting 1504
Remediation 1506
Region Support 1506
Setting Up Manual Remediation 1510
Setting Up Auto Remediation 1511
Deleting Remediation Actions 1514

Aggregators 1515
Use Cases 1515
Terminology 1516
Region Support 1516
Aggregator Dashboard 1521
Using the Aggregator Dashboard 1521
Compliance Dashboard 1524
Inventory Dashboard 1526
Creating Aggregators 1528
Registering a Delegated Administrator 1533
Editing Aggregators 1535
Deleting Aggregators 1537
Authorizing Aggregator Accounts 1538
Considerations 1538
Adding Authorization 1539
Deleting Authorizations 1541
Considerations 1541
Deleting Authorization 1541
Viewing Aggregators 1542
Troubleshooting 1543
Advanced Queries 1546
Features 1547
Query Components 1547
Synopsis 1547
Parameters 1548
Examples 1548
Query Editor (Console) 1549
Considerations 1549
Use an Amazon Sample Query 1549
Create your custom query 1550
Query Editor (Amazon CLI) 1551
Considerations 1551
Query Resource Configuration Data 1552
Save a Query 1553
View all the Saved Queries 1554
Get Details of a Saved Query 1555

Delete a Saved Query 1555
Natural language query processor 1555
Considerations 1556
Query using the natural language query processor 1549
Example prompts 1557
Providing feedback 1561
Region Support 1561
Examples Queries 1561
Example Relationship Queries 1567
Limitations 1569
CIDR notation/IP range 1571
Multiple properties within an array 1572
Region Support 1572
Deleting Data 1577
Setting Data Retention Period (Console) 1579
Security 1581
Data Protection 1582
Encryption of Data in Transit 1583
Encryption of Data in Transit 1583
Identity and Access Management 1583
Audience 1584
Authenticating with identities 1584
Managing access using policies 1587
How Amazon Config works with IAM 1590
Identity-based policy examples 1596
Amazon managed policies 1613
Permissions for the IAM Role 1779
Updating the IAM Role 1784
Permissions for the Amazon S3 Bucket 1785
Permissions for the KMS Key 1790
Permissions for the Amazon SNS Topic 1793
Troubleshooting 1796
Using Service-Linked Roles 1798
Incident Response 1800
Compliance Validation 1801
Resilience 1802

Infrastructure Security ... 1802
Configuration and Vulnerability Analysis ... 1802
Cross-service confused deputy prevention ... 1803
Best Practices ... 1803
Logging and Monitoring ... 1805
Logging ... 1805
Amazon Config Information in CloudTrail ... 1805
Understanding Amazon Config Log File Entries ... 1806
Example Log Files ... 1807
Monitoring ... 1814
Using Amazon SQS ... 1815
Using Amazon EventBridge ... 1817
Amazon VPC endpoints ... 1824
Create a VPC Endpoint ... 1824
FAQs ... 1825
Unable to see my latest configuration changes ... 1825
Can I expect to view my configuration changes right away? ... 1825
Indirect Relationships in Amazon Config ... 1825
What is resource relationship? ... 1825
What is a direct and an indirect relationship with respect to a resource? ... 1826
Which indirect relationships does Amazon Config support? ... 1826
Which scenarios uses indirect relationship? ... 1828
How are the configuration items created due to direct and indirect relationship? ... 1830
What are the configuration items generated due to indirect relationships? ... 1830
How do I disable indirect relationship? ... 1832
How do I retrieve configuration data related to indirect relationships? ... 1833
Code examples ... 1834
Basics ... 1834
Actions ... 1835
Document History ... 1871
Earlier Updates ... 2012

What Is Amazon Config?

Amazon Config provides a detailed view of the configuration of Amazon resources in your Amazon account. This includes how the resources are related to one another and how they were configured in the past so that you can see how the configurations and relationships change over time.

An Amazon *resource* is an entity you can work with in Amazon, such as an Amazon Elastic Compute Cloud (EC2) instance, an Amazon Elastic Block Store (EBS) volume, a security group, or an Amazon Virtual Private Cloud (VPC). For a complete list of Amazon resources supported by Amazon Config, see Supported Resource Types for Amazon Config.

Considerations

- **Amazon Web Services account**: You need an active Amazon Web Services account. For more information, see Signing up for Amazon.
- **Amazon S3 Bucket**: You need an S3 bucket to receive data for your configuration snapshots and history. For more information, see Permissions for the Amazon S3 Bucket.
- **Amazon SNS Topic**: You need an Amazon SNS to receive notifications when there are changes to your configuration snapshots and history. For more information, see Permissions for the Amazon SNS Topic.
- **IAM Role**: You need an IAM role that has the necessary permissions to access Amazon Config. For more information, see Permissions for the IAM Role.
- **Resource types**: You can decide which resource types you want Amazon Config to record. For more information, see Recording Amazon Resources.

Ways to Use Amazon Config

When you run your applications on Amazon, you usually use Amazon resources, which you must create and manage collectively. As the demand for your application keeps growing, so does your need to keep track of your Amazon resources. Amazon Config is designed to help you oversee your application resources in the following scenarios:

Resource Administration

To exercise better governance over your resource configurations and to detect resource misconfigurations, you need fine-grained visibility into what resources exist and how these

resources are configured at any time. You can use Amazon Config to notify you whenever resources are created, modified, or deleted without having to monitor these changes by polling the calls made to each resource.

You can use Amazon Config rules to evaluate the configuration settings of your Amazon resources. When Amazon Config detects that a resource violates the conditions in one of your rules, Amazon Config flags the resource as noncompliant and sends a notification. Amazon Config continuously evaluates your resources as they are created, changed, or deleted.

Auditing and Compliance

You might be working with data that requires frequent audits to ensure compliance with internal policies and best practices. To demonstrate compliance, you need access to the historical configurations of your resources. This information is provided by Amazon Config.

Managing and Troubleshooting Configuration Changes

When you use multiple Amazon resources that depend on one another, a change in the configuration of one resource might have unintended consequences on related resources. With Amazon Config, you can view how the resource you intend to modify is related to other resources and assess the impact of your change.

You can also use the historical configurations of your resources provided by Amazon Config to troubleshoot issues and to access the last known good configuration of a problem resource.

Security Analysis

To analyze potential security weaknesses, you need detailed historical information about your Amazon resource configurations, such as the Amazon Identity and Access Management (IAM) permissions that are granted to your users, or the Amazon EC2 security group rules that control access to your resources.

You can use Amazon Config to view the IAM policy that was assigned to a user, group, or role at any time in which Amazon Config was recording. This information can help you determine the permissions that belonged to a user at a specific time: for example, you can view whether the user `John Doe` had permission to modify Amazon VPC settings on Jan 1, 2015.

You can also use Amazon Config to view the configuration of your EC2 security groups, including the port rules that were open at a specific time. This information can help you determine whether a security group blocked incoming TCP traffic to a specific port.

Partner Solutions

Amazon partners with third-party specialists in logging and analysis to provide solutions that use Amazon Config output. For more information, visit the Amazon Config detail page at Amazon Config.

Features

When you set up Amazon Config, you can complete the following:

Resource management

- Specify the resource types you want Amazon Config to record.

- Set up an Amazon S3 bucket to receive a configuration snapshot on request and configuration history.
- Set up Amazon SNS to send configuration stream notifications.
- Grant Amazon Config the permissions it needs to access the Amazon S3 bucket and the Amazon SNS topic.

  For more information, see Viewing Amazon Resource Configurations and History and Managing Amazon Resource Configurations and History.

Rules and conformance packs

- Specify the rules that you want Amazon Config to use to evaluate compliance information for the recorded resource types.
- Use conformance packs, or a collection of rules that can be deployed and monitored as a single entity in your Amazon Web Services account.

  For more information, see Evaluating Resources with Amazon Config Rules and Conformance Packs.

Remediation

- Remediate noncompliant resources that are evaluated by Amazon Config Rules.

  For more information, see Remediation.

Aggregators

- Use an aggregator to get a centralized view of your resource inventory and compliance. An aggregator collects Amazon Config configuration and compliance data from multiple Amazon Web Services accounts and Amazon Regions into a single account and Region.

  For more information, see Multi-Account Multi-Region Data Aggregation.

Advanced queries

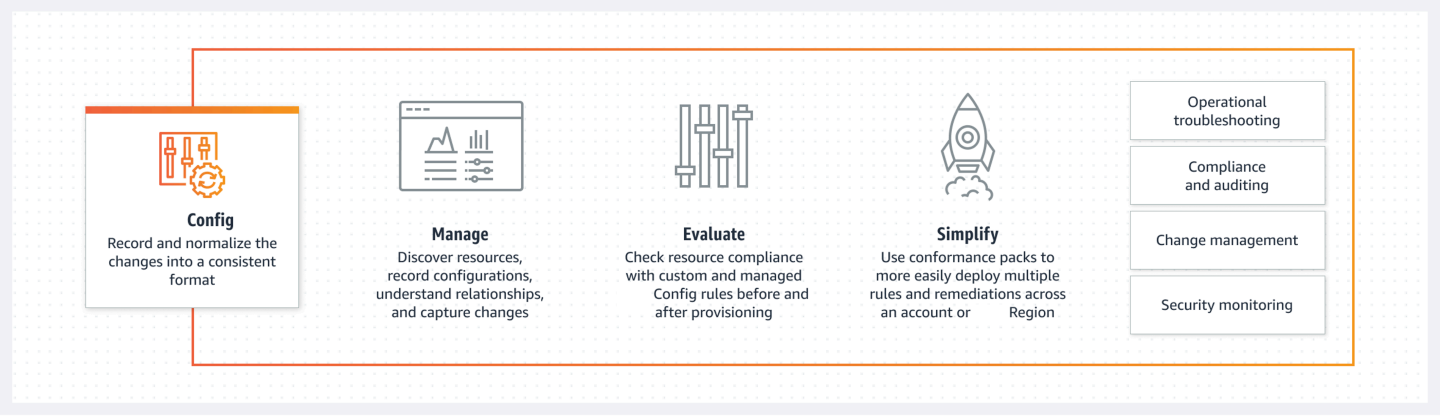
- Use one of the sample queries or write your own query by referring to the configuration schema of the Amazon resource.

  For more information, see Querying the Current Configuration State of Amazon Resources .

How Amazon Config Works

Amazon Config provides a detailed view of the configuration of Amazon resources in your Amazon account. This includes how the resources are related to one another and how they were configured in the past so that you can see how the configurations and relationships change over time.

An Amazon *resource* is an entity you can work with in Amazon, such as an Amazon Elastic Compute Cloud (EC2) instance, an Amazon Elastic Block Store (EBS) volume, a security group, or an Amazon Virtual Private Cloud (VPC). For a complete list of Amazon resources supported by Amazon Config, see Supported Resource Types for Amazon Config.



Resource Discovery

When you turn on Amazon Config, it first discovers the supported Amazon resources that exist in your account and generates a configuration item for each resource.

Amazon Config also generates configuration items when the configuration of a resource changes, and it maintains historical records of the configuration items of your resources from the time you start the configuration recorder. By default, Amazon Config creates configuration items for every supported resource in the region. If you don't want Amazon Config to create configuration items for all supported resources, you can specify the resource types that you want it to track.

Before specifying a resource type for Amazon Config to track, check Resource Coverage by Region Availability to see if the resource type is supported in the Amazon Region where you are setting up Amazon Config. If a resource type is supported by Amazon Config in at least one Region, you can enable the recording of that resource type in all Regions supported by Amazon Config, even if the specified resource type is not supported the Amazon Region where you are setting up Amazon Config.

Resource Tracking

Amazon Config keeps track of all changes to your resources by invoking the Describe or the List API call for each resource in your account. The service uses those same API calls to capture configuration details for all related resources.

For example, removing an egress rule from a VPC security group causes Amazon Config to invoke a Describe API call on the security group. Amazon Config then invokes a Describe API call on all of the instances associated with the security group. The updated configurations of the security group (the resource) and of each instance (the related resources) are recorded as configuration items and delivered in a configuration stream to an Amazon Simple Storage Service (Amazon S3) bucket.

Amazon Config also tracks the configuration changes that were not initiated by the API. Amazon Config examines the resource configurations periodically and generates configuration items for the configurations that have changed.

If you are using Amazon Config rules, Amazon Config continuously evaluates your Amazon resource configurations for desired settings. Depending on the rule, Amazon Config will evaluate your resources either in response to configuration changes or periodically. Each rule is associated with an Amazon Lambda function, which contains the evaluation logic for the rule. When Amazon Config evaluates your resources, it invokes the rule's Amazon Lambda function. The function

returns the compliance status of the evaluated resources. If a resource violates the conditions of a rule, Amazon Config flags the resource and the rule as noncompliant. When the compliance status of a resource changes, Amazon Config sends a notification to your Amazon SNS topic.

Delivery of Configuration Items

Amazon Config can deliver configuration items through one of the following channels:

Amazon S3 Bucket

Amazon Config tracks changes in the configuration of your Amazon resources, and it regularly sends updated configuration details to an Amazon S3 bucket that you specify. For each resource type that Amazon Config records, it sends a *configuration history file* every six hours. Each configuration history file contains details about the resources that changed in that six-hour period. Each file includes resources of one type, such as Amazon EC2 instances or Amazon EBS volumes. If no configuration changes occur, Amazon Config does not send a file.

Amazon Config sends a *configuration snapshot* to your Amazon S3 bucket when you use the deliver-config-snapshot command with the Amazon CLI, or when you use the DeliverConfigSnapshot action with the Amazon Config API. A configuration snapshot contains configuration details for all resources that Amazon Config records in your Amazon Web Services account. The configuration history file and configuration snapshot are in JSON format.

> **Note**
>
> Amazon Config only delivers the configuration history files and configuration snapshots to the specified S3 bucket; Amazon Config doesn't modify the lifecycle policies for objects in the S3 bucket. You can use lifecycle policies to specify whether you want to delete or archive objects to Amazon S3 Glacier. For more information, see Managing Lifecycle Configuration in the *Amazon Simple Storage Service User Guide*. You can also see the Archiving Amazon S3 Data to S3 Glacier blog post.

Amazon SNS Topic

An Amazon Simple Notification Service (Amazon SNS) topic is a communication channel that Amazon SNS uses to deliver messages (or *notifications*) to subscribing endpoints such as an email address or clients. Other types of Amazon SNS notifications include push notification messages to apps on mobile phones, Short Message Service (SMS) notifications to SMS-enabled mobile phones

and smart phones, and HTTP POST requests. For best results, use Amazon SQS as the notification endpoint for the SNS topic and then process the information in the notification programmatically.

Amazon Config uses the Amazon SNS topic that you specify to send you notifications. The type of notification that you are receiving is indicated by the value for the `messageType` key in the message body, as in the following example:

```
"messageType": "ConfigurationHistoryDeliveryCompleted"
```

The notifications can be any of the following message types.

Message type	Description
ComplianceChangeNotification	The compliance type of a resource that Amazon Config evaluates has changed. The compliance type indicates whether the resource complies with a specific Amazon Config rule, and it is represented by the `ComplianceType` key in the message. The message includes `newEvaluationResult` and `oldEvaluationResult` objects for comparison.
ConfigRulesEvaluationStarted	Amazon Config started evaluating your rule against the specified resources.
ConfigurationSnapshotDeliveryStarted	Amazon Config started delivering the configuration snapshot to your Amazon S3 bucket. The name of the Amazon S3 bucket is provided for the `s3Bucket` key in the message.
ConfigurationSnapshotDeliveryCompleted	Amazon Config successfully delivered the configuration snapshot to your Amazon S3 bucket.
ConfigurationSnapshotDeliveryFailed	Amazon Config failed to deliver the configura tion snapshot to your Amazon S3 bucket.

Message type	Description
ConfigurationHistoryDeliveryCompleted	Amazon Config successfully delivered the configuration history to your Amazon S3 bucket.
ConfigurationItemChangeNotification	A resource has been created, deleted, or changed in configuration. This message includes the details of the configuration item that Amazon Config creates for this change, and it includes the type of change. These notifications are delivered within minutes of a change and are collectively known as the *configuration stream*.
OversizedConfigurationItemChangeNotification	This message type is delivered when a configuration item change notification exceeded the maximum size allowed by Amazon SNS. The message includes a summary of the configuration item. With the exception of SMS messages, Amazon SNS messages can contain up to 256 KB of text data, including XML, JSON, and unformatted text. You can view the complete notification in the specified Amazon S3 bucket location.
OversizedConfigurationItemChangeDeliveryFailed	Amazon Config failed to deliver the oversized configuration item change notification to your Amazon S3 bucket.

For example notifications, see Notifications that Amazon Config Sends to an Amazon SNS topic. For more information about Amazon SNS, see the Amazon Simple Notification Service Developer Guide.

Note

Why can't I see my latest configuration changes?

Amazon Config usually records configuration changes to your resources right after a change is detected, or at the frequency that you specify. However, this is on a best effort basis and can take longer at times. If issues persist after sometime, contact Amazon Web Services Support and provide your Amazon Config metrics that are supported by Amazon CloudWatch. For information about these metrics, see Amazon Config Usage and Success Metrics.

Control Access to Amazon Config

Amazon Identity and Access Management is a web service that enables Amazon Web Services (Amazon) customers to manage users and user permissions.

To provide access, add permissions to your users, groups, or roles:

- Users managed in IAM through an identity provider:

  Create a role for identity federation. Follow the instructions in Create a role for a third-party identity provider (federation) in the *IAM User Guide*.
- IAM users:
  - Create a role that your user can assume. Follow the instructions in Create a role for an IAM user in the *IAM User Guide*.
  - (Not recommended) Attach a policy directly to a user or add a user to a user group. Follow the instructions in Adding permissions to a user (console) in the *IAM User Guide*.

Amazon Config terminology and concepts

To help you understand Amazon Config, this topic explains some of the key concepts.

Contents

- Amazon Config Interfaces
  - Amazon Config Console
  - Amazon Config CLI
  - Amazon Config APIs
  - Amazon Config SDKs
- Resource Management

- Amazon Resources
- Resource Relationship
- Configuration Recorder
- Delivery Channel
  - Configuration Items
  - Configuration History
  - Configuration Snapshot
  - Configuration Stream
- Amazon Config Rules
  - Evaluation Results
  - Rule Types
  - Trigger Types
  - Evaluation modes

Amazon Config Interfaces

Amazon Config Console

You can manage the service using the Amazon Config console. For more information about the Amazon Web Services Management Console, see Amazon Web Services Management Console.

Amazon Config CLI

The Amazon Command Line Interface is a unified tool that you can use to interact with Amazon Config from the command line. For more information, see the Amazon Command Line Interface User Guide. For a complete list of Amazon Config CLI commands, see Available Commands.

Amazon Config APIs

In addition to the console and the CLI, you can also use the Amazon Config RESTful APIs to program Amazon Config directly. For more information, see the Amazon Config API Reference.

Amazon Config SDKs

As an alternative to using the Amazon Config API, you can use one of the Amazon SDKs. Each SDK consists of libraries and sample code for various programming languages and platforms. The SDKs

provide a convenient way to create programmatic access to Amazon Config. For example, you can use the SDKs to sign requests cryptographically, manage errors, and retry requests automatically. For more information, see the Tools for Amazon Web Services page.

Resource Management

Understanding the basic components of Amazon Config will help you track resource inventory and changes and evaluate configurations of your Amazon resources.

Amazon Resources

Amazon resources are entities that you create and manage using the Amazon Web Services Management Console, the Amazon Command Line Interface (CLI), the Amazon SDKs, or Amazon partner tools. Examples of Amazon resources include Amazon EC2 instances, security groups, Amazon VPCs, and Amazon Elastic Block Store. Amazon Config refers to each resource using its unique identifier, such as the resource ID or an Amazon Resource Name (ARN). For a list of resource types that Amazon Config supports, see Supported Resource Types for Amazon Config.

Resource Relationship

Amazon Config discovers Amazon resources in your account and then creates a map of relationships between Amazon resources. For example, a relationship might include an Amazon EBS volume `vol-123ab45d` attached to an Amazon EC2 instance `i-a1b2c3d4` that is associated with security group `sg-ef678hk`.

For more information, see Supported Resource Types for Amazon Config.

Configuration Recorder

The *configuration recorder* stores the configuration changes to the resource types in scope as configuration items. For more information, see Working with the configuration recorder.

There are two types of configuration recorders.

Type	Description
Customer managed configuration recorder	A configuration recorder that you managed. The resource types in scope are set by you. By default, a customer managed configuration

Type	Description
	recorder records all supported resources in the Amazon Web Services Region where Amazon Config is running.
Service-linked configuration recorder	A configuration recorder that is linked to a specific Amazon Web Services service. The resource types in scope are set by the linked service.

Delivery Channel

As Amazon Config continually records the changes that occur to your Amazon resources, it sends notifications and updated configuration states through the *delivery channel*. You can manage the delivery channel to control where Amazon Config sends configuration updates.

Configuration Items

A *configuration item* represents a point-in-time view of the various attributes of a supported Amazon resource that exists in your account. The components of a configuration item include metadata, attributes, relationships, current configuration, and related events. Amazon Config creates a configuration item whenever it detects a change to a resource type that it is recording. For example, if Amazon Config is recording Amazon S3 buckets, Amazon Config creates a configuration item whenever a bucket is created, updated, or deleted. You can also select for Amazon Config to create a configuration item at the recording frequency that you set.

For more information, see Components of a Configuration Item and Recording Frequency.

Configuration History

A *configuration history* is a collection of the configuration items for a given resource over any time period. A configuration history can help you answer questions about, for example, when the resource was first created, how the resource has been configured over the last month, and what configuration changes were introduced yesterday at 9 AM. The configuration history is available to you in multiple formats. Amazon Config automatically delivers a configuration history file for each resource type that is being recorded to an Amazon S3 bucket that you specify. You can select a given resource in the Amazon Config console and navigate to all previous configuration items for

that resource using the timeline. Additionally, you can access the historical configuration items for a resource from the API.

For more information, see Viewing Compliance History and Querying Compliance History.

Configuration Snapshot

A *configuration snapshot* is a collection of the configuration items for the supported resources that exist in your account. This configuration snapshot is a complete picture of the resources that are being recorded and their configurations. The configuration snapshot can be a useful tool for validating your configuration. For example, you may want to examine the configuration snapshot regularly for resources that are configured incorrectly or that potentially should not exist. The configuration snapshot is available in multiple formats. You can have the configuration snapshot delivered to an Amazon Simple Storage Service (Amazon S3) bucket that you specify. Additionally, you can select a point in time in the Amazon Config console and navigate through the snapshot of configuration items using the relationships between the resources.

For more information, see Delivering Configuration Snapshots, Viewing Configuration Snapshots, and Example Configuration Snapshot.

Configuration Stream

A *configuration stream* is an automatically updated list of all configuration items for the resources that Amazon Config is recording. Every time a resource is created, modified, or deleted, Amazon Config creates a configuration item and adds to the configuration stream. The configuration stream works by using an Amazon Simple Notification Service (Amazon SNS) topic of your choice. The configuration stream is helpful for observing configuration changes as they occur so that you can spot potential problems, generating notifications if certain resources are changed, or updating external systems that need to reflect the configuration of your Amazon resources.

Amazon Config Rules

An Amazon Config rule is a compliance check that helps you manage your ideal configuration settings for specific Amazon resources. Amazon Config evaluates whether your resource configurations comply with relevant rules and displays the compliance results.

Evaluation Results

There are four possible evaluation results for an Amazon Config rule.

Evaluation result	Description
COMPLIANT	The rule passes the conditions of the compliance check.
NON_COMPLIANT	The rule fails the conditions of the compliance check.
ERROR	The one of the required/optional parameter s is not valid, not of the correct type, or is formatted incorrectly.
NOT_APPLICABLE	Used to filter out resources that the logic of the rule cannot be applied to. For example, the alb-desync-mode-check rule only checks Application Load Balancers, and ignores Network Load Balancers and Gateway Load Balancers.

Rule Types

There are two types of rules. For more information about the structure of rule definitions and rule metadata, see Components of an Amazon Config Rule.

Type	Description	More information
Managed rules	Predefined, customizable rules created by Amazon Config.	For a list of managed rules, see List of Amazon Config Managed Rules.
Custom rules	Rules that you create from scratch. There are two ways to create Amazon Config custom rules: Lambda functions (Amazon Lambda Developer Guide) and Guard (Guard GitHub Repository)	For more information, see Creating Amazon Config Custom Policy Rules and Creating Amazon Config Custom Lambda Rules.

Trigger Types

After you add a rule to your account, Amazon Config compares your resources to the conditions of the rule. After this initial evaluation, Amazon Config continues to run evaluations each time one is triggered. The evaluation triggers are defined as part of the rule, and they can include the following types.

Trigger type	Description
Configuration changes	Amazon Config runs evaluations for the rule when there is a resource that matches the rule's scope and there is a change in configura tion of the resource. The evaluation runs after Amazon Config sends a configuration item change notification. You choose which resources initiate the evaluation by defining the rule's *scope*. The scope can include the following: • One or more resource types • A combination of a resource type and a resource ID • A combination of a tag key and value • When any recorded resource is created, updated, or deleted Amazon Config runs the evaluation when it detects a change to a resource that matches the rule's scope. You can use the scope to define which resources initiate evaluations.
Periodic	Amazon Config runs evaluations for the rule at a frequency that you choose; for example, every 24 hours.

Trigger type	Description
Hybrid	Some rules have both configuration change and periodic triggers. For these rules, Amazon Config evaluates your resources when it detects a configuration change and also at the frequency that you specify.

Evaluation modes

There are two evaluation modes for Amazon Config rules.

Evaluation mode	Description
Proactive	Use proactive evaluation to evaluate resources before they have been deployed. This allows you to evaluate whether a set of resource properties, if used to define an Amazon resource, would be COMPLIANT or NON_COMPLIANT given the set of proactive rules that you have in your account in your Region. For more information, see Evaluation modes. For a list of managed rules that support proactive evaluation, see List of Amazon Config Managed Rules by Evaluation Mode.
Detective	Use detective evaluation to evaluate resources that have already been deployed. This allows you to evaluate the configuration settings of your existing resources.

> **Note**
>
> Proactive rules do not remediate resources that are flagged as NON_COMPLIANT or prevent them from being deployed.

Amazon Service Integrations with Amazon Config

Amazon Config supports integrations with several other Amazon services. This list is non-exhaustive.

Amazon Organizations

You can use Amazon Organizations to define the accounts to use for Amazon Config's multi-account, multi-Region data aggregation capability. Amazon Organizations is an account management service that helps you consolidate multiple Amazon Web Services accounts into an organization that you create and centrally manage. By providing your Amazon Organizations details, you can monitor the compliance status across your organization. For more information, Amazon Config and Amazon Organizations in the *Amazon Organizations User Guide*.

Amazon Control Tower

Amazon Control Tower enables Amazon Config on all enrolled accounts, so that it can monitor compliance through detective controls, record resource changes, and deliver resource change logs to the log archive account. For more information, see Monitor resource changes with Amazon Config in the *Amazon Control Tower User Guide*.

Amazon CloudTrail

Amazon Config integrates with Amazon CloudTrail to correlate configuration changes to particular events in your account. You can use the CloudTrail logs to obtain the details of the event that invoked the change, including who made the request, at what time, and from which IP address. You can navigate to the Amazon Config timeline from the CloudTrail console to view the configuration changes related to your Amazon API activities.

For more information, see Logging Amazon Config API Calls with Amazon CloudTrail in the *Amazon Config Developer Guide* and Create an event data store for Amazon Config configuration items with the console in the *Amazon CloudTrail User Guide*.

Amazon Security Hub

Amazon Security Hub centralizes security checks from other Amazon services, including Amazon Config rules. Security Hub enables and controls Amazon Config rules to verify your resource configurations are aligned to best practices. Enable Amazon Config on all accounts in all Regions where Security Hub is to run security checks on your environment's resources. For more information, see Amazon services that send findings to Security Hub in the *Amazon Security Hub User Guide*.

Some Security Hub-related rules are periodic and do not depend on configuration items

Some Security Hub-related rules are periodic. These rule can run without the configuration recorder being enabled and do not depend on configuration items (CI).
This means that if you view the rule page, there is no listed CI or supported resource. If you select the resource ID, you will see the following error: `The provided resource ID and resource type cannot be found`. This is expected behavior.

Amazon Trusted Advisor

Amazon Config managed rules power a set of Trusted Advisor checks across all categories. When you enable certain managed rules, the corresponding Trusted Advisor checks are automatically enabled. To see which Trusted Advisor checks are powered by specific Amazon Config managed rules, see Amazon Trusted Advisor check reference in the *Amazon Web Services Support User Guide*.

The Amazon Config powered checks are available to customers with Amazon Business Support, Amazon Enterprise On-Ramp, and Amazon Enterprise Support plans. If you enable Amazon Config and you have one of these Amazon Support plans, then you automatically see recommendations powered by corresponding deployed Amazon Config managed rules.

Refresh requests are not allowed and resources cannot be excluded

Results for these checks are automatically refreshed based on change-triggered updates to Amazon Config managed rules. Refresh requests are not allowed. Currently, you can't exclude resources from these checks.

For more information, see View Trusted Advisor checks powered by Amazon Config in the *Amazon Web Services Support User Guide*.

Amazon Audit Manager

You can use Audit Manager to capture Amazon Config evaluations as evidence for audits. When you create or edit a custom control, you can specify one or more Amazon Config rules as a data source mapping for evidence collection. Amazon Config performs compliance checks based on these rules, and Audit Manager reports the results as compliance check evidence. For more information, see Amazon Config Rules supported by Amazon Audit Manager in the *Amazon Audit Manager User Guide*.

Amazon Systems Manager

Amazon Config integrates with Systems Manager to record configuration changes to software on your Amazon EC2 instances and servers in your on-premises environment. With this integration, you can gain visibility into operating system (OS) configurations, system-level updates, installed applications, network configuration, and more. Amazon Config also provides a history of OS and system-level configuration changes alongside infrastructure configuration changes recorded for Amazon EC2 instances. You can navigate to the Amazon Config timeline from the Systems Manager console to view the configuration changes of your managed Amazon EC2 instances. You can use Amazon Config to view Systems Manager inventory history and track changes for all your managed instances.

For more information, see Integration with Amazon services | Management and Governance, Amazon Config configuration recorder, and Amazon Config conformance pack deployment in the *Amazon Systems Manager User Guide*.

Amazon Firewall Manager

To use Firewall Manager, you must enable Amazon Config for each of your Amazon Organizations member accounts. When new applications are created, Firewall Manager is the single service to build firewall rules, create security policies, and enforce them consistently. For more information, see Enable Amazon Config in the *Amazon WAF, Amazon Firewall Manager, and Amazon Shield Advanced Developer Guide*.

> **Note**
>
> Firewall Manager depends on continuous recording to monitor your resources. If you are using Firewall Manager, it is recommended that you set the recording frequency to Continuous. For more information on continuous recording and daily recording, see Recording Frequency.

Amazon EC2 Dedicated Hosts

Amazon Config integrates with Amazon EC2 Dedicated Hosts to assess license compliance. Amazon Config records when instances are launched, stopped, or shut down on a Dedicated Host, and pairs this information with host and instance level information relevant to software licensing, such as Host ID, Amazon Machine Image (AMI) IDs, number of sockets, and physical cores. This helps you use Amazon Config as a data source for your license reporting. You can navigate to the Amazon Config timeline from the Amazon EC2 Dedicated Hosts console to view the configuration changes of your Amazon EC2 Dedicated Hosts.

For more information, see Track configuration changes in the *Amazon Elastic Compute Cloud User Guide for Linux Instances* or Track configuration changes in the *Amazon Elastic Compute Cloud User Guide for Windows Instances*.

Application Load Balancers

Amazon Config integrates with the Elastic Load Balancing (ELB) service to record configuration changes to Application Load Balancers. Amazon Config also includes relationships with associated Amazon EC2 security groups, VPCs, and subnets. You can use this information for security analysis and troubleshooting. For example, you can check which security groups are associated with your Application Load Balancer at any point in time. You can navigate to the Amazon Config timeline from the ELB console to view the configuration changes of your Application Load Balancers.

Amazon CodeBuild

Amazon Configprovides an inventory of your Amazon resources and a history of configuration changes to these resources. Amazon Config supports Amazon CodeBuild; as an Amazon resource, which means the service can track your CodeBuild projects. For more information, see Use Amazon Config with CodeBuild sample in the *Amazon CodeBuild User Guide*.

Amazon X-Ray

Amazon X-Ray integrates with Amazon Config to record configuration changes made to your X-Ray encryption resources. You can use Amazon Config to inventory X-Ray encryption resources, audit the X-Ray configuration history, and send notifications based on resource changes. For more information, see Tracking X-Ray encryption configuration changes with Amazon Config in the *Amazon X-Ray Developer Guide*.

Amazon Service Management Connector

The Amazon Service Management Connector for ServiceNow can synchronize Amazon Config data from multiple accounts and Regions using an Aggregator. For more information, see Integrating Amazon Config in ServiceNow in the *Amazon Service Management Connector Administrator Guide*.

Amazon API Gateway

You can use Amazon Config to record configuration changes made to your API Gateway API resources and send notifications based on resource changes. Maintaining a configuration change history for API Gateway resources is useful for operational troubleshooting, audit, and compliance use cases. For more information, see Monitoring API Gateway API configuration with Amazon Config in the *API Gateway Developer Guide*.

Region Support for Amazon Config

Considerations

Some features of Amazon Config are only supported in a subset of the Amazon Regions where Amazon Config is supported.

Resource Management

- For a list of which Amazon resource types are supported in which Regions, see Resource Coverage by Region Availability.

Amazon Config Rules

- For a list of which Amazon Config rules are supported in which Regions, see List of Amazon Config Managed Rules by Region Availability.

- For a list of Regions which support the organizational deployment of Amazon Config rules, see Organizational Rules | Region Support.

Aggregators

Advanced Queries

- For a list of Regions which support advanced queries, see Advanced Queries | Region Support.
- For a list of Regions which support the natural language query processor for advanced queries, see Natural language query processor for advanced queries | Region Support.

List of Supported Regions

The following table lists the Amazon Regions where you can enable Amazon Config.

Region Name	Region	Endpoint	Protocol
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
		config-fips.us-east-2.amazonaws.com	HTTPS
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
		config-fips.us-east-1.amazonaws.com	HTTPS
US West (N. California)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
		config-fips.us-west-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
		config-fips.us-west-2.amazonaws.com	HTTPS
Africa (Cape Town)	af-south-1	config.af-south-1.amazonaws.com	HTTPS

Region Name	Region	Endpoint	Protocol	
Asia Pacific (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS	
Asia Pacific (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS	
Asia Pacific (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS	
Asia Pacific (Malaysia)	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS	
Asia Pacific (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS	
Asia Pacific (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS	
Asia Pacific (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS	
Asia Pacific (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS	

Region Name	Region	Endpoint	Protocol	
Asia Pacific (Singapore)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS	
Asia Pacific (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS	
Asia Pacific (Taipei)	ap-east-2	config.ap-east-2.amazonaws.com	HTTPS	
Asia Pacific (Thailand)	ap-southeast-7	config.ap-southeast-7.amazonaws.com	HTTPS	
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS	
Canada (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS	
Canada West (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS	
China (Beijing)	cn-north-1	config.cn-north-1.amazonaws.com.cn	HTTPS	
China (Ningxia)	cn-northwest-1	config.cn-northwest-1.amazonaws.com.cn	HTTPS	

Region Name	Region	Endpoint	Protocol	
Europe (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS	
Europe (Ireland)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS	
Europe (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS	
Europe (Milan)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS	
Europe (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS	
Europe (Spain)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS	
Europe (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS	
Europe (Zurich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS	
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS	
Mexico (Central)	mx-central-1	config.mx-central-1.amazonaws.com	HTTPS	
Middle East (Bahrain)	me-south-1	config.me-south-1.amazonaws.com	HTTPS	

Region Name	Region	Endpoint	Protocol	
Middle East (UAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS	
South America (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS	

Service Limits for Amazon Config

The following table describes limits within Amazon Config. Unless noted otherwise, the quotas can be increased upon request. You can request a quota increase.

For information about other limits in Amazon, see Amazon Service Limits.

Resource tags

Description	Limit Value	Can be increased
Maximum number of tags per resource	50	No

Amazon Config rules

Description	Limit Value	Can be increased
Maximum number of Amazon Config Rules per Region per account	1000	No

Single Account Conformance Packs

Description	Limit Value	Can be increased
Maximum number of conformance packs per account	50	No
Maximum number of Amazon Config Rules per conformance pack	130	No

Note

Amazon Config rules in conformance packs count in the limit for the Maximum number of Amazon Config Rules per Region per account.

Organization Conformance Packs

Description	Limit Value	Can be increased
Maximum number of conformance packs per organization	50	No
Maximum number of Amazon Config Rules per organization conformance pack	130	No

Note

Deploying at the organization level counts in the limit for child accounts. Amazon Config rules in conformance packs count in the limit for the Maximum number of Amazon Config Rules per Region per account.

Aggregators

Description	Limit Value	Can be increased
Maximum number of configuration aggregators	50	Yes
Maximum number of accounts in an aggregator	10000	No
Maximum number of accounts added or deleted per week for all aggregators	1000	Yes

> **Note**
>
> Organization level aggregators and individual account aggregators both count in the limit for the Maximum number of configuration aggregators.

Advanced queries

Description	Limit Value	Can be increased
Maximum number of saved queries in a single account and a Region	300	Yes

Supplemental Information and Related Resources for Amazon Config

The following related resources can help you as you work with this service.

- **Amazon Config** – The primary web page for information about Amazon Config.
- **Amazon Config Pricing**
- **Technical FAQ**

- **Amazon Config Rule Development Kit (RDK)** – An open-source tool that helps you set up Amazon Config, author rules, and then test them using a variety of Amazon resource types.
- **Partners** – Links to partner products that are fully integrated with Amazon Config to help you visualize, monitor, and manage the data from your configuration stream, configuration snapshots, or configuration history.

- Getting Started Resource Center – Learn how to set up your Amazon Web Services account, join the Amazon community, and launch your first application.
- Amazon Web Services Support Center – The hub for creating and managing your Amazon Web Services Support cases. Also includes links to other helpful resources, such as forums, technical FAQs, service health status, and Amazon Trusted Advisor.
- Amazon Web Services Support – The primary webpage for information about Amazon Web Services Support, a one-on-one, fast-response support channel to help you build and run applications in the cloud.
- Contact Us – A central contact point for inquiries concerning Amazon billing, account, events, abuse, and other issues.
- Amazon Site Terms – Detailed information about our copyright and trademark; your account, license, and site access; and other topics.

Amazon Software Development Kits for Amazon Config

An Amazon software development kit (SDK) makes it easier to build applications that access cost-effective, scalable, and reliable Amazon infrastructure services. With Amazon SDKs, you can get started in minutes with a single, downloadable package that includes the library, code samples, and reference documentation. The following table lists the available SDKs and third-party libraries you can use to access Amazon Config programmatically.

Type of Access	Description
Amazon SDKs	Amazon provides the following SDKs: • Amazon SDK for C++ Documentation • Amazon Mobile SDK for iOS Documentation • Amazon SDK for Go Documentation • Amazon SDK for Java Documentation

Type of Access	Description
	• Amazon SDK for JavaScript Documentation • Amazon SDK for .NET Documentation • Amazon SDK for PHP Documentation • Amazon SDK for Python (Boto) Documentation • Amazon SDK for Ruby Documentation
Third-party libraries	Developers in the Amazon developer community also provide their own libraries, which you can find at the following Amazon developer centers: • Amazon Java Developer Center • Amazon JavaScript Developer Center • Amazon PHP Developer Center • Amazon Python Developer Center • Amazon Ruby Developer Center • Amazon Windows and .NET Developer Center

Getting Started with Amazon Config

Amazon Config provides a detailed view of the configuration of Amazon resources in your Amazon Web Services account. With Amazon Config, you can review changes in configurations and relationships between Amazon resources, explore resource configuration history, and use rules to determine compliance. For more information, see What Is Amazon Config? and How Amazon Config Works.

Signing up for Amazon

Topics

- Sign up for an Amazon Web Services account
- Secure IAM users

Sign up for an Amazon Web Services account

If you do not have an Amazon Web Services account, use the following procedure to create one.

To sign up for Amazon Web Services

1. Open http://www.amazonaws.cn/ and choose **Sign Up**.
2. Follow the on-screen instructions.

Amazon sends you a confirmation email after the sign-up process is complete. At any time, you can view your current account activity and manage your account by going to http://www.amazonaws.cn/ and choosing **My Account**.

Secure IAM users

After you sign up for an Amazon Web Services account, safeguard your administrative user by turning on multi-factor authentication (MFA). For instructions, see Enable a virtual MFA device for an IAM user (console) in the *IAM User Guide*.

To give other users access to your Amazon Web Services account resources, create IAM users. To secure your IAM users, turn on MFA and only give the IAM users the permissions needed to perform their tasks.

For more information about creating and securing IAM users, see the following topics in the *IAM User Guide*:

- Creating an IAM user in your Amazon Web Services account
- Access management for Amazon resources
- Example IAM identity-based policies

Ways to Get Started with Amazon Config

After you sign up for an Amazon Web Services account, you can get started with Amazon Config with the Amazon Web Services Management Console, Amazon CLI, or the Amazon SDKs.

- Setting Up Amazon Config with the Console
- Setting Up Amazon Config with the Amazon CLI
- Using Amazon Config service with the Amazon SDK

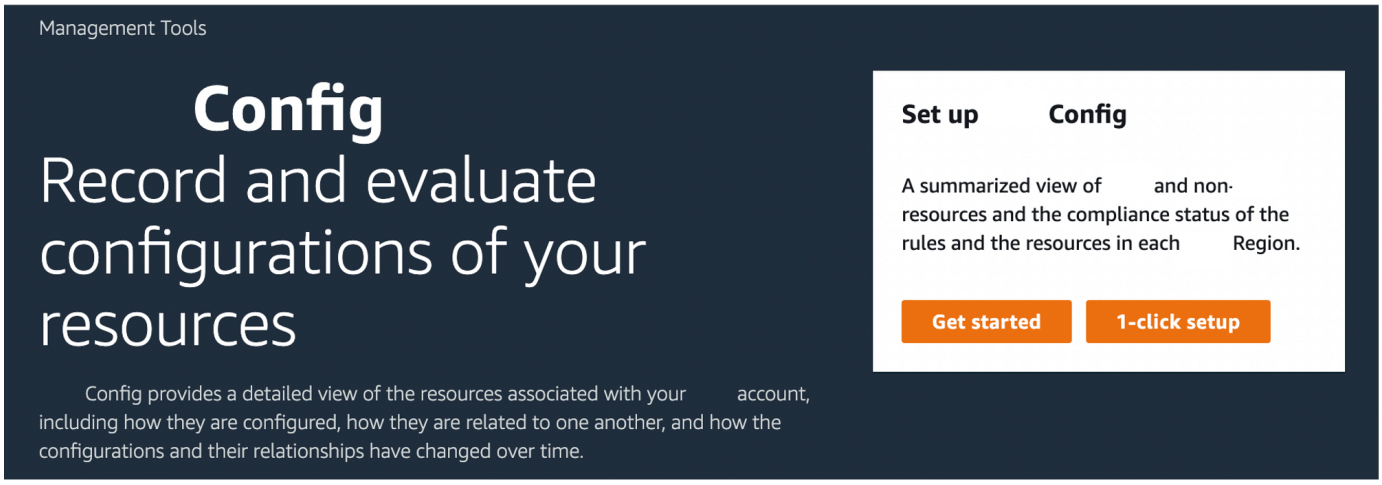
Setting Up Amazon Config with the Console

The Amazon Web Services Management Console provides a quick and streamlined process for setting up Amazon Config.

Setting up

To set up Amazon Config with the console

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. If this is the first time you are opening the Amazon Config console or you are setting up Amazon Config in a new region, the Amazon Config console page looks like the following:



3. Choose **1-click setup** to launch Amazon Config based on Amazon best practices. You can also choose **Get started** to go through a more detailed setup process.

Topics

- 1-click setup for Amazon Config
- Manual setup for Amazon Config

1-click setup for Amazon Config

Amazon Config **1-click setup** helps simplify the getting started process for Amazon Config console customers by reducing the number of manual selections. To go through all the manual selections of the setup process, see Manual setup.

To set up Amazon Config with the console using 1-click setup

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. Choose **1-click setup**.

The set up page includes three steps, but through the **1-click setup** workflow, you are automatically directed to Step 3 (Review). The following provides a breakdown of that procedure.

- **Settings**: To select the manner by which the Amazon Config console records resources and roles, and choose where configuration history and configuration snapshot files are sent.

- **Rules**: For Amazon Web Services Regions that support Amazon Config rules, this step is available for you to configure initial managed rules that you can add to your account. After setting up, Amazon Config will evaluate your Amazon resources against the rules that you chose. Additional rules can be created and existing ones can be updated in your account after setup.
- **Review**: To verify your setup details.

Step 1: Settings

Recording strategy

The option to record **All resource types with customizable overrides** is selected for you. Amazon Config will record all current and future supported resource types in this Region. For more information, see Supported Resource Types.

- **Default settings**

  The default recording frequency is set to **Continuous** for you. This means Amazon Config records configuration changes continuously whenever a change occurs.

  Amazon Config also supports the option to set the recording frequency to **Daily**. If you select this option after setup, you will receive a configuration item (CI) representing the most recent state of your resources over the last 24-hour period, only if it's different from the previous CI recorded. For more information see, Recording Frequency.

  > **Note**
  >
  > Amazon Firewall Manager depends on continuous recording to monitor your resources. If you are using Firewall Manager, it is recommended that you set the recording frequency to Continuous.

- **Override settings – *optional***

  Optionally, after setup you can override the record frequency for specific resource types, or exclude specific resource types from recording. To override the default settings, choose **Settings** in the left navigation of the Amazon Config console, and then choose **Edit**.

Considerations When Recording Resources

High Number of Amazon Config Evaluations

You might notice increased activity in your account during your initial month recording with Amazon Config when compared to subsequent months. During the initial bootstrapping process, Amazon Config runs evaluations on all the resources in your account that you have selected for Amazon Config to record.

If you are running ephemeral workloads, you may see increased activity from Amazon Config as it records configuration changes associated with creating and deleting these temporary resources. An *ephemeral workload* is a temporary use of computing resources that are loaded and run when needed. Examples include Amazon Elastic Compute Cloud (Amazon EC2) Spot Instances, Amazon EMR jobs, and Amazon Auto Scaling. If you want to avoid the increased activity from running ephemeral workloads, you can set up the configuration recorder to exclude these resource types from being recorded, or run these types of workloads in a separate account with Amazon Config turned off to avoid increased configuration recording and rule evaluations.

Global resource types | Aurora global clusters are initially included in recording

The `AWS::RDS::GlobalCluster` resource type will be recorded in all supported Amazon Config Regions where the configuration recorder is enabled.

If you do not want to record `AWS::RDS::GlobalCluster` in all enabled Regions, you can exclude this resource type from recording after setup. Choose **Settings** in the left navigation bar, and then choosing **Edit**. From **Edit**, go to **Override settings** in the **Recording method** section, choose `AWS::RDS::GlobalCluster`, and choose the override "Exclude from recording".

Global resource types | IAM resource types are initially excluded from recording

"All globally recorded IAM resource types" are initially excluded from recording to help you reduce costs. This bundle includes IAM users, groups, roles, and customer managed policies. Choose **Remove** to remove the override and include these resources in your recording.

Additionally, the global IAM resource types (`AWS::IAM::User`, `AWS::IAM::Group`, `AWS::IAM::Role`, and `AWS::IAM::Policy`) cannot be recorded in Regions supported by Amazon Config after February 2022. For a list of those Regions, see Recording Amazon Resources | Global Resources.

Data governance

The default data retention period to retain Amazon Config data for 7 years (2557 days) is selected for you in this section.

The option to **Use an existing Amazon Config service-linked role** is selected for you and set to the **Amazon Config role**. Service-linked roles are predefined by Amazon Config and include all the permissions that the service requires to call other Amazon services.

Delivery method

The option to **Choose a bucket from your account** is selected for you in this section. This selection will default to the bucket in your account that is named in the format `config-bucket-`*`accountid`*. For example, `config-bucket-012345678901`. If you don't have a bucket created in that format, one will be created for you. If you want to create your own bucket, see Creating a bucket in the *Amazon Simple Storage Service User Guide*.

For more information about S3 buckets, see Buckets overview in the *Amazon Simple Storage Service User Guide*.

Step 2: Rules

Under **Amazon Managed Rules**, no rules are selected for you at this step. Instead, you are encouraged to create and update rules after you have finished setting up your account.

Step 3: Review

Review your Amazon Config setup details. You can go back to edit changes for each section. Choose **Confirm** to finish setting up Amazon Config.

Manual setup for Amazon Config

With the **Get started** workflow, you can go through all the manual selections of the setup process to get started with the Amazon Config console. For a simplified getting started process, see 1-click setup.

To set up Amazon Config with the console using Get started

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. Choose **Get started**.

The setup page includes three steps. The following provides a breakdown of that procedure after you choose **Get started**.

- **Settings**: To select the manner by which the Amazon Config console records resources and roles, and choose where configuration history and configuration snapshot files are sent.
- **Rules**: For Amazon Web Services Regions that support Amazon Config rules, this step is available for you to configure initial managed rules that you can add to your account. After setting up, Amazon Config will evaluate your Amazon resources against the rules that you chose. Additional rules can be created and existing ones can be updated and in your account after setup.
- **Review**: To verify your setup details.

Step 1: Settings

Recording strategy

In the **Recording method** section, choose a recording strategy. You can specify the Amazon resources that you want Amazon Config to record.

All resource types with customizable overrides

Set up Amazon Config to record configuration changes for all current and future supported resource types in this Region. You can override the recording frequency for specific resource types or exclude specific resource types from recording. For more information, see Supported Resource Types.

- **Default settings**

  Configure the default recording frequency for all current and future supported resource types. For more information see, Recording Frequency.

  - Continuous recording – Amazon Config will record configuration changes continuously whenever a change occurs.
  - Daily recording – You will receive a configuration item (CI) representing the most recent state of your resources over the last 24-hour period, only if it's different from the previous CI recorded.

> **Note**
>
> Amazon Firewall Manager depends on continuous recording to monitor your resources. If you are using Firewall Manager, it is recommended that you set the recording frequency to Continuous.

- **Override settings**

  Override the recording frequency for specific resource types, or exclude specific resource types from recording. If you change the recording frequency for a resource type or stop recording a resource type, the configuration items that were already recorded will remain unchanged.

Specific resource types

Set Amazon Config to record configuration changes for only the resource types that you specify.

- **Specific resource types**

  Choose a resource type to record and its frequency. For more information see, Recording Frequency.

  - Continuous recording – Amazon Config will record configuration changes continuously whenever a change occurs.
  - Daily recording – You will receive a configuration item (CI) representing the most recent state of your resources over the last 24-hour period, only if it's different from the previous CI recorded.

  > **Note**
  >
  > Amazon Firewall Manager depends on continuous recording to monitor your resources. If you are using Firewall Manager, it is recommended that you set the recording frequency to Continuous.

  If you change the recording frequency for a resource type or stop recording a resource type, the configuration items that were already recorded will remain unchanged.

Considerations When Recording Resources

High Number of Amazon Config Evaluations

You might notice increased activity in your account during your initial month recording with Amazon Config when compared to subsequent months. During the initial bootstrapping process,

Amazon Config runs evaluations on all the resources in your account that you have selected for Amazon Config to record.

If you are running ephemeral workloads, you may see increased activity from Amazon Config as it records configuration changes associated with creating and deleting these temporary resources. An *ephemeral workload* is a temporary use of computing resources that are loaded and run when needed. Examples include Amazon Elastic Compute Cloud (Amazon EC2) Spot Instances, Amazon EMR jobs, and Amazon Auto Scaling. . If you want to avoid the increased activity from running ephemeral workloads, you can set up the configuration recorder to exclude these resource types from being recorded, or run these types of workloads in a separate account with Amazon Config turned off to avoid increased configuration recording and rule evaluations.

Considerations: All resource types with customizable overrides

Globally recorded resource types | Aurora global clusters are initially included in recording

The `AWS::RDS::GlobalCluster` resource type will be recorded in all supported Amazon Config Regions where the configuration recorder is enabled.

If you do not want to record `AWS::RDS::GlobalCluster` in all enabled Regions, choose "Amazon RDS GlobalCluster", and choose the override "Exclude from recording".

Global resource types | IAM resource types are initially excluded from recording

The global IAM resource types are initially excluded from recording to help you reduce costs. This bundle includes IAM users, groups, roles, and customer managed policies. Choose **Remove** to remove the override and include these resources in your recording.

Additionally, the global IAM resource types (`AWS::IAM::User`, `AWS::IAM::Group`, `AWS::IAM::Role`, and `AWS::IAM::Policy`) cannot be recorded in Regions supported by Amazon Config after February 2022. For a list of those Regions, see Recording Amazon Resources | Global Resources.

Limits

You can add up to 100 frequency overrides and 600 exclusion overrides.

Daily recording cannot be specified for the following resource types:

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`

- `AWS::Config::ConfigurationRecorder`

Considerations: Specific resource types

Region Availability

Before specifying a resource type for Amazon Config to track, check Resource Coverage by Region Availability to see if the resource type is supported in the Amazon Region where you set up Amazon Config. If a resource type is supported by Amazon Config in at least one Region, you can enable the recording of that resource type in all Regions supported by Amazon Config, even if the specified resource type is not supported in the Amazon Region where you set up Amazon Config.

Limits

No limits if all resource types have the same frequency. You can add up to 100 resource types with Daily frequency if at least one resource type is set to Continuous.

The Daily frequency is not supported for the following resource types:

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

Data governance

- For **Data retention period**, choose either the default retention period to retain Amazon Config data for 7 years (2557) or set a custom rentention period for items recorded by Amazon Config.

  Amazon Config allows you to delete your data by specifying a retention period for your `ConfigurationItems`. When you specify a retention period, Amazon Config retains your `ConfigurationItems` for that specified period. You can choose a period between a minimum of 30 days and a maximum of 7 years (2557 days). Amazon Config deletes data older than your specified retention period.
- For **IAM role for Amazon Config**, choose either an existing Amazon Config service-linked role or an IAM role from your account.
  - Service-linked roles are predefined by Amazon Config and include all the permissions that the service requires to call other Amazon services.

> **Note**
>
> **Recommended: Use the Service-linked role**
> It is recommended that you use the service-linked role. A service-linked role adds all the necessary permissions for Amazon Config to run as expected.

- Otherwise, choose an IAM role from one of your pre-existing roles and permission policies.

> **Note**
>
> **Policies and compliance results**
> IAM policies and other policies managed in Amazon Organizations can impact whether Amazon Config has permissions to record configuration changes for your resources. Additionally, rules directly evaluate the configuration of a resource and rules don't take into account these policies when running evaluations. Make sure that the policies in effect align with how you intend to use Amazon Config.
> **Keep Minimum Permisions When Reusing an IAM role**
> If you use an Amazon service that uses Amazon Config, such as Amazon Security Hub or Amazon Control Tower, and an IAM role has already been created, make sure that the IAM role that you use when setting up Amazon Config keeps the same minimum permissions as the pre-existing IAM role. You must do this to ensure that the other Amazon service continues to run as expected.
> For example, if Amazon Control Tower has an IAM role that allows Amazon Config to read S3 objects, make sure that the same permissions are granted to the IAM role you use when setting up Amazon Config. Otherwise, it may interfere with how Amazon Control Tower operates.

Delivery method

- For **Delivery method**, choose the S3 bucket to which Amazon Config sends configuration history and configuration snapshot files:
  - **Create a bucket** – For **S3 bucket name**, type a name for your S3 bucket.

    The name that you type must be unique across all existing bucket names in Amazon S3. One way to help ensure uniqueness is to include a prefix; for example, the name of your

organization. You can't change the bucket name after it is created. For more information, see Bucket Restrictions and Limitations in the *Amazon Simple Storage Service User Guide*.

- **Choose a bucket from your account** – For **S3 bucket name**, choose your preferred bucket.
- **Choose a bucket from another account** – For **S3 bucket name**, type the bucket name.

> **Note**
>
> **Bucket Permissions**
> If you choose a bucket from another account, that bucket must have policies that grant access permissions to Amazon Config. For more information, see Permissions for the Amazon S3 Bucket for the Amazon Config Delivery Channel.

- For **Amazon SNS topic**, choose **Stream configuration changes and notifications to an Amazon SNS topic** to have Amazon Config send notifications such as configuration history delivery, configuration snapshot delivery, and compliance.
- If you chose to have Amazon Config stream to an Amazon SNS topic, choose the target topic:
  - **Create a topic** – For **Topic Name**, type a name for your SNS topic.
  - **Choose a topic from your account** – For **Topic Name**, select your preferred topic.
  - **Choose a topic from another account** – For **Topic ARN**, type the Amazon Resource Name (ARN) of the topic. If you choose a topic from another account, the topic must have policies that grant access permissions to Amazon Config. For more information, see Permissions for the Amazon SNS Topic.

> **Note**
>
> **Region for the Amazon SNS Topic**
> The Amazon SNS topic must exist in the same Region as the Region in which you set up Amazon Config.

Step 2: Rules

If you are setting up Amazon Config in a Region that supports rules, choose **Next**.

Step 3: Review

Review your Amazon Config set up details. You can go back to edit changes for each section. Choose **Confirm** to finish setting up Amazon Config.

For more information

For information about looking up the existing resources in your account and understanding the configurations of your resources, see Looking up Resources, Viewing Compliance Informance, and Viewing Compliance History.

You can also use Amazon Simple Queue Service to monitor Amazon resources programmatically. For more information, see Monitoring Amazon Resource Changes with Amazon SQS.

Setting Up Amazon Config with the Amazon CLI

The Amazon CLI is a unified tool to manage your Amazon services. With just one tool to download and configure, you can control multiple Amazon services from the command line and use scripts to automate them. For more information about the Amazon CLI and for instructions on installing the Amazon CLI tools, see the following in the *Amazon Command Line Interface User Guide*.

- Amazon Command Line Interface User Guide
- Getting Set Up with the Amazon Command Line Interface

If necessary, enter `aws configure` to configure the Amazon CLI to use an Amazon Region where Amazon Config is available.

Setting up

See the following topics to set up Amazon Config with the Amazon CLI.

Topics

- Prerequisites for Setting Up Amazon Config with the Amazon CLI
- Starting Amazon Config with a customer managed configuration recorder using the Amazon CLI
- Verifying that Amazon Config is Successfully Started with the Amazon CLI

Prerequisites for Setting Up Amazon Config with the Amazon CLI

Before setting up Amazon with the Amazon CLI, you need to create an Amazon S3 bucket, an Amazon SNS topic, and an IAM role with attached policies as prerequisites. You can then use the Amazon CLI to specify the bucket, topic, and role for Amazon Config. Follow this procedure to set up your prerequisites for Amazon Config.

Topics

- Step 1: Creating an Amazon S3 Bucket
- Step 2: Creating an Amazon SNS Topic
- Step 3: Creating an IAM Role

Step 1: Creating an Amazon S3 Bucket

If you already have an Amazon S3 bucket in your account and want to use it, skip this step and go to Step 2: Creating an Amazon SNS Topic.

Using the S3 console

To create a bucket

1. Open the Amazon S3 console at https://console.amazonaws.cn/s3/.
2. Choose **Create bucket**.
3. In **Bucket name**, enter a DNS-compliant name for your bucket.

   The bucket name must:

   - Be unique across all of Amazon S3.
   - Be between 3 and 63 characters long.
   - Not contain uppercase characters.
   - Start with a lowercase letter or number.

   After you create the bucket, you can't change its name. Make sure the bucket name you choose is unique across all existing bucket names in Amazon S3. For more information on bucket naming rules and conventions, see Bucket restrictions and Limitations in the *Amazon Simple Storage Service User Guide*.

> **Important**
>
> Avoid including sensitive information in the bucket name. The bucket name is visible in the URLs that point to the objects in the bucket.

4. In **Region**, choose the Amazon Region where you want the bucket to reside.

   Choose a Region close to you to minimize latency and costs and address regulatory requirements. Objects stored in a Region never leave that Region unless you explicitly transfer them to another Region. For a list of Amazon S3 Amazon Regions, see Amazon service endpoints in the *Amazon Web Services General Reference*.

5. In **Bucket settings for Block Public Access**, choose the Block Public Access settings that you want to apply to the bucket.

   We recommend that you leave all settings enabled unless you know you need to turn one or more of them off for your use case, such as to host a public website. Block public access settings that you enable for the bucket will also be enabled for all access points that you create on the bucket. For more information about blocking public access, see Using Amazon S3 Block Public Access in the *Amazon Simple Storage Service User Guide*.

6. (Optional) If you want to enable S3 Object Lock:

   a. Choose **Advanced settings**, and read the message that appears.

      > **Important**
      >
      > You can only enable S3 Object Lock for a bucket when you create it. If you enable Object Lock for the bucket, you can't disable it later. Enabling Object Lock also enables versioning for the bucket. After you enable Object Lock for the bucket, you must configure the Object Lock settings before any objects in the bucket will be protected. For more information about configuring protection for objects, see Configuring S3 Object Lock using the Amazon S3 console.

   b. If you want to enable Object Lock, enter *enable* in the text box and choose **Confirm**.

   For more information about the S3 Object Lock feature, see Locking Objects Using Amazon S3 Object Lock in the *Amazon Simple Storage Service User Guide*.

7. Choose **Create bucket**.

Using the Amazon SDKs

When you use the Amazon SDKs to create a bucket, you must create a client and then use the client to send a request to create a bucket. As a best practice, you should create your client and bucket in the same Amazon Web Services Region. If you don't specify a Region when you create a client or a bucket, Amazon S3 uses the default Region US East (N. Virginia).

To create a client to access a dual-stack endpoint, you must specify an Amazon Web Services Region. For more information, see Amazon S3 dual-stack endpoints. For a list of available Amazon Web Services Regions, see Regions and endpoints in the *Amazon Web Services General Reference*.

When you create a client, the Region maps to the Region-specific endpoint. The client uses this endpoint to communicate with Amazon S3: `s3.<region>.amazonaws.com.cn`. If your Region launched after March 20, 2019, your client and bucket must be in the same Region. However, you can use a client in the US East (N. Virginia) Region to create a bucket in any Region that launched before March 20, 2019. For more information, see Legacy Endpoints.

These Amazon SDK code examples perform the following tasks:

- **Create a client by explicitly specifying an Amazon Web Services Region** — In the example, the client uses the `s3.us-west-2.amazonaws.com.cn` endpoint to communicate with Amazon S3. You can specify any Amazon Web Services Region. For a list of Amazon Web Services Regions, see Regions and endpoints in the *Amazon General Reference*.
- **Send a create bucket request by specifying only a bucket name** — The client sends a request to Amazon S3 to create the bucket in the Region where you created a client.
- **Retrieve information about the location of the bucket** — Amazon S3 stores bucket location information in the *location* subresource that is associated with the bucket.

The following code examples show how to use `CreateBucket`.

.NET

Amazon SDK for .NET

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
        /// <summary>
        /// Shows how to create a new Amazon S3 bucket.
        /// </summary>
        /// <param name="client">An initialized Amazon S3 client object.</param>
        /// <param name="bucketName">The name of the bucket to create.</param>
        /// <returns>A boolean value representing the success or failure of
        /// the bucket creation process.</returns>
        public static async Task<bool> CreateBucketAsync(IAmazonS3 client, string
bucketName)
        {
            try
            {
                var request = new PutBucketRequest
                {
                    BucketName = bucketName,
                    UseClientRegion = true,
                };

                var response = await client.PutBucketAsync(request);
                return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
            }
            catch (AmazonS3Exception ex)
            {
                Console.WriteLine($"Error creating bucket: '{ex.Message}'");
                return false;
            }
        }
```

Create a bucket with object lock enabled.

```
    /// <summary>
    /// Create a new Amazon S3 bucket with object lock actions.
    /// </summary>
    /// <param name="bucketName">The name of the bucket to create.</param>
    /// <param name="enableObjectLock">True to enable object lock on the
bucket.</param>
    /// <returns>True if successful.</returns>
    public async Task<bool> CreateBucketWithObjectLock(string bucketName, bool
enableObjectLock)
    {
        Console.WriteLine($"\tCreating bucket {bucketName} with object lock
{enableObjectLock}.");
        try
        {
            var request = new PutBucketRequest
            {
                BucketName = bucketName,
                UseClientRegion = true,
                ObjectLockEnabledForBucket = enableObjectLock,
            };

            var response = await _amazonS3.PutBucketAsync(request);

            return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
        }
        catch (AmazonS3Exception ex)
        {
            Console.WriteLine($"Error creating bucket: '{ex.Message}'");
            return false;
        }
    }
```

- For API details, see CreateBucket in *Amazon SDK for .NET API Reference*.

Bash

Amazon CLI with Bash script

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
##############################################################################
# function iecho
#
# This function enables the script to display the specified text only if
# the global variable $VERBOSE is set to true.
##############################################################################
function iecho() {
  if [[ $VERBOSE == true ]]; then
    echo "$@"
  fi
}

##############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
##############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

##############################################################################
# function create-bucket
#
# This function creates the specified bucket in the specified AWS Region, unless
# it already exists.
#
# Parameters:
#       -b bucket_name  -- The name of the bucket to create.
#       -r region_code  -- The code for an AWS Region in which to
#                          create the bucket.
#
```

```
# Returns:
#       The URL of the bucket that was created.
#     And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function create_bucket() {
  local bucket_name region_code response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function create_bucket"
    echo "Creates an Amazon S3 bucket. You must supply a bucket name:"
    echo "  -b bucket_name    The name of the bucket. It must be globally
 unique."
    echo "  [-r region_code]    The code for an AWS Region in which the bucket is
 created."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "b:r:h" option; do
    case "${option}" in
      b) bucket_name="${OPTARG}" ;;
      r) region_code="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done

  if [[ -z "$bucket_name" ]]; then
    errecho "ERROR: You must provide a bucket name with the -b parameter."
    usage
    return 1
  fi
```

```
  local bucket_config_arg
  # A location constraint for "us-east-1" returns an error.
  if [[ -n "$region_code" ]] && [[ "$region_code" != "us-east-1" ]]; then
    bucket_config_arg="--create-bucket-configuration LocationConstraint=
$region_code"
  fi

  iecho "Parameters:\n"
  iecho "    Bucket name:   $bucket_name"
  iecho "    Region code:   $region_code"
  iecho ""

  # If the bucket already exists, we don't want to try to create it.
  if (bucket_exists "$bucket_name"); then
    errecho "ERROR: A bucket with that name already exists. Try again."
    return 1
  fi

  # shellcheck disable=SC2086
  response=$(aws s3api create-bucket \
    --bucket "$bucket_name" \
    $bucket_config_arg)

  # shellcheck disable=SC2181
  if [[ ${?} -ne 0 ]]; then
    errecho "ERROR: AWS reports create-bucket operation failed.\n$response"
    return 1
  fi
}
```

- For API details, see CreateBucket in *Amazon CLI Command Reference*.

C++

SDK for C++

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
bool AwsDoc::S3::createBucket(const Aws::String &bucketName,
                              const Aws::S3::S3ClientConfiguration &clientConfig)
 {
    Aws::S3::S3Client client(clientConfig);
    Aws::S3::Model::CreateBucketRequest request;
    request.SetBucket(bucketName);

    if (clientConfig.region != "us-east-1") {
        Aws::S3::Model::CreateBucketConfiguration createBucketConfig;
        createBucketConfig.SetLocationConstraint(

 Aws::S3::Model::BucketLocationConstraintMapper::GetBucketLocationConstraintForName(
                        clientConfig.region));
        request.SetCreateBucketConfiguration(createBucketConfig);
    }

    Aws::S3::Model::CreateBucketOutcome outcome = client.CreateBucket(request);
    if (!outcome.IsSuccess()) {
        auto err = outcome.GetError();
        std::cerr << "Error: createBucket: " <<
                  err.GetExceptionName() << ": " << err.GetMessage() <<
 std::endl;
    } else {
        std::cout << "Created bucket " << bucketName <<
                  " in the specified AWS Region." << std::endl;
    }

    return outcome.IsSuccess();
}
```

- For API details, see CreateBucket in *Amazon SDK for C++ API Reference*.

CLI

Amazon CLI

Example 1: To create a bucket

The following `create-bucket` example creates a bucket named `amzn-s3-demo-bucket`:

```
aws s3api create-bucket \
```

```
    --bucket amzn-s3-demo-bucket \
    --region us-east-1
```

Output:

```
{
    "Location": "/amzn-s3-demo-bucket"
}
```

For more information, see Creating a bucket in the *Amazon S3 User Guide*.

Example 2: To create a bucket with owner enforced

The following `create-bucket` example creates a bucket named `amzn-s3-demo-bucket` that uses the bucket owner enforced setting for S3 Object Ownership.

```
aws s3api create-bucket \
    --bucket amzn-s3-demo-bucket \
    --region us-east-1 \
    --object-ownership BucketOwnerEnforced
```

Output:

```
{
    "Location": "/amzn-s3-demo-bucket"
}
```

For more information, see Controlling ownership of objects and disabling ACLs in the *Amazon S3 User Guide*.

Example 3: To create a bucket outside of the ``us-east-1`` region

The following `create-bucket` example creates a bucket named `amzn-s3-demo-bucket` in the `eu-west-1` region. Regions outside of `us-east-1` require the appropriate `LocationConstraint` to be specified in order to create the bucket in the desired region.

```
aws s3api create-bucket \
    --bucket amzn-s3-demo-bucket \
    --region eu-west-1 \
    --create-bucket-configuration LocationConstraint=eu-west-1
```

Output:

```
{
    "Location": "http://amzn-s3-demo-bucket.s3.amazonaws.com/"
}
```

For more information, see Creating a bucket in the *Amazon S3 User Guide*.

- For API details, see CreateBucket in *Amazon CLI Command Reference*.

Go

SDK for Go V2

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

Create a bucket with default configuration.

```
import (
 "bytes"
 "context"
 "errors"
 "fmt"
 "io"
 "log"
 "os"
 "time"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/feature/s3/manager"
 "github.com/aws/aws-sdk-go-v2/service/s3"
 "github.com/aws/aws-sdk-go-v2/service/s3/types"
 "github.com/aws/smithy-go"
)

// BucketBasics encapsulates the Amazon Simple Storage Service (Amazon S3)
 actions
```

```
// used in the examples.
// It contains S3Client, an Amazon S3 service client that is used to perform
 bucket
// and object actions.
type BucketBasics struct {
 S3Client *s3.Client
}



// CreateBucket creates a bucket with the specified name in the specified Region.
func (basics BucketBasics) CreateBucket(ctx context.Context, name string, region
 string) error {
 _, err := basics.S3Client.CreateBucket(ctx, &s3.CreateBucketInput{
  Bucket: aws.String(name),
  CreateBucketConfiguration: &types.CreateBucketConfiguration{
   LocationConstraint: types.BucketLocationConstraint(region),
  },
 })
 if err != nil {
  var owned *types.BucketAlreadyOwnedByYou
  var exists *types.BucketAlreadyExists
  if errors.As(err, &owned) {
   log.Printf("You already own bucket %s.\n", name)
   err = owned
  } else if errors.As(err, &exists) {
   log.Printf("Bucket %s already exists.\n", name)
   err = exists
  }
 } else {
  err = s3.NewBucketExistsWaiter(basics.S3Client).Wait(
   ctx, &s3.HeadBucketInput{Bucket: aws.String(name)}, time.Minute)
  if err != nil {
   log.Printf("Failed attempt to wait for bucket %s to exist.\n", name)
  }
 }
 return err
}
```

Create a bucket with object locking and wait for it to exist.

```
import (
 "bytes"
 "context"
 "errors"
 "fmt"
 "log"
 "time"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/feature/s3/manager"
 "github.com/aws/aws-sdk-go-v2/service/s3"
 "github.com/aws/aws-sdk-go-v2/service/s3/types"
 "github.com/aws/smithy-go"
)

// S3Actions wraps S3 service actions.
type S3Actions struct {
 S3Client  *s3.Client
 S3Manager *manager.Uploader
}



// CreateBucketWithLock creates a new S3 bucket with optional object locking
 enabled
// and waits for the bucket to exist before returning.
func (actor S3Actions) CreateBucketWithLock(ctx context.Context, bucket string,
 region string, enableObjectLock bool) (string, error) {
 input := &s3.CreateBucketInput{
  Bucket: aws.String(bucket),
  CreateBucketConfiguration: &types.CreateBucketConfiguration{
   LocationConstraint: types.BucketLocationConstraint(region),
  },
 }

 if enableObjectLock {
  input.ObjectLockEnabledForBucket = aws.Bool(true)
 }

 _, err := actor.S3Client.CreateBucket(ctx, input)
 if err != nil {
  var owned *types.BucketAlreadyOwnedByYou
```

```
  var exists *types.BucketAlreadyExists
  if errors.As(err, &owned) {
   log.Printf("You already own bucket %s.\n", bucket)
   err = owned
  } else if errors.As(err, &exists) {
   log.Printf("Bucket %s already exists.\n", bucket)
   err = exists
  }
 } else {
  err = s3.NewBucketExistsWaiter(actor.S3Client).Wait(
   ctx, &s3.HeadBucketInput{Bucket: aws.String(bucket)}, time.Minute)
  if err != nil {
   log.Printf("Failed attempt to wait for bucket %s to exist.\n", bucket)
  }
 }

 return bucket, err
}
```

- For API details, see CreateBucket in *Amazon SDK for Go API Reference*.

Java

SDK for Java 2.x

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

Create a bucket.

```
    /**
     * Creates an S3 bucket asynchronously.
     *
     * @param bucketName the name of the S3 bucket to create
     * @return a {@link CompletableFuture} that completes when the bucket is
created and ready
```

```
     * @throws RuntimeException if there is a failure while creating the bucket
     */
    public CompletableFuture<Void> createBucketAsync(String bucketName) {
        CreateBucketRequest bucketRequest = CreateBucketRequest.builder()
            .bucket(bucketName)
            .build();

        CompletableFuture<CreateBucketResponse> response =
getAsyncClient().createBucket(bucketRequest);
        return response.thenCompose(resp -> {
            S3AsyncWaiter s3Waiter = getAsyncClient().waiter();
            HeadBucketRequest bucketRequestWait = HeadBucketRequest.builder()
                .bucket(bucketName)
                .build();

            CompletableFuture<WaiterResponse<HeadBucketResponse>>
waiterResponseFuture =
                s3Waiter.waitUntilBucketExists(bucketRequestWait);
            return waiterResponseFuture.thenAccept(waiterResponse -> {
                waiterResponse.matched().response().ifPresent(headBucketResponse
-> {
                    logger.info(bucketName + " is ready");
                });
            });
        }).whenComplete((resp, ex) -> {
            if (ex != null) {
                throw new RuntimeException("Failed to create bucket", ex);
            }
        });
    }
```

Create a bucket with object lock enabled.

```
    // Create a new Amazon S3 bucket with object lock options.
    public void createBucketWithLockOptions(boolean enableObjectLock, String
bucketName) {
        S3Waiter s3Waiter = getClient().waiter();
        CreateBucketRequest bucketRequest = CreateBucketRequest.builder()
            .bucket(bucketName)
            .objectLockEnabledForBucket(enableObjectLock)
            .build();
```

```
        getClient().createBucket(bucketRequest);
        HeadBucketRequest bucketRequestWait = HeadBucketRequest.builder()
            .bucket(bucketName)
            .build();

        // Wait until the bucket is created and print out the response.
        s3Waiter.waitUntilBucketExists(bucketRequestWait);
        System.out.println(bucketName + " is ready");
    }
```

- For API details, see CreateBucket in *Amazon SDK for Java 2.x API Reference*.

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

Create the bucket.

```
import {
  BucketAlreadyExists,
  BucketAlreadyOwnedByYou,
  CreateBucketCommand,
  S3Client,
  waitUntilBucketExists,
} from "@aws-sdk/client-s3";

/**
 * Create an Amazon S3 bucket.
 * @param {{ bucketName: string }} config
 */
export const main = async ({ bucketName }) => {
  const client = new S3Client({});

  try {
    const { Location } = await client.send(
```

```
      new CreateBucketCommand({
        // The name of the bucket. Bucket names are unique and have several other
 constraints.
        // See https://docs.aws.amazon.com/AmazonS3/latest/userguide/
bucketnamingrules.html
        Bucket: bucketName,
      }),
    );
    await waitUntilBucketExists({ client }, { Bucket: bucketName });
    console.log(`Bucket created with location ${Location}`);
  } catch (caught) {
    if (caught instanceof BucketAlreadyExists) {
      console.error(
        `The bucket "${bucketName}" already exists in another AWS account. Bucket
 names must be globally unique.`,
      );
    }
    // WARNING: If you try to create a bucket in the North Virginia region,
    // and you already own a bucket in that region with the same name, this
    // error will not be thrown. Instead, the call will return successfully
    // and the ACL on that bucket will be reset.
    else if (caught instanceof BucketAlreadyOwnedByYou) {
      console.error(
        `The bucket "${bucketName}" already exists in this AWS account.`,
      );
    } else {
      throw caught;
    }
  }
};
```

- For more information, see Amazon SDK for JavaScript Developer Guide.
- For API details, see CreateBucket in *Amazon SDK for JavaScript API Reference*.

Kotlin

SDK for Kotlin

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
suspend fun createNewBucket(bucketName: String) {
    val request =
        CreateBucketRequest {
            bucket = bucketName
        }

    S3Client { region = "us-east-1" }.use { s3 ->
        s3.createBucket(request)
        println("$bucketName is ready")
    }
}
```

- For API details, see CreateBucket in *Amazon SDK for Kotlin API reference*.

PHP

SDK for PHP

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

Create a bucket.

```
        $s3client = new Aws\S3\S3Client(['region' => 'us-west-2']);

        try {
```

```
            $this->s3client->createBucket([
                'Bucket' => $this->bucketName,
                'CreateBucketConfiguration' => ['LocationConstraint' => $region],
            ]);
            echo "Created bucket named: $this->bucketName \n";
        } catch (Exception $exception) {
            echo "Failed to create bucket $this->bucketName with error: " .
 $exception->getMessage();
            exit("Please fix error with bucket creation before continuing.");
        }
```

- For API details, see CreateBucket in *Amazon SDK for PHP API Reference*.

Python

SDK for Python (Boto3)

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

Create a bucket with default settings.

```
class BucketWrapper:
    """Encapsulates S3 bucket actions."""

    def __init__(self, bucket):
        """
        :param bucket: A Boto3 Bucket resource. This is a high-level resource in
 Boto3
                       that wraps bucket actions in a class-like structure.
        """
        self.bucket = bucket
        self.name = bucket.name


    def create(self, region_override=None):
        """
```

```
        Create an Amazon S3 bucket in the default Region for the account or in
 the
        specified Region.

        :param region_override: The Region in which to create the bucket. If this
 is
                                not specified, the Region configured in your
 shared
                                credentials is used.
        """
        if region_override is not None:
            region = region_override
        else:
            region = self.bucket.meta.client.meta.region_name
        try:
            self.bucket.create(CreateBucketConfiguration={"LocationConstraint":
 region})

            self.bucket.wait_until_exists()
            logger.info("Created bucket '%s' in region=%s", self.bucket.name,
 region)
        except ClientError as error:
            logger.exception(
                "Couldn't create bucket named '%s' in region=%s.",
                self.bucket.name,
                region,
            )
            raise error
```

Create a versioned bucket with a lifecycle configuration.

```
def create_versioned_bucket(bucket_name, prefix):
    """
    Creates an Amazon S3 bucket, enables it for versioning, and configures a
 lifecycle
    that expires noncurrent object versions after 7 days.

    Adding a lifecycle configuration to a versioned bucket is a best practice.
    It helps prevent objects in the bucket from accumulating a large number of
    noncurrent versions, which can slow down request performance.
```

```
    Usage is shown in the usage_demo_single_object function at the end of this
module.

    :param bucket_name: The name of the bucket to create.
    :param prefix: Identifies which objects are automatically expired under the
                   configured lifecycle rules.
    :return: The newly created bucket.
    """
    try:
        bucket = s3.create_bucket(
            Bucket=bucket_name,
            CreateBucketConfiguration={
                "LocationConstraint": s3.meta.client.meta.region_name
            },
        )
        logger.info("Created bucket %s.", bucket.name)
    except ClientError as error:
        if error.response["Error"]["Code"] == "BucketAlreadyOwnedByYou":
            logger.warning("Bucket %s already exists! Using it.", bucket_name)
            bucket = s3.Bucket(bucket_name)
        else:
            logger.exception("Couldn't create bucket %s.", bucket_name)
            raise

    try:
        bucket.Versioning().enable()
        logger.info("Enabled versioning on bucket %s.", bucket.name)
    except ClientError:
        logger.exception("Couldn't enable versioning on bucket %s.", bucket.name)
        raise

    try:
        expiration = 7
        bucket.LifecycleConfiguration().put(
            LifecycleConfiguration={
                "Rules": [
                    {
                        "Status": "Enabled",
                        "Prefix": prefix,
                        "NoncurrentVersionExpiration": {"NoncurrentDays":
expiration},
                    }
                ]
            }
```

```
        )
        logger.info(
            "Configured lifecycle to expire noncurrent versions after %s days "
            "on bucket %s.",
            expiration,
            bucket.name,
        )
    except ClientError as error:
        logger.warning(
            "Couldn't configure lifecycle on bucket %s because %s. "
            "Continuing anyway.",
            bucket.name,
            error,
        )

    return bucket
```

- For API details, see CreateBucket in *Amazon SDK for Python (Boto3) API Reference*.

Ruby

SDK for Ruby

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
require 'aws-sdk-s3'

# Wraps Amazon S3 bucket actions.
class BucketCreateWrapper
  attr_reader :bucket

  # @param bucket [Aws::S3::Bucket] An Amazon S3 bucket initialized with a name.
 This is a client-side object until
  #                                 create is called.
  def initialize(bucket)
```

```
    @bucket = bucket
  end

  # Creates an Amazon S3 bucket in the specified AWS Region.
  #
  # @param region [String] The Region where the bucket is created.
  # @return [Boolean] True when the bucket is created; otherwise, false.
  def create?(region)
    @bucket.create(create_bucket_configuration: { location_constraint: region })
    true
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't create bucket. Here's why: #{e.message}"
    false
  end

  # Gets the Region where the bucket is located.
  #
  # @return [String] The location of the bucket.
  def location
    if @bucket.nil?
      'None. You must create a bucket before you can get its location!'
    else
      @bucket.client.get_bucket_location(bucket:
 @bucket.name).location_constraint
    end
  rescue Aws::Errors::ServiceError => e
    "Couldn't get the location of #{@bucket.name}. Here's why: #{e.message}"
  end
end

# Example usage:
def run_demo
  region = "us-west-2"
  wrapper = BucketCreateWrapper.new(Aws::S3::Bucket.new("amzn-s3-demo-bucket-
#{Random.uuid}"))
  return unless wrapper.create?(region)

  puts "Created bucket #{wrapper.bucket.name}."
  puts "Your bucket's region is: #{wrapper.location}"
end

run_demo if $PROGRAM_NAME == __FILE__
```

- For API details, see CreateBucket in *Amazon SDK for Ruby API Reference*.

Rust

SDK for Rust

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
pub async fn create_bucket(
    client: &aws_sdk_s3::Client,
    bucket_name: &str,
    region: &aws_config::Region,
) -> Result<Option<aws_sdk_s3::operation::create_bucket::CreateBucketOutput>,
 S3ExampleError> {
    let constraint =
 aws_sdk_s3::types::BucketLocationConstraint::from(region.to_string().as_str());
    let cfg = aws_sdk_s3::types::CreateBucketConfiguration::builder()
        .location_constraint(constraint)
        .build();
    let create = client
        .create_bucket()
        .create_bucket_configuration(cfg)
        .bucket(bucket_name)
        .send()
        .await;

    // BucketAlreadyExists and BucketAlreadyOwnedByYou are not problems for this
 task.
    create.map(Some).or_else(|err| {
        if err
            .as_service_error()
            .map(|se| se.is_bucket_already_exists() ||
 se.is_bucket_already_owned_by_you())
            == Some(true)
        {
            Ok(None)
        } else {
            Err(S3ExampleError::from(err))
```

```
        }
    })
}
```

- For API details, see CreateBucket in *Amazon SDK for Rust API reference*.

SAP ABAP

SDK for SAP ABAP

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
    TRY.
        " determine our region from our session
        DATA(lv_region) = CONV /aws1/s3_bucketlocationcnstrnt( lo_session-
>get_region( ) ).
        DATA lo_constraint TYPE REF TO /aws1/cl_s3_createbucketconf.
        " When in the us-east-1 region, you must not specify a constraint
        " In all other regions, specify the region as the constraint
        IF lv_region = 'us-east-1'.
          CLEAR lo_constraint.
        ELSE.
          lo_constraint = NEW /aws1/cl_s3_createbucketconf( lv_region ).
        ENDIF.

        lo_s3->createbucket(
            iv_bucket = iv_bucket_name
            io_createbucketconfiguration  = lo_constraint ).
        MESSAGE 'S3 bucket created.' TYPE 'I'.
      CATCH /aws1/cx_s3_bucketalrdyexists.
        MESSAGE 'Bucket name already exists.' TYPE 'E'.
      CATCH /aws1/cx_s3_bktalrdyownedbyyou.
        MESSAGE 'Bucket already exists and is owned by you.' TYPE 'E'.
    ENDTRY.
```

- For API details, see CreateBucket in *Amazon SDK for SAP ABAP API reference*.

Swift

SDK for Swift

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
import AWSS3

    public func createBucket(name: String) async throws {
        var input = CreateBucketInput(
            bucket: name
        )

        // For regions other than "us-east-1", you must set the
 locationConstraint in the createBucketConfiguration.
        // For more information, see LocationConstraint in the S3 API guide.
        // https://docs.aws.amazon.com/AmazonS3/latest/API/
API_CreateBucket.html#API_CreateBucket_RequestBody
        if let region = configuration.region {
            if region != "us-east-1" {
                input.createBucketConfiguration =
 S3ClientTypes.CreateBucketConfiguration(locationConstraint:
 S3ClientTypes.BucketLocationConstraint(rawValue: region))
            }
        }

        do {
            _ = try await client.createBucket(input: input)
        }
        catch let error as BucketAlreadyOwnedByYou {
            print("The bucket '\(name)' already exists and is owned by you. You
 may wish to ignore this exception.")
            throw error
        }
        catch {
            print("ERROR: ", dump(error, name: "Creating a bucket"))
```

```
            throw error
        }
    }
```

- For API details, see CreateBucket in *Amazon SDK for Swift API reference*.

> **Note**
>
> You can also use an Amazon S3 bucket from a different account, but you may need to create a policy for the bucket that grants access permissions to Amazon Config. For information on granting permissions to an Amazon S3 bucket, see Permissions for the Amazon S3 Bucket for the Amazon Config Delivery Channel, and then go to Step 2: Creating an Amazon SNS Topic.

Step 2: Creating an Amazon SNS Topic

If you already have an Amazon SNS topic in your account and want to use it, skip this step and go to Step 3: Creating an IAM Role.

Using the SNS console

To create an Amazon SNS topic

1. Open the Amazon SNS console at https://console.amazonaws.cn/sns/v3/home.
2. Do one of the following:
   - If no topics have ever been created under your Amazon Web Services account before, read the description of Amazon SNS on the home page.
   - If topics have been created under your Amazon Web Services account before, on the navigation panel, choose **Topics**.
3. On the **Topics** page, choose **Create topic**.
4. On the **Create topic** page, in the **Details** section, do the following:
   a. For **Type**, choose a topic type (**Standard** or **FIFO**).
   b. Enter a **Name** for the topic. For a FIFO topic, add **.fifo** to the end of the name.

c. (Optional) Enter a **Display name** for the topic.

d. (Optional) For a FIFO topic, you can choose **content-based message deduplication** to enable default message deduplication. For more information, see Message deduplication for FIFO topics.

5. (Optional) Expand the **Encryption** section and do the following. For more information, see Encryption at rest.

a. Choose **Enable encryption**.

b. Specify the customer master key (CMK). For more information, see Key terms.

For each CMK type, the **Description**, **Account**, and **CMK ARN** are displayed.

> **Important**
>
> If you aren't the owner of the CMK, or if you log in with an account that doesn't have the `kms:ListAliases` and `kms:DescribeKey` permissions, you won't be able to view information about the CMK on the Amazon SNS console.
> Ask the owner of the CMK to grant you these permissions. For more information, see the Amazon KMS API Permissions: Actions and Resources Reference in the *Amazon Key Management Service Developer Guide*.

- The Amazon managed CMK for Amazon SNS **(Default) alias/aws/sns** is selected by default.

> **Note**
>
> Keep the following in mind:
>
> - The first time you use the Amazon Web Services Management Console to specify the Amazon managed CMK for Amazon SNS for a topic, Amazon KMS creates the Amazon managed CMK for Amazon SNS.
> - Alternatively, the first time you use the `Publish` action on a topic with SSE enabled, Amazon KMS creates the Amazon managed CMK for Amazon SNS.

- To use a custom CMK from your Amazon Web Services account, choose the **Customer master key (CMK)** field and then choose the custom CMK from the list.

> **Note**
>
> For instructions on creating custom CMKs, see Creating Keys in the *Amazon Key Management Service Developer Guide*

- To use a custom CMK ARN from your Amazon Web Services account or from another Amazon account, enter it into the **Customer master key (CMK)** field.

6. (Optional) By default, only the topic owner can publish or subscribe to the topic. To configure additional access permissions, expand the **Access policy** section. For more information, see Identity and access management in Amazon SNS and Example cases for Amazon SNS access control.

> **Note**
>
> When you create a topic using the console, the default policy uses the `aws:SourceOwner` condition key. This key is similar to `aws:SourceAccount`.

7. (Optional) To configure how Amazon SNS retries failed message delivery attempts, expand the **Delivery retry policy (HTTP/S)** section. For more information, see Amazon SNS message delivery retries.
8. (Optional) To configure how Amazon SNS logs the delivery of messages to CloudWatch, expand the **Delivery status logging** section. For more information, see Amazon SNS message delivery status.
9. (Optional) To add metadata tags to the topic, expand the **Tags** section, enter a **Key** and a **Value** (optional) and choose **Add tag**. For more information, see Amazon SNS topic tagging.
10. Choose **Create topic**.

    The topic is created and the ***MyTopic*** page is displayed.

    The topic's **Name**, **ARN**, (optional) **Display name**, and **Topic owner**'s Amazon account ID are displayed in the **Details** section.
11. Copy the topic ARN to the clipboard, for example:

```
arn:aws:sns:us-west-2:123456789012:MyTopic
```

To subscribe an email address to the Amazon SNS topic

1. Open the Amazon SNS console at https://console.amazonaws.cn/sns/v3/home.
2. In the left navigation pane, choose **Subscriptions**.
3. On the **Subscriptions** page, choose **Create subscription**.
4. On the **Create subscription** page, in the **Details** section, do the following:
   a. For **Topic ARN**, choose the Amazon Resource Name (ARN) of a topic.
   b. For **Protocol**, choose an endpoint type. The available endpoint types are:
      - HTTP/HTTPS
      - Email/Email-JSON
      - Amazon Data Firehose
      - Amazon SQS

      > **Note**
      >
      > To subscribe to an SNS FIFO topic, choose this option.

      - Amazon Lambda
      - Platform application endpoint
      - SMS
   c. For **Endpoint**, enter the endpoint value, such as an email address or the ARN of an Amazon SQS queue.
   d. Firehose endpoints only: For **Subscription role ARN**, specify the ARN of the IAM role that you created for writing to Firehose delivery streams. For more information, see Prerequisites for subscribing Firehose delivery streams to Amazon SNS topics.
   e. (Optional) For Firehose, Amazon SQS, HTTP/S endpoints, you can also enable raw message delivery. For more information, see Amazon SNS raw message delivery.
   f. (Optional) To configure a filter policy, expand the **Subscription filter policy** section. For more information, see Amazon SNS subscription filter policies.
   g. (Optional) To configure a dead-letter queue for the subscription, expand the **Redrive policy (dead-letter queue)** section. For more information, see Amazon SNS dead-letter queues (DLQs).
   h. Choose **Create subscription**.

The console creates the subscription and opens the subscription's **Details** page.

Using the Amazon SDKs

To use an Amazon SDK, you must configure it with your credentials. For more information, see The shared config and credentials files in the *Amazon SDKs and Tools Reference Guide*.

The following code examples show how to use `CreateTopic`.

.NET

Amazon SDK for .NET

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

Create a topic with a specific name.

```
    using System;
    using System.Threading.Tasks;
    using Amazon.SimpleNotificationService;
    using Amazon.SimpleNotificationService.Model;

    /// <summary>
    /// This example shows how to use Amazon Simple Notification Service
    /// (Amazon SNS) to add a new Amazon SNS topic.
    /// </summary>
    public class CreateSNSTopic
    {
        public static async Task Main()
        {
            string topicName = "ExampleSNSTopic";

            IAmazonSimpleNotificationService client = new
AmazonSimpleNotificationServiceClient();

            var topicArn = await CreateSNSTopicAsync(client, topicName);
            Console.WriteLine($"New topic ARN: {topicArn}");
```

```
        }

        /// <summary>
        /// Creates a new SNS topic using the supplied topic name.
        /// </summary>
        /// <param name="client">The initialized SNS client object used to
        /// create the new topic.</param>
        /// <param name="topicName">A string representing the topic name.</param>
        /// <returns>The Amazon Resource Name (ARN) of the created topic.</
returns>
        public static async Task<string>
 CreateSNSTopicAsync(IAmazonSimpleNotificationService client, string topicName)
        {
            var request = new CreateTopicRequest
            {
                Name = topicName,
            };

            var response = await client.CreateTopicAsync(request);

            return response.TopicArn;
        }
    }
```

Create a new topic with a name and specific FIFO and de-duplication attributes.

```
    /// <summary>
    /// Create a new topic with a name and specific FIFO and de-duplication
 attributes.
    /// </summary>
    /// <param name="topicName">The name for the topic.</param>
    /// <param name="useFifoTopic">True to use a FIFO topic.</param>
    /// <param name="useContentBasedDeduplication">True to use content-based de-
duplication.</param>
    /// <returns>The ARN of the new topic.</returns>
    public async Task<string> CreateTopicWithName(string topicName, bool
 useFifoTopic, bool useContentBasedDeduplication)
    {
        var createTopicRequest = new CreateTopicRequest()
        {
            Name = topicName,
```

```
        };

        if (useFifoTopic)
        {
            // Update the name if it is not correct for a FIFO topic.
            if (!topicName.EndsWith(".fifo"))
            {
                createTopicRequest.Name = topicName + ".fifo";
            }

            // Add the attributes from the method parameters.
            createTopicRequest.Attributes = new Dictionary<string, string>
            {
                { "FifoTopic", "true" }
            };
            if (useContentBasedDeduplication)
            {
                createTopicRequest.Attributes.Add("ContentBasedDeduplication",
"true");
            }
        }

        var createResponse = await
_amazonSNSClient.CreateTopicAsync(createTopicRequest);
        return createResponse.TopicArn;
    }
```

- For API details, see CreateTopic in *Amazon SDK for .NET API Reference*.

C++

SDK for C++

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
//! Create an Amazon Simple Notification Service (Amazon SNS) topic.
/*!
```

```
  \param topicName: An Amazon SNS topic name.
  \param topicARNResult: String to return the Amazon Resource Name (ARN) for the
 topic.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SNS::createTopic(const Aws::String &topicName,
                              Aws::String &topicARNResult,
                              const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SNS::SNSClient snsClient(clientConfiguration);

    Aws::SNS::Model::CreateTopicRequest request;
    request.SetName(topicName);

    const Aws::SNS::Model::CreateTopicOutcome outcome =
 snsClient.CreateTopic(request);

    if (outcome.IsSuccess()) {
        topicARNResult = outcome.GetResult().GetTopicArn();
        std::cout << "Successfully created an Amazon SNS topic " << topicName
                  << " with topic ARN '" << topicARNResult
                  << "'." << std::endl;

    }
    else {
        std::cerr << "Error creating topic " << topicName << ":" <<
                  outcome.GetError().GetMessage() << std::endl;
        topicARNResult.clear();
    }

    return outcome.IsSuccess();
}
```

- For API details, see CreateTopic in *Amazon SDK for C++ API Reference*.

CLI

Amazon CLI

To create an SNS topic

The following `create-topic` example creates an SNS topic named `my-topic`.

```
aws sns create-topic \
    --name my-topic
```

Output:

```
{
    "ResponseMetadata": {
        "RequestId": "1469e8d7-1642-564e-b85d-a19b4b341f83"
    },
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:my-topic"
}
```

For more information, see Using the Amazon Command Line Interface with Amazon SQS and Amazon SNS in the *Amazon Command Line Interface User Guide*.

- For API details, see CreateTopic in *Amazon CLI Command Reference*.

Go

SDK for Go V2

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
import (
 "context"
 "encoding/json"
 "log"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/sns"
 "github.com/aws/aws-sdk-go-v2/service/sns/types"
)
```

```
// SnsActions encapsulates the Amazon Simple Notification Service (Amazon SNS)
 actions
// used in the examples.
type SnsActions struct {
 SnsClient *sns.Client
}



// CreateTopic creates an Amazon SNS topic with the specified name. You can
 optionally
// specify that the topic is created as a FIFO topic and whether it uses content-
based
// deduplication instead of ID-based deduplication.
func (actor SnsActions) CreateTopic(ctx context.Context, topicName string,
 isFifoTopic bool, contentBasedDeduplication bool) (string, error) {
 var topicArn string
 topicAttributes := map[string]string{}
 if isFifoTopic {
  topicAttributes["FifoTopic"] = "true"
 }
 if contentBasedDeduplication {
  topicAttributes["ContentBasedDeduplication"] = "true"
 }
 topic, err := actor.SnsClient.CreateTopic(ctx, &sns.CreateTopicInput{
  Name:       aws.String(topicName),
  Attributes: topicAttributes,
 })
 if err != nil {
  log.Printf("Couldn't create topic %v. Here's why: %v\n", topicName, err)
 } else {
  topicArn = *topic.TopicArn
 }

 return topicArn, err
}
```

- For API details, see CreateTopic in *Amazon SDK for Go API Reference*.

Java

SDK for Java 2.x

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.sns.SnsClient;
import software.amazon.awssdk.services.sns.model.CreateTopicRequest;
import software.amazon.awssdk.services.sns.model.CreateTopicResponse;
import software.amazon.awssdk.services.sns.model.SnsException;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
public class CreateTopic {
    public static void main(String[] args) {
        final String usage = """

                Usage:    <topicName>

                Where:
                   topicName - The name of the topic to create (for example,
 mytopic).

                """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }
```

```
        String topicName = args[0];
        System.out.println("Creating a topic with name: " + topicName);
        SnsClient snsClient = SnsClient.builder()
                .region(Region.US_EAST_1)
                .build();

        String arnVal = createSNSTopic(snsClient, topicName);
        System.out.println("The topic ARN is" + arnVal);
        snsClient.close();
    }

    public static String createSNSTopic(SnsClient snsClient, String topicName) {
        CreateTopicResponse result;
        try {
            CreateTopicRequest request = CreateTopicRequest.builder()
                    .name(topicName)
                    .build();

            result = snsClient.createTopic(request);
            return result.topicArn();

        } catch (SnsException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
        return "";
    }
}
```

- For API details, see CreateTopic in *Amazon SDK for Java 2.x API Reference*.

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

Create the client in a separate module and export it.

```
import { SNSClient } from "@aws-sdk/client-sns";

// The AWS Region can be provided here using the `region` property. If you leave
 it blank
// the SDK will default to the region set in your AWS config.
export const snsClient = new SNSClient({});
```

Import the SDK and client modules and call the API.

```
import { CreateTopicCommand } from "@aws-sdk/client-sns";
import { snsClient } from "../libs/snsClient.js";

/**
 * @param {string} topicName - The name of the topic to create.
 */
export const createTopic = async (topicName = "TOPIC_NAME") => {
  const response = await snsClient.send(
    new CreateTopicCommand({ Name: topicName }),
  );
  console.log(response);
  // {
  //   '$metadata': {
  //     httpStatusCode: 200,
  //     requestId: '087b8ad2-4593-50c4-a496-d7e90b82cf3e',
  //     extendedRequestId: undefined,
  //     cfId: undefined,
  //     attempts: 1,
  //     totalRetryDelay: 0
  //   },
  //   TopicArn: 'arn:aws:sns:us-east-1:xxxxxxxxxxxx:TOPIC_NAME'
  // }
  return response;
};
```

- For more information, see Amazon SDK for JavaScript Developer Guide.
- For API details, see CreateTopic in *Amazon SDK for JavaScript API Reference*.

Kotlin

SDK for Kotlin

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
suspend fun createSNSTopic(topicName: String): String {
    val request =
        CreateTopicRequest {
            name = topicName
        }

    SnsClient { region = "us-east-1" }.use { snsClient ->
        val result = snsClient.createTopic(request)
        return result.topicArn.toString()
    }
}
```

- For API details, see CreateTopic in *Amazon SDK for Kotlin API reference*.

PHP

SDK for PHP

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
require 'vendor/autoload.php';

use Aws\Exception\AwsException;
use Aws\Sns\SnsClient;
```

```
/**
 * Create a Simple Notification Service topics in your AWS account at the
 requested region.
 *
 * This code expects that you have AWS credentials set up per:
 * https://docs.aws.amazon.com/sdk-for-php/v3/developer-guide/
guide_credentials.html
 */

$SnSclient = new SnsClient([
    'profile' => 'default',
    'region' => 'us-east-1',
    'version' => '2010-03-31'
]);

$topicname = 'myTopic';

try {
    $result = $SnSclient->createTopic([
        'Name' => $topicname,
    ]);
    var_dump($result);
} catch (AwsException $e) {
    // output error message if fails
    error_log($e->getMessage());
}
```

- For more information, see Amazon SDK for PHP Developer Guide.
- For API details, see CreateTopic in *Amazon SDK for PHP API Reference*.

Python

SDK for Python (Boto3)

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
class SnsWrapper:
    """Encapsulates Amazon SNS topic and subscription functions."""

    def __init__(self, sns_resource):
        """
        :param sns_resource: A Boto3 Amazon SNS resource.
        """
        self.sns_resource = sns_resource


    def create_topic(self, name):
        """
        Creates a notification topic.

        :param name: The name of the topic to create.
        :return: The newly created topic.
        """
        try:
            topic = self.sns_resource.create_topic(Name=name)
            logger.info("Created topic %s with ARN %s.", name, topic.arn)
        except ClientError:
            logger.exception("Couldn't create topic %s.", name)
            raise
        else:
            return topic
```

- For API details, see CreateTopic in *Amazon SDK for Python (Boto3) API Reference*.

Ruby

SDK for Ruby

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
# This class demonstrates how to create an Amazon Simple Notification Service
 (SNS) topic.
class SNSTopicCreator
  # Initializes an SNS client.
  #
  # Utilizes the default AWS configuration for region and credentials.
  def initialize
    @sns_client = Aws::SNS::Client.new
  end

  # Attempts to create an SNS topic with the specified name.
  #
  # @param topic_name [String] The name of the SNS topic to create.
  # @return [Boolean] true if the topic was successfully created, false
 otherwise.
  def create_topic(topic_name)
    @sns_client.create_topic(name: topic_name)
    puts "The topic '#{topic_name}' was successfully created."
    true
  rescue Aws::SNS::Errors::ServiceError => e
    # Handles SNS service errors gracefully.
    puts "Error while creating the topic named '#{topic_name}': #{e.message}"
    false
  end
end

# Example usage:
if $PROGRAM_NAME == __FILE__
  topic_name = 'YourTopicName' # Replace with your topic name
  sns_topic_creator = SNSTopicCreator.new

  puts "Creating the topic '#{topic_name}'..."
  unless sns_topic_creator.create_topic(topic_name)
    puts 'The topic was not created. Stopping program.'
    exit 1
  end
end
```

- For more information, see Amazon SDK for Ruby Developer Guide.
- For API details, see CreateTopic in *Amazon SDK for Ruby API Reference*.

Rust

SDK for Rust

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
async fn make_topic(client: &Client, topic_name: &str) -> Result<(), Error> {
    let resp = client.create_topic().name(topic_name).send().await?;

    println!(
        "Created topic with ARN: {}",
        resp.topic_arn().unwrap_or_default()
    );

    Ok(())
}
```

- For API details, see CreateTopic in *Amazon SDK for Rust API reference*.

SAP ABAP

SDK for SAP ABAP

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
    TRY.
        oo_result = lo_sns->createtopic( iv_name = iv_topic_name ). " oo_result
 is returned for testing purposes. "
        MESSAGE 'SNS topic created' TYPE 'I'.
      CATCH /aws1/cx_snstopiclimitexcdex.
```

```
        MESSAGE 'Unable to create more topics. You have reached the maximum
number of topics allowed.' TYPE 'E'.
    ENDTRY.
```

- For API details, see CreateTopic in *Amazon SDK for SAP ABAP API reference*.

Swift

SDK for Swift

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
import AWSSNS

        let config = try await SNSClient.SNSClientConfiguration(region: region)
        let snsClient = SNSClient(config: config)

        let output = try await snsClient.createTopic(
            input: CreateTopicInput(name: name)
        )

        guard let arn = output.topicArn else {
            print("No topic ARN returned by Amazon SNS.")
            return
        }
```

- For API details, see CreateTopic in *Amazon SDK for Swift API reference*.

> **Note**
>
> You can also use an Amazon SNS topic in a different account, but in that case you might need to create a policy for topic that grants access permissions to Amazon Config. For

information on granting permissions to an Amazon SNS topic, see Permissions for the Amazon SNS Topic and then go to Step 3: Creating an IAM Role.

Step 3: Creating an IAM Role

Important

(Recommended) Use the Amazon Config service-linked role
It is recommended to use the Amazon Config service-linked role: `AWSServiceRoleForConfig`. Service-linked roles are predefined and include all the permissions that Amazon Config requires to call other Amazon Web Services services. The Amazon Config service-linked role is required for service-linked configuration recorders. For more information, see Using Service-Linked Roles for Amazon Config.

Using the IAM console

You can use the IAM console to create an IAM role that grants Amazon Config permissions to access your Amazon S3 bucket, access your Amazon SNS topic, and get configuration details for supported Amazon resources. When you use the console to create an IAM role, Amazon Config automatically attaches the required permissions to the role for you.

Note

If you have used an Amazon service that uses Amazon Config (such as Amazon Security Hub or Amazon Control Tower) and an Amazon Config role has already been created, you should make sure that the IAM role you use when setting up Amazon Config keeps the same minimum privileges as the already created Amazon Config role in order for the other Amazon service to continue to run as expected.
For example, if Amazon Control Tower has an IAM role that allows Amazon Config to read Amazon S3 objects, you should guarantee the same permissions are granted within the IAM role you use when setting up Amazon Config. Otherwise, it may interfere with Amazon Control Tower's operations.
For more information about IAM roles for Amazon Config, see Amazon Identity and Access Management.

To create a role for an Amazon service

1. Sign in to the Amazon Web Services Management Console and open the IAM console at https://console.amazonaws.cn/iam/.
2. In the navigation pane of the IAM console, choose **Roles**, and then choose **Create role**.
3. For **Select trusted entity**, choose **Amazon service**.
4. Choose the use case you want for Amazon Config: **Config - Customizable**, **Config - Organizations**, **Config**, or **Config - Conformance Packs**. Then, choose **Next**.
5. On the **Name, review, and create** page, review the details about your role, and choose **Create Role**.

Using the Amazon SDKs

To use an Amazon SDK, you must configure it with your credentials. For more information, see The shared config and credentials files in the *Amazon SDKs and Tools Reference Guide*.

The following code examples show how to use `CreateRole`.

.NET

Amazon SDK for .NET

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
    /// <summary>
    /// Create a new IAM role.
    /// </summary>
    /// <param name="roleName">The name of the IAM role.</param>
    /// <param name="rolePolicyDocument">The name of the IAM policy document
    /// for the new role.</param>
    /// <returns>The Amazon Resource Name (ARN) of the role.</returns>
    public async Task<string> CreateRoleAsync(string roleName, string
rolePolicyDocument)
    {
        var request = new CreateRoleRequest
```

```
        {
            RoleName = roleName,
            AssumeRolePolicyDocument = rolePolicyDocument,
        };

        var response = await _IAMService.CreateRoleAsync(request);
        return response.Role.Arn;
    }
```

- For API details, see CreateRole in *Amazon SDK for .NET API Reference*.

Bash

Amazon CLI with Bash script

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function iam_create_role
#
# This function creates an IAM role.
#
# Parameters:
#       -n role_name -- The name of the IAM role.
#       -p policy_json -- The assume role policy document.
#
# Returns:
```

```
#       The ARN of the role.
#     And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function iam_create_role() {
  local role_name policy_document response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_create_user_access_key"
    echo "Creates an AWS Identity and Access Management (IAM) role."
    echo "  -n role_name   The name of the IAM role."
    echo "  -p policy_json -- The assume role policy document."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "n:p:h" option; do
    case "${option}" in
      n) role_name="${OPTARG}" ;;
      p) policy_document="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$role_name" ]]; then
    errecho "ERROR: You must provide a role name with the -n parameter."
    usage
    return 1
  fi

  if [[ -z "$policy_document" ]]; then
    errecho "ERROR: You must provide a policy document with the -p parameter."
```

```
    usage
    return 1
  fi

  response=$(aws iam create-role \
    --role-name "$role_name" \
    --assume-role-policy-document "$policy_document" \
    --output text \
    --query Role.Arn)

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports create-role operation failed.\n$response"
    return 1
  fi

  echo "$response"

  return 0
}
```

- For API details, see CreateRole in *Amazon CLI Command Reference*.

C++

SDK for C++

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
bool AwsDoc::IAM::createIamRole(
        const Aws::String &roleName,
        const Aws::String &policy,
        const Aws::Client::ClientConfiguration &clientConfig) {
    Aws::IAM::IAMClient client(clientConfig);
    Aws::IAM::Model::CreateRoleRequest request;
```

```
    request.SetRoleName(roleName);
    request.SetAssumeRolePolicyDocument(policy);

    Aws::IAM::Model::CreateRoleOutcome outcome = client.CreateRole(request);
    if (!outcome.IsSuccess()) {
        std::cerr << "Error creating role. " <<
                  outcome.GetError().GetMessage() << std::endl;
    }
    else {
        const Aws::IAM::Model::Role iamRole = outcome.GetResult().GetRole();
        std::cout << "Created role " << iamRole.GetRoleName() << "\n";
        std::cout << "ID: " << iamRole.GetRoleId() << "\n";
        std::cout << "ARN: " << iamRole.GetArn() << std::endl;
    }

    return outcome.IsSuccess();
}
```

- For API details, see CreateRole in *Amazon SDK for C++ API Reference*.

CLI

Amazon CLI

Example 1: To create an IAM role

The following `create-role` command creates a role named `Test-Role` and attaches a trust policy to it.

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json
```

Output:

```
{
    "Role": {
        "AssumeRolePolicyDocument": "<URL-encoded-JSON>",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "CreateDate": "2013-06-07T20:43:32.821Z",
```

```
        "RoleName": "Test-Role",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:role/Test-Role"
    }
}
```

The trust policy is defined as a JSON document in the *Test-Role-Trust-Policy.json* file. (The file name and extension do not have significance.) The trust policy must specify a principal.

To attach a permissions policy to a role, use the `put-role-policy` command.

For more information, see Creating IAM roles in the *Amazon IAM User Guide*.

Example 2: To create an IAM role with specified maximum session duration

The following `create-role` command creates a role named `Test-Role` and sets a maximum session duration of 7200 seconds (2 hours).

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json \
    --max-session-duration 7200
```

Output:

```
{
    "Role": {
        "Path": "/",
        "RoleName": "Test-Role",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "Arn": "arn:aws:iam::12345678012:role/Test-Role",
        "CreateDate": "2023-05-24T23:50:25+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Sid": "Statement1",
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": "arn:aws:iam::12345678012:root"
                    },
                    "Action": "sts:AssumeRole"
                }
```

```
            ]
        }
    }
}
```

For more information, see Modifying a role maximum session duration (Amazon API) in the *Amazon IAM User Guide*.

Example 3: To create an IAM Role with tags

The following command creates an IAM Role `Test-Role` with tags. This example uses the `--tags` parameter flag with the following JSON-formatted tags: `'{"Key": "Department", "Value": "Accounting"}' '{"Key": "Location", "Value": "Seattle"}'`. Alternatively, the `--tags` flag can be used with tags in the shorthand format: `'Key=Department,Value=Accounting Key=Location,Value=Seattle'`.

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json \
    --tags '{"Key": "Department", "Value": "Accounting"}' '{"Key": "Location",
 "Value": "Seattle"}'
```

Output:

```
{
    "Role": {
        "Path": "/",
        "RoleName": "Test-Role",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "Arn": "arn:aws:iam::123456789012:role/Test-Role",
        "CreateDate": "2023-05-25T23:29:41+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Sid": "Statement1",
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": "arn:aws:iam::123456789012:root"
                    },
                    "Action": "sts:AssumeRole"
                }
```

```
            ]
        },
        "Tags": [
            {
                "Key": "Department",
                "Value": "Accounting"
            },
            {
                "Key": "Location",
                "Value": "Seattle"
            }
        ]
    }
}
```

For more information, see Tagging IAM roles in the *Amazon IAM User Guide*.

- For API details, see CreateRole in *Amazon CLI Command Reference*.

Go

SDK for Go V2

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
import (
 "context"
 "encoding/json"
 "log"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/iam"
 "github.com/aws/aws-sdk-go-v2/service/iam/types"
)

// RoleWrapper encapsulates AWS Identity and Access Management (IAM) role actions
// used in the examples.
```

```
// It contains an IAM service client that is used to perform role actions.
type RoleWrapper struct {
 IamClient *iam.Client
}



// CreateRole creates a role that trusts a specified user. The trusted user can
 assume
// the role to acquire its permissions.
// PolicyDocument shows how to work with a policy document as a data structure
 and
// serialize it to JSON by using Go's JSON marshaler.
func (wrapper RoleWrapper) CreateRole(ctx context.Context, roleName string,
 trustedUserArn string) (*types.Role, error) {
 var role *types.Role
 trustPolicy := PolicyDocument{
  Version: "2012-10-17",
  Statement: []PolicyStatement{{
   Effect:    "Allow",
   Principal: map[string]string{"AWS": trustedUserArn},
   Action:    []string{"sts:AssumeRole"},
  }},
 }
 policyBytes, err := json.Marshal(trustPolicy)
 if err != nil {
  log.Printf("Couldn't create trust policy for %v. Here's why: %v\n",
 trustedUserArn, err)
  return nil, err
 }
 result, err := wrapper.IamClient.CreateRole(ctx, &iam.CreateRoleInput{
  AssumeRolePolicyDocument: aws.String(string(policyBytes)),
  RoleName:                 aws.String(roleName),
 })
 if err != nil {
  log.Printf("Couldn't create role %v. Here's why: %v\n", roleName, err)
 } else {
  role = result.Role
 }
 return role, err
}
```

- For API details, see CreateRole in *Amazon SDK for Go API Reference*.

Java

SDK for Java 2.x

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
import org.json.simple.JSONObject;
import org.json.simple.parser.JSONParser;
import software.amazon.awssdk.services.iam.model.CreateRoleRequest;
import software.amazon.awssdk.services.iam.model.CreateRoleResponse;
import software.amazon.awssdk.services.iam.model.IamException;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.iam.IamClient;
import java.io.FileReader;

/*
*   This example requires a trust policy document. For more information, see:
*   https://aws.amazon.com/blogs/security/how-to-use-trust-policies-with-iam-
roles/
*
*
*  In addition, set up your development environment, including your credentials.
*
*  For information, see this documentation topic:
*
*  https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */

public class CreateRole {
    public static void main(String[] args) throws Exception {
        final String usage = """
                Usage:
                    <rolename> <fileLocation>\s

                Where:
```

```
                    rolename - The name of the role to create.\s
                    fileLocation - The location of the JSON document that
represents the trust policy.\s
                """";

        if (args.length != 2) {
            System.out.println(usage);
            System.exit(1);
        }

        String rolename = args[0];
        String fileLocation = args[1];
        Region region = Region.AWS_GLOBAL;
        IamClient iam = IamClient.builder()
                .region(region)
                .build();

        String result = createIAMRole(iam, rolename, fileLocation);
        System.out.println("Successfully created user: " + result);
        iam.close();
    }

    public static String createIAMRole(IamClient iam, String rolename, String
fileLocation) throws Exception {
        try {
            JSONObject jsonObject = (JSONObject)
readJsonSimpleDemo(fileLocation);
            CreateRoleRequest request = CreateRoleRequest.builder()
                    .roleName(rolename)
                    .assumeRolePolicyDocument(jsonObject.toJSONString())
                    .description("Created using the AWS SDK for Java")
                    .build();

            CreateRoleResponse response = iam.createRole(request);
            System.out.println("The ARN of the role is " +
response.role().arn());

        } catch (IamException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
        return "";
    }
```

```
    public static Object readJsonSimpleDemo(String filename) throws Exception {
        FileReader reader = new FileReader(filename);
        JSONParser jsonParser = new JSONParser();
        return jsonParser.parse(reader);
    }
}
```

- For API details, see CreateRole in *Amazon SDK for Java 2.x API Reference*.

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

Create the role.

```
import { CreateRoleCommand, IAMClient } from "@aws-sdk/client-iam";

const client = new IAMClient({});

/**
 *
 * @param {string} roleName
 */
export const createRole = (roleName) => {
  const command = new CreateRoleCommand({
    AssumeRolePolicyDocument: JSON.stringify({
      Version: "2012-10-17",
      Statement: [
        {
          Effect: "Allow",
          Principal: {
            Service: "lambda.amazonaws.com",
          },
          Action: "sts:AssumeRole",
        },
```

```
      ],
    }),
    RoleName: roleName,
  });

  return client.send(command);
};
```

- For API details, see CreateRole in *Amazon SDK for JavaScript API Reference*.

PHP

SDK for PHP

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
$uuid = uniqid();
$service = new IAMService();

$assumeRolePolicyDocument = "{
                \"Version\": \"2012-10-17\",
                \"Statement\": [{
                    \"Effect\": \"Allow\",
                    \"Principal\": {\"AWS\": \"{$user['Arn']}\"},
                    \"Action\": \"sts:AssumeRole\"
                }]
            }";
$assumeRoleRole = $service->createRole("iam_demo_role_$uuid",
 $assumeRolePolicyDocument);
echo "Created role: {$assumeRoleRole['RoleName']}\n";

    /**
     * @param string $roleName
     * @param string $rolePolicyDocument
     * @return array
     * @throws AwsException
     */
```

```
    public function createRole(string $roleName, string $rolePolicyDocument)
    {
        $result = $this->customWaiter(function () use ($roleName,
 $rolePolicyDocument) {
            return $this->iamClient->createRole([
                'AssumeRolePolicyDocument' => $rolePolicyDocument,
                'RoleName' => $roleName,
            ]);
        });
        return $result['Role'];
    }
```

- For API details, see CreateRole in *Amazon SDK for PHP API Reference*.

PowerShell

Tools for PowerShell V4

Example 1: This example creates a new role named `MyNewRole` and attaches to it the policy found in the file `NewRoleTrustPolicy.json`. Note that you must use the `-Raw` switch parameter to successfully process the JSON policy file. The policy document displayed in the output is URL encoded. It is decoded in this example with the `UrlDecode` .NET method.

```
$results = New-IAMRole -AssumeRolePolicyDocument (Get-Content -raw
 NewRoleTrustPolicy.json) -RoleName MyNewRole
$results
```

Output:

```
Arn                       : arn:aws:iam::123456789012:role/MyNewRole
AssumeRolePolicyDocument : %7B%0D%0A%20%20%22Version%22%3A%20%222012-10-17%22%2C
%0D%0A%20%20%22Statement%22
                           %3A%20%5B%0D%0A%20%20%20%20%7B%0D%0A
%20%20%20%20%20%20%22Sid%22%3A%20%22%22%2C
                           %0D%0A%20%20%20%20%20%20%22Effect%22%3A%20%22Allow
%22%2C%0D%0A%20%20%20%20%20%20
                           %22Principal%22%3A%20%7B%0D%0A
%20%20%20%20%20%20%20%20%22AWS%22%3A%20%22arn%3Aaws
```

```
                            %3Aiam%3A%3A123456789012%3ADavid%22%0D%0A
%20%20%20%20%20%20%7D%2C%0D%0A%20%20%20
                            %20%20%20%22Action%22%3A%20%22sts%3AAssumeRole%22%0D
%0A%20%20%20%20%7D%0D%0A%20
                            %20%5D%0D%0A%7D
CreateDate               : 4/15/2015 11:04:23 AM
Path                     : /
RoleId                   : V5PAJI2KPN4EAEXAMPLE1
RoleName                 : MyNewRole

[System.Reflection.Assembly]::LoadWithPartialName("System.Web.HttpUtility")
[System.Web.HttpUtility]::UrlDecode($results.AssumeRolePolicyDocument)
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:David"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- For API details, see CreateRole in *Amazon Tools for PowerShell Cmdlet Reference (V4)*.

Tools for PowerShell V5

Example 1: This example creates a new role named `MyNewRole` and attaches to it the policy found in the file `NewRoleTrustPolicy.json`. Note that you must use the `-Raw` switch parameter to successfully process the JSON policy file. The policy document displayed in the output is URL encoded. It is decoded in this example with the `UrlDecode` .NET method.

```
$results = New-IAMRole -AssumeRolePolicyDocument (Get-Content -raw
 NewRoleTrustPolicy.json) -RoleName MyNewRole
$results
```

Output:

```
Arn                      : arn:aws:iam::123456789012:role/MyNewRole
```

```
AssumeRolePolicyDocument : %7B%0D%0A%20%20%22Version%22%3A%20%222012-10-17%22%2C
%0D%0A%20%20%22Statement%22
                           %3A%20%5B%0D%0A%20%20%20%20%7B%0D%0A
%20%20%20%20%20%20%22Sid%22%3A%20%22%22%2C
                           %0D%0A%20%20%20%20%20%20%22Effect%22%3A%20%22Allow
%22%2C%0D%0A%20%20%20%20%20%20
                           %22Principal%22%3A%20%7B%0D%0A
%20%20%20%20%20%20%20%20%22AWS%22%3A%20%22arn%3Aaws
                           %3Aiam%3A%3A123456789012%3ADavid%22%0D%0A
%20%20%20%20%20%20%7D%2C%0D%0A%20%20%20
                           %20%20%20%22Action%22%3A%20%22sts%3AAssumeRole%22%0D
%0A%20%20%20%20%7D%0D%0A%20
                           %20%5D%0D%0A%7D
CreateDate               : 4/15/2015 11:04:23 AM
Path                     : /
RoleId                   : V5PAJI2KPN4EAEXAMPLE1
RoleName                 : MyNewRole

[System.Reflection.Assembly]::LoadWithPartialName("System.Web.HttpUtility")
[System.Web.HttpUtility]::UrlDecode($results.AssumeRolePolicyDocument)
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:David"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- For API details, see CreateRole in *Amazon Tools for PowerShell Cmdlet Reference (V5)*.

Python

SDK for Python (Boto3)

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
def create_role(role_name, allowed_services):
    """
    Creates a role that lets a list of specified services assume the role.

    :param role_name: The name of the role.
    :param allowed_services: The services that can assume the role.
    :return: The newly created role.
    """
    trust_policy = {
        "Version": "2012-10-17",
        "Statement": [
            {
                "Effect": "Allow",
                "Principal": {"Service": service},
                "Action": "sts:AssumeRole",
            }
            for service in allowed_services
        ],
    }

    try:
        role = iam.create_role(
            RoleName=role_name, AssumeRolePolicyDocument=json.dumps(trust_policy)
        )
        logger.info("Created role %s.", role.name)
    except ClientError:
        logger.exception("Couldn't create role %s.", role_name)
        raise
    else:
        return role
```

- For API details, see CreateRole in *Amazon SDK for Python (Boto3) API Reference*.

Ruby

SDK for Ruby

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
 # Creates a role and attaches policies to it.
 #
 # @param role_name [String] The name of the role.
 # @param assume_role_policy_document [Hash] The trust relationship policy
document.
 # @param policy_arns [Array<String>] The ARNs of the policies to attach.
 # @return [String, nil] The ARN of the new role if successful, or nil if an
error occurred.
 def create_role(role_name, assume_role_policy_document, policy_arns)
   response = @iam_client.create_role(
     role_name: role_name,
     assume_role_policy_document: assume_role_policy_document.to_json
   )
   role_arn = response.role.arn

   policy_arns.each do |policy_arn|
     @iam_client.attach_role_policy(
       role_name: role_name,
       policy_arn: policy_arn
     )
   end

   role_arn
 rescue Aws::IAM::Errors::ServiceError => e
   @logger.error("Error creating role: #{e.message}")
   nil
 end
```

- For API details, see CreateRole in *Amazon SDK for Ruby API Reference*.

Rust

SDK for Rust

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
pub async fn create_role(
    client: &iamClient,
    role_name: &str,
    role_policy_document: &str,
) -> Result<Role, iamError> {
    let response: CreateRoleOutput = loop {
        if let Ok(response) = client
            .create_role()
            .role_name(role_name)
            .assume_role_policy_document(role_policy_document)
            .send()
            .await
        {
            break response;
        }
    };

    Ok(response.role.unwrap())
}
```

- For API details, see CreateRole in *Amazon SDK for Rust API reference*.

Swift

SDK for Swift

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
import AWSIAM
import AWSS3


    public func createRole(name: String, policyDocument: String) async throws ->
 String {
        let input = CreateRoleInput(
            assumeRolePolicyDocument: policyDocument,
            roleName: name
        )
        do {
            let output = try await client.createRole(input: input)
            guard let role = output.role else {
                throw ServiceHandlerError.noSuchRole
            }
            guard let id = role.roleId else {
                throw ServiceHandlerError.noSuchRole
            }
            return id
        } catch {
            print("ERROR: createRole:", dump(error))
            throw error
        }
    }
```

- For API details, see CreateRole in *Amazon SDK for Swift API reference*.

Starting Amazon Config with a customer managed configuration recorder using the Amazon CLI

You can start Amazon Config by creating a customer managed configuration recorder. To create a customer managed configuration recorder with the Amazon CLI, use the following commands: `put-configuration-recorder`, `put-delivery-channel`, and `start-configuration-recorder`.

- The `put-configuration-recorder` command creates a customer managed configuration recorder.
- The `put-delivery-channel` command creates a delivery channel where Amazon Config delivers configuration information to an S3 bucket and SNS topic.
- The `start-configuration-recorder` starts the customer managed configuration recorder. The customer managed configuration recorder will begin recording configuration changes for the resource types you specify.

Topics

- Considerations
- Step 1: Run the put-configuration-recorder
- Step 2: Run the put-delivery-channel command
- Step 3: Run the start-configuration-recorder command

Considerations

S3 bucket, SNS topic, and IAM role are required

To create a customer managed configuration recorder, you need to create an S3 bucket, an SNS topic, and an IAM role with attached policies as prerequisites. To set up your prerequisites for Amazon Config, see Prerequisites.

One customer managed configuration recorder per account per Region

You can have only one customer managed configuration recorder for each Amazon Web Services account for each Amazon Web Services Region.

One delivery channel per account per Region

You can have only one delivery channel region for each Amazon Web Services account for each Amazon Web Services Region.

Policies and compliance results

IAM policies and other policies managed in Amazon Organizations can impact whether Amazon Config has permissions to record configuration changes for your resources. Additionally, rules directly evaluate the configuration of a resource and rules don't take into account these policies when running evaluations. Make sure that the policies in effect align with how you intend to use Amazon Config.

Step 1: Run the put-configuration-recorder

Use the `put-configuration-recorder` command to create a customer managed configuration recorder:

This command uses the `--configuration-recorder` and `---recording-group` fields.

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

The `configuration-recorder` field

The `configurationRecorder.json` file specifies `name` and `roleArn` as well as the default recording frequency for the configuration recorder (`recordingMode`). You can also use this field to override the recording frequency for specific resource types.

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include in the
 override ]
        }
    ]
  }
```

```
}
```

The `recording-group` field

The `recordingGroup.json` file specifies which resource types are recorded.

```
{
    "allSupported": boolean,
    "exclusionByResourceTypes": {
        "resourceTypes": [ Comma-separated list of resource types to exclude ]
    },
    "includeGlobalResourceTypes": boolean,
    "recordingStrategy": {
        "useOnly": "Recording strategy for the configuration recorder"
    },
    "resourceTypes": [ Comma-separated list of resource types to include]
}
```

For more information about these fields, see `put-configuration-recorder` in the *Amazon CLI Command Reference*.

Step 2: Run the put-delivery-channel command

Use the `put-delivery-channel` command to create a delivery channel:

This command uses the `--delivery-channel` field.

```
$ aws configservice put-delivery-channel --delivery-channel file://deliveryChannel.json
```

The `delivery-channel` field

The `deliveryChannel.json` file specifies the following:

- The `name` for the delivery channel.
- The `s3BucketName` where Amazon Config sends configuration snapshots.
- The `snsTopicARN` where Amazon Config sends notifications
- The `configSnapshotDeliveryProperties` which sets how often Amazon Config delivers configuration snapshots and how often it invokes evaluations for periodic rules.

```
{
```

```
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

For more information about these fields, see put-delivery-channel in the *Amazon CLI Command Reference*.

Step 3: Run the start-configuration-recorder command

Use the start-configuration-recorder command to start Amazon Config:

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

For more information about these fields, see start-configuration-recorder in the *Amazon CLI Command Reference*.

Verifying that Amazon Config is Successfully Started with the Amazon CLI

After you have started Amazon Config, you can use Amazon CLI commands to check that the Amazon Config is running and that Amazon Config has created a configuration recorder and a delivery channel. You can also confirm that Amazon Config has started recording and delivering configurations to the delivery channel.

Topics

- Step 1: Check that a delivery channel is Created
- Step 2: Check that a configuration recorder is Created
- Step 3: Check that Amazon Config has started recording

Step 1: Check that a delivery channel is Created

Use the describe-delivery-channels command to check that your Amazon S3 bucket and Amazon SNS topic is configured.

You can use the `--delivery-channel-names` field to specify a list of delivery channel. If a delivery channel is not specified, this command returns the details of all delivery channels associated with the account.

```
$ aws configservice describe-delivery-channels
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-west-2:0123456789012:my-config-topic",
            "name": "my-delivery-channel",
            "s3BucketName": "my-config-bucket"
        }
    ]
}
```

Step 2: Check that a configuration recorder is Created

Use the `describe-configuration-recorders` command to check that a configuration recorder is created.

You can use the `arn` and `configuration-recorder-names` fields to specify a list of configuration recorders. If a configuration recorder is not specified, this command returns the details of all configuration recorders associated with the account.

```
$ aws configservice describe-configuration-recorders
{
    "ConfigurationRecorders": [
        {
            "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",
            "name": "default"
        }
    ]
}
```

Step 3: Check that Amazon Config has started recording

Use the `describe-configuration-recorder-status` command to check that the configuration recorder is successfully recording the resource types in scope.

You can use the `arn` and `configuration-recorder-names` fields to specify a list of configuration recorders. If a configuration recorder is not specified, this command returns the details of all configuration recorders associated with the account.

```
$ aws configservice describe-configuration-recorder-status
{
    "ConfigurationRecordersStatus": [
        {
            "name": "default",
            "lastStatus": "SUCCESS",
            "lastStopTime": 1414511624.914,
            "lastStartTime": 1414708460.276,
            "recording": true,
            "lastStatusChangeTime": 1414816537.148,
            "lastErrorMessage": "NA",
            "lastErrorCode": "400"
        }
    ]
}
```

The `true` value in the `recording` field confirms that the configuration recorder has started recording configurations. Amazon Config records the time in UTC. The output is displayed as a Unix timestamp.

Using Amazon Config with an Amazon SDK

Amazon software development kits (SDKs) are available for many popular programming languages. Each SDK provides an API, code examples, and documentation that make it easier for developers to build applications in their preferred language.

SDK documentation
Amazon CLI
Amazon SDK for Java
Amazon SDK for JavaScript
Amazon SDK for .NET

SDK documentation
Amazon SDK for PHP
Amazon Tools for PowerShell
Amazon SDK for Python (Boto3)
Amazon SDK for Ruby
Amazon SDK for SAP ABAP

For examples specific to Amazon Config, see Code examples for Amazon Config using Amazon SDKs.

Working with the configuration recorder

The *configuration recorder* stores the configuration changes to the resource types in scope as configuration items (CIs).

There are two types of configuration recorders.

Type	Description
Customer managed configuration recorder	A configuration recorder that you managed. The resource types in scope are set by you. By default, a customer managed configuration recorder records all supported resources in the Amazon Web Services Region where Amazon Config is running.
Service-linked configuration recorder	A configuration recorder that is linked to a specific Amazon Web Services service. The resource types in scope are set by the linked service.

Topics

- Considerations for the customer managed configuration recorder
- Considerations for service-linked configuration recorders
- Drift detection for the configuration recorder
- Starting the customer managed configuration recorder
- Stopping the customer managed configuration recorder
- Changing the recording frequency for the customer managed configuration recorder
- Renaming the customer managed configuration recorder
- Viewing your configuration recorders
- Deleting your configuration recorders

Considerations for the customer managed configuration recorder

One customer managed configuration recorder per account per Region

You can have only one customer managed configuration recorder for each Amazon Web Services account for each Amazon Web Services Region.

Default is to record all supported resource types, excluding the global IAM resource types

The default for a customer managed configuration recorder is to record all supported resource types, excluding the following global IAM resource types: `AWS::IAM::Group`, `AWS::IAM::Policy`, `AWS::IAM::Role`, and `AWS::IAM::User` You can specify which resource types you want to include or exclude from recording.

For more information, see Recording Amazon Resources with Amazon Config.

You are charged service usage fees for using the customer managed configuration recorder

You are charged service usage fees when Amazon Config starts recording configurations with the customer managed configuration recorder.

For pricing information, see Amazon Config Pricing.

Use Amazon Systems Manager to create a customer managed configuration recorder across an organization

You can use Amazon Systems Manager Quick Setup to create a customer managed configuration recorder across multiple organizational units (OUs) and Amazon Web Services Regions using Amazon best practices.

For more information, see Create an Amazon Config configuration recorder using Quick Setup in the *Systems Manager User Guide*.

Important

Policies and compliance results
IAM policies and other policies managed in Amazon Organizations can impact whether Amazon Config has permissions to record configuration changes for your resources. Additionally, rules directly evaluate the configuration of a resource and rules don't take into

account these policies when running evaluations. Make sure that the policies in effect align with how you intend to use Amazon Config.

Stale evaluation results for deleted resources can persist if the configuration recorder is turned off

If the customer managed configuration recorder is turned off, it disables the ability of Amazon Config Config to track changes to the configuration of the resources you specified, including their deletions. This means you might see stale evaluation results for resources that are deleted when the customer managed configuration recorder is turned off since Amazon Config cannot capture deletion events if recording is not on.

Considerations for service-linked configuration recorders

The Amazon Config service-linked role must be used

The Amazon Config service-linked role is required for service-linked configuration recorders.

For more information, see Using Service-Linked Roles for Amazon Config.

Service-linked configuration recorders are always recording

You cannot stop or start recording for service-linked configuration recorders. To stop recording, you must delete the service-linked configuration recorder.

For more information, see Deleting the Configuration Recorder.

The recording scope determines if you receive configuration items

The recording scope is set by the service that is linked to the configuration recorder and determines whether you receive configuration items (CIs) in the delivery channel. If the recording scope is internal, you will not receive CIs in the delivery channel.

The recording scope determines if you are charged a service fee

The recording scope is set by the service that is linked to the configuration recorder and determines whether the configuration items (CIs) in scope are recorded for free (INTERNAL) or if it impacts the costs of your bill (PAID).

Supported services

Service-linked configuration recorders are supported for the following services:

Amazon service	Service principal	Benefits of using with Amazon Config	Learn more
Amazon CloudWatch	`observabilityadmin.amazonaws.com`	You can use Amazon CloudWatch Observability Admin to discover and understand the state of telemetry configuration in CloudWatch for your Amazon Organization or account.	For more information, see Auditing CloudWatch telemetry configurations in the *CloudWatch User Guide*.

Drift detection for the configuration recorder

The `AWS::Config::ConfigurationRecorder` resource type is a *configuration item* (CI) for the configuration recorder that tracks all changes to the state of configuration recorder. You can use this CI to check if the state of the configuration recorder differs, or has *drifted*, from its previous state.

For example, this CI tracks if there are updates to resource types that you have enabled Amazon Config to track, if you have stopped or started the configuration recorder, or if you have deleted or uninstalled the configuration recorder. A drifted configuration recorder indicates that you are not accurately detecting changes to your intended resource types. If your configuration recorder has been drifted, this can result in false negative or false positive compliance results.

The `AWS::Config::ConfigurationRecorder` resource type is a system resource type of Amazon Config and recording of this resource type is enabled by default in all supported Regions. Recording for the `AWS::Config::ConfigurationRecorder` resource type comes with no additional charge.

Starting the customer managed configuration recorder

You can use the Amazon Config console or the Amazon CLI start the customer managed configuration recorder.

To start the customer managed configuration recorder (Console)

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. Choose **Settings** in the navigation pane.
3. On the **Customer managed recorder** tab, choose **Start recording**. When prompted, choose **Confirm**.

To start the customer managed configuration recorder (CLI)

Use the `start-configuration-recorder` command:

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

Stopping the customer managed configuration recorder

> **Note**
>
> **Service-linked configuration recorders are always recording**
> You cannot stop a service-linked configuration recorder because service-linked configuration recorders are always recording. To stop recording, you must delete the service-linked configuration recorder. For more information, see Deleting the Configuration Recorder.

You can use the Amazon Config console or the Amazon CLI stop the customer managed configuration recorder.

To stop the customer managed configuration recorder (Console)

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. Choose **Settings** in the navigation pane.
3. On the **Customer managed recorder** tab, choose **Stop recording**. When prompted, choose **Confirm**.

To stop the customer managed configuration recorder (CLI)

Use the `stop-configuration-recorder` command:

```
$ aws configservice stop-configuration-recorder --configuration-recorder-
name configRecorderName
```

Changing the recording frequency for the customer managed configuration recorder

Amazon Config supports continuous recording and daily recording:

- *Continuous recording* allows you to record configuration changes continuously whenever a change occurs.
- *Daily recording* allows you to receive a configuration item (CI) representing the most recent state of your resources over the last 24-hour period, only if it's different from the previous CI recorded. For more information see, Recording Frequency.

You can use the Amazon Config console or the Amazon CLI change the recording frequency.

To change the recording frequency for the customer managed configuration recorder (Console)

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. Choose **Settings** in the navigation pane.
3. On the **Customer managed recorder** tab, choose **Start recording**.
4. For **Recording method managed recorder**, choose **All resource types with customizable overrides**.
5. For **Default settings**, choose a recording frequency.
6. Choose **Save**.

To change the recording frequency (CLI)

Use the `put-configuration-recorder` command to change the recording frequency for the configuration recorder:

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json
```

The `configurationRecorder.json` file specifies `name` and `roleArn` as well as the default recording frequency for the configuration recorder (`recordingMode`). You can also use this field override the recording frequency for specific resource types.

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include in
 the override ]
        }
    ]
  }
}
```

[put-configuration-recorder](#) uses the following fields for the `--configuration-recorder` parameter:

- `name` – The name of the configuration recorder. Amazon Config automatically assigns the name of "default" when creating the configuration recorder.
- `roleARN` – Amazon Resource Name (ARN) of the IAM role assumed by Amazon Config and used by the configuration recorder.
- `recordingMode` – Specifies the default recording frequency that Amazon Config uses to record configuration changes. Amazon Config supports *Continuous recording* and *Daily recording*. Continuous recording allows you to record configuration changes continuously whenever a change occurs. Daily recording allows you to receive a configuration item (CI) representing the most recent state of your resources over the last 24-hour period, only if it's different from the previous CI recorded.
  - `recordingFrequency` – The default recording frequency that Amazon Config uses to record configuration changes.

> **Note**
>
> Amazon Firewall Manager depends on continuous recording to monitor your resources. If you are using Firewall Manager, it is recommended that you set the recording frequency to Continuous.

- `recordingModeOverrides` – This field allows you to specify your overrides for the recording mode. It is an array of `recordingModeOverride` objects. Each `recordingModeOverride` object in the `recordingModeOverrides` array consists of three fields:
  - `description` – A description that you provide for the override.
  - `recordingFrequency` – The recording frequency that will be applied to all the resource types specified in the override.
  - `resourceTypes` – A comma-separated list that specifies which resource types Amazon Config includes in the override.

> **Note**
>
> **Required and optional fields**
> The `recordingMode` field for `put-configuration-recorder` is optional. By default, the recording frequency for the configuration recorder is set to Continuous recording.

> **Note**
>
> **Limits**
> Daily recording is not supported for the following resource types:
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`

For the **Record all current and future supported resource types** (ALL_SUPPORTED_RESOURCE_TYPES) recording strategy, these resource types will be set to Continuous recording.

Renaming the customer managed configuration recorder

You must use the Amazon CLI to rename the customer managed configuration recorder. To change the name of the customer managed configuration recorder, you must delete it and create a new configuration recorder with your specified name.

Renaming the customer managed configuration recorder using the Amazon CLI

1. Use the describe-configuration-recorders command to look up the name of your current customer managed configuration recorder:

```
$ aws configservice describe-configuration-recorders
{
    "ConfigurationRecorders": [
        {
            "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",
            "name": "default"
        }
    ]
}
```

2. Use the delete-configuration-recorder command to delete your customer managed current configuration recorder:

```
$ aws configservice delete-configuration-recorder --configuration-recorder-
name default
```

3. Use the put-configuration-recorder command to create a customer managed configuration recorder with the new name:

```
$ aws configservice put-configuration-recorder --configuration-recorder
 name=configRecorderName,roleARN=arn:aws:iam::012345678912:role/myConfigRole
```

4. Use the start-configuration-recorder command to resume recording:

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

Viewing your configuration recorders

You can use the Amazon Config console or the Amazon CLI view details about your configuration recorders.

To view your configuration recorders (Console)

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. Choose **Settings** in the navigation pane.
3. For the customer managed configuration recorder, you can view details on the **Customer managed recorder** tab.
4. For service-linked configuration recorders, choose a service-linked configuration recorders on the **Service-linked recorders** tab, and then choose **View**.

To view your configuration recorders (CLI)

Use the `describe-configuration-recorders` command to view details about your configuration recorders:

```
$ aws configservice describe-configuration-recorders
{
    "ConfigurationRecorders": [
        {
            "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",
            "name": "default"
        }
    ]
}
```

Use the `describe-configuration-recorder-status` command to view the current status of your configuration recorders:

```
$ aws configservice describe-configuration-recorder-status
```

```
{
    "ConfigurationRecordersStatus": [
        {
            "name": "default",
            "lastStatus": "SUCCESS",
            "lastStopTime": 1414511624.914,
            "lastStartTime": 1414708460.276,
            "recording": true,
            "lastStatusChangeTime": 1414816537.148,
            "lastErrorMessage": "NA",
            "lastErrorCode": "400"
        }
    ]
}
```

For both of these commands, you can use the `arn` and `configuration-recorder-names` fields to specify a list of configuration recorders. For service-linked configuration recorders, you can use the `service-principal` field to specify a configuration recorder.

If a configuration recorder is not specified, this command returns the details of all configuration recorders associated with the account.

Deleting your configuration recorders

You must use the Amazon CLI to delete the customer managed configuration recorder. You can use Amazon Config console or the Amazon CLI to delete a service-linked configuration recorder.

To delete the customer managed configuration recorder (CLI)

Use the `delete-configuration-recorder` command:

```
$ aws configservice delete-configuration-recorder --configuration-recorder-
name default
```

To delete a service-linked configuration recorder (Console)

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. Choose **Settings** in the navigation pane.

3. On the **Service-linked recorders** tab, choose a service-linked configuration recorders on the **Service-linked recorders** tab, and then choose **Delete**. When prompted, choose **Delete**.

To delete a service-linked configuration recorder (CLI)

Use the `delete-service-linked-configuration-recorder` command:

This command uses the `--service-principal` field.

```
$ aws configservice delete-service-linked-configuration-recorder --service-principal
 "The service principal of the Amazon Web Services service for the service-linked
 configuration recorder that you want to delete"
```

Working with the Delivery Channel

As Amazon Config continually records the changes that occur to your Amazon resources, it sends notifications and updated configuration states through the *delivery channel*. You can manage the delivery channel to control where Amazon Config sends configuration updates.

Topics

- Considerations
- Terminology
- Components of a Configuration Item
- Viewing the Delivery Channel
- Updating the Delivery Channel
- Renaming the Delivery Channel
- Delivering Configuration Snapshots to an Amazon S3 Bucket
- Verifying Delivery Status
- Viewing Configuration Snapshots in Amazon S3 bucket
- Example Configuration Snapshot from Amazon Config
- Notifications that Amazon Config Sends to an Amazon SNS topic

Considerations

One delivery channel per Region per account

You can have only one delivery channel per Amazon Region region per Amazon Web Services account, and the delivery channel is required to use Amazon Config.

Oversized configuration item notifications include a brief summary

When Amazon Config detects a configuration change for a resource and the notification exceeds the maximum size allowed by Amazon SNS, the notification includes a brief summary of the configuration item. You can view the complete notification in the Amazon S3 bucket location specified in the `s3BucketLocation` field. For more information, see Example Oversized Configuration Item Change Notification.

Amazon Config supports Amazon KMS encryption for Amazon S3 buckets used by Amazon Config

You can provide an Amazon Key Management Service (Amazon KMS) key or alias Amazon Resource Name (ARN) to encrypt the data delivered to your Amazon Simple Storage Service (Amazon S3) bucket. By default, Amazon Config delivers configuration history and snapshot files to your Amazon S3 bucket and encrypts the data at rest using S3 AES-256 server-side encryption, SSE-S3. However, if you provide Amazon Config with your KMS key or alias ARN, Amazon Config uses that KMS key instead of AES-256 encryption.

Amazon Config does not support the delivery channel to an Amazon S3 bucket where object lock is enabled with default retention enabled. For more information, see How S3 Object Lock works.

Terminology

A *configuration item* represents a point-in-time view of the various attributes of a supported Amazon resource that exists in your account. The components of a configuration item include metadata, attributes, relationships, current configuration, and related events. Amazon Config creates a configuration item whenever it detects a change to a resource type that it is recording. For example, if Amazon Config is recording Amazon S3 buckets, Amazon Config creates a configuration item whenever a bucket is created, updated, or deleted. You can also select for Amazon Config to create a configuration item at the recording frequency that you set.

A *configuration history* is a collection of the configuration items for a given resource over any time period. A configuration history can help you answer questions about, for example, when the resource was first created, how the resource has been configured over the last month, and what configuration changes were introduced yesterday at 9 AM. The configuration history is available to you in multiple formats. Amazon Config automatically delivers a configuration history file for each resource type that is being recorded to an Amazon S3 bucket that you specify. You can select a given resource in the Amazon Config console and navigate to all previous configuration items for that resource using the timeline. Additionally, you can access the historical configuration items for a resource from the API.

A *configuration snapshot* is a collection of the configuration items for the supported resources that exist in your account. This configuration snapshot is a complete picture of the resources that are being recorded and their configurations. The configuration snapshot can be a useful tool for validating your configuration. For example, you may want to examine the configuration snapshot regularly for resources that are configured incorrectly or that potentially should not exist. The configuration snapshot is available in multiple formats. You can have the configuration snapshot

delivered to an Amazon Simple Storage Service (Amazon S3) bucket that you specify. Additionally, you can select a point in time in the Amazon Config console and navigate through the snapshot of configuration items using the relationships between the resources.

A *configuration stream* is an automatically updated list of all configuration items for the resources that Amazon Config is recording. Every time a resource is created, modified, or deleted, Amazon Config creates a configuration item and adds to the configuration stream. The configuration stream works by using an Amazon Simple Notification Service (Amazon SNS) topic of your choice. The configuration stream is helpful for observing configuration changes as they occur so that you can spot potential problems, generating notifications if certain resources are changed, or updating external systems that need to reflect the configuration of your Amazon resources.

Components of a Configuration Item

A *configuration item* represents a point-in-time view of the various attributes of a supported Amazon resource that exists in your account. The components of a configuration item include metadata, attributes, relationships, current configuration, and related events. Amazon Config creates a configuration item whenever it detects a change to a resource type that it is recording. For example, if Amazon Config is recording Amazon S3 buckets, Amazon Config creates a configuration item whenever a bucket is created, updated, or deleted. You can also select for Amazon Config to create a configuration item at the recording frequency that you set.

A configuration item consists of the following components.

Component	Description	Contains
Metadata	Information about this configuration item	• Version ID • Time when the configuration item was captured • Status of the configuration item indicatin g whether the item was captured successfully • State ID indicating the ordering of the configuration items of a resource
Attributes	Resource attributes	• Resource ID • List of key–value tags for this resource

Component	Description	Contains
		• Resource type (see Supported Resource Types for Amazon Config) • Amazon Resource Name (ARN) • Availability Zone that contains this resource, if applicable • Time the resource was created
Relationships	How the resource is related to other resources associated with the account	Description of the relationship, such as Amazon EBS volume `vol-1234567` is attached to an Amazon EC2 instance `i-a1b2c3d4`
Current configuration	Information returned through a call to the Describe or List API of the resource	For example, `DescribeVolumes` API returns the following information about the volume: • Availability Zone the volume is in • Time the volume was attached • ID of the EC2 instance it is attached to • Current status of the volume • State of DeleteOnTermination flag • Device the volume is attached to • Type of volume, such as `gp2`, `io1`, or `standard`

Notes

1. A configuration item relationship does not include network flow or data flow dependencies. Configuration items cannot be customized to represent your application architecture.
2. As of Version 1.3, the relatedEvents field is empty. You can access the LookupEvents API in the *Amazon CloudTrail API Reference* to retrieve the events for the resource.
3. As of Version 1.3, the configurationItemMD5Hash field is empty. You can use the configurationStateId field to ensure you have the latest configuration item.

4. If a resource type does not support tagging or does not include tag information in its describe API response, Amazon Config won't capture tag data in the configuration items (CIs) for that resource type. Amazon Config will still record these resources. However, any functionality that relies on tag data won't work. This affects tag-based filtering, grouping, or compliance evaluation that relies on tag data.

Viewing the Delivery Channel

You must use the Amazon CLI to view details about the delivery channel.

The following code examples show how to use `DescribeDeliveryChannels`.

CLI

Amazon CLI

To get details about the delivery channel

The following command returns details about the delivery channel:

```
aws configservice describe-delivery-channels
```

Output:

```
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

- For API details, see DescribeDeliveryChannels in *Amazon CLI Command Reference*.

PowerShell

Tools for PowerShell V4

Example 1: This example retrieves the delivery channel for the region and displays details.

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

Output:

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- For API details, see DescribeDeliveryChannels in *Amazon Tools for PowerShell Cmdlet Reference (V4)*.

Tools for PowerShell V5

Example 1: This example retrieves the delivery channel for the region and displays details.

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

Output:

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- For API details, see DescribeDeliveryChannels in *Amazon Tools for PowerShell Cmdlet Reference (V5)*.

Updating the Delivery Channel

When you update the delivery channel, you can set the following options:

- The Amazon S3 bucket where Amazon Config sends configuration snapshots and configuration history files.
- How often Amazon Config delivers configuration snapshots to your Amazon S3 bucket.
- The Amazon SNS topic to which Amazon Config sends notifications about configuration changes.

To update the delivery channel (Console)

You can use the Amazon Config console to set the Amazon S3 bucket and the Amazon SNS topic for your delivery channel. For steps to manage these settings, see Setting Up Amazon Config with the Console.

The console does not provide options to rename the delivery channel, set the frequency for configuration snapshots, or delete the delivery channel. To do these tasks, you must use the Amazon CLI, the Amazon Config API, or one of the Amazon SDKs.

To update the delivery channel (Amazon SDKs)

The following code examples show how to use `PutDeliveryChannel`.

CLI

Amazon CLI

To create a delivery channel

The following command provides the settings for the delivery channel as JSON code:

```
aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

The `deliveryChannel.json` file specifies the delivery channel attributes:

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
```

```
}
```

This example sets the following attributes:

`name` - The name of the delivery channel. By default, Amazon Config assigns the name `default` to a new delivery channel.You cannot update the delivery channel name with the `put-delivery-channel` command. For the steps to change the name, see Renaming the Delivery Channel.`s3BucketName` - The name of the Amazon S3 bucket to which Amazon Config delivers configuration snapshots and configuration history files.If you specify a bucket that belongs to another Amazon account, that bucket must have policies that grant access permissions to Amazon Config. For more information, see Permissions for the Amazon S3 Bucket.

`snsTopicARN` - The Amazon Resource Name (ARN) of the Amazon SNS topic to which Amazon Config sends notifications about configuration changes.If you choose a topic from another account, the topic must have policies that grant access permissions to Amazon Config. For more information, see Permissions for the Amazon SNS Topic.

`configSnapshotDeliveryProperties` - Contains the `deliveryFrequency` attribute, which sets how often Amazon Config delivers configuration snapshots and how often it invokes evaluations for periodic Config rules.

If the command succeeds, Amazon Config returns no output. To verify the settings of your delivery channel, run the describe-delivery-channels command.

- For API details, see PutDeliveryChannel in *Amazon CLI Command Reference*.

PowerShell

Tools for PowerShell V4

Example 1: This example changes the deliveryFrequency property of an existing delivery channel.

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 amzn-s3-demo-bucket -DeliveryChannel_S3KeyPrefix my
```

- For API details, see PutDeliveryChannel in *Amazon Tools for PowerShell Cmdlet Reference (V4)*.

Tools for PowerShell V5

Example 1: This example changes the deliveryFrequency property of an existing delivery channel.

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 amzn-s3-demo-bucket -DeliveryChannel_S3KeyPrefix my
```

- For API details, see PutDeliveryChannel in *Amazon Tools for PowerShell Cmdlet Reference (V5)*.

(Optional) You can use the `describe-delivery-channels` command to verify that the delivery channel settings are updated:

```
$ aws configservice describe-delivery-channels
{
    "DeliveryChannels": [
        {
            "configSnapshotDeliveryProperties": {
                "deliveryFrequency": "Twelve_Hours"
            },
            "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

The following code examples show how to use `DescribeDeliveryChannels`.

CLI

Amazon CLI

To get details about the delivery channel

The following command returns details about the delivery channel:

```
aws configservice describe-delivery-channels
```

Output:

```
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

- For API details, see DescribeDeliveryChannels in *Amazon CLI Command Reference*.

PowerShell

Tools for PowerShell V4

Example 1: This example retrieves the delivery channel for the region and displays details.

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

Output:

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- For API details, see DescribeDeliveryChannels in *Amazon Tools for PowerShell Cmdlet Reference (V4)*.

Tools for PowerShell V5

Example 1: This example retrieves the delivery channel for the region and displays details.

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

Output:

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- For API details, see DescribeDeliveryChannels in *Amazon Tools for PowerShell Cmdlet Reference (V5)*.

Renaming the Delivery Channel

To change the delivery channel name, you must delete it and create a new delivery channel with your specified name. Before you can delete the delivery channel, you must temporarily stop the configuration recorder. The Amazon Config console does not provide the option to delete the delivery channel. You must use the Amazon CLI, the Amazon Config API, or one of the Amazon SDKs.

Renaming the delivery channel using the Amazon CLI

1. Use the `stop-configuration-recorder` command to stop the configuration recorder:

```
$ aws configservice stop-configuration-recorder --configuration-recorder-
name configRecorderName
```

2. Use the `describe-delivery-channels` command, and take note of your delivery channel's attributes:

```
$ aws configservice describe-delivery-channels
{
    "DeliveryChannels": [
        {
            "configSnapshotDeliveryProperties": {
                "deliveryFrequency": "Twelve_Hours"
            },
            "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
            "name": "default",
```

```
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

3. Use the [delete-delivery-channel] command to delete the delivery channel:

```
$ aws configservice delete-delivery-channel --delivery-channel-name default
```

4. Use the [put-delivery-channel] command to create a delivery channel with the desired name:

```
$ aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

The deliveryChannel.json file specifies the delivery channel attributes:

```
{
    "name": "myCustomDeliveryChannelName",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

5. Use the `start-configuration-recorder` command to resume recording:

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

Delivering Configuration Snapshots to an Amazon S3 Bucket

A *configuration snapshot* is a collection of the configuration items for the supported resources that exist in your account. This configuration snapshot is a complete picture of the resources that are being recorded and their configurations. The configuration snapshot can be a useful tool for validating your configuration. For example, you may want to examine the configuration snapshot regularly for resources that are configured incorrectly or that potentially should not exist. The configuration snapshot is available in multiple formats. You can have the configuration snapshot

delivered to an Amazon Simple Storage Service (Amazon S3) bucket that you specify. Additionally, you can select a point in time in the Amazon Config console and navigate through the snapshot of configuration items using the relationships between the resources.

Delivering Configuration Snapshots

Amazon Config generates configuration snapshots when you invoke the DeliverConfigSnapshot action or you run the Amazon CLI `deliver-config-snapshot` command. Amazon Config stores configuration snapshots in the Amazon S3 bucket that you specified when you enabled Amazon Config.

Enter the `deliver-config-snapshot` command by specifying the name assigned by Amazon Config when you configured your delivery channel, for example:

```
$ aws configservice deliver-config-snapshot --delivery-channel-name default
{
    "configSnapshotId": "94ccff53-83be-42d9-996f-b4624b3c1a55"
}
```

Verifying Delivery Status

Enter the `describe-delivery-channel-status` command to verify that the Amazon Config has started delivering the configurations to the specified delivery channel:

```
aws configservice describe-delivery-channel-status
```

The response lists the status of all the three delivery formats that Amazon Config uses to deliver configurations to your bucket and topic.

```
{
    "DeliveryChannelsStatus": [
        {
            "configStreamDeliveryInfo": {
                "lastStatusChangeTime": 1415138614.125,
                "lastStatus": "SUCCESS"
            },
            "configHistoryDeliveryInfo": {
                "lastSuccessfulTime": 1415148744.267,
                "lastStatus": "SUCCESS",
                "lastAttemptTime": 1415148744.267
```

```
            },
            "configSnapshotDeliveryInfo": {
                "lastSuccessfulTime": 1415333113.4159999,
                "lastStatus": "SUCCESS",
                "lastAttemptTime": 1415333113.4159999
            },
            "name": "default"
        }
    ]
}
```

View the `lastSuccessfulTime` field in `configSnapshotDeliveryInfo`. The time should match the time you last requested the delivery of the configuration snapshot.

> **Note**
>
> Amazon Config uses the UTC format (Coordinated Universal Time) to record the time.

Viewing Configuration Snapshots in Amazon S3 bucket

A *configuration snapshot* is a collection of the configuration items for the supported resources that exist in your account. This configuration snapshot is a complete picture of the resources that are being recorded and their configurations. The configuration snapshot can be a useful tool for validating your configuration. For example, you may want to examine the configuration snapshot regularly for resources that are configured incorrectly or that potentially should not exist. The configuration snapshot is available in multiple formats. You can have the configuration snapshot delivered to an Amazon Simple Storage Service (Amazon S3) bucket that you specify. Additionally, you can select a point in time in the Amazon Config console and navigate through the snapshot of configuration items using the relationships between the resources.

Viewing Configuration Snapshots

1. Sign in to the Amazon Web Services Management Console and open the Amazon S3 console at https://console.amazonaws.cn/s3/.
2. In the Amazon S3 console **All Buckets** list, choose the name of your Amazon S3 bucket.
3. Go through the nested folders in your bucket until you see the `ConfigSnapshot` object with a snapshot ID that matches with the ID returned by the command. Download and open the object to view the configuration snapshot.. The S3 bucket also contains an empty file named

`ConfigWritabilityCheckFile`. Amazon Config creates this file to verify that the service can successfully write to the S3 bucket.

Example Configuration Snapshot from Amazon Config

The following is an example of the information that Amazon Config includes in a configuration snapshot. The snapshot describes the configuration for the resources that Amazon Config is recording in the current region for your Amazon Web Services account, and it describes the relationships between these resources.

> **Note**
>
> The configuration snapshot can include references to resources types and resource IDs that are not supported.

```
{
    "fileVersion": "1.0",
    "requestId": "asudf8ow-4e34-4f32-afeb-0ace5bf3trye",
    "configurationItems": [
        {
            "configurationItemVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
            "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
```

```
                "name": "Attached to Instance"
            }
        ],
        "configuration": {
            "volumeId": "vol-ce676ccc",
            "size": 1,
            "snapshotId": "",
            "availabilityZone": "us-west-2b",
            "state": "in-use",
            "createTime": "2014-02-27T21:43:53.0885+0000",
            "attachments": [
                {
                    "volumeId": "vol-ce676ccc",
                    "instanceId": "i-344c463d",
                    "device": "/dev/sdf",
                    "state": "attached",
                    "attachTime": "2014-03-07T23:46:28.0000+0000",
                    "deleteOnTermination": false
                }
            ],
            "tags": [
                {
                    "tagName": "environment",
                    "tagValue": "PROD"
                },
                {
                    "tagName": "name",
                    "tagValue": "DataVolume1"
                }
            ],
            "volumeType": "standard"
        }
    },
    {
        "configurationItemVersion": "1.0",
        "resourceId": "i-344c463d",
        "accountId": "12345678910",
        "arn": "arn:aws:ec2:us-west-2b:123456789012:instance/i-344c463d",
        "configurationItemCaptureTime": "2014-03-07T23:47:09.523Z",
        "configurationStateID": "cdb571fa-ce7a-4ec5-8914-0320466a355e",
        "configurationItemStatus": "OK",
        "relatedEvents": [
            "06c12a39-eb35-11de-ae07-adb69edbb1e4",
            "c376e30d-71a2-4694-89b7-a5a04ad92281"
```

```
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Instance",
            "resourceCreationTime": "2014-02-26T22:56:35.000Z",
            "tags": {
                "Name": "integ-test-1",
                "examplename": "examplevalue"
            },
            "relationships": [
                {
                    "resourceId": "vol-ce676ccc",
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Attached Volume"
                },
                {
                    "resourceId": "vol-ef0e06ed",
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Attached Volume",
                    "direction": "OUT"
                },
                {
                    "resourceId": "subnet-47b4cf2c",
                    "resourceType": "AWS::EC2::SUBNET",
                    "name": "Is contained in Subnet",
                    "direction": "IN"
                }
            ],
            "configuration": {
                "instanceId": "i-344c463d",
                "imageId": "ami-ccf297fc",
                "state": {
                    "code": 16,
                    "name": "running"
                },
                "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
                "publicDnsName": "ec2-54-218-4-189.us-west-2.compute.amazonaws.com",
                "stateTransitionReason": "",
                "keyName": "configDemo",
                "amiLaunchIndex": 0,
                "productCodes": [],
                "instanceType": "t1.micro",
                "launchTime": "2014-02-26T22:56:35.0000+0000",
                "placement": {
                    "availabilityZone": "us-west-2b",
```

```
                    "groupName": "",
                    "tenancy": "default"
                },
                "kernelId": "aki-fc8f11cc",
                "monitoring": {
                    "state": "disabled"
                },
                "subnetId": "subnet-47b4cf2c",
                "vpcId": "vpc-41b4cf2a",
                "privateIpAddress": "172.31.21.63",
                "publicIpAddress": "54.218.4.189",
                "architecture": "x86_64",
                "rootDeviceType": "ebs",
                "rootDeviceName": "/dev/sda1",
                "blockDeviceMappings": [
                    {
                        "deviceName": "/dev/sda1",
                        "ebs": {
                            "volumeId": "vol-ef0e06ed",
                            "status": "attached",
                            "attachTime": "2014-02-26T22:56:38.0000+0000",
                            "deleteOnTermination": true
                        }
                    },
                    {
                        "deviceName": "/dev/sdf",
                        "ebs": {
                            "volumeId": "vol-ce676ccc",
                            "status": "attached",
                            "attachTime": "2014-03-07T23:46:28.0000+0000",
                            "deleteOnTermination": false
                        }
                    }
                ],
                "virtualizationType": "paravirtual",
                "clientToken": "aBCDe123456",
                "tags": [
                    {
                        "key": "Name",
                        "value": "integ-test-1"
                    },
                    {
                        "key": "examplekey",
                        "value": "examplevalue"
```

```
                    }
                ],
                "securityGroups": [
                    {
                        "groupName": "launch-wizard-2",
                        "groupId": "sg-892adfec"
                    }
                ],
                "sourceDestCheck": true,
                "hypervisor": "xen",
                "networkInterfaces": [
                    {
                        "networkInterfaceId": "eni-55c03d22",
                        "subnetId": "subnet-47b4cf2c",
                        "vpcId": "vpc-41b4cf2a",
                        "description": "",
                        "ownerId": "12345678910",
                        "status": "in-use",
                        "privateIpAddress": "172.31.21.63",
                        "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
                        "sourceDestCheck": true,
                        "groups": [
                            {
                                "groupName": "launch-wizard-2",
                                "groupId": "sg-892adfec"
                            }
                        ],
                        "attachment": {
                            "attachmentId": "eni-attach-bf90c489",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2014-02-26T22:56:35.0000+0000",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.218.4.189",
                            "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [
                            {
                                "privateIpAddress": "172.31.21.63",
```

```
                                "privateDnsName": "ip-172-31-21-63.us-
west-2.compute.internal",
                                "primary": true,
                                "association": {
                                    "publicIp": "54.218.4.189",
                                    "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
                                    "ipOwnerId": "amazon"
                                }
                            }
                        ]
                    }
                ],
                "ebsOptimized": false
            }
        }
    ]
}
```

The next step is to verify that configuration snapshot was delivered successfully to the delivery channel.

Notifications that Amazon Config Sends to an Amazon SNS topic

> **Note**
>
> Before Amazon Config can send notifications to an Amazon SNS topic, you must first set up the configuration recorder and the delivery channel. For more information, see Managing the Configuration Recorder and Managing the Delivery Channel.

You can configure Amazon Config to stream configuration changes and notifications to an Amazon SNS topic. For example, when a resource is updated, you can get a notification sent to your email, so that you can view the changes. You can also be notified when Amazon Config evaluates your custom or managed rules against your resources. For more information, see Logging and Monitoring in Amazon Config.

Amazon Config sends notifications for the following events:

- Configuration item change for a resource.
- Configuration history for a resource was delivered for your account.
- Configuration snapshot for recorded resources was started and delivered for your account.
- Compliance state of your resources and whether they are compliant with your rules.
- Evaluation started for a rule against your resources.
- Amazon Config failed to deliver the notification to your account.

Topics

- Example Configuration Item Change Notifications
- Example Configuration History Delivery Notification
- Example Configuration Snapshot Delivery Started Notification
- Example Configuration Snapshot Delivery Notification
- Example Compliance Change Notification
- Example Rules Evaluation Started Notification
- Example Oversized Configuration Item Change Notification
- Example Delivery Failed Notification

Example Configuration Item Change Notifications

Amazon Config uses Amazon SNS to deliver notifications to subscription endpoints. These notifications provide the delivery status for configuration snapshots and configuration histories, and they provide each configuration item that Amazon Config creates when the configurations of recorded Amazon resources change. Amazon Config also sends notifications that show whether your resources are compliant against your rules. If you choose to have notifications sent by email, you can use filters in your email client application based on the subject line and message body of the email.

The following is an example payload of an Amazon SNS notification that is generated when Amazon Config detects that the Amazon Elastic Block Store volume `vol-ce676ccc` is attached to the instance with an ID of `i-344c463d`. The notification contains the configuration item change for the resource.

```
{
    "Type": "Notification",
```

```
    "MessageId": "8b945cb0-db34-5b72-b032-1724878af488",
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:example",
    "Message": {
        "MessageVersion": "1.0",
        "NotificationCreateTime": "2014-03-18T10:11:00Z",
        "messageType": "ConfigurationItemChangeNotification",
        "configurationItem": [
            {
                "configurationItemVersion": "1.0",
                "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
                "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
                "resourceId": "vol-ce676ccc",
                "awsAccountId": "123456789012",
                "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
                "configurationItemStatus": "OK",
                "relatedEvents": [],
                "availabilityZone": "us-west-2b",
                "resourceType": "AWS::EC2::VOLUME",
                "resourceCreationTime": "2014-02-27T21:43:53.885Z",
                "tags": {},
                "relationships": [
                    {
                        "resourceId": "i-344c463d",
                        "resourceType": "AWS::EC2::INSTANCE",
                        "name": "Attached to Instance"
                    }
                ],
                "configuration": {
                    "volumeId": "vol-ce676ccc",
                    "size": 1,
                    "snapshotId": "",
                    "availabilityZone": "us-west-2b",
                    "state": "in-use",
                    "createTime": "2014-02-27T21:43:53.0885+0000",
                    "attachments": [
                        {
                            "volumeId": "vol-ce676ccc",
                            "instanceId": "i-344c463d",
                            "device": "/dev/sdf",
                            "state": "attached",
                            "attachTime": "2014-03-07T23:46:28.0000+0000",
                            "deleteOnTermination": false
                        }
                    ],
```

```
                    "tags": [],
                    "volumeType": "standard"
                }
            }
        ],
        "configurationItemDiff": {
            "changeType": "UPDATE",
            "changedProperties": {
                "Configuration.State": {
                    "previousValue": "available",
                    "updatedValue": "in-use",
                    "changeType": "UPDATE"
                },
                "Configuration.Attachments.0": {
                    "updatedValue": {
                        "VolumeId": "vol-ce676ccc",
                        "InstanceId": "i-344c463d",
                        "Device": "/dev/sdf",
                        "State": "attached",
                        "AttachTime": "FriMar0723: 46: 28UTC2014",
                        "DeleteOnTermination": "false"
                    },
                    "changeType": "CREATE"
                }
            }
        }
    },
    "Timestamp": "2014-03-07T23:47:10.001Z",
    "SignatureVersion": "1",
    "Signature": "LgfJNB5aOk/w3omqsYrv5cUFY8yvIJvO5ZZh46/
KGPApk6HXRTBRlkhjacnxIXJEWsGI9mxvMmoWPLJGYEAR5FF/+/Ro9QTmiTNcEjQ5kB8wGsRWVrk/
whAzT2lVtofc365En2T1Ncd9iSFFXfJchgBmI7EACZ28t
+n2mWFgo57n6eGDvHTedslzC6KxkfWTfXsR6zHXzkB3XuZImktflg3iPKtvBb3Zc9iVbNsBEI4FITFWktSqqomYDjc5h0kg
+qZhMzEbHWpzFlEzvFl55KaZXxDbznBD1ZkqPgno/WufuxszCiMrsmV8pUNUnkU1TA==",
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-
e372f8ca30337fdb084e8ac449342c77.pem",
    "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:123456789012:example:a6859fee-3638-407c-907e-879651c9d143"
}
```

Configuration Items for Resources with Relationships

If a resource is related to other resources, a change to that resource can result in multiple configuration items. The following example shows how Amazon Config creates configuration items for resources with relationships.

1. You have an Amazon EC2 instance with an ID of `i-007d374c8912e3e90`, and the instance is associated with an Amazon EC2 security group, `sg-c8b141b4`.
2. You update your EC2 instance to change the security group to another security group, `sg-3f1fef43`.
3. Because the EC2 instance is related to another resource, Amazon Config creates multiple configuration items like the following examples:

This notification contains the configuration item change for the EC2 instance when the security group is replaced.

```
{
    "Type": "Notification",
    "MessageId": "faeba85e-ef46-570a-b01c-f8b0faae8d5d",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::EC2::Instance i-007d374c8912e3e90 Updated
 in Account 123456789012",
    "Message": {
        "configurationItemDiff": {
            "changedProperties": {
                "Configuration.NetworkInterfaces.0": {
                    "previousValue": {
                        "networkInterfaceId": "eni-fde9493f",
                        "subnetId": "subnet-2372be7b",
                        "vpcId": "vpc-14400670",
                        "description": "",
                        "ownerId": "123456789012",
                        "status": "in-use",
                        "macAddress": "0e:36:a2:2d:c5:e0",
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "sourceDestCheck": true,
                        "groups": [{
                            "groupName": "example-security-group-1",
                            "groupId": "sg-c8b141b4"
                        }],
```

```
                        "attachment": {
                            "attachmentId": "eni-attach-85bd89d9",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2017-01-09T19:36:02.000Z",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [{
                            "privateIpAddress": "172.31.16.84",
                            "privateDnsName": "ip-172-31-16-84.ec2.internal",
                            "primary": true,
                            "association": {
                                "publicIp": "54.175.43.43",
                                "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                                "ipOwnerId": "amazon"
                            }
                        }]
                    },
                    "updatedValue": null,
                    "changeType": "DELETE"
                },
                "Relationships.0": {
                    "previousValue": {
                        "resourceId": "sg-c8b141b4",
                        "resourceName": null,
                        "resourceType": "AWS::EC2::SecurityGroup",
                        "name": "Is associated with SecurityGroup"
                    },
                    "updatedValue": null,
                    "changeType": "DELETE"
                },
                "Configuration.NetworkInterfaces.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "networkInterfaceId": "eni-fde9493f",
                        "subnetId": "subnet-2372be7b",
                        "vpcId": "vpc-14400670",
```

```
                        "description": "",
                        "ownerId": "123456789012",
                        "status": "in-use",
                        "macAddress": "0e:36:a2:2d:c5:e0",
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "sourceDestCheck": true,
                        "groups": [{
                            "groupName": "example-security-group-2",
                            "groupId": "sg-3f1fef43"
                        }],
                        "attachment": {
                            "attachmentId": "eni-attach-85bd89d9",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2017-01-09T19:36:02.000Z",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [{
                            "privateIpAddress": "172.31.16.84",
                            "privateDnsName": "ip-172-31-16-84.ec2.internal",
                            "primary": true,
                            "association": {
                                "publicIp": "54.175.43.43",
                                "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                                "ipOwnerId": "amazon"
                            }
                        }]
                    },
                    "changeType": "CREATE"
                },
                "Relationships.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "resourceId": "sg-3f1fef43",
                        "resourceName": null,
                        "resourceType": "AWS::EC2::SecurityGroup",
```

```
                    "name": "Is associated with SecurityGroup"
                },
                "changeType": "CREATE"
            },
            "Configuration.SecurityGroups.1": {
                "previousValue": null,
                "updatedValue": {
                    "groupName": "example-security-group-2",
                    "groupId": "sg-3f1fef43"
                },
                "changeType": "CREATE"
            },
            "Configuration.SecurityGroups.0": {
                "previousValue": {
                    "groupName": "example-security-group-1",
                    "groupId": "sg-c8b141b4"
                },
                "updatedValue": null,
                "changeType": "DELETE"
            }
        },
        "changeType": "UPDATE"
    },
    "configurationItem": {
        "relatedEvents": [],
        "relationships": [
            {
                "resourceId": "eni-fde9493f",
                "resourceName": null,
                "resourceType": "AWS::EC2::NetworkInterface",
                "name": "Contains NetworkInterface"
            },
            {
                "resourceId": "sg-3f1fef43",
                "resourceName": null,
                "resourceType": "AWS::EC2::SecurityGroup",
                "name": "Is associated with SecurityGroup"
            },
            {
                "resourceId": "subnet-2372be7b",
                "resourceName": null,
                "resourceType": "AWS::EC2::Subnet",
                "name": "Is contained in Subnet"
            },
```

```
                {
                    "resourceId": "vol-0a2d63a256bce35c5",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Is attached to Volume"
                },
                {
                    "resourceId": "vpc-14400670",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::VPC",
                    "name": "Is contained in Vpc"
                }
            ],
            "configuration": {
                "instanceId": "i-007d374c8912e3e90",
                "imageId": "ami-9be6f38c",
                "state": {
                    "code": 16,
                    "name": "running"
                },
                "privateDnsName": "ip-172-31-16-84.ec2.internal",
                "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
                "stateTransitionReason": "",
                "keyName": "ec2-micro",
                "amiLaunchIndex": 0,
                "productCodes": [],
                "instanceType": "t2.micro",
                "launchTime": "2017-01-09T20:13:28.000Z",
                "placement": {
                    "availabilityZone": "us-east-2c",
                    "groupName": "",
                    "tenancy": "default",
                    "hostId": null,
                    "affinity": null
                },
                "kernelId": null,
                "ramdiskId": null,
                "platform": null,
                "monitoring": {"state": "disabled"},
                "subnetId": "subnet-2372be7b",
                "vpcId": "vpc-14400670",
                "privateIpAddress": "172.31.16.84",
                "publicIpAddress": "54.175.43.43",
                "stateReason": null,
```

```
                "architecture": "x86_64",
                "rootDeviceType": "ebs",
                "rootDeviceName": "/dev/xvda",
                "blockDeviceMappings": [{
                    "deviceName": "/dev/xvda",
                    "ebs": {
                        "volumeId": "vol-0a2d63a256bce35c5",
                        "status": "attached",
                        "attachTime": "2017-01-09T19:36:03.000Z",
                        "deleteOnTermination": true
                    }
                }],
                "virtualizationType": "hvm",
                "instanceLifecycle": null,
                "spotInstanceRequestId": null,
                "clientToken": "bIYqA1483990561516",
                "tags": [{
                    "key": "Name",
                    "value": "value"
                }],
                "securityGroups": [{
                    "groupName": "example-security-group-2",
                    "groupId": "sg-3f1fef43"
                }],
                "sourceDestCheck": true,
                "hypervisor": "xen",
                "networkInterfaces": [{
                    "networkInterfaceId": "eni-fde9493f",
                    "subnetId": "subnet-2372be7b",
                    "vpcId": "vpc-14400670",
                    "description": "",
                    "ownerId": "123456789012",
                    "status": "in-use",
                    "macAddress": "0e:36:a2:2d:c5:e0",
                    "privateIpAddress": "172.31.16.84",
                    "privateDnsName": "ip-172-31-16-84.ec2.internal",
                    "sourceDestCheck": true,
                    "groups": [{
                        "groupName": "example-security-group-2",
                        "groupId": "sg-3f1fef43"
                    }],
                    "attachment": {
                        "attachmentId": "eni-attach-85bd89d9",
                        "deviceIndex": 0,
```

```
                        "status": "attached",
                        "attachTime": "2017-01-09T19:36:02.000Z",
                        "deleteOnTermination": true
                    },
                    "association": {
                        "publicIp": "54.175.43.43",
                        "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
                        "ipOwnerId": "amazon"
                    },
                    "privateIpAddresses": [{
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "primary": true,
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        }
                    }]
                }],
                "iamInstanceProfile": null,
                "ebsOptimized": false,
                "sriovNetSupport": null,
                "enaSupport": true
            },
            "supplementaryConfiguration": {},
            "tags": {"Name": "value"},
            "configurationItemVersion": "1.2",
            "configurationItemCaptureTime": "2017-01-09T22:50:14.328Z",
            "configurationStateId": 1484002214328,
            "awsAccountId": "123456789012",
            "configurationItemStatus": "OK",
            "resourceType": "AWS::EC2::Instance",
            "resourceId": "i-007d374c8912e3e90",
            "resourceName": null,
            "ARN": "arn:aws:ec2:us-east-2:123456789012:instance/i-007d374c8912e3e90",
            "awsRegion": "us-east-2",
            "availabilityZone": "us-east-2c",
            "configurationStateMd5Hash": "8d0f41750f5965e0071ae9be063ba306",
            "resourceCreationTime": "2017-01-09T20:13:28.000Z"
        },
        "notificationCreationTime": "2017-01-09T22:50:15.928Z",
        "messageType": "ConfigurationItemChangeNotification",
```

```
        "recordVersion": "1.2"
    },
    "Timestamp": "2017-01-09T22:50:16.358Z",
    "SignatureVersion": "1",
    "Signature": "lpJTEYOSr8fUbiaaRNw1ECawJFVoD7I67mIeEkfAWJkqvvpak1ULHLlC
+I0sS/01A4P1Yci8GSK/cOEC/O2XBntlw4CAtbMUgTQvb345Z2YZwcpK0kPNi6v6N51DuZ/6DZA8EC
+gVTNTO09xtNIH8aMlvqyvUSXuh278xayExC5yTRXEg+ikdZRd4QzS7obSK1kgRZWI6ipxPNL6rd56/
VvPxyhcbS7Vm40/2+e0nVb3bjNHBxjQTXSs1Xhuc9eP2gEsC4Sl32bGqdeDU1Y4dFGukuzPYoHuEtDPh
+GkLUq3KeiDAQshxAZLmOIRcQ7iJ/bELDJTN9AcX6lqlDZ79w==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


This notification contains the configuration item change for the EC2 security group, `sg-3f1fef43`, which is associated with the instance.


```
{
    "Type": "Notification",
    "MessageId": "564d873e-711e-51a3-b48c-d7d064f65bf4",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::EC2::SecurityGroup sg-3f1fef43 Created in
 Account 123456789012",
    "Message": {
        "configurationItemDiff": {
            "changedProperties": {},
            "changeType": "CREATE"
        },
        "configurationItem": {
            "relatedEvents": [],
            "relationships": [{
                "resourceId": "vpc-14400670",
                "resourceName": null,
                "resourceType": "AWS::EC2::VPC",
                "name": "Is contained in Vpc"
            }],
            "configuration": {
                "ownerId": "123456789012",
                "groupName": "example-security-group-2",
                "groupId": "sg-3f1fef43",
                "description": "This is an example security group.",
```

```
                "ipPermissions": [],
                "ipPermissionsEgress": [{
                    "ipProtocol": "-1",
                    "fromPort": null,
                    "toPort": null,
                    "userIdGroupPairs": [],
                    "ipRanges": ["0.0.0.0/0"],
                    "prefixListIds": []
                }],
                "vpcId": "vpc-14400670",
                "tags": []
            },
            "supplementaryConfiguration": {},
            "tags": {},
            "configurationItemVersion": "1.2",
            "configurationItemCaptureTime": "2017-01-09T22:50:15.156Z",
            "configurationStateId": 1484002215156,
            "awsAccountId": "123456789012",
            "configurationItemStatus": "ResourceDiscovered",
            "resourceType": "AWS::EC2::SecurityGroup",
            "resourceId": "sg-3f1fef43",
            "resourceName": null,
            "ARN": "arn:aws:ec2:us-east-2:123456789012:security-group/sg-3f1fef43",
            "awsRegion": "us-east-2",
            "availabilityZone": "Not Applicable",
            "configurationStateMd5Hash": "7399608745296f67f7fe1c9ca56d5205",
            "resourceCreationTime": null
        },
        "notificationCreationTime": "2017-01-09T22:50:16.021Z",
        "messageType": "ConfigurationItemChangeNotification",
        "recordVersion": "1.2"
    },
    "Timestamp": "2017-01-09T22:50:16.413Z",
    "SignatureVersion": "1",
    "Signature": "GocX31Uu/zNFo85hZqzsNy30skwmLnjPjj+UjaJzkih
+dCP6gXYGQ0bK7uMzaLL2C/ibYOOsT7I/XY4NW6Amc5T46ydyHDjFRtQi8UfUQTqLXYRTnpOO/
hyK9lMFfhUNs4NwQpmx3n3mYEMpLuMs8DCgeBmB3AQ+hXPhNuNuR3mJVgo25S8AqphN9O0okZ2MKNUQy8iJm/
CVAx70TdnYsfUMZ24n88bUzAfiHGzc8QTthMdrFVUwXxa1h/7Zl8+A7BwoGmjo7W8CfLDVwaIQv1Uplgk3qd95Z0AXOzXVx
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
```

```
}
```

Understanding the `configurationItemDiff` field in Amazon SNS `ConfigurationItemChangeNotification` notifications

Amazon Config creates a configuration item whenever the configuration of a resource changes (create/update/delete). For a list of supported resource types that Amazon Config can record, see Supported Resource Types for Amazon Config. Amazon Config uses Amazon SNS to deliver a notification as the changes occur. The Amazon SNS notification payload includes fields to help you track the resource changes in a given Amazon Region.

To understand why you receive a `ConfigurationItemChangeNotification` notification, review the `configurationItemDiff` details. The fields vary depending on the change type and can form different combinations such as UPDATE-UPDATE, UPDATE-CREATE, and DELETE-DELETE. The following are explanations of some common combinations.

UPDATE-CREATE and UPDATE-UPDATE

The following example includes changes in the resource direct relationships and resource configurations. The `configurationItemDiff` details reveal the following information:

Action performed: A managed policy present in the account was attached to an Amazon Identity and Access Management (IAM) role.

Basic operation performed: UPDATE (updating the number of associations of the resource type `AWS::IAM::Policy` in an account).

Change type combinations:

1. Resource direct relationship change UPDATE-CREATE. A new attachment or association was created between an IAM policy and an IAM role.
2. Resource configuration change UPDATE-UPDATE. The number IAM policy associations increased from 2 to 3 when the policy was attached to the IAM role.

Example UPDATE-CREATE and UPDATE-UPDATE `configurationItemDiff` notification:

```
{
    "configurationItemDiff": {
        "changedProperties": {
            "Relationships.0": {
```

```
                "previousValue": null,
                "updatedValue": {
                    "resourceId": "AROA6D3M4S53*********",
                    "resourceName": "Test1",
                    "resourceType": "AWS::IAM::Role",
                    "name": "Is attached to Role"
                },
                "changeType": "CREATE"                >>>>>>>>>>>>>>>>>>>> 1
            },
            "Configuration.AttachmentCount": {
                "previousValue": 2,
                "updatedValue": 3,
                "changeType": "UPDATE"                >>>>>>>>>>>>>>>>>>>> 2
            }
        },
        "changeType": "UPDATE"
    }
}
```

UPDATE-DELETE

The following example includes changes in the resource direct relationships and resource configurations. The `configurationItemDiff` details reveal the following information:

Action performed: A managed policy present in the account was detached from an IAM user.

Basic operation performed: UPDATE (updating the permissions policy associated with the resource type `AWS::IAM::User`).

Change type combinations: Resource direct relationship change UPDATE-DELETE. The association between an IAM user and an IAM policy in an account was deleted.

Example UPDATE-DELETE `configurationItemDiff` notification:

```
{
  "configurationItemDiff": {
    "changedProperties": {
      "Configuration.UserPolicyList.0": {
        "previousValue": {
          "policyName": "Test2",
          "policyDocument": "{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/VPCId": "*"
                }
            }
        }
    ]
}"
        },
        "updatedValue": null,
        "changeType": "DELETE"                          >>>>>>>>>>>>>>>>>>>> 3
      }
    },
    "changeType": "UPDATE"
  }
}
```

DELETE-DELETE

The following example includes changes in the resource direct relationships and resource configurations. The `configurationItemDiff` details reveal the following information:

Action performed: An IAM role present in an account was deleted.

Basic operation performed: DELETE (a resource of the resource type `AWS::IAM::Role` was deleted).

Change type combinations: Resource direct relationship change and resource configuration change DELETE-DELETE. The deletion of the IAM role also deleted the association of the IAM policy with the IAM role.

Example DELETE-DELETE `configurationItemDiff` notification:

```
{
  "configurationItemDiff": {
    "changedProperties": {
      "Relationships.0": {
        "previousValue": {
```

```
          "resourceId": "ANPAIJ5MXUKK*********",
          "resourceName": "AWSCloudTrailAccessPolicy",
          "resourceType": "AWS::IAM::Policy",
          "name": "Is attached to CustomerManagedPolicy"
        },
        "updatedValue": null,
        "changeType": "DELETE"
      },
      "Configuration": {
        "previousValue": {
          "path": "/",
          "roleName": "CloudTrailRole",
          "roleId": "AROAJITJ6YGM*********",
          "arn": "arn:aws:iam::123456789012:role/CloudTrailRole",
          "createDate": "2017-12-06T10:27:51.000Z",
          "assumeRolePolicyDocument": "{"Version":"2012-10-17","Statement":
[{"Sid":"","Effect":"Allow","Principal":
{"AWS":"arn:aws:iam::123456789012:root"},"Action":"sts:AssumeRole","Condition":
{"StringEquals":{"sts:ExternalId":"123456"}}}]}",
          "instanceProfileList": [],
          "rolePolicyList": [],
          "attachedManagedPolicies": [
            {
              "policyName": "AWSCloudTrailAccessPolicy",
              "policyArn": "arn:aws:iam::123456789012:policy/AWSCloudTrailAccessPolicy"
            }
          ],
          "permissionsBoundary": null,
          "tags": [],
          "roleLastUsed": null
        },
        "updatedValue": null,
        "changeType": "DELETE"
      }
    },
    "changeType": "DELETE"
}
```


Example Configuration History Delivery Notification

The configuration history is a collection of the configuration items for a resource type over a time period. The following is an example notification that Amazon Config sends when the configuration history for a CloudTrail trail resource is delivered for your account.

```
{
    "Type": "Notification",
    "MessageId": "ce49bf2c-d03a-51b0-8b6a-ef480a8b39fe",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration History Delivery Completed for
 Account 123456789012",
    "Message": {
        "s3ObjectKey": "AWSLogs/123456789012/Config/us-east-2/2016/9/27/
ConfigHistory/123456789012_Config_us-
east-2_ConfigHistory_AWS::CloudTrail::Trail_20160927T195818Z_20160927T195818Z_1.json.gz",
        "s3Bucket": "config-bucket-123456789012-ohio",
        "notificationCreationTime": "2016-09-27T20:37:05.217Z",
        "messageType": "ConfigurationHistoryDeliveryCompleted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-09-27T20:37:05.315Z",
    "SignatureVersion": "1",
    "Signature": "OuIcS5RAKXTR6chQEJp3if4KJQVlBz2kmXh7QE1/
RJQiCPsCNfG0J0rUZ1rqfKMqpps/Ka+zF0kg4dUCWV9PF0dliuwnjfbtYmDZpP4EBOoGmxcTliUn1AIe/
yeGFDuc6P3EotP3zt02rhmxjezjf3c11urstFZ8rTLVXp0z0xeyk4da0UetLsWZxUFEG0Z5uhk09mBo5dg/4mryIOovidhr
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Example Configuration Snapshot Delivery Started Notification

The following is an example notification that Amazon Config sends when Amazon Config starts delivering the configuration snapshot for your account.


```
{
    "Type": "Notification",
    "MessageId": "a32d0487-94b1-53f6-b4e6-5407c9c00be6",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration Snapshot Delivery Started for
 Account 123456789012",
    "Message": {
        "configSnapshotId": "108e0794-84a7-4cca-a179-76a199ddd11a",
        "notificationCreationTime": "2016-10-18T17:26:09.572Z",
        "messageType": "ConfigurationSnapshotDeliveryStarted",
```

```
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-10-18T17:26:09.840Z",
    "SignatureVersion": "1",
    "Signature": "BBA0DeKsfteTpYyZH5HPANpOLmW/jumOMBsghRq/kimY9tjNlkF/
V3BpLG1HVmDQdQzBh6oKE0h0rxcazbyGf5KF5W5r1zKKlEnS9xugFzALPUx//
olSJ4neWalLBKNIq1xvAQgu9qHfDR7dS2aCwe4scQfqOjn1Ev7PlZqxmT+ux3SR/
C54cbfcduDpDsPwdo868+TpZvMtaU30ySnX04fmOgxoiA8AJO/EnjduQ08/zd4SYXhm
+H9wavcwXB9XECelHhRW70Y+wHQixfx40S1SaSRzvnJE+m9mHphFQs64YraRDRv6tMaenTk6CVPO
+81ceAXIg2E1m7hZ7lz4PA==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

Example Configuration Snapshot Delivery Notification

The configuration snapshot is a collection of configuration items for all recorded resources and their configurations in your account. The following is an example notification that Amazon Config sends when the configuration snapshot is delivered for your account.

```
{
    "Type": "Notification",
    "MessageId": "9fc82f4b-397e-5b69-8f55-7f2f86527100",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration Snapshot Delivery Completed for
 Account 123456789012",
    "Message": {
        "configSnapshotId": "16da64e4-cb65-4846-b061-e6c3ba43cb96",
        "s3ObjectKey": "AWSLogs/123456789012/Config/us-east-2/2016/9/27/
ConfigSnapshot/123456789012_Config_us-east-2_ConfigSnapshot_20160927T183939Z_16da64e4-
cb65-4846-b061-e6c3ba43cb96.json.gz",
        "s3Bucket": "config-bucket-123456789012-ohio",
        "notificationCreationTime": "2016-09-27T18:39:39.853Z",
        "messageType": "ConfigurationSnapshotDeliveryCompleted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-09-27T18:39:40.062Z",
    "SignatureVersion": "1",
    "Signature": "PMkWfUuj/fKIEXA7s2wTDLbZoF/MDsUkPspYghOpwu9n6m+C
+zrm0cEZXPxxJPvhnWozG7SVqkHYf9QgI/diW2twP/HPDn5GQs2rNDc+YlaByEXnKVtHV1Gd4r1kN57E/
```

```
oOW5NVLNczk5ymxAW+WGdptZJkCgyVuhJ28s08m3Z3Kqz96PPSnXzYZoCfCn/
yP6CqXoN7olr4YCbYxYwn8zOUYcPmc45yYNSUTKZi+RJQRnDJkL2qb
+s4h9w2fjbBBj8xe830VbFJqbHp7UkSfpc64Y+tRvmMLY5CI1cYrnuPRhTLdUk+R0sshg5G+JMtSLVG/
TvWbjz44CKXJprjIQg==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Example Compliance Change Notification

When Amazon Config evaluates your resources against a custom or managed rule, Amazon Config sends a notification that shows whether the resources are compliant against the rule.

The following is an example notification where the CloudTrail trail resource is compliant against the `cloudtrail-enabled` managed rule.


```
{
    "Type": "Notification",
    "MessageId": "11fd05dd-47e1-5523-bc01-55b988bb9478",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::::Account 123456789012 is COMPLIANT with
 cloudtrail-enabled in Accoun...",
    "Message": {
        "awsAccountId": "123456789012",
        "configRuleName": "cloudtrail-enabled",
        "configRuleARN": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-9rpvxc",
        "resourceType": "AWS::::Account",
        "resourceId": "123456789012",
        "awsRegion": "us-east-2",
        "newEvaluationResult": {
            "evaluationResultIdentifier": {
                "evaluationResultQualifier": {
                    "configRuleName": "cloudtrail-enabled",
                    "resourceType": "AWS::::Account",
                    "resourceId": "123456789012"
                },
                "orderingTimestamp": "2016-09-27T19:48:40.619Z"
            },
            "complianceType": "COMPLIANT",
```

```
            "resultRecordedTime": "2016-09-27T19:48:41.405Z",
            "configRuleInvokedTime": "2016-09-27T19:48:40.914Z",
            "annotation": null,
            "resultToken": null
        },
        "oldEvaluationResult": {
            "evaluationResultIdentifier": {
                "evaluationResultQualifier": {
                    "configRuleName": "cloudtrail-enabled",
                    "resourceType": "AWS::::Account",
                    "resourceId": "123456789012"
                },
                "orderingTimestamp": "2016-09-27T16:30:49.531Z"
            },
            "complianceType": "NON_COMPLIANT",
            "resultRecordedTime": "2016-09-27T16:30:50.717Z",
            "configRuleInvokedTime": "2016-09-27T16:30:50.105Z",
            "annotation": null,
            "resultToken": null
        },
        "notificationCreationTime": "2016-09-27T19:48:42.620Z",
        "messageType": "ComplianceChangeNotification",
        "recordVersion": "1.0"
    },
    "Timestamp": "2016-09-27T19:48:42.749Z",
    "SignatureVersion": "1",
    "Signature": "XZ9FfLb2ywkW9yj0yBkNtIP5q7Cry6JtCEyUiHmG9gpOZi3seQ41udhtAqCZoiNiizAEi
+6gcttHCRV1hNemzp/
YmBmTfO6azYXt0FJDaEvd86k68VCS9aqRlBBjYlNo7ILi4Pqd5rE4BX2YBQSzcQyERGkUfTZ2BIFyAmb1Q/
y4/6ez8rDyi545FDSlgcGEb4LKLNR6eDi4FbKtMGZHA7Nz8obqs1dHbgWYnp3c80mVLl7ohP4hilcxdywAgXrbsN32ekYr1
+BIZ21ZtkcUtY5B3ImgRlUO7Yhn3L3c6rZxQ==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Example: Config Configuration Item Change | Amazon EventBridge


```
{
  "version": "0",
  "id": "00bdf13e-1111-b2f5-cef0-e9cbbe7cd533",
```

```
  "detail-type": "Config Configuration Item Change",
  "source": "aws.config",
  "account": "123456789012",
  "time": "2022-03-16T01:10:51Z",
  "region": "us-east-1",
  "resources": ["arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95"],
  "detail": {
    "recordVersion": "1.3",
    "messageType": "ConfigurationItemChangeNotification",
    "configurationItemDiff": {
      "changedProperties": {
        "Configuration.FileSystemTags.0": {
          "updatedValue": {
            "Key": "test",
            "Value": "me"
          },
          "changeType": "CREATE"
        },
        "Tags.2": {
          "updatedValue": "me",
          "changeType": "CREATE"
        }
      },
      "changeType": "UPDATE"
    },
    "notificationCreationTime": "2022-03-16T01:10:51.976Z",
    "configurationItem": {
      "relatedEvents": [],
      "relationships": [],
      "configuration": {
        "FileSystemId": "fs-01f0d526165b57f95",
        "Arn": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95",
        "Encrypted": true,
        "FileSystemTags": [{
          "Key": "Name",
          "Value": "myname"
        }, {
          "Key": "test",
          "Value": "me"
        }],
        "PerformanceMode": "generalPurpose",
        "ThroughputMode": "bursting",
```

```
        "LifecyclePolicies": [{
          "TransitionToIA": "AFTER_30_DAYS"
        }, {
          "TransitionToPrimaryStorageClass": "AFTER_1_ACCESS"
        }],
        "BackupPolicy": {
          "Status": "ENABLED"
        },
        "FileSystemPolicy": {},
        "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/0e6c91d5-e23b-4ed3-
bd36-1561fbbc0a2d"
      },
      "supplementaryConfiguration": {},
      "tags": {
        "aws:elasticfilesystem:default-backup": "enabled",
        "test": "me",
        "Name": "cloudcontroltest1"
      },
      "configurationItemVersion": "1.3",
      "configurationItemCaptureTime": "2022-03-16T01:10:50.837Z",
      "configurationStateId": 1647393050837,
      "awsAccountId": "123456789012",
      "configurationItemStatus": "OK",
      "resourceType": "AWS::EFS::FileSystem",
      "resourceId": "fs-01f0d526165b57f95",
      "resourceName": "fs-01f0d526165b57f95",
      "ARN": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95",
      "awsRegion": "us-east-1",
      "availabilityZone": "Regional",
      "configurationStateMd5Hash": ""
    }
  }
}
```

Example Rules Evaluation Started Notification

Amazon Config sends a notification when it starts to evaluate your custom or managed rule against your resources. The following is an example notification when Amazon Config starts to evaluate the `iam-password-policy` managed rule.

```
{
    "Type": "Notification",
```

```
    "MessageId": "358c8e65-e27a-594e-82d0-de1fe77393d7",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Config Rules Evaluation Started for Account
 123456789012",
    "Message": {
        "awsAccountId": "123456789012",
        "awsRegion": "us-east-2",
        "configRuleNames": ["iam-password-policy"],
        "notificationCreationTime": "2016-10-13T21:55:21.339Z",
        "messageType": "ConfigRulesEvaluationStarted",
        "recordVersion": "1.0"
    },
    "Timestamp": "2016-10-13T21:55:21.575Z",
    "SignatureVersion": "1",
    "Signature": "DE431D+24zzFRboyPY2bPTsznJWe8L6TjDC+ItYlLFkE9jACSBl3sQ1uSjYzEhEbN7Cs
+wBoHnJ/DxOSpyCxt4giqgKd+H2I636BvrQwHDhJwJm7qI6P8IozEliRvRWbM38zDTvHqkmmXQbdDHRsK/
MssMeVTBKuW0x8ivMrj+KpwuF57tE62eXeFhjBeJ0DKQV+aC+i3onsuT7HQvXQDBPdOM
+cSuLrJaMQJ6TcMU5G76qg/
gl494ilb4Vj4udboGWpHSgUvI3guFsc1SsTrlWXQKXabWtsCQPfdOhkKgmViCfMZrLRp8Pjnu
+uspYQELkEfwBchDVVzd15iMrAzQ==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Example Oversized Configuration Item Change Notification

When Amazon Config detects a configuration change for a resource, it sends a configuration item (CI) notification. If the notification exceeds the maximum size allowed by Amazon Simple Notification Service (Amazon SNS), the notification includes a brief summary of the configuration item.

You can view the complete notification in the Amazon S3 bucket location specified in the `s3BucketLocation` field.

The following example notification shows a CI for an Amazon EC2 instance. The notification includes a summary of the changes and the location of the notification in the Amazon S3 bucket.

```
View the Timeline for this Resource in the Console:
```

```
    https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/
AWS::EC2::Instance/resourceId_14b76876-7969-4097-ab8e-a31942b02e80?
time=2016-10-06T16:46:16.261Z

    The full configuration item change notification for this resource exceeded the
 maximum size allowed by Amazon Simple Notification Service (SNS). A summary of the
 configuration item is provided here. You can view the complete notification in the
 specified Amazon S3 bucket location.

    New State Record Summary:
    ---------------------------
    {
      "configurationItemSummary": {
        "changeType": "UPDATE",
        "configurationItemVersion": "1.2",
        "configurationItemCaptureTime": "2016-10-06T16:46:16.261Z",
        "configurationStateId": 0,
        "awsAccountId": "123456789012",
        "configurationItemStatus": "OK",
        "resourceType": "AWS::EC2::Instance",
        "resourceId": "resourceId_14b76876-7969-4097-ab8e-a31942b02e80",
        "resourceName": null,
        "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/
resourceId_14b76876-7969-4097-ab8e-a31942b02e80",
        "awsRegion": "us-west-2",
        "availabilityZone": null,
        "configurationStateMd5Hash": "8f1ee69b287895a0f8bc5753eca68e96",
        "resourceCreationTime": "2016-10-06T16:46:10.489Z"
      },
      "s3DeliverySummary": {
        "s3BucketLocation": "amzn-s3-demo-bucket/AWSLogs/123456789012/
Config/us-west-2/2016/10/6/OversizedChangeNotification/AWS::EC2::Instance/
resourceId_14b76876-7969-4097-ab8e-a31942b02e80/123456789012_Config_us-
west-2_ChangeNotification_AWS::EC2::Instance_resourceId_14b76876-7969-4097-ab8e-
a31942b02e80_20161006T164616Z_0.json.gz",
        "errorCode": null,
        "errorMessage": null
      },
      "notificationCreationTime": "2016-10-06T16:46:16.261Z",
      "messageType": "OversizedConfigurationItemChangeNotification",
      "recordVersion": "1.0"
    }
```

How to access oversized configuration items

When a configuration item is oversized, only a summary is sent to Amazon SNS. The complete configuration item (CI) is stored in Amazon S3

The following code example shows how to access the the complete CI.

```
import boto3
import json

def handle_oversized_configuration_item(event):
    """
    Example of handling an oversized configuration item notification

    When a configuration item is oversized:
    1. AWS Config sends a summary notification through SNS
    2. The complete configuration item is stored in S3
    3. Use get_resource_config_history API to retrieve the complete configuration
    """

    # Extract information from the summary notification
    if event['messageType'] == 'OversizedConfigurationItemChangeNotification':
        summary = event['configurationItemSummary']
        resource_type = summary['resourceType']
        resource_id = summary['resourceId']

        # Initialize AWS Config client
        config_client = boto3.client('config')

        # Retrieve the complete configuration item
        response = config_client.get_resource_config_history(
            resourceType=resource_type,
            resourceId=resource_id
        )

        if response['configurationItems']:
            config_item = response['configurationItems'][0]

            # For EC2 instances, the configuration contains instance details
            configuration = json.loads(config_item['configuration'])
            print(f"Instance Configuration: {configuration}")

            # Handle supplementary configuration if present
```

```
            if 'supplementaryConfiguration' in config_item:
                for key, value in config_item['supplementaryConfiguration'].items():
                    if isinstance(value, str):
                        config_item['supplementaryConfiguration'][key] =
 json.loads(value)
                print(f"Supplementary Configuration:
 {config_item['supplementaryConfiguration']}")

            return config_item

        # If needed, you can also access the complete notification from S3
        s3_location = event['s3DeliverySummary']['s3BucketLocation']
        print(f"Complete notification available in S3: {s3_location}")

    return None
```

How it works

1. The function accepts an event parameter containing the Amazon Config notification.
2. It checks if the message type is an oversized configuration notification.
3. The function extracts the resource type and ID from the summary.
4. Using the Amazon Config client, it retrieves the complete configuration history.
5. The function processes both main and supplementary configurations.
6. If needed, you can access the complete notification from the provided S3 location.

Example Delivery Failed Notification

Amazon Config sends a delivery failed notification if Amazon Config can't deliver the configuration snapshot or an oversized configuration item change notification to your Amazon S3 bucket. Verify that you specified a valid Amazon S3 bucket.

```
View the Timeline for this Resource in the Console:
    https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/
AWS::EC2::Instance/test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457?
time=2016-10-06T16:46:13.749Z

     The full configuration item change notification for this resource exceeded the
 maximum size allowed by Amazon Simple Notification Service (SNS). A summary of the
 configuration item is provided here. You can view the complete notification in the
 specified Amazon S3 bucket location.
```

```
    New State Record Summary:
    ----------------------------
    {
      "configurationItemSummary": {
        "changeType": "UPDATE",
        "configurationItemVersion": "1.2",
        "configurationItemCaptureTime": "2016-10-06T16:46:13.749Z",
        "configurationStateId": 0,
        "awsAccountId": "123456789012",
        "configurationItemStatus": "OK",
        "resourceType": "AWS::EC2::Instance",
        "resourceId": "test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",
        "resourceName": null,
        "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/
test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",
        "awsRegion": "us-west-2",
        "availabilityZone": null,
        "configurationStateMd5Hash": "6de64b95eacd30e7b63d4bba7cd80814",
        "resourceCreationTime": "2016-10-06T16:46:10.489Z"
      },
      "s3DeliverySummary": {
        "s3BucketLocation": null,
        "errorCode": "NoSuchBucket",
        "errorMessage": "Failed to deliver notification to bucket: bucket-example for
 account 123456789012 in region us-west-2."
      },
      "notificationCreationTime": "2016-10-06T16:46:13.749Z",
      "messageType": "OversizedConfigurationItemChangeDeliveryFailed",
      "recordVersion": "1.0"
    }
```

Viewing the Amazon Config Dashboard

Use the **Dashboard** to see an overview of your resources, rules, conformance packs, and their compliance states and to visualize your Amazon Config usage and success metrics with Amazon CloudWatch. This page helps you quickly identify the top resources in your Amazon account, the conformance packs with the lowest level of compliance in your Amazon Web Services account, what rules or resources are noncompliant in your Amazon Web Services account, what traffic is driving your Amazon Config usage, and key metrics for success and failure that have occured in your workflows.

To use the Amazon Config Dashboard

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. In the left navigation pane, choose **Dashboard**.

Contents

- Compliance and Resource Inventory
- Amazon Config Usage and Success Metrics

Compliance and Resource Inventory

After setup, Amazon Config starts recording your specified resources and evaluating them against your rules. It may take a few minutes for Amazon Config to display your resources, rules, conformance packs, and their compliance states.

Conformance packs by compliance score

Conformance packs by compliance score displays up to 10 of your conformance packs with the lowest compliance score. A compliance score is the percentage of the number of compliant rule-resource combinations in a conformance pack compared to the number of total possible rule-resource combinations in the conformance pack.

This metric provides you with a high-level view of the compliance state of your conformance packs, and can be used to identify, investigate, and understand the level of compliance in your conformance packs. You can use the compliance score to track remediation progress, perform

comparisons across different sets of requirements, and see the impact a specific change or deployment has on a conformance pack.

To view the deployment status, compliance score, compliance score timeline, and rules for a conformance pack in a detailed view, choose the name of the conformance pack under **Conformance pack**.

Compliance status

Compliance status displays the number of your compliant and noncompliant rules and compliant and noncompliant resources. Resources are compliant or noncompliant based on an evaluation of the rule associated with it. If a resource does not follow the rule's specifications, the resource and the rule are flagged as noncompliant.

To view the list of noncompliant rules and resources, choose **Noncompliant rule(s)** or **Noncompliant resource(s)**.

Rules by noncompliant resources

Rules by noncompliant resources displays your top noncompliant rules in descending order by the number of resources. Choose a rule to view its details, parameters, and the resources in scope for that specific rule.

For a comprehensive list of noncompliant rules, choose **View all noncompliant rules**.

Resource inventory

Resource inventory displays the total number of resources that Amazon Config is recording in descending order by the number of resources, and the count of each resource type in your Amazon Web Services account. To open all resources for a resource type, choose that resource type to go to its **Resources inventory** page.

You can use the dropdown list to indicate which resource totals you want to view. By default, it is set to view **All resources**, but you can change it to Amazon resources, Third-party resources, or Custom resources.

> **Note**
>
> The **Evaluate your Amazon resource configuration using Config rules** message may appear on the **Dashboard** for the following reasons:

- You haven't set up Amazon Config Rules for your Amazon Web Services account. You can choose **Add rule** to go to the **Rules** page.
- Amazon Config is still evaluating your resources against your rules. You can refresh the page to see the latest evaluation results.
- Amazon Config evaluated your resources against your rules and did not find any resources in scope. You can specify the resources for Amazon Config to record in the **Settings** page. For more information, see Recording Amazon Resources with Amazon Config.

Amazon Config Usage and Success Metrics

You can use Amazon CloudWatch dashboards in the Amazon Config console to visualize your Amazon Config usage and success metrics.

For each dashboard, you can do the following:

- Adjust the dashboard time range to display data from the past **3 Hours**, **1 Day**, or **1 Week**.
- Choose the **Calender icon**, to enter a custom time range: either a **Relative** time for a past specified amount of time or an **Absolute** time range between two dates.
- You can change the time format to display dashboard data in **UTC** (Coordinated Universal Time) or **Local time zone** (the time zone specified as your local time zone in the operating system of your device).
- Use the **Drop arrow** next the **Refresh icon** to specify how often the data in a dashboard should refresh, or to turn off the automatic refresh. Choose **Off**, **10 Seconds**, **1 Minute**, **2 Minutes**, **5 Minutes**, or **15 Minutes** to change the refresh internal.
- Choose **More options** (the vertical ellipsis menu) to add the Amazon Config usage metrics or the Amazon Config success metrics you are currently viewing in the Amazon Config Dashboard to the CloudWatch console. This opens a new tab in the CloudWatch console that allows you to create a new custom dashboard in CloudWatch with information copied from your current Amazon Config usage metrics or Amazon Config success metrics.

If you want to perform additional analyses of these metrics with CloudWatch, choose **Metrics** in the left navigation pane of the CloudWatch console and then choose **Amazon/Config**. For more

information on what you can do from the CloudWatch console, see Using Amazon CloudWatch dashboards and Using Amazon CloudWatch metrics in the *CloudWatch User Guide*.

Amazon Config Usage Metrics

Metric	Description	Unit
`Configuration Items Recorded`	The number of configuration items recorded for each resource type or all resource types. A configuration item represents a point-in-time view of the various attributes of a supported Amazon resource. For more information about configuration items or supported resource types, see Configuration Items and Supported Resource Types.	Count

You can select the resource type that you want to view by using the dropdown list. By default, it is set to view all resource types.

Amazon Config Success Metrics

Metric	Description	Unit
`Change Notifications Delivery Failed`	The number of failed change notification deliveries to the Amazon SNS topic for your delivery channel. A change notification informs you about a change to the configuration state of your Amazon resources. You can use the ConfigStreamDeliveryInfo API to get the `lastErrorCode` or `lastErrorMessage` for the last attempted delivery for a change notification. For more information, see Managing the Delivery Channel.	Count
`Config History`	The number of failed configuration history exports to your Amazon S3 bucket. A configuration history is a collection of the configuration items for a given resource	Count

Metric	Description	Unit
`Export Failed`	over a specified time period. For more information about configuration history, see Configuration History.	
`Configuration Recorder Insufficient Permissions Failure`	The number of failed permission access attempts due to the IAM role policy for all the configuration recorders in your account and Amazon Web Services Region having insufficient permissions. The configuration recorder detects changes in to the resource types in scope. For the configuration recorder to record your Amazon resource configurations, it requires the necessary IAM permissions. For more information, see IAM Role Policy for Getting Configuration Details.	Count
`Config Snapshot Export Failed`	The number of failed configuration snapshot exports to your Amazon S3 bucket. A configuration snapshot is a collection of the configuration items for the supported resources in your account. For more information about configuration snapshots, see Configuration Snapshot.	Count

Managing and Viewing Amazon Resource Configurations with Amazon Config

Amazon Config allows you to assess, audit, and evaluate the configurations of Amazon resources.

Amazon resources are entities that you create and manage using the Amazon Web Services Management Console, the Amazon Command Line Interface (CLI), the Amazon SDKs, or Amazon partner tools. Examples of Amazon resources include Amazon EC2 instances, security groups, Amazon VPCs, and Amazon Elastic Block Store. Amazon Config refers to each resource using its unique identifier, such as the resource ID or an Amazon Resource Name (ARN).

Some common use cases include:

- **Cloud administrator**: You can track and manage resource configurations to help ensure compliance, troubleshoot issues, and maintain an understanding of your Amazon environment
- **Security analyst**: You can evaluate resource configurations against desired states to help identify vulnerabilities and assess security posture.
- **Compliance officer**: You can continuously audit and monitor resource configurations to help ensure adherence to organizational policies and industry standards.

Topics

- Supported Resource Types for Amazon Config
- Resource Coverage by Region Availability
- Recording Amazon Resources with Amazon Config
- Recording Configurations with Amazon Config for Third-Party Resources using the Amazon CLI
- Recording Software Configuration for Managed Instances with Amazon Config
- Looking Up Resources That Are Discovered by Amazon Config
- Viewing Compliance Information and Evaluation Results for your Amazon Resources with Amazon Config
- Viewing Compliance History for your Amazon Resources with Amazon Config
- Querying Compliance History for your Amazon Resources
- Tagging Your Amazon Config Resources

Supported Resource Types for Amazon Config

Important

This page is updated on a monthly cadence at the beginning of each month.

Amazon Config supports the following Amazon resources types and resource relationships.

- For more detailed information about a resource type, see its reference information (such as syntax, properties and return values) in the Amazon resource and property types reference in the Amazon CloudFormation User Guide.
- For Amazon Config recording, some Amazon Regions support a subset of these resource types. For information on which resource types are supported in which Regions, see Resource Coverage by Region Availability.
- Advanced queries for Amazon Config supports a subset of these resource types. For a list of those supported resource types, see Supported Resource Types for Advanced Queries.
- Proactive evaluation for Amazon Config supports a subset of these resource types. For a list of those supported resource types, see Supported Resource Types for Proactive Evaluation.
- Periodic rules run without the configuration recorder being enabled since periodic rules do not depend on configuration items (CIs). For more information on the difference between change–triggered rules and periodic rules, see Evaluation Mode and Trigger Types for Amazon Config Rules.

  This means that if you view the rule page, there is no listed CI or supported resource. If you select the resource ID, you will see the following error: `The provided resource ID and resource type cannot be found`. This is expected behavior.

Note

Region availability for resource types
Before specifying a resource type for Amazon Config to track, check Resource Coverage by Region Availability to see if the resource type is supported in the Amazon Region where you set up Amazon Config. If a resource type is supported by Amazon Config in at least one Region, you can enable the recording of that resource type in all Regions supported by

Amazon Config, even if the specified resource type is not supported in the Amazon Region where you set up Amazon Config.

Tagging support for resource types

If a resource type does not support tagging or does not include tag information in its describe API response, Amazon Config won't capture tag data in the configuration items (CIs) for that resource type. Amazon Config will still record these resources. However, any functionality that relies on tag data won't work. This affects tag-based filtering, grouping, or compliance evaluation that relies on tag data.

Amazon AppStream

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon AppStream	`AWS::AppStream::DirectoryConfig`	NA	NA
	`AWS::AppStream::Application`	NA	NA
	`AWS::AppStream::Stack`	NA	NA
	`AWS::AppStream::Fleet`	NA	NA

Amazon AppFlow

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon AppFlow	`AWS::AppFlow::Flow`	NA	NA

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon AppIntegrations	`AWS::AppIntegrations::EventIntegration`	NA	NA
	`AWS::AppIntegrations::Application`	NA	NA

Amazon API Gateway

Amazon Service	Resource Type Value	Relationship	Related Resource
API Gateway	`AWS::ApiGateway::Stage`	is contained in	ApiGateway Rest Api
		is associated with	WAFRegional WebACL
	`AWS::ApiGateway::RestApi`	contains	ApiGateway Stage
API Gateway V2	`AWS::ApiGatewayV2::Stage`	is contained in	ApiGatewayV2 Api
	`AWS::ApiGatewayV2::Api`	contains	ApiGatewayV2 Stage

To learn more about how Amazon Config integrates with Amazon API Gateway, see Monitoring API Gateway API Configuration with Amazon Config.

Amazon Athena

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Athena	AWS::Athena::WorkGroup	NA	NA
	AWS::Athena::DataCatalog	NA	NA
	AWS::Athena::PreparedStatement	NA	NA

Amazon Bedrock

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Bedrock	AWS::Bedrock::Guardrail	NA	NA
	AWS::Bedrock::KnowledgeBase	NA	NA

Amazon CloudFront

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon CloudFront	AWS::CloudFront::Distribution	is associated with	Amazon WAF WebACL
			ACM Certificate
			S3 Bucket

Amazon Service	Resource Type Value	Relationship	Related Resource
			IAM Server Certificate
	AWS::CloudFront::StreamingDistribution	is associated with	Amazon WAF WebACL
			ACM Certificate
			S3 Bucket
			IAM Server Certificate

Amazon CloudWatch

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon CloudWatch	AWS::CloudWatch::Alarm	NA	NA
	AWS::CloudWatch::MetricStream	NA	NA
Amazon CloudWatch Logs	AWS::Logs::Destination	NA	NA
Amazon CloudWatch RUM	AWS::RUM::AppMonitor	NA	NA
Amazon CloudWatch Evidently	AWS::Evidently::Project	NA	NA
	AWS::Evidently::Launch	NA	NA
	AWS::Evidently::Segment	NA	NA

Amazon CodeGuru

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon CodeGuru Reviewer	`AWS::CodeGuruReviewer::RepositoryAssociation`	NA	NA
Amazon CodeGuru Profiler	`AWS::CodeGuruProfiler::ProfilingGroup`	NA	NA

Amazon Cognito

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Cognito	`AWS::Cognito::UserPool`	NA	NA
	`AWS::Cognito::UserPoolClient`	NA	NA
	`AWS::Cognito::UserPoolGroup`	NA	NA
	`AWS::Cognito::IdentityPool`	NA	NA

Amazon Connect

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Connect	AWS::Connect::PhoneNumber	NA	NA
	AWS::Connect::QuickConnect	NA	NA
	AWS::Connect::Instance	NA	NA
	AWS::Connect::Rule	NA	NA
	AWS::Connect::User	NA	NA
Amazon Connect Customer Profiles	AWS::CustomerProfiles::Domain	NA	NA
	AWS::CustomerProfiles::ObjectType	NA	NA

Amazon Detective

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Detective	AWS::Detective::Graph	NA	NA

Amazon DynamoDB

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon DynamoDB	`AWS::DynamoDB::Table`	NA	NA

Amazon Elastic Compute Cloud

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Elastic Compute Cloud	`AWS::EC2::Host` *	contains	EC2 instance
	`AWS::EC2::EIP`	is attached to	EC2 instance
			Network interface
	`AWS::EC2::Instance`	contains	EC2 network interface
		is associated with	EC2 security group
		is attached to	Amazon EBS volume
			EC2 Elastic IP (EIP)
		is contained in	EC2 Dedicated host
			Route table
			Subnet
			Virtual private cloud (VPC)
	`AWS::EC2::NetworkInterface`	is associated with	EC2 security group
		is attached to	EC2 Elastic IP (EIP)

Amazon Service	Resource Type Value	Relationship	Related Resource
		is contained in	EC2 instance
			Route table
			Subnet
			Virtual private cloud (VPC)
	AWS::EC2::SecurityGroup *	is associated with	EC2 instance
			EC2 network interface
			Virtual private cloud (VPC)
	AWS::EC2::NatGateway	is contained in	Virtual private cloud (VPC)
		is contained in	Subnet
	AWS::EC2::EgressOnlyInternetGateway	is attached to	Virtual private cloud (VPC)
	AWS::EC2::EC2Fleet	NA	NA
	AWS::EC2::SpotFleet	NA	NA
	AWS::EC2::PrefixList	NA	NA
	AWS::EC2::FlowLog	NA	NA

Amazon Service	Resource Type Value	Relationship	Related Resource
	AWS::EC2::TransitGateway	NA	NA
	AWS::EC2::TransitGatewayAttachment	NA	NA
	AWS::EC2::TransitGatewayRouteTable	NA	NA
	AWS::EC2::VPCEndpoint	is contained in	Virtual private cloud (VPC)
		is attached to	Network interface
		is contained in	Subnet
		is contained in	Route table
	AWS::EC2::VPCEndpointService	is associated with	ElasticLoadBalancingV2 LoadBalancer
	AWS::EC2::VPCPeeringConnection	is associated with	Virtual private cloud (VPC)
	AWS::EC2::RegisteredHAInstance	is associated with	EC2 instance

Amazon Service	Resource Type Value	Relationship	Related Resource
	AWS::EC2::SubnetRouteTableAssociation	NA	NA
	AWS::EC2::LaunchTemplate	NA	NA
	AWS::EC2::NetworkInsightsAccessScopeAnalysis	NA	NA
	AWS::EC2::TrafficMirrorTarget	NA	NA
	AWS::EC2::TrafficMirrorSession	NA	NA
	AWS::EC2::DHCPOptions	NA	NA
	AWS::EC2::IPAM	NA	NA
	AWS::EC2::IPAMResourceDiscovery	NA	NA

Amazon Service	Resource Type Value	Relationship	Related Resource
	AWS::EC2::IPAMResourceDiscoveryAssociation	NA	NA
	AWS::EC2::NetworkInsightsPath	NA	NA
	AWS::EC2::TrafficMirrorFilter	NA	NA
	AWS::EC2::CapacityReservation	NA	NA
	AWS::EC2::ClientVpnEndpoint	NA	NA
	AWS::EC2::CustomerGateway	is attached to	VPN connection
	AWS::EC2::InternetGateway	is attached to	Virtual private cloud (VPC)
	AWS::EC2::NetworkAcl	NA	NA
	AWS::EC2::RouteTable	contains	EC2 instance
			EC2 network interface

Amazon Service	Resource Type Value	Relationship	Related Resource
			Subnet
			VPN gateway
		is contained in	Virtual private cloud (VPC)
	AWS::EC2::Subnet	contains	EC2 instance
			EC2 network interface
		is attached to	Network ACL
		is contained in	Route table
			Virtual private cloud (VPC)
	AWS::EC2::VPC	contains	EC2 instance
			EC2 network interface
			Network ACL
			Route table
			Subnet
		is associated with	Security group
		is attached to	Internet gateway
			VPN gateway
	AWS::EC2::VPNConnection	is attached to	Customer gateway
			VPN gateway

Amazon Service	Resource Type Value	Relationship	Related Resource
	AWS::EC2::VPNConnectionRoute	NA	NA
	AWS::EC2::VPNGateway	is attached to	Virtual private cloud (VPC)
			VPN connection
		is contained in	Route table
	AWS::EC2::IPAMScope	NA	NA
	AWS::EC2::CarrierGateway	NA	NA
	AWS::EC2::TransitGatewayConnect	NA	NA
	AWS::EC2::IPAMPool	NA	NA
	AWS::EC2::TransitGatewayMulticastDomain	NA	NA
	AWS::EC2::NetworkInsightsAccessScope	NA	NA

Amazon Service	Resource Type Value	Relationship	Related Resource
	AWS::EC2::NetworkInsightsAnalysis	NA	NA
	AWS::EC2::VPCBlockPublicAccessOptions	NA	NA
	AWS::EC2::VPCBlockPublicAccessExclusion	NA	NA
	AWS::EC2::EIPAssociation	NA	NA
	AWS::EC2::InstanceConnectEndpoint	NA	NA
	AWS::EC2::SnapshotBlockPublicAccess	NA	NA
	AWS::EC2::VPCEndpointConnectionNotification	NA	NA

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Elastic Block Store	`AWS::EC2::Volume`	is attached to	EC2 instance
EC2 Image Builder	`AWS::ImageBuilder::ImagePipeline`	NA	NA
	`AWS::ImageBuilder::DistributionConfiguration`	NA	NA
	`AWS::ImageBuilder::ContainerRecipe`	NA	NA
	`AWS::ImageBuilder::InfrastructureConfiguration`	NA	NA
	`AWS::ImageBuilder::ImageRecipe`	NA	NA

*Amazon Config records the configuration details of Dedicated hosts and the instances that you launch on them. As a result, you can use Amazon Config as a data source when you report compliance with your server-bound software licenses. For example, you can view the configuration history of an instance and determine which Amazon Machine Image (AMI) it is based on. Then, you can look up the configuration history of the host, which includes details such as the numbers of sockets and cores, to check that the host complies with the license requirements of the AMI. For

more information, see Tracking Configuration Changes with Amazon Config in the *Amazon EC2 User Guide*.

*The EC2 SecurityGroup Properties definition contains IP CIDR blocks, which are converted to IP ranges internally, and may return unexpected results when trying to find a specific IP range. For workarounds to search for specific IP ranges, see Limitations for Advanced Queries.

Amazon Elastic Container Registry

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Elastic Container Registry	`AWS::ECR::Repository`	NA	NA
	`AWS::ECR::RegistryPolicy`	NA	NA
	`AWS::ECR::PullThroughCacheRule`	NA	NA
Amazon Elastic Container Registry Public	`AWS::ECR::PublicRepository`	NA	NA

Amazon Elastic Container Service

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Elastic Container Service	`AWS::ECS::Cluster`	NA	NA
	`AWS::ECS::TaskDefinition`	NA	NA

Amazon Service	Resource Type Value	Relationship	Related Resource
	AWS::ECS::Service *	NA	NA
	AWS::ECS::TaskSet	NA	NA
	AWS::ECS::CapacityProvider	NA	NA

*This service currently only support the new Amazon Resource Name (ARN) format. For more information, see Amazon Resource Names (ARNs) and IDs in the ECS developer guide.

Old (not supported): `arn:aws:ecs:region:aws_account_id:service/service-name`

New (supported): `arn:aws:ecs:region:aws_account_id:service/cluster-name/service-name`

Amazon Elastic File System

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Elastic File System	AWS::EFS::FileSystem	NA	NA
	AWS::EFS::AccessPoint	NA	NA

Amazon Elastic Kubernetes Service

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Elastic Kubernetes Service	AWS::EKS::Cluster	NA	NA

Amazon Service	Resource Type Value	Relationship	Related Resource
	AWS::EKS::FargateProfile	NA	NA
	AWS::EKS::IdentityProviderConfig	NA	NA
	AWS::EKS::Addon	NA	NA

Amazon EMR

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon EMR	AWS::EMR::SecurityConfiguration	NA	NA

Amazon EventBridge

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon EventBridge	AWS::Events::EventBus	NA	NA
	AWS::Events::ApiDestination	NA	NA
	AWS::Events::Archive	NA	NA
	AWS::Events::Endpoint	NA	NA

Amazon Service	Resource Type Value	Relationship	Related Resource
	AWS::Events::Connection	NA	NA
	AWS::Events::Rule	NA	NA
Amazon EventBridge schemas	AWS::EventSchemas::RegistryPolicy	NA	NA
	AWS::EventSchemas::Discoverer	NA	NA
	AWS::EventSchemas::Schema	NA	NA
	AWS::EventSchemas::Registry	NA	NA

Amazon Forecast

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Forecast	AWS::Forecast::Dataset	NA	NA
	AWS::Forecast::DatasetGroup	NA	NA

Amazon Fraud Detector

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Fraud Detector	AWS::FraudDetector::Label	NA	NA
	AWS::FraudDetector::EntityType	NA	NA
	AWS::FraudDetector::Variable	NA	NA
	AWS::FraudDetector::Outcome	NA	NA

Amazon GuardDuty

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon GuardDuty	AWS::GuardDuty::Detector	NA	NA
	AWS::GuardDuty::ThreatIntelSet	NA	NA
	AWS::GuardDuty::IPSet	NA	NA
	AWS::GuardDuty::Filter	NA	NA

Amazon Inspector

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Inspector	AWS::InspectorV2::Filter	NA	NA
	AWS::InspectorV2::Activation	NA	NA

Amazon Interactive Video Service

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Interactive Video Service	AWS::IVS::Channel	NA	NA
	AWS::IVS::RecordingConfiguration	NA	NA
	AWS::IVS::PlaybackKeyPair	NA	NA

Amazon Keyspaces (for Apache Cassandra)

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Keyspaces (for Apache Cassandra)	AWS::Cassandra::Keyspace	NA	NA

Amazon OpenSearch Service

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon OpenSearch Service (legacy Elasticsearch)	`AWS::Elasticsearch::Domain`	is associated with	KMS Key
			EC2 security group
			EC2 subnet
			Virtual private cloud (VPC)
Amazon OpenSearch Service	`AWS::OpenSearch::Domain`	NA	NA
Amazon OpenSearch Serverless	`AWS::OpenSearchServerless::VpcEndpoint`	NA	NA
	`AWS::OpenSearchServerless::Collection`	NA	NA

Amazon OpenSearch Service rename

On September 8, 2021, Amazon Elasticsearch Service was renamed to Amazon OpenSearch Service. OpenSearch Service supports OpenSearch as well as legacy Elasticsearch OSS. For more information, see Amazon OpenSearch Service - Summary of changes.
You might continue to see your data for `AWS::OpenSearch::Domain` under the existing `AWS::Elasticsearch::Domain` resource type for several weeks, even if you upgrade one or more domains to OpenSearch.

Amazon Personalize

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Personalize	AWS::Personalize::Dataset	NA	NA
	AWS::Personalize::Schema	NA	NA
	AWS::Personalize::Solution	NA	NA
	AWS::Personalize::DatasetGroup	NA	NA

Amazon Pinpoint

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Pinpoint	AWS::Pinpoint::ApplicationSettings	NA	NA
	AWS::Pinpoint::Segment	NA	NA
	AWS::Pinpoint::App	NA	NA
	AWS::Pinpoint::Campaign	NA	NA

Amazon Service	Resource Type Value	Relationship	Related Resource
	AWS::Pinpoint::InAppTemplate	NA	NA
	AWS::Pinpoint::EmailChannel	NA	NA
	AWS::Pinpoint::EmailTemplate	NA	NA
	AWS::Pinpoint::EventStream	NA	NA

Amazon Quantum Ledger Database (Amazon QLDB)

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon QLDB	AWS::QLDB::Ledger	NA	NA

Amazon Kendra

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Kendra	AWS::Kendra::Index	NA	NA

Amazon Kinesis

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Kinesis	AWS::Kinesis::Stream	NA	NA
	AWS::Kinesis::StreamConsumer	NA	NA
Amazon Kinesis Analytics V2	AWS::KinesisAnalyticsV2::Application	NA	NA
Amazon Data Firehose	AWS::KinesisFirehose::DeliveryStream	NA	NA
Kinesis video stream	AWS::KinesisVideo::SignalingChannel	NA	NA
	AWS::KinesisVideo::Stream	NA	NA

Amazon Lex

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Lex	AWS::Lex::BotAlias	NA	NA

Amazon Service	Resource Type Value	Relationship	Related Resource
	AWS::Lex::Bot	NA	NA

Amazon Lightsail

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Lightsail	AWS::Lightsail::Disk	NA	NA
	AWS::Lightsail::Certificate	NA	NA
	AWS::Lightsail::Bucket	NA	NA
	AWS::Lightsail::StaticIp	NA	NA

Amazon Lookout for Metrics

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Lookout for Metrics	AWS::LookoutMetrics::Alert	NA	NA

Amazon Lookout for Vision

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Lookout for Vision	`AWS::LookoutVision::Project`	NA	NA

Amazon Macie

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Macie	`AWS::Macie::Session`	NA	NA

Amazon Managed Grafana

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Managed Grafana	`AWS::Grafana::Workspace`	NA	NA

Amazon Managed Service for Prometheus

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Managed Service for Prometheus	`AWS::APS::RuleGroupsNamespace`	NA	NA

Amazon MemoryDB

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon MemoryDB	`AWS::MemoryDB::SubnetGroup`	NA	NA

Amazon MQ

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon MQ	`AWS::AmazonMQ::Broker`	NA	NA

Amazon Managed Streaming for Apache Kafka

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Managed Streaming for Apache Kafka	`AWS::MSK::Cluster`	NA	NA
	`AWS::MSK::Configuration`	NA	NA
	`AWS::MSK::BatchScramSecret`	NA	NA
	`AWS::MSK::ClusterPolicy`	NA	NA
	`AWS::MSK::VpcConnection`	NA	NA

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Managed Streaming for Apache Kafka Connect	`AWS::KafkaConnect::Connector`	NA	NA

Amazon QuickSight

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon QuickSight	`AWS::QuickSight::DataSource`	NA	NA
	`AWS::QuickSight::Template`	NA	NA
	`AWS::QuickSight::Theme`	NA	NA

Amazon Redshift

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Redshift	`AWS::Redshift::Cluster`	is associated with	Cluster parameter group
			Cluster security group
			Cluster subnet group
			Security group
			Virtual private cloud (VPC)

Amazon Service	Resource Type Value	Relationship	Related Resource
	AWS::Redshift::ClusterParameterGroup	NA	NA
	AWS::Redshift::ClusterSecurityGroup	NA	NA
	AWS::Redshift::ScheduledAction	NA	NA
	AWS::Redshift::ClusterSnapshot	is associated with	Cluster
			Virtual private cloud (VPC)
	AWS::Redshift::ClusterSubnetGroup	is associated with	Subnet
			Virtual private cloud (VPC)
	AWS::Redshift::EventSubscription	NA	NA
	AWS::Redshift::EndpointAccess	NA	NA
	AWS::Redshift::EndpointAuthorization	NA	NA

Amazon Relational Database Service

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Relational Database Service	AWS::RDS::DBInstance	is associated with	EC2 security group
			RDS DB security group
			RDS DB subnet group
	AWS::RDS::DBSecurityGroup	is associated with	EC2 security group
			Virtual private cloud (VPC)
	AWS::RDS::DBSnapshot	is associated with	Virtual private cloud (VPC)
	AWS::RDS::DBSubnetGroup	is associated with	EC2 security group
			Virtual private cloud (VPC)
	AWS::RDS::EventSubscription	NA	NA
	AWS::RDS::DBCluster	contains	RDS DB instance
		is associated with	RDS DB subnet group
			EC2 security group
	AWS::RDS::DBClusterSnapshot	is associated with	RDS DB cluster
			Virtual private cloud (VPC)

Amazon Service	Resource Type Value	Relationship	Related Resource
	AWS::RDS::GlobalCluster	NA	NA
	AWS::RDS::OptionGroup	NA	NA

Amazon Route 53

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Route 53	AWS::Route53::HostedZone	NA	NA
	AWS::Route53::HealthCheck	NA	NA
Amazon Route 53 Profiles	AWS::Route53Profiles::Profile	NA	NA
Amazon Route 53 Resolver	AWS::Route53Resolver::ResolverEndpoint	NA	NA
	AWS::Route53Resolver::ResolverRule	NA	NA
	AWS::Route53Resolver::ResolverRuleAssociation	NA	NA
	AWS::Route53Resolver::FirewallDomainList	NA	NA
	AWS::Route53Resolver::FirewallRuleGroupAssociation	NA	NA
	AWS::Route53Resolver::ResolverQueryLoggingConfig	NA	NA

Amazon Service	Resource Type Value	Relationship	Related Resource
	AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	NA	NA
	AWS::Route53Resolver::FirewallRuleGroup	NA	NA
Amazon Application Recovery Controller (ARC)	AWS::Route53RecoveryReadiness::Cell	NA	NA
	AWS::Route53RecoveryReadiness::ReadinessCheck	NA	NA
	AWS::Route53RecoveryReadiness::RecoveryGroup	NA	NA
	AWS::Route53RecoveryControl::Cluster	NA	NA
	AWS::Route53RecoveryControl::ControlPanel	NA	NA
	AWS::Route53RecoveryControl::RoutingControl	NA	NA
	AWS::Route53RecoveryControl::SafetyRule	NA	NA
	AWS::Route53RecoveryReadiness::ResourceSet	NA	NA

Amazon SageMaker AI

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon SageMaker AI	AWS::SageMaker::CodeRepository	NA	NA
	AWS::SageMaker::Domain	NA	NA

Amazon Service	Resource Type Value	Relationship	Related Resource
	AWS::SageMaker::AppImageConfig	NA	NA
	AWS::SageMaker::Image	NA	NA
	AWS::SageMaker::Model	NA	NA
	AWS::SageMaker::NotebookInstance	NA	NA
	AWS::SageMaker::NotebookInstanceLifecycleConfig	NA	NA
	AWS::SageMaker::EndpointConfig	NA	NA
	AWS::SageMaker::Workteam	NA	NA
	AWS::SageMaker::FeatureGroup	NA	NA
	AWS::SageMaker::InferenceExperiment	NA	NA

Amazon Simple Email Service

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Simple Email Service	AWS::SES::ConfigurationSet	NA	NA
	AWS::SES::ContactList	NA	NA
	AWS::SES::Template	NA	NA
	AWS::SES::ReceiptFilter	NA	NA
	AWS::SES::ReceiptRuleSet	NA	NA

Amazon Simple Notification Service

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Simple Notification Service	AWS::SNS::Topic	NA	NA

Amazon Simple Queue Service

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Simple Queue Service	AWS::SQS::Queue	NA	NA

Amazon Simple Storage Service

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Simple Storage Service	`AWS::S3::Bucket` *	NA	NA
	`AWS::S3::AccountPublicAccessBlock`	NA	NA
	`AWS::S3::MultiRegionAccessPoint`	NA	NA
	`AWS::S3::StorageLens`	NA	NA
	`AWS::S3::AccessPoint`	NA	NA
	`AWS::S3::StorageLensGroup`	NA	NA
Amazon S3 Express One Zone	`AWS::S3Express::DirectoryBucket`	NA	NA
	`AWS::S3Express::BucketPolicy`	NA	NA

*If you configured Amazon Config to record your S3 buckets, and are not receiving configuration change notifications, check that your S3 bucket policies have the required permissions. For more information, see Managing Permissions for S3 Bucket Recording.

Amazon S3 Bucket Attributes

Amazon Config also records the following attributes for the Amazon S3 bucket resource type.

Attributes	Description
AccelerateConfiguration	Transfer acceleration for data over long distances between your client and a bucket.
BucketAcl	Access control list used to manage access to buckets and objects.
BucketPolicy	Policy that defines the permissions to the bucket.
CrossOriginConfiguration	Allow cross-origin requests to the bucket.
LifecycleConfiguration	Rules that define the lifecycle for objects in your bucket.
LoggingConfiguration	Logging used to track requests for access to the bucket.
NotificationConfiguration	Event notifications used to send alerts or trigger workflows for specified bucket events.
ReplicationConfiguration	Automatic, asynchronous copying of objects across buckets in different Amazon Regions.
RequestPaymentConfiguration	Requester pays is enabled.
TaggingConfiguration	Tags added to the bucket to categorize. You can also use tagging to track billing.
WebsiteConfiguration	Static website hosting is enabled for the bucket.
VersioningConfiguration	Versioning is enabled for objects in the bucket.

For more information about the attributes, see Bucket Configuration Options in the *Amazon Simple Storage Service User Guide*.

Amazon WorkSpaces

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon WorkSpaces	`AWS::WorkSpaces::ConnectionAlias`	NA	NA
	`AWS::WorkSpaces::Workspace`	NA	NA

Amazon Amplify

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Amplify	`AWS::Amplify::App`	NA	NA
	`AWS::Amplify::Branch`	NA	NA

Amazon AppConfig

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon AppConfig	`AWS::AppConfig::Application`	NA	NA
	`AWS::AppConfig::Environment`	NA	NA
	`AWS::AppConfig::Co`	NA	NA

Amazon Service	Resource Type Value	Relationship	Related Resource
	nfigurati onProfile		
	AWS::AppC onfig::De ploymentS trategy	NA	NA
	AWS::AppC onfig::Ho stedConfi gurationV ersion	NA	NA
	AWS::AppC onfig::Ex tensionAs sociation	NA	NA

Amazon App Runner

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon App Runner	AWS::AppR unner::Vp cConnector	NA	NA
	AWS::AppR unner::Service	NA	NA

Amazon App Mesh

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon App Mesh	AWS::AppMesh::VirtualNode	NA	NA
	AWS::AppMesh::VirtualService	NA	NA
	AWS::AppMesh::VirtualGateway	NA	NA
	AWS::AppMesh::VirtualRouter	NA	NA
	AWS::AppMesh::Route	NA	NA
	AWS::AppMesh::GatewayRoute	NA	NA
	AWS::AppMesh::Mesh	NA	NA

Amazon AppSync

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon AppSync	AWS::AppSync::GraphQLApi	NA	NA

Amazon Audit Manager

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Audit Manager	`AWS::AuditManager::Assessment`	NA	NA

Amazon Auto Scaling

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`	contains	Amazon EC2 instance
		is associated with	Classic Load Balancer
			Auto Scaling launch configuration
			Subnet
	`AWS::AutoScaling::LaunchConfiguration`	is associated with	Amazon EC2 security group
	`AWS::AutoScaling::ScalingPolicy`	is associated with	Auto Scaling group
			Alarm
	`AWS::AutoScaling::ScheduledAction`	is associated with	Auto Scaling group

Amazon Service	Resource Type Value	Relationship	Related Resource
	AWS::AutoScaling::WarmPool	NA	NA

Amazon Backup

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Backup	AWS::Backup::BackupPlan	NA	NA*
	AWS::Backup::BackupSelection	NA	NA
	AWS::Backup::BackupVault	NA	NA*
	AWS::Backup::RecoveryPoint	NA	NA
	AWS::Backup::ReportPlan	NA	NA

Due to how Amazon Backup works, some of these resource types relate to the other Amazon Backup resource types in this table.

`AWS::Backup::BackupPlan` is related to `AWS::Backup::BackupSelection` where a Backup Plan has many selections, and `AWS::Backup::BackupVault` is related to `AWS::Backup::RecoveryPoint` where an Amazon Backup Vault has multiple recovery points.

For more information, see Managing backups using backup plans and Working with backup vaults.

Amazon Batch

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Batch	AWS::Batch::JobQueue	NA	NA
	AWS::Batch::ComputeEnvironment	NA	NA
	AWS::Batch::SchedulingPolicy	NA	NA

Amazon Budgets

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Budgets	AWS::Budgets::BudgetsAction	NA	NA

Amazon Certificate Manager

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Certificate Manager	AWS::ACM::Certificate	NA	NA

Amazon CloudFormation

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon CloudFormation	`AWS::CloudFormation::Stack` *	contains	Supported Amazon resource types

*Amazon Config records configuration changes to Amazon CloudFormation stacks and supported resource types in the stacks. Amazon Config does not record configuration changes for resource types in the stack that are not yet supported. Unsupported resource types appear in the supplementary configuration section of the configuration item for the stack.

Amazon CloudTrail

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon CloudTrail	`AWS::CloudTrail::Trail`	NA	NA

Amazon Cloud9

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Cloud9	`AWS::Cloud9::EnvironmentEC2`	NA	NA

Amazon Cloud9 access no longer available to new users

After careful consideration, we have made the decision to close new customer access to Amazon Cloud9, effective July 25, 2024. Amazon Cloud9 existing customers can continue to use the service as normal. Amazon continues to invest in security, availability, and performance improvements for Amazon Cloud9, but we do not plan to introduce new

features. For more information, see How to migrate from Amazon Cloud9 to Amazon IDE Toolkits or Amazon CloudShell.

Amazon Cloud Map

Amazon Service	Resource Type Value	Relationship	Related Resource
Service Discovery	`AWS::ServiceDiscovery::Service`	NA	NA
	`AWS::ServiceDiscovery::PublicDnsNamespace`	NA	NA
	`AWS::ServiceDiscovery::HttpNamespace`	NA	NA
`AWS::ServiceDiscovery::Instance`	NA	NA	

Amazon CodeArtifact

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon CodeArtifact	`AWS::CodeArtifact::Repository`	NA	NA

Amazon CodeBuild

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon CodeBuild	`AWS::CodeBuild::Project` *	is associated with	S3 bucket
			IAM role
	`AWS::CodeBuild::ReportGroup`	NA	NA

*To learn more about how Amazon Config integrates with Amazon CodeBuild, see Use Amazon Config with Amazon CodeBuild Sample.

Amazon CodeDeploy

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon CodeDeploy	`AWS::CodeDeploy::Application`	contains	DeploymentGroup
	`AWS::CodeDeploy::DeploymentConfig`	NA	NA
	`AWS::CodeDeploy::DeploymentGroup`	is contained in	Application

Amazon CodePipeline

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon CodePipeline	`AWS::CodePipeline::Pipeline` *	is attached to	S3 bucket
		is associated with	IAM role
			Code project
			Lambda function
			Cloudformation stack
			ElasticBeanstalk application

*Amazon Config records configuration changes to CodePipeline pipelines and supported resource types in the pipelines. Amazon Config does not record configuration changes for resource types in the pipelines that are not yet supported. Unsupported resource types such as `CodeCommit repository`, `CodeDeploy application`, `ECS cluster`, and `ECS service` appear in the supplementary configuration section of the configuration item for the stack.

Amazon Config

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Config	`AWS::Config::ResourceCompliance` *	is associated with	All resources*
	`AWS::Config::ConformancePackCompliance`	NA	NA
	`AWS::Config::Confi`	NA	NA

Amazon Service	Resource Type Value	Relationship	Related Resource
	gurationR ecorder *		

*The relationship between AWS::Config::ResourceCompliance and a related resource depends on how AWS::Config::ResourceCompliance reports compliance for that specific resource type.

*AWS::Config::ConfigurationRecorder is a system resource type of Amazon Config and recording of this resource type is enabled by default.

> **Note**
>
> Recording for the AWS::Config::ConformancePackCompliance and AWS::Config::ConfigurationRecorder resource types come with no additional charge.

Amazon Database Migration Service

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Database Migration Service	AWS::DMS: :EventSub scription	NA	NA
	AWS::DMS: :Replicat ionSubnetGroup	NA	NA
	AWS::DMS: :Replicat ionInstance	NA	NA

Amazon Service	Resource Type Value	Relationship	Related Resource
	AWS::DMS::ReplicationTask	NA	NA
	AWS::DMS::Certificate	NA	NA
	AWS::DMS::Endpoint	NA	NA

Amazon DataSync

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon DataSync	AWS::DataSync::LocationSMB	NA	NA
	AWS::DataSync::LocationFSxLustre	NA	NA
	AWS::DataSync::LocationFSxWindows	NA	NA
	AWS::DataSync::LocationS3	NA	NA
	AWS::DataSync::LocationEFS	NA	NA

Amazon Service	Resource Type Value	Relationship	Related Resource
	AWS::DataSync::LocationNFS	NA	NA
	AWS::DataSync::LocationHDFS	NA	NA
	AWS::DataSync::LocationObjectStorage	NA	NA
	AWS::DataSync::Task	NA	NA

Amazon Device Farm

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Device Farm	AWS::DeviceFarm::TestGridProject	NA	NA
	AWS::DeviceFarm::InstanceProfile	NA	NA
	AWS::DeviceFarm::Project	NA	NA

Amazon Elastic Beanstalk

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Elastic Beanstalk	`AWS::ElasticBeanstalk::Application`	contains	Elastic Beanstalk Application Version
			Elastic Beanstalk Environment
		is associated with	IAM role
	`AWS::ElasticBeanstalk::ApplicationVersion`	is contained in	Elastic Beanstalk Application
		is associated with	Elastic Beanstalk Environment
			S3 bucket
	`AWS::ElasticBeanstalk::Environment`	is contained in	Elastic Beanstalk Application
		is associated with	Elastic Beanstalk Application Version
			IAM role
		contains	CloudFormation Stack

Amazon Fault Injection Service

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Fault Injection Service	`AWS::FIS::ExperimentTemplate`	NA	NA

Amazon Global Accelerator

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Global Accelerator	`AWS::GlobalAccelerator::Listener`	NA	NA
	`AWS::GlobalAccelerator::EndpointGroup`	NA	NA
	`AWS::GlobalAccelerator::Accelerator`	NA	NA

Amazon Glue

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Glue	`AWS::Glue::Job`	NA	NA
	`AWS::Glue::Classifier`	NA	NA
	`AWS::Glue::MLTransform`	NA	NA

Amazon Ground Station

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Ground Station	`AWS::GroundStation::Config`	NA	NA
	`AWS::GroundStation::MissionProfile`	NA	NA
	`AWS::GroundStation::DataflowEndpointGroup`	NA	NA

Amazon HealthLake

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon HealthLake	`AWS::HealthLake::FHIRDatastore`	NA	NA

Amazon Identity and Access Management (IAM)

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Identity and Access Management	`AWS::IAM::User`	is attached to	IAM group
			IAM customer managed policy

Amazon Service	Resource Type Value	Relationship	Related Resource
	AWS::IAM::Group	contains	IAM user
		is attached to	IAM customer managed policy
	AWS::IAM::Role	is attached to	IAM customer managed policy
	AWS::IAM::Policy	is attached to	IAM user
			IAM group
			IAM role
	AWS::IAM::SAMLProvider	NA	NA
	AWS::IAM::ServerCertificate	NA	NA
	AWS::IAM::InstanceProfile	NA	NA
	AWS::IAM::OIDCProvider	NA	NA
Amazon Identity and Access Management Access Analyzer	AWS::AccessAnalyzer::Analyzer	NA	NA

Amazon Config includes inline policies with the configuration details that it records. For more information on inline policies, see Managed policies and inline policies in the IAM User Guide.

Amazon IoT

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon IoT	AWS::IoT::Authorizer	NA	NA
	AWS::IoT::SecurityProfile	NA	NA
	AWS::IoT::RoleAlias	NA	NA
	AWS::IoT::Dimension	NA	NA
	AWS::IoT::Policy	NA	NA
	AWS::IoT::MitigationAction	NA	NA
	AWS::IoT::ScheduledAudit	NA	NA
	AWS::IoT::AccountAuditConfiguration	NA	NA
	AWS::IoTSiteWise::Gateway	NA	NA

Amazon Service	Resource Type Value	Relationship	Related Resource
	AWS::IoT::CustomMetric	NA	NA
	AWS::IoT::JobTemplate	NA	NA
	AWS::IoT::ProvisioningTemplate	NA	NA
	AWS::IoT::CACertificate	NA	NA
Amazon IoT Wireless	AWS::IoTWireless::ServiceProfile	NA	NA
	AWS::IoTWireless::MulticastGroup	NA	NA
	AWS::IoTWireless::FuotaTask	NA	NA
Amazon IoT Core	AWS::IoT::FleetMetric	NA	NA
Amazon IoT Analytics	AWS::IoTAnalytics::Datastore	NA	NA
	AWS::IoTAnalytics::Dataset	NA	NA

Amazon Service	Resource Type Value	Relationship	Related Resource
	AWS::IoTAnalytics::Pipeline	NA	NA
	AWS::IoTAnalytics::Channel	NA	NA
Amazon IoT Events	AWS::IoTEvents::Input	NA	NA
	AWS::IoTEvents::DetectorModel	NA	NA
	AWS::IoTEvents::AlarmModel	NA	NA
Amazon IoT TwinMaker	AWS::IoTTwinMaker::Workspace	NA	NA
	AWS::IoTTwinMaker::Entity	NA	NA
	AWS::IoTTwinMaker::Scene	NA	NA
	AWS::IoTTwinMaker::SyncJob	NA	NA

Amazon Service	Resource Type Value	Relationship	Related Resource
	AWS::IoTTwinMaker::ComponentType	NA	NA
Amazon IoT SiteWise	AWS::IoTSiteWise::Dashboard	NA	NA
	AWS::IoTSiteWise::Project	NA	NA
	AWS::IoTSiteWise::Portal	NA	NA
	AWS::IoTSiteWise::AssetModel	NA	NA
Amazon IoT Greengrass Version 2	AWS::GreengrassV2::ComponentVersion	NA	NA

Amazon Key Management Service

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Key Management Service	AWS::KMS::Key	NA	NA
	AWS::KMS::Alias	NA	NA

Amazon Lambda

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Lambda	`AWS::Lambda::Function`	is associated with	IAM role
			EC2 security group
		is contained in	EC2 subnet
	`AWS::Lambda::CodeSigningConfig`	NA	NA

Amazon Mainframe Modernization

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Mainframe Modernization	`AWS::M2::Environment`	NA	NA

Amazon Network Firewall

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Network Firewall	`AWS::NetworkFirewall::Firewall`	is attached to	EC2 Subnet
		is associated with	NetworkFirewall FirewallPolicy
	`AWS::NetworkFirewall::FirewallPolicy`	is associated with	NetworkFirewall RuleGroup

Amazon Service	Resource Type Value	Relationship	Related Resource
	AWS::NetworkFirewall::RuleGroup	NA	NA
	AWS::NetworkFirewall::TLSInspectionConfiguration	NA	NA
	AWS::NetworkFirewall::VpcEndpointAssociation	NA	NA

Amazon Network Manager

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Network Manager	AWS::NetworkManager::TransitGatewayRegistration	NA	NA
	AWS::NetworkManager::Site	NA	NA
	AWS::NetworkManager::Device	NA	NA

Amazon Service	Resource Type Value	Relationship	Related Resource
	AWS::NetworkManager::Link	NA	NA
	AWS::NetworkManager::GlobalNetwork	NA	NA
	AWS::NetworkManager::CustomerGatewayAssociation	NA	NA
	AWS::NetworkManager::LinkAssociation	NA	NA
	AWS::NetworkManager::ConnectPeer	NA	NA

Amazon Panorama

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Panorama	AWS::Panorama::Package	NA	NA

Amazon Private Certificate Authority

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Private Certificate Authority	`AWS::ACMPCA::CertificateAuthority`	NA	NA
	`AWS::ACMPCA::CertificateAuthorityActivation`	NA	NA

Amazon Resilience Hub

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Resilience Hub	`AWS::ResilienceHub::ResiliencyPolicy`	NA	NA
	`AWS::ResilienceHub::App`	NA	NA

Amazon Resource Explorer

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Resource Explorer	`AWS::ResourceExplorer2::Index`	NA	NA

Amazon RoboMaker

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon RoboMaker	AWS::RoboMaker::RobotApplicationVersion	NA	NA
	AWS::RoboMaker::RobotApplication	NA	NA
	AWS::RoboMaker::SimulationApplication	NA	NA

Amazon Signer

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Signer	AWS::Signer::SigningProfile	NA	NA

Amazon Secrets Manager

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Secrets Manager	AWS::SecretsManager::Secret	is associated with	Lambda function
		is associated with	KMS Key

Amazon Security Hub

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Security Hub	`AWS::SecurityHub::Standard`	NA	NA

Amazon Service Catalog

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Service Catalog	`AWS::ServiceCatalog::CloudFormationProduct`	is contained in	Portfolio
		is associated with	CloudFormationProvisionedProduct
	`AWS::ServiceCatalog::CloudFormationProvisionedProduct`	is associated with	Portfolio
			CloudFormationProduct
			CloudFormationStack
	`AWS::ServiceCatalog::Portfolio`	contains	CloudFormationProduct

Amazon Shield

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Shield	`AWS::Shield::Protection`	is associated with	Amazon CloudFront distribution

Amazon Service	Resource Type Value	Relationship	Related Resource
	AWS::ShieldRegional::Protection	is associated with	EC2 EIP
		is associated with	ElasticLoadBalancing Balancer
		is associated with	ElasticLoadBalancingV2 LoadBalancer

Amazon Step Functions

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Step Functions	AWS::StepFunctions::Activity	NA	NA
	AWS::StepFunctions::StateMachine	NA	NA

Amazon Systems Manager

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Systems Manager	AWS::SSM::ManagedInstanceInventory *	is associated with	EC2 instance
	AWS::SSM::PatchCompliance	is associated with	Managed Instance Inventory

Amazon Service	Resource Type Value	Relationship	Related Resource
	AWS::SSM::AssociationCompliance	is associated with	Managed Instance Inventory
	AWS::SSM::FileData	is associated with	Managed Instance Inventory
	AWS::SSM::Document	NA	NA

*To learn more about managed instance inventory, see Recording Software Configuration for Managed Instances.

Amazon Transfer Family

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon Transfer Family	AWS::Transfer::Agreement	NA	NA
	AWS::Transfer::Connector	NA	NA
	AWS::Transfer::Workflow	NA	NA
	AWS::Transfer::Certificate	NA	NA
	AWS::Transfer::Profile	NA	NA

Amazon WAF

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon WAF	AWS::WAF::RateBasedRule	NA	NA
	AWS::WAF::Rule	NA	NA
	AWS::WAF::WebACL	is associated with	WAF Rule
			WAF rate based rule
			WAF Rulegroup
	AWS::WAF::RuleGroup	is associated with	WAF Rule
	AWS::WAFRegional::RateBasedRule	NA	NA
	AWS::WAFRegional::Rule	NA	NA
	AWS::WAFRegional::WebACL	is associated with	ElasticLoadBalancingV2 LoadBalancer
			WAFRegional Rule
			WAFRegional rate based rule
			WAFRegional Rulegroup
	AWS::WAFRegional::RuleGroup	is associated with	WAFRegional Rule

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon WAF V2	`AWS::WAFv2::WebACL`	is associated with	ElasticLoadBalancingV2 LoadBalancer
			ApiGateway Stage
			WAFv2 IPSet
			WAFv2 RegexPatternSet
			WAFv2 RuleGroup
			WAFv2 ManagedRuleSet
	`AWS::WAFv2::RuleGroup`	is associated with	WAFv2 IPSet
			WAFv2 RegexPatternSet
	`AWS::WAFv2::ManagedRuleSet`	is associated with	WAFv2 RuleGroup
	`AWS::WAFv2::IPSet`	NA	NA
	`AWS::WAFv2::RegexPatternSet`	NA	NA

Amazon X-Ray

Amazon Service	Resource Type Value	Relationship	Related Resource
Amazon X-Ray	`AWS::XRay::EncryptionConfig`	NA	NA

Elastic Load Balancing

Amazon Service	Resource Type Value	Relationship	Related Resource
Elastic Load Balancing	Application Load Balancer `AWS::ElasticLoadBalancingV2::LoadBalancer`	is associated with	EC2 security group
		is attached to	Subnet
		is contained in	Virtual private cloud (VPC)
	Application Load Balancer Listener `AWS::ElasticLoadBalancingV2::Listener`	NA	NA
	Classic Load Balancer `AWS::ElasticLoadBalancing::LoadBalancer`	is associated with	EC2 security group
		is attached to	Subnet
		is contained in	Virtual private cloud (VPC)
	Network Load Balancer	NA	NA

Amazon Service	Resource Type Value	Relationship	Related Resource
	AWS::ElasticLoadBalancingV2::LoadBalancer		

AWS Elemental MediaConnect

Amazon Service	Resource Type Value	Relationship	Related Resource
AWS Elemental MediaConnect	AWS::MediaConnect::FlowEntitlement	NA	NA
	AWS::MediaConnect::FlowVpcInterface	NA	NA
	AWS::MediaConnect::FlowSource	NA	NA
	AWS::MediaConnect::Gateway	NA	NA

AWS Elemental MediaPackage

Amazon Service	Resource Type Value	Relationship	Related Resource
AWS Elemental MediaPackage	AWS::MediaPackage:	NA	NA

Amazon Service	Resource Type Value	Relationship	Related Resource
	`:Packagin gGroup`		
	`AWS::Medi aPackage: :Packagin gConfiguration`	NA	NA

AWS Elemental MediaTailor

Amazon Service	Resource Type Value	Relationship	Related Resource
AWS Elemental MediaTailor	`AWS::Medi aTailor:: PlaybackC onfiguration`	NA	NA

Resource Coverage by Region Availability

North and South America Regions

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::ACM::Certificate	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::ACMPCA::CertificateAuthority	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::ACMPCA::CertificateAuthorityActivation	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::APS::RuleGroupsNamespace	No	Yes	Yes	Yes	No	No	No	Yes
AWS::AccessAnalyzer::Analyzer	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::AmazonMQ::Broker	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::Amplify::App	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::Amplify::Branch	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::ApiGateway::RestApi	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ApiGateway::Stage	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ApiGatewayV2::Api	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ApiGatewayV2::Stage	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::AppConfig::Application	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::AppConfig::ConfigurationProfile	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::AppConfig::DeploymentStrategy	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::AppConfig::Environment	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::AppConfig::ExtensionAssociation	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::AppConfig::HostedConfigurationVersion	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::AppFlow::Flow	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::AppIntegrations::Application	No	Yes	Yes	No	No	Yes	No	No
AWS::AppIntegrations::EventIntegration	No	Yes	Yes	No	No	Yes	No	No
AWS::AppMesh::GatewayRoute	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::AppMesh::Mesh	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::AppMesh::Route	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::AppMesh::VirtualGateway	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::AppMesh::VirtualNode	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::AppMesh::VirtualRouter	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::AppMesh::VirtualService	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::AppRunner::Service	No	Yes	Yes	Yes	No	No	No	No

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::AppRunner::VpcConnector	No	Yes	Yes	Yes	No	No	No	No
AWS::AppStream::Application	No	Yes	Yes	Yes	No	Yes	No	Yes
AWS::AppStream::DirectoryConfig	No	Yes	Yes	Yes	No	Yes	No	Yes
AWS::AppStream::Fleet	No	Yes	Yes	Yes	No	Yes	No	No
AWS::AppStream::Stack	No	Yes	Yes	Yes	No	Yes	No	No
AWS::AppSync::ApiCache	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::AppSync::GraphQLApi	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::Athena::DataCatalog	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::Athena::PreparedStatement	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::Athena::WorkGroup	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::AuditManager::Assessment	Yes	Yes	Yes	Yes	No	Yes	No	No
AWS::AutoScaling::AutoScalingGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::AutoScaling::LaunchConfiguration	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::AutoScaling::ScalingPolicy	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::AutoScaling::ScheduledAction	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::AutoScaling::WarmPool	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::Backup::BackupPlan	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::Backup::BackupSelection	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::Backup::BackupVault	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::Backup::RecoveryPoint	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::Backup::ReportPlan	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::Batch::ComputeEnvironment	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::Batch::JobQueue	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::Batch::SchedulingPolicy	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::Bedrock::Guardrail	No	Yes	Yes	Yes	No	Yes	No	Yes
AWS::Bedrock::KnowledgeBase	No	Yes	Yes	Yes	No	Yes	No	Yes
AWS::Budgets::BudgetsAction	No	Yes	No	No	No	No	No	No
AWS::Cassandra::Keyspace	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::Cloud9::EnvironmentEC2	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::CloudFormation::Stack	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::CloudFront::Distribution	No	Yes	No	No	No	No	No	No
AWS::CloudFront::StreamingDistribution	No	Yes	No	No	No	No	No	No
AWS::CloudTrail::Trail	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::CloudWatch::Alarm	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::CloudWatch::MetricStream	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::CodeArtifact::Repository	No	Yes	Yes	Yes	No	No	No	No
AWS::CodeBuild::Project	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::CodeBuild::ReportGroup	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::CodeDeploy::Application	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::CodeDeploy::DeploymentConfig	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::CodeDeploy::DeploymentGroup	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::CodeGuruProfiler::ProfilingGroup	No	Yes	Yes	Yes	No	No	No	No

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::CodeGuruReviewer::RepositoryAssociation	No	Yes	Yes	Yes	No	No	No	No
AWS::CodePipeline::Pipeline	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::Cognito::IdentityPool	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::Cognito::UserPool	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::Cognito::UserPoolClient	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::Cognito::UserPoolGroup	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::Config::ConfigurationRecorder	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::Config::ConformancePackCompliance	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::Config::ResourceCompliance	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Connect::Instance	No	Yes	Yes	No	No	Yes	No	No
AWS::Connect::PhoneNumber	No	Yes	Yes	No	No	Yes	No	No
AWS::Connect::QuickConnect	No	Yes	Yes	No	No	Yes	No	No
AWS::Connect::Rule	No	Yes	Yes	No	No	Yes	No	No
AWS::Connect::User	No	Yes	Yes	No	No	Yes	No	No

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::CustomerProfiles::Domain	No	Yes	Yes	No	No	Yes	No	No
AWS::CustomerProfiles::ObjectType	No	Yes	Yes	No	No	Yes	No	No
AWS::DMS::Certificate	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::DMS::Endpoint	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::DMS::EventSubscription	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::DMS::ReplicationInstance	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::DMS::ReplicationSubnetGroup	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::DMS::ReplicationTask	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::DataSync::LocationEFS	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::DataSync::LocationFSxLustre	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::DataSync::LocationFSxWindows	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::DataSync::LocationHDFS	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::DataSync::LocationNFS	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::DataSync::LocationObjectStorage	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::DataSync::LocationS3	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::DataSync::LocationSMB	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::DataSync::Task	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::Detective::Graph	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::DeviceFarm::InstanceProfile	No	No	Yes	No	No	No	No	No
AWS::DeviceFarm::Project	No	No	Yes	No	No	No	No	No
AWS::DeviceFarm::TestGridProject	No	No	Yes	No	No	No	No	No

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::DynamoDB::Table	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::Capacity Reservation	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::EC2::CarrierGateway	No	Yes	Yes	Yes	No	Yes	No	No
AWS::EC2::ClientVpnEndpoint	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::EC2::ClientVpnTargetNetworkAssociation	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::EC2::CustomerGateway	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::DHCPOptions	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::EC2::EC2Fleet	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::EC2::EIP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::EIPAssociation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::EgressOnlyInternetGateway	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::EC2::FlowLog	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::EC2::Host	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::IPAM	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::EC2::IPAMPool	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::EC2::IPAMResourceDiscovery	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::EC2::IPAMResourceDiscoveryAssociation	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::EC2::IPAMScope	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::EC2::Instance	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::InstanceConnectEndpoint	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::EC2::InternetGateway	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::EC2::LaunchTemplate	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::EC2::NatGateway	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::EC2::NetworkAcl	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::NetworkInsightsAccessScope	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::EC2::NetworkInsightsAccessScopeAnalysis	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::EC2::NetworkInsightsAnalysis	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::EC2::NetworkInsightsPath	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::EC2::NetworkInterface	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::PrefixList	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::EC2::RegisteredHAInstance	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::EC2::RouteTable	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::SecurityGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::SnapshotBlockPublicAccess	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::EC2::SpotFleet	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::EC2::Subnet	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::SubnetRouteTableAssociation	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::EC2::TrafficMirrorFilter	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::EC2::TrafficMirrorSession	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::EC2::TrafficMirrorTarget	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::EC2::TransitGateway	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::EC2::TransitGatewayAttachment	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::EC2::TransitGatewayConnect	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::EC2::TransitGatewayMulticastDomain	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::EC2::TransitGatewayRouteTable	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::EC2::VPC	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::VPCBlockPublicAccessExclusion	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::EC2::VPCBlockPublicAccessOptions	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::EC2::VPCEndpoint	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::EC2::VPCEndpointConnectionNotification	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::VPCEndpointService	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::VPCPeeringConnection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::VPNConnection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::VPNConnectionRoute	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::EC2::VPNGateway	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::Volume	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::ECR::PublicRepository	No	Yes	No	No	No	No	No	No
AWS::ECR::PullThroughCacheRule	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::ECR::RegistryPolicy	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::ECR::Repository	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::ECS::CapacityProvider	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::ECS::Cluster	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ECS::Service	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::ECS::TaskDefinition	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ECS::TaskSet	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::EFS::AccessPoint	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::EFS::FileSystem	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::EKS::Addon	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::EKS::Cluster	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::EKS::FargateProfile	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::EKS::IdentityProviderConfig	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::EMR::SecurityConfiguration	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::ElasticBeanstalk::Application	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::ElasticBeanstalk::ApplicationVersion	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::ElasticBeanstalk::Environment	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::ElasticLoadBalancing::LoadBalancer	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ElasticLoadBalancingV2::Listener	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::ElasticLoadBalancingV2::LoadBalancer	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Elasticsearch::Domain	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EventSchemas::Discoverer	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::EventSchemas::Registry	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::EventSchemas::RegistryPolicy	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::EventSchemas::Schema	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::Events::ApiDestination	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::Events::Archive	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::Events::Connection	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::Events::Endpoint	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::Events::EventBus	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::Events::Rule	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::Evidently::Launch	No	Yes	Yes	Yes	No	No	No	No
AWS::Evidently::Project	No	Yes	Yes	Yes	No	No	No	No

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::Evidently::Segment	No	Yes	Yes	Yes	No	No	No	No
AWS::FIS::ExperimentTemplate	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::Forecast::Dataset	No	Yes	Yes	Yes	No	No	No	No
AWS::Forecast::DatasetGroup	No	Yes	Yes	Yes	No	No	No	No
AWS::FraudDetector::EntityType	No	Yes	Yes	Yes	No	No	No	No
AWS::FraudDetector::Label	No	Yes	Yes	Yes	No	No	No	No
AWS::FraudDetector::Outcome	No	Yes	Yes	Yes	No	No	No	No

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::FraudDetector::Variable	No	Yes	Yes	Yes	No	No	No	No
AWS::GlobalAccelerator::Accelerator	No	No	Yes	No	No	No	No	No
AWS::GlobalAccelerator::EndpointGroup	No	No	Yes	No	No	No	No	No
AWS::GlobalAccelerator::Listener	No	No	Yes	No	No	No	No	No
AWS::Glue::Classifier	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::Glue::Job	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::Glue::MLTransform	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::Grafana::Workspace	No	Yes	Yes	Yes	No	No	No	No
AWS::GreengrassV2::ComponentVersion	No	Yes	Yes	Yes	No	Yes	No	No
AWS::GroundStation::Config	No	Yes	Yes	Yes	No	No	No	Yes
AWS::GroundStation::DataflowEndpointGroup	No	Yes	Yes	Yes	No	No	No	Yes
AWS::GroundStation::MissionProfile	No	Yes	Yes	Yes	No	No	No	Yes
AWS::GuardDuty::Detector	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::GuardDuty::Filter	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::GuardDuty::IPSet	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::GuardDuty::ThreatIntelSet	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::HealthLake::FHIRDatastore	No	Yes	Yes	Yes	No	No	No	No
AWS::IAM::Group	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::IAM::InstanceProfile	No	Yes	No	No	No	No	No	No
AWS::IAM::OIDCProvider	No	Yes	No	No	No	No	No	No
AWS::IAM::Policy	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::IAM::Role	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::IAM::SAMLProvider	No	Yes	No	No	No	No	No	No
AWS::IAM::ServerCertificate	No	Yes	No	No	No	No	No	No
AWS::IAM::User	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::IVS::Channel	No	Yes	Yes	No	No	No	No	No
AWS::IVS::PlaybackKeyPair	No	Yes	Yes	No	No	No	No	No
AWS::IVS::RecordingConfiguration	No	Yes	Yes	No	No	No	No	No

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::ImageBuilder::ContainerRecipe	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::ImageBuilder::DistributionConfiguration	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::ImageBuilder::ImagePipeline	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::ImageBuilder::ImageRecipe	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::ImageBuilder::InfrastructureConfiguration	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::InspectorV2::Activation	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::InspectorV2::Filter	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::IoT::AccountAuditConfiguration	Yes	Yes	Yes	Yes	No	Yes	No	No
AWS::IoT::Authorizer	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::IoT::CACertificate	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::IoT::CustomMetric	Yes	Yes	Yes	Yes	No	Yes	No	No
AWS::IoT::Dimension	Yes	Yes	Yes	Yes	No	Yes	No	No
AWS::IoT::FleetMetric	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::IoT::JobTemplate	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::IoT::MitigationAction	Yes	Yes	Yes	Yes	No	Yes	No	No
AWS::IoT::Policy	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::IoT::ProvisioningTemplate	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::IoT::RoleAlias	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::IoT::ScheduledAudit	Yes	Yes	Yes	Yes	No	Yes	No	No
AWS::IoT::SecurityProfile	Yes	Yes	Yes	Yes	No	Yes	No	No
AWS::IoTAnalytics::Channel	No	Yes	Yes	Yes	No	No	No	No

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::IoTAnalytics::Dataset	No	Yes	Yes	Yes	No	No	No	No
AWS::IoTAnalytics::Datastore	No	Yes	Yes	Yes	No	No	No	No
AWS::IoTAnalytics::Pipeline	No	Yes	Yes	Yes	No	No	No	No
AWS::IoTEvents::AlarmModel	No	Yes	Yes	Yes	No	Yes	No	No
AWS::IoTEvents::DetectorModel	No	Yes	Yes	Yes	No	Yes	No	No
AWS::IoTEvents::Input	No	Yes	Yes	Yes	No	Yes	No	No
AWS::IoTSiteWise::AssetModel	No	Yes	Yes	Yes	No	Yes	No	No

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::IoTSiteWise::Dashboard	No	Yes	Yes	Yes	No	Yes	No	No
AWS::IoTSiteWise::Gateway	No	Yes	Yes	Yes	No	Yes	No	No
AWS::IoTSiteWise::Portal	No	Yes	Yes	Yes	No	Yes	No	No
AWS::IoTSiteWise::Project	No	Yes	Yes	Yes	No	Yes	No	No
AWS::IoTTwinMaker::ComponentType	No	Yes	Yes	No	No	No	No	No
AWS::IoTTwinMaker::Entity	No	Yes	Yes	No	No	No	No	No
AWS::IoTTwinMaker::Scene	No	Yes	Yes	No	No	No	No	No

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::IoTTwinMaker::SyncJob	No	Yes	Yes	No	No	No	No	No
AWS::IoTTwinMaker::Workspace	No	Yes	Yes	No	No	No	No	No
AWS::IoTWireless::FuotaTask	No	Yes	Yes	No	No	No	No	Yes
AWS::IoTWireless::MulticastGroup	No	Yes	Yes	No	No	No	No	Yes
AWS::IoTWireless::ServiceProfile	No	Yes	Yes	No	No	No	No	Yes
AWS::KMS::Alias	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::KMS::Key	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::KafkaConnect::Connector	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::Kendra::Index	No	Yes	Yes	Yes	No	Yes	No	No
AWS::Kinesis::Stream	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::Kinesis::StreamConsumer	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::KinesisAnalyticsV2::Application	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::KinesisFirehose::DeliveryStream	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::KinesisVideo::SignalingChannel	No	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::KinesisVideo::Stream	No	Yes	Yes	Yes	No	Yes	No	Yes
AWS::Lambda::CodeSigningConfig	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::Lambda::Function	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Lex::Bot	No	Yes	Yes	No	No	Yes	No	No
AWS::Lex::BotAlias	No	Yes	Yes	No	No	Yes	No	No
AWS::Lightsail::Bucket	No	Yes	Yes	Yes	No	Yes	No	No
AWS::Lightsail::Certificate	No	Yes	Yes	Yes	No	Yes	No	No

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::Lightsail::Disk	No	Yes	Yes	Yes	No	Yes	No	No
AWS::Lightsail::StaticIp	No	Yes	Yes	Yes	No	Yes	No	No
AWS::Logs::Destination	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::LookoutMetrics::Alert	No	Yes	Yes	Yes	No	No	No	No
AWS::LookoutVision::Project	No	Yes	Yes	Yes	No	No	No	No
AWS::M2::Environment	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::MSK::BatchScramSecret	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::MSK::Cluster	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::MSK::ClusterPolicy	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::MSK::Configuration	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::MSK::VpcConnection	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::Macie::Session	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::MediaConnect::FlowEntitlement	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::MediaConnect::FlowSource	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::MediaConnect::FlowVpcInterface	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::MediaConnect::Gateway	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::MediaPackage::PackagingConfiguration	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::MediaPackage::PackagingGroup	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::MediaTailor::PlaybackConfiguration	No	Yes	Yes	Yes	No	Yes	No	Yes
AWS::MemoryDB::SubnetGroup	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::NetworkFirewall::Firewall	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::NetworkFirewall::FirewallPolicy	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::NetworkFirewall::RuleGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::NetworkFirewall::TLSInspectionConfiguration	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::NetworkFirewall::VpcEndpointAssociation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::NetworkManager::ConnectPeer	No	No	Yes	No	No	No	No	No
AWS::NetworkManager::CustomerGatewayAssociation	No	No	Yes	No	No	No	No	No
AWS::NetworkManager::Device	No	No	Yes	No	No	No	No	No

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::NetworkManager::GlobalNetwork	No	No	Yes	No	No	No	No	No
AWS::NetworkManager::Link	No	No	Yes	No	No	No	No	No
AWS::NetworkManager::LinkAssociation	No	No	Yes	No	No	No	No	No
AWS::NetworkManager::Site	No	No	Yes	No	No	No	No	No
AWS::NetworkManager::TransitGatewayRegistration	No	No	Yes	No	No	No	No	No
AWS::OpenSearch::Domain	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::OpenSearchServerless::Collection	No	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::OpenSearchServerless::VpcEndpoint	No	Yes	Yes	Yes	No	Yes	No	Yes
AWS::Panorama::Package	No	Yes	Yes	No	No	Yes	No	No
AWS::Personalize::Dataset	No	Yes	Yes	Yes	No	Yes	No	No
AWS::Personalize::DatasetGroup	No	Yes	Yes	Yes	No	Yes	No	No
AWS::Personalize::Schema	No	Yes	Yes	Yes	No	Yes	No	No
AWS::Personalize::Solution	No	Yes	Yes	Yes	No	Yes	No	No
AWS::Pinpoint::App	No	Yes	Yes	No	No	Yes	No	No

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::Pinpoint::ApplicationSettings	No	Yes	Yes	No	No	Yes	No	No
AWS::Pinpoint::Campaign	No	Yes	Yes	No	No	Yes	No	No
AWS::Pinpoint::EmailChannel	No	Yes	Yes	No	No	Yes	No	No
AWS::Pinpoint::EmailTemplate	No	Yes	Yes	No	No	Yes	No	No
AWS::Pinpoint::EventStream	No	Yes	Yes	No	No	Yes	No	No
AWS::Pinpoint::InAppTemplate	No	Yes	Yes	Yes	No	Yes	No	No
AWS::Pinpoint::Segment	No	Yes	Yes	No	No	Yes	No	No

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::QLDB::Ledger	No	Yes	Yes	Yes	No	Yes	No	No
AWS::QuickSight::DataSource	No	Yes	Yes	Yes	No	Yes	No	Yes
AWS::QuickSight::Template	No	Yes	Yes	Yes	No	Yes	No	Yes
AWS::QuickSight::Theme	No	Yes	Yes	Yes	No	Yes	No	Yes
AWS::RDS::DBCluster	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::RDS::DBClusterSnapshot	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::RDS::DBInstance	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::RDS::DBSecurityGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::RDS::DBSnapshot	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::RDS::DBSubnetGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::RDS::EventSubscription	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::RDS::GlobalCluster	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::RDS::OptionGroup	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::RUM::AppMonitor	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::Redshift::Cluster	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Redshift::ClusterParameterGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Redshift::ClusterSecurityGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Redshift::ClusterSnapshot	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Redshift::ClusterSubnetGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Redshift::EndpointAccess	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::Redshift::EndpointAuthorization	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::Redshift::EventSubscription	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Redshift::ScheduledAction	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::ResilienceHub::App	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::ResilienceHub::ResiliencyPolicy	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::ResourceExplorer2::Index	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::RoboMaker::RobotApplication	No	Yes	Yes	Yes	No	No	No	No
AWS::RoboMaker::RobotApplicationVersion	No	Yes	Yes	Yes	No	No	No	No

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::RoboMaker::SimulationApplication	No	Yes	Yes	Yes	No	No	No	No
AWS::Route53::HealthCheck	No	Yes	No	No	No	No	No	No
AWS::Route53::HostedZone	No	Yes	No	No	No	No	No	No
AWS::Route53Profiles::Profile	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::Route53RecoveryControl::Cluster	No	No	Yes	No	No	No	No	No
AWS::Route53RecoveryControl::ControlPanel	No	No	Yes	No	No	No	No	No
AWS::Route53RecoveryControl::RoutingControl	No	No	Yes	No	No	No	No	No

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::Route53RecoveryControl::SafetyRule	No	No	Yes	No	No	No	No	No
AWS::Route53RecoveryReadiness::Cell	No	No	Yes	No	No	No	No	No
AWS::Route53RecoveryReadiness::ReadinessCheck	No	No	Yes	No	No	No	No	No
AWS::Route53RecoveryReadiness::RecoveryGroup	No	No	Yes	No	No	No	No	No
AWS::Route53RecoveryReadiness::ResourceSet	No	No	Yes	No	No	No	No	No
AWS::Route53Resolver::FirewallDomainList	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::Route53Resolver::FirewallRuleGroup	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::Route53Resolver::FirewallRuleGroupAssociation	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::Route53Resolver::ResolverEndpoint	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::Route53Resolver::ResolverQueryLoggingConfig	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::Route53Resolver::ResolverRule	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::Route53Resolver::ResolverRuleAssociation	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::S3::AccessPoint	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::S3::AccountPublicAccessBlock	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::S3::Bucket	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::S3::MultiRegionAccessPoint	No	No	Yes	No	No	No	No	No
AWS::S3::StorageLens	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::S3::StorageLensGroup	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::S3Express::BucketPolicy	No	Yes	Yes	Yes	No	No	No	No
AWS::S3Express::DirectoryBucket	No	Yes	Yes	Yes	No	No	No	No

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::SES::ConfigurationSet	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::SES::ContactList	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::SES::ReceiptFilter	No	Yes	Yes	Yes	No	Yes	No	No
AWS::SES::ReceiptRuleSet	No	Yes	Yes	Yes	No	Yes	No	No
AWS::SES::Template	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::SNS::Topic	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::SQS::Queue	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::SSM::AssociationCompliance	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::SSM::Document	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::SSM::FileData	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::SSM::ManagedInstanceInventory	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::SSM::PatchCompliance	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::SageMaker::AppImageConfig	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::SageMaker::CodeRepository	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::SageMaker::Domain	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::SageMaker::EndpointConfig	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::SageMaker::FeatureGroup	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::SageMaker::Image	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::SageMaker::InferenceExperiment	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::SageMaker::Model	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::SageMaker::NotebookInstance	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::SageMaker::NotebookInstanceLifecycleConfig	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::SageMaker::Workteam	No	Yes	Yes	Yes	No	Yes	No	No
AWS::SecretsManager::Secret	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::SecurityHub::Standard	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ServiceCatalog::CloudFormationProduct	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::ServiceCatalog::Portfolio	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::ServiceDiscovery::HttpNamespace	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::ServiceDiscovery::Instance	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::ServiceDiscovery::PublicDnsNamespace	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::ServiceDiscovery::Service	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::Shield::Protection	No	Yes	No	No	No	No	No	No
AWS::ShieldRegional::Protection	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::Signer::SigningProfile	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::Step Functions::Activity	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::StepFunctions ::StateMachine	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::Transfer::Agreement	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::Transfer::Certificate	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::Transfer::Connector	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::Transfer::Profile	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::Transfer::Workflow	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::WAF::RateBasedRule	No	Yes	No	No	No	No	No	No
AWS::WAF::Rule	No	Yes	No	No	No	No	No	No
AWS::WAF::RuleGroup	No	Yes	No	No	No	No	No	No
AWS::WAF::WebACL	No	Yes	No	No	No	No	No	No
AWS::WAFRegional::RateBasedRule	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::WAFRegional::Rule	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::WAFRegional::RuleGroup	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::WAFRegional::WebACL	Yes	Yes	Yes	Yes	No	Yes	No	Yes
AWS::WAFv2::IPSet	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::WAFv2::ManagedRuleSet	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::WAFv2::RegexPatternSet	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::WAFv2::RuleGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::WAFv2::WebACL	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::WorkSpaces::ConnectionAlias	No	Yes	Yes	No	No	Yes	No	Yes

Resource type	US West (N. California)	US East (N. Virginia)	US West (Oregon)	US East (Ohio)	Canada West (Calgary)	Canada (Central)	Mexico (Central)	South America (São Paulo)
AWS::WorkSpaces::Workspace	No	Yes	Yes	No	No	Yes	No	Yes
AWS::XRay::EncryptionConfig	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Europe Regions

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::ACM::Certificate	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ACMPCA::CertificateAuthority	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ACMPCA::CertificateAuthorityActivation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::APS::RuleGroupsNamespace	Yes	Yes	Yes	Yes	Yes	No	No	No

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::AccessAnalyzer::Analyzer	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::AmazonMQ::Broker	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::Amplify::App	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::Amplify::Branch	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::ApiGateway::RestApi	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ApiGateway::Stage	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ApiGatewayV2::Api	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ApiGatewayV2::Stage	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::AppConfig::Application	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::AppConfig::ConfigurationProfile	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::AppConfig::DeploymentStrategy	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::AppConfig::Environment	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::AppConfig::ExtensionAssociation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::AppConfig::HostedConfigurationVersion	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::AppFlow::Flow	Yes	Yes	Yes	Yes	No	No	No	No
AWS::AppIntegrations::Application	No	Yes	Yes	No	No	No	No	No

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::AppIntegrations::EventIntegration	No	Yes	Yes	No	No	No	No	No
AWS::AppMesh::GatewayRoute	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::AppMesh::Mesh	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::AppMesh::Route	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::AppMesh::VirtualGateway	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::AppMesh::VirtualNode	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::AppMesh::VirtualRouter	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::AppMesh::VirtualService	Yes	Yes	Yes	Yes	Yes	Yes	No	No

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::AppRunner::Service	Yes	Yes	Yes	Yes	No	No	No	No
AWS::AppRunner::VpcConnector	Yes	Yes	No	Yes	No	No	No	No
AWS::AppStream::Application	Yes	Yes	Yes	No	No	No	No	No
AWS::AppStream::DirectoryConfig	Yes	Yes	Yes	No	No	No	No	No
AWS::AppStream::Fleet	Yes	Yes	Yes	No	No	No	No	No
AWS::AppStream::Stack	Yes	Yes	Yes	No	No	No	No	No
AWS::AppSync::ApiCache	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::AppSync::GraphQLApi	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::Athena::DataCatalog	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Athena::PreparedStatement	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
AWS::Athena::WorkGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::AuditManager::Assessment	Yes	Yes	Yes	No	No	No	No	No
AWS::AutoScaling::AutoScalingGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::AutoScaling::LaunchConfiguration	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::AutoScaling::ScalingPolicy	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::AutoScaling::ScheduledAction	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::AutoScaling::WarmPool	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::Backup::BackupPlan	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Backup::BackupSelection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Backup::BackupVault	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Backup::RecoveryPoint	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Backup::ReportPlan	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::Batch::ComputeEnvironment	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Batch::JobQueue	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::Batch::SchedulingPolicy	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Bedrock::Guardrail	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Bedrock::KnowledgeBase	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Cassandra::Keyspace	Yes	Yes	Yes	Yes	Yes	No	No	No
AWS::Cloud9::EnvironmentEC2	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::CloudFormation::Stack	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::CloudTrail::Trail	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::CloudWatch::Alarm	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::CloudWatch::MetricStream	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::CodeArtifact::Repository	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::CodeBuild::Project	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::CodeBuild::ReportGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::CodeDeploy::Application	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::CodeDeploy::DeploymentConfig	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::CodeDeploy::DeploymentGroup	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::CodeGuruProfiler::ProfilingGroup	Yes	Yes	Yes	No	Yes	No	No	No

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::CodeGuruReviewer::RepositoryAssociation	Yes	Yes	Yes	No	Yes	No	No	No
AWS::CodePipeline::Pipeline	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Cognito::IdentityPool	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Cognito::UserPool	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Cognito::UserPoolClient	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Cognito::UserPoolGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Config::ConfigurationRecorder	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Config::ConformancePackCompliance	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::Config::ResourceCompliance	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Connect::Instance	No	Yes	Yes	No	No	No	No	No
AWS::Connect::PhoneNumber	No	Yes	Yes	No	No	No	No	No
AWS::Connect::QuickConnect	No	Yes	Yes	No	No	No	No	No
AWS::Connect::Rule	No	Yes	Yes	No	No	No	No	No
AWS::Connect::User	No	Yes	Yes	No	No	No	No	No
AWS::CustomerProfiles::Domain	No	Yes	Yes	No	No	No	No	No
AWS::CustomerProfiles::ObjectType	No	Yes	Yes	No	No	No	No	No

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::DMS::Certificate	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::DMS::Endpoint	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::DMS::EventSubscription	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::DMS::ReplicationInstance	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::DMS::ReplicationSubnetGroup	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::DMS::ReplicationTask	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::DataSync::LocationEFS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::DataSync::LocationFSxLustre	Yes	Yes	Yes	Yes	Yes	Yes	No	No

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::DataSync::LocationFSxWindows	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::DataSync::LocationHDFS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::DataSync::LocationNFS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::DataSync::LocationObjectStorage	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::DataSync::LocationS3	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::DataSync::LocationSMB	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::DataSync::Task	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Detective::Graph	Yes	Yes	Yes	Yes	Yes	Yes	No	No

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::DynamoDB::Table	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::Capacity Reservation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::CarrierGateway	Yes	Yes	Yes	Yes	No	No	No	No
AWS::EC2::ClientVpnEndpoint	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::EC2::ClientVpnTargetNetworkAssociation	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::EC2::CustomerGateway	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::DHCPOptions	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::EC2Fleet	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::EC2::EIP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::EIPAssociation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::EgressOnlyInternetGateway	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::EC2::FlowLog	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::EC2::Host	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::IPAM	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::IPAMPool	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::IPAMResourceDiscovery	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::EC2::IPAMResourceDiscoveryAssociation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::IPAMScope	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::Instance	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::InstanceConnectEndpoint	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::InternetGateway	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::LaunchTemplate	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::EC2::NatGateway	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::EC2::NetworkAcl	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::EC2::NetworkInsightsAccessScope	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::EC2::NetworkInsightsAccessScopeAnalysis	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::EC2::NetworkInsightsAnalysis	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::EC2::NetworkInsightsPath	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::EC2::NetworkInterface	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::PrefixList	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::RegisteredHAInstance	Yes	Yes	Yes	Yes	Yes	No	No	No
AWS::EC2::RouteTable	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::EC2::SecurityGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::Snapshot BlockPublicAccess	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::SpotFleet	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::Subnet	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::SubnetRouteTableAssociation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::TrafficMirrorFilter	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::TrafficMirrorSession	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EC2::TrafficMirrorTarget	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::EC2::TransitGateway	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::TransitGatewayAttachment	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::TransitGatewayConnect	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::EC2::TransitGatewayMulticastDomain	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::TransitGatewayRouteTable	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::EC2::VPC	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::VPCBlockPublicAccessExclusion	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::VPCBlockPublicAccessOptions	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::EC2::VPCEndpoint	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::VPCEndpointConnectionNotification	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::VPCEndpointService	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::VPCPeeringConnection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::VPNConnection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::VPNConnectionRoute	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::VPNGateway	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::Volume	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::ECR::PullThroughCacheRule	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ECR::RegistryPolicy	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ECR::Repository	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ECS::CapacityProvider	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ECS::Cluster	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ECS::Service	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ECS::TaskDefinition	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ECS::TaskSet	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::EFS::AccessPoint	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EFS::FileSystem	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EKS::Addon	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EKS::Cluster	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EKS::FargateProfile	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EKS::IdentityProviderConfig	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EMR::SecurityConfiguration	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ElasticBeanstalk::Application	Yes	Yes	Yes	Yes	Yes	Yes	No	No

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::ElasticBeanstalk::ApplicationVersion	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::ElasticBeanstalk::Environment	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::ElasticLoadBalancing::LoadBalancer	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ElasticLoadBalancingV2::Listener	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::ElasticLoadBalancingV2::LoadBalancer	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Elasticsearch::Domain	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EventSchemas::Discoverer	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EventSchemas::Registry	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::EventSchemas::RegistryPolicy	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EventSchemas::Schema	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Events::ApiDestination	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Events::Archive	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Events::Connection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Events::Endpoint	Yes	Yes	Yes	Yes	Yes	No	No	No
AWS::Events::EventBus	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Events::Rule	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::Evidently::Launch	Yes	Yes	No	No	Yes	No	No	No
AWS::Evidently::Project	Yes	Yes	No	No	Yes	No	No	No
AWS::Evidently::Segment	Yes	Yes	No	No	Yes	No	No	No
AWS::FIS::ExperimentTemplate	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
AWS::Forecast::Dataset	Yes	Yes	No	No	No	No	No	No
AWS::Forecast::DatasetGroup	Yes	Yes	No	No	No	No	No	No
AWS::FraudDetector::EntityType	Yes	No	No	No	No	No	No	No
AWS::FraudDetector::Label	Yes	No	No	No	No	No	No	No

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::FraudDetector::Outcome	Yes	No	No	No	No	No	No	No
AWS::FraudDetector::Variable	Yes	No	No	No	No	No	No	No
AWS::Glue::Classifier	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Glue::Job	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Glue::MLTransform	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Grafana::Workspace	Yes	Yes	Yes	No	No	No	No	No
AWS::GreengrassV2::ComponentVersion	Yes	Yes	Yes	No	No	No	No	No
AWS::GroundStation::Config	Yes	Yes	No	No	Yes	No	No	No

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::GroundStation::DataflowEndpointGroup	Yes	Yes	No	No	Yes	No	No	No
AWS::GroundStation::MissionProfile	Yes	Yes	No	No	Yes	No	No	No
AWS::GuardDuty::Detector	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::GuardDuty::Filter	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::GuardDuty::IPSet	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::GuardDuty::ThreatIntelSet	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::IAM::Group	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::IAM::Policy	Yes	Yes	Yes	Yes	Yes	Yes	No	No

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::IAM::Role	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::IAM::User	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::IVS::Channel	Yes	Yes	No	No	No	No	No	No
AWS::IVS::PlaybackKeyPair	Yes	Yes	No	No	No	No	No	No
AWS::IVS::RecordingConfiguration	Yes	Yes	No	No	No	No	No	No
AWS::ImageBuilder::ContainerRecipe	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ImageBuilder::DistributionConfiguration	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ImageBuilder::ImagePipeline	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::ImageBuilder::ImageRecipe	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ImageBuilder::InfrastructureConfiguration	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::InspectorV2::Activation	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::InspectorV2::Filter	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::IoT::AccountAuditConfiguration	Yes	Yes	Yes	Yes	Yes	No	No	No
AWS::IoT::Authorizer	Yes	Yes	Yes	Yes	Yes	No	No	No
AWS::IoT::CACertificate	Yes	Yes	Yes	Yes	Yes	No	No	No
AWS::IoT::CustomMetric	Yes	Yes	Yes	Yes	Yes	No	No	No

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::IoT::Dimension	Yes	Yes	Yes	Yes	Yes	No	No	No
AWS::IoT::FleetMetric	Yes	Yes	Yes	Yes	Yes	No	No	No
AWS::IoT::JobTemplate	Yes	Yes	Yes	Yes	Yes	No	No	No
AWS::IoT::MitigationAction	Yes	Yes	Yes	Yes	Yes	No	No	No
AWS::IoT::Policy	Yes	Yes	Yes	Yes	Yes	No	No	No
AWS::IoT::ProvisioningTemplate	Yes	Yes	Yes	Yes	Yes	No	No	No
AWS::IoT::RoleAlias	Yes	Yes	Yes	Yes	Yes	No	No	No
AWS::IoT::ScheduledAudit	Yes	Yes	Yes	Yes	Yes	No	No	No

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::IoT::SecurityProfile	Yes	Yes	Yes	Yes	Yes	No	No	No
AWS::IoTAnalytics::Channel	Yes	Yes	No	No	No	No	No	No
AWS::IoTAnalytics::Dataset	Yes	Yes	No	No	No	No	No	No
AWS::IoTAnalytics::Datastore	Yes	Yes	No	No	No	No	No	No
AWS::IoTAnalytics::Pipeline	Yes	Yes	No	No	No	No	No	No
AWS::IoTEvents::AlarmModel	Yes	Yes	Yes	No	No	No	No	No
AWS::IoTEvents::DetectorModel	Yes	Yes	Yes	No	No	No	No	No
AWS::IoTEvents::Input	Yes	Yes	Yes	No	No	No	No	No

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::IoTSiteWise::AssetModel	Yes	Yes	No	No	No	No	No	No
AWS::IoTSiteWise::Dashboard	Yes	Yes	No	No	No	No	No	No
AWS::IoTSiteWise::Gateway	Yes	Yes	No	No	No	No	No	No
AWS::IoTSiteWise::Portal	Yes	Yes	No	No	No	No	No	No
AWS::IoTSiteWise::Project	Yes	Yes	No	No	No	No	No	No
AWS::IoTTwinMaker::ComponentType	Yes	Yes	No	No	No	No	No	No
AWS::IoTTwinMaker::Entity	Yes	Yes	No	No	No	No	No	No
AWS::IoTTwinMaker::Scene	Yes	Yes	No	No	No	No	No	No

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::IoTTwinMaker::SyncJob	Yes	Yes	No	No	No	No	No	No
AWS::IoTTwinMaker::Workspace	Yes	Yes	No	No	No	No	No	No
AWS::IoTWireless::FuotaTask	Yes	Yes	No	No	No	No	No	No
AWS::IoTWireless::MulticastGroup	Yes	Yes	No	No	No	No	No	No
AWS::IoTWireless::ServiceProfile	Yes	Yes	No	No	No	No	No	No
AWS::KMS::Alias	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::KMS::Key	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::KafkaConnect::Connector	Yes	Yes	Yes	Yes	Yes	No	No	No

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::Kendra::Index	Yes	No	Yes	No	No	No	No	No
AWS::Kinesis::Stream	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Kinesis::StreamConsumer	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::KinesisAnalyticsV2::Application	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::KinesisFirehose::DeliveryStream	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::KinesisVideo::SignalingChannel	Yes	Yes	Yes	Yes	No	No	No	No
AWS::KinesisVideo::Stream	Yes	Yes	Yes	Yes	No	No	No	No
AWS::Lambda::CodeSigningConfig	Yes	Yes	Yes	Yes	Yes	Yes	No	No

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::Lambda::Function	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Lex::Bot	Yes	Yes	Yes	No	No	No	No	No
AWS::Lex::BotAlias	Yes	Yes	Yes	No	No	No	No	No
AWS::Lightsail::Bucket	Yes	Yes	Yes	Yes	Yes	No	No	No
AWS::Lightsail::Certificate	Yes	Yes	Yes	Yes	Yes	No	No	No
AWS::Lightsail::Disk	Yes	Yes	Yes	Yes	Yes	No	No	No
AWS::Lightsail::StaticIp	Yes	Yes	Yes	Yes	Yes	No	No	No
AWS::Logs::Destination	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::LookoutMetrics::Alert	Yes	Yes	No	No	Yes	No	No	No
AWS::LookoutVision::Project	Yes	Yes	No	No	No	No	No	No
AWS::M2::Environment	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::MSK::BatchScramSecret	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::MSK::Cluster	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::MSK::ClusterPolicy	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::MSK::Configuration	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::MSK::VpcConnection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::Macie::Session	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::MediaConnect::FlowEntitlement	Yes	Yes	Yes	Yes	Yes	No	No	No
AWS::MediaConnect::FlowSource	Yes	Yes	Yes	Yes	Yes	No	No	No
AWS::MediaConnect::FlowVpcInterface	Yes	Yes	Yes	Yes	Yes	No	No	No
AWS::MediaConnect::Gateway	Yes	Yes	Yes	Yes	Yes	No	No	No
AWS::MediaPackage::PackagingConfiguration	Yes	Yes	Yes	Yes	Yes	No	No	No
AWS::MediaPackage::PackagingGroup	Yes	Yes	Yes	Yes	Yes	No	No	No
AWS::MediaTailor::PlaybackConfiguration	Yes	Yes	No	Yes	Yes	No	No	No

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::MemoryDB::SubnetGroup	Yes	Yes	Yes	No	Yes	No	No	No
AWS::NetworkFirewall::Firewall	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::NetworkFirewall::FirewallPolicy	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::NetworkFirewall::RuleGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::NetworkFirewall::TLSInspectionConfiguration	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::NetworkFirewall::VpcEndpointAssociation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::OpenSearch::Domain	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::OpenSearchServerless::Collection	Yes	Yes	Yes	Yes	No	No	No	No

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::OpenSearchServerless::VpcEndpoint	Yes	Yes	Yes	Yes	No	No	No	No
AWS::Panorama::Package	Yes	No	No	No	No	No	No	No
AWS::Personalize::Dataset	Yes	Yes	No	No	No	No	No	No
AWS::Personalize::DatasetGroup	Yes	Yes	No	No	No	No	No	No
AWS::Personalize::Schema	Yes	Yes	No	No	No	No	No	No
AWS::Personalize::Solution	Yes	Yes	No	No	No	No	No	No
AWS::Pinpoint::App	Yes	Yes	Yes	No	No	No	No	No
AWS::Pinpoint::ApplicationSettings	Yes	Yes	Yes	No	No	No	No	No

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::Pinpoint::Campaign	Yes	Yes	Yes	No	No	No	No	No
AWS::Pinpoint::EmailChannel	Yes	Yes	Yes	No	No	No	No	No
AWS::Pinpoint::EmailTemplate	Yes	Yes	Yes	No	No	No	No	No
AWS::Pinpoint::EventStream	Yes	Yes	Yes	No	No	No	No	No
AWS::Pinpoint::InAppTemplate	Yes	Yes	Yes	No	No	No	No	No
AWS::Pinpoint::Segment	Yes	Yes	Yes	No	No	No	No	No
AWS::QLDB::Ledger	Yes	Yes	Yes	No	No	No	No	No
AWS::QuickSight::DataSource	Yes	Yes	Yes	Yes	Yes	No	No	No

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::QuickSight::Template	Yes	Yes	Yes	Yes	Yes	No	No	No
AWS::QuickSight::Theme	Yes	Yes	Yes	Yes	Yes	No	No	No
AWS::RDS::DBCluster	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::RDS::DBClusterSnapshot	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::RDS::DBInstance	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::RDS::DBSecurityGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::RDS::DBSnapshot	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::RDS::DBSubnetGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::RDS::EventSubscription	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::RDS::GlobalCluster	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::RDS::OptionGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::RUM::AppMonitor	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Redshift::Cluster	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Redshift::ClusterParameterGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Redshift::ClusterSecurityGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Redshift::ClusterSnapshot	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::Redshift::ClusterSubnetGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Redshift::EndpointAccess	Yes	Yes	Yes	Yes	Yes	No	No	No
AWS::Redshift::EndpointAuthorization	Yes	Yes	Yes	Yes	Yes	No	No	No
AWS::Redshift::EventSubscription	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Redshift::ScheduledAction	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::ResilienceHub::App	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::ResilienceHub::ResiliencyPolicy	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::ResourceExplorer2::Index	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::RoboMaker::RobotApplication	Yes	Yes	No	No	No	No	No	No
AWS::RoboMaker::RobotApplicationVersion	Yes	Yes	No	No	No	No	No	No
AWS::RoboMaker::SimulationApplication	Yes	Yes	No	No	No	No	No	No
AWS::Route53Profiles::Profile	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Route53Resolver::FirewallDomainList	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::Route53Resolver::FirewallRuleGroup	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::Route53Resolver::FirewallRuleGroupAssociation	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::Route53Resolver::ResolverEndpoint	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::Route53Resolver::ResolverQueryLoggingConfig	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::Route53Resolver::ResolverRule	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Route53Resolver::ResolverRuleAssociation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::S3::AccessPoint	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::S3::AccountPublicAccessBlock	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::S3::Bucket	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::S3::StorageLens	Yes	Yes	Yes	Yes	Yes	No	No	No

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::S3::StorageLensGroup	Yes	Yes	Yes	Yes	Yes	No	No	No
AWS::S3Express::BucketPolicy	Yes	No	No	No	Yes	No	No	No
AWS::S3Express::DirectoryBucket	Yes	No	No	No	Yes	No	No	No
AWS::SES::ConfigurationSet	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::SES::ContactList	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::SES::ReceiptFilter	Yes	Yes	Yes	No	No	No	No	No
AWS::SES::ReceiptRuleSet	Yes	Yes	Yes	No	No	No	No	No
AWS::SES::Template	Yes	Yes	Yes	Yes	Yes	Yes	No	No

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::SNS::Topic	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::SQS::Queue	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::SSM::AssociationCompliance	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::SSM::Document	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::SSM::FileData	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::SSM::ManagedInstanceInventory	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::SSM::PatchCompliance	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::SageMaker::AppImageConfig	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::SageMaker::CodeRepository	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::SageMaker::Domain	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::SageMaker::EndpointConfig	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::SageMaker::FeatureGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
AWS::SageMaker::Image	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
AWS::SageMaker::InferenceExperiment	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::SageMaker::Model	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::SageMaker::NotebookInstance	Yes	Yes	Yes	Yes	Yes	Yes	No	No

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::SageMaker::NotebookInstanceLifecycleConfig	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::SageMaker::Workteam	Yes	Yes	Yes	No	No	No	No	No
AWS::SecretsManager::Secret	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::SecurityHub::Standard	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ServiceCatalog::CloudFormationProduct	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ServiceCatalog::Portfolio	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ServiceDiscovery::HttpNamespace	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::ServiceDiscovery::Instance	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::ServiceDiscovery::PublicDnsNamespace	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ServiceDiscovery::Service	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::ShieldRegional::Protection	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::Signer::SigningProfile	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AWS::StepFunctions::Activity	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::StepFunctions::StateMachine	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Transfer::Agreement	Yes	Yes	Yes	Yes	Yes	Yes	No	No

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::Transfer::Certificate	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Transfer::Connector	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Transfer::Profile	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Transfer::Workflow	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::WAFRegional::RateBasedRule	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::WAFRegional::Rule	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::WAFRegional::RuleGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::WAFRegional::WebACL	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	Europe (Ireland)	Europe (Frankfurt)	Europe (London)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Spain)	Europe (Zurich)
AWS::WAFv2::IPSet	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::WAFv2::ManagedRuleSet	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::WAFv2::RegexPatternSet	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::WAFv2::RuleGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::WAFv2::WebACL	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::WorkSpaces::ConnectionAlias	Yes	Yes	Yes	No	No	No	No	No
AWS::WorkSpaces::Workspace	Yes	Yes	Yes	No	No	No	No	No
AWS::XRay::EncryptionConfig	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Asia Pacific Regions

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::ACM::Certificate	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ACMPCA::CertificateAuthority	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::ACMPCA::CertificateAuthorityActivation	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::APS::RuleGroupsNamespace	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::AccessAnalyzer::Analyzer	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::AmazonMQ::Broker	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Amplify::App	Yes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Amplify::Branch	Yes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::ApiGateway::RestApi	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
AWS::ApiGateway::Stage	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
AWS::ApiGatewayV2::Api	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
AWS::ApiGatewayV2::Stage	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
AWS::AppConfig::Application	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::AppConfig::ConfigurationProfile	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::AppConfig::DeploymentStrategy	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::AppConfig::Environment	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::AppConfig::ExtensionAssociation	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::AppConfig::HostedConfigurationVersion	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::AppFlow::Flow	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::AppIntegrations::Application	No	No	No	No	No	No	No	Yes	Yes	Yes	No	No	Yes
AWS::AppIntegrations::EventIntegration	No	No	No	No	No	No	No	Yes	Yes	Yes	No	No	Yes
AWS::AppMesh::GatewayRoute	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::AppMesh::Mesh	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::AppMesh::Route	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::AppMesh::VirtualGateway	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::AppMesh::VirtualNode	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::AppMesh::VirtualRouter	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::AppMesh::VirtualService	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::AppRunner::Service	No	No	No	No	No	Yes	No	No	Yes	Yes	No	No	Yes
AWS::AppRunner::VpcConnector	No	No	No	No	No	Yes	No	No	Yes	Yes	No	No	Yes
AWS::AppStream::Application	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::AppStream::DirectoryConfig	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::AppStream::Fleet	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::AppStream::Stack	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::AppSync::ApiCache	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::AppSync::GraphQLApi	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Athena::DataCatalog	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Athena::PreparedStatement	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Athena::WorkGroup	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::AuditManager::Assessment	No	No	No	No	No	Yes	No	No	Yes	Yes	No	No	Yes
AWS::AutoScaling::AutoScalingGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::AutoScaling::LaunchConfiguration	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::AutoScaling::ScalingPolicy	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::AutoScaling::ScheduledAction	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::AutoScaling::WarmPool	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Backup::BackupPlan	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Backup::BackupSelection	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Backup::BackupVault	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Backup::RecoveryPoint	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Backup::ReportPlan	Yes	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::Batch::ComputeEnvironment	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Batch::JobQueue	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::Batch::SchedulingPolicy	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Bedrock::Guardrail	No	Yes	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
AWS::Bedrock::KnowledgeBase	No	No	No	No	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes
AWS::Cassandra::Keyspace	Yes	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::Cloud9::EnvironmentEC2	Yes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::CloudFormation::Stack	Yes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::CloudTrail::Trail	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::CloudWatch::Alarm	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::CloudWatch::MetricStream	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::CodeArtifact::Repository	No	No	No	No	No	Yes	No	No	Yes	Yes	No	No	Yes
AWS::CodeBuild::Project	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::CodeBuild::ReportGroup	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::CodeDeploy::Application	Yes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::CodeDeploy::DeploymentConfig	Yes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::CodeDeploy::DeploymentGroup	Yes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::CodeGuruProfiler::ProfilingGroup	No	No	No	No	No	No	No	No	Yes	Yes	No	No	Yes
AWS::CodeGuruReviewer::RepositoryAssociation	No	No	No	No	No	No	No	No	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::CodePipeline::Pipeline	Yes	Yes	No	No	Yes	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::Cognito::IdentityPool	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Cognito::UserPool	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Cognito::UserPoolClient	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Cognito::UserPoolGroup	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Config::ConfigurationRecorder	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Config::ConformancePackCompliance	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Config::ResourceCompliance	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Connect::Instance	No	No	No	No	No	No	No	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::Connect::PhoneNumber	No	No	No	No	No	No	No	Yes	Yes	Yes	No	No	Yes
AWS::Connect::QuickConnect	No	No	No	No	No	No	No	Yes	Yes	Yes	No	No	Yes
AWS::Connect::Rule	No	No	No	No	No	No	No	Yes	Yes	Yes	No	No	Yes
AWS::Connect::User	No	No	No	No	No	No	No	Yes	Yes	Yes	No	No	Yes
AWS::CustomerProfiles::Domain	No	No	No	No	No	No	No	Yes	Yes	Yes	No	No	Yes
AWS::CustomerProfiles::ObjectType	No	No	No	No	No	No	No	Yes	Yes	Yes	No	No	Yes
AWS::DMS::Certificate	Yes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::DMS::Endpoint	Yes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::DMS::EventSubscription	Yes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::DMS::ReplicationInstance	Yes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::DMS::ReplicationSubnetGroup	Yes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::DMS::ReplicationTask	Yes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::DataSync::LocationEFS	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::DataSync::LocationFSxLustre	Yes	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::DataSync::LocationFSxWindows	Yes	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::DataSync::LocationHDFS	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::DataSync::LocationNFS	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::DataSync::LocationObjectStorage	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::DataSync::LocationS3	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::DataSync::LocationSMB	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::DataSync::Task	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Detective::Graph	Yes	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::DynamoDB::Table	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::CapacityReservation	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EC2::CarrierGateway	No	No	No	No	No	No	No	Yes	No	Yes	No	No	Yes
AWS::EC2::ClientVpnEndpoint	Yes	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::EC2::ClientVpnTargetNetworkAssociation	Yes	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EC2::CustomerGateway	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::DHCPOptions	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EC2::EC2Fleet	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EC2::EIP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::EIPAssociation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
AWS::EC2::EgressOnlyInternetGateway	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EC2::FlowLog	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EC2::Host	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::EC2::IPAM	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EC2::IPAMPool	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EC2::IPAMResourceDiscovery	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EC2::IPAMResourceDiscoveryAssociation	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EC2::IPAMScope	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EC2::Instance	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::InstanceConnectEndpoint	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EC2::InternetGateway	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::LaunchTemplate	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::EC2::NatGateway	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EC2::NetworkAcl	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::NetworkInsightsAccessScope	Yes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EC2::NetworkInsightsAccessScopeAnalysis	Yes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EC2::NetworkInsightsAnalysis	Yes	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::EC2::NetworkInsightsPath	Yes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EC2::NetworkInterface	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::PrefixList	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::EC2::RegisteredHAInstance	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::EC2::RouteTable	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::SecurityGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::SnapshotBlockPublicAccess	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EC2::SpotFleet	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EC2::Subnet	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::SubnetRouteTableAssociation	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EC2::TrafficMirrorFilter	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EC2::TrafficMirrorSession	Yes	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::EC2::TrafficMirrorTarget	Yes	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EC2::TransitGateway	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EC2::TransitGatewayAttachment	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EC2::TransitGatewayConnect	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EC2::TransitGatewayMulticastDomain	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EC2::TransitGatewayRouteTable	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EC2::VPC	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::EC2::VPCBlockPublicAccessExclusion	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EC2::VPCBlockPublicAccessOptions	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EC2::VPCEndpoint	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::VPCEndpointConnectionNotification	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
AWS::EC2::VPCEndpointService	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::VPCPeeringConnection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::VPNConnection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::VPNConnectionRoute	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::EC2::VPNGateway	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EC2::Volume	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ECR::PullThroughCacheRule	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::ECR::RegistryPolicy	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::ECR::Repository	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::ECS::CapacityProvider	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::ECS::Cluster	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ECS::Service	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ECS::TaskDefinition	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ECS::TaskSet	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::EFS::AccessPoint	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EFS::FileSystem	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EKS::Addon	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EKS::Cluster	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EKS::FargateProfile	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EKS::IdentityProviderConfig	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EMR::SecurityConfiguration	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::ElasticBeanstalk::Application	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::ElasticBeanstalk::ApplicationVersion	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::ElasticBeanstalk::Environment	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::ElasticLoadBalancing::LoadBalancer	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::ElasticLoadBalancingV2::Listener	Yes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::ElasticLoadBalancingV2::LoadBalancer	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Elasticsearch::Domain	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::EventSchemas::Discoverer	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EventSchemas::Registry	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::EventSchemas::RegistryPolicy	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::EventSchemas::Schema	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Events::ApiDestination	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Events::Archive	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Events::Connection	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Events::Endpoint	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Events::EventBus	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Events::Rule	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Evidently::Launch	No	No	No	No	No	No	No	No	Yes	Yes	No	No	Yes
AWS::Evidently::Project	No	No	No	No	No	No	No	No	Yes	Yes	No	No	Yes
AWS::Evidently::Segment	No	No	No	No	No	No	No	No	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::FIS::ExperimentTemplate	Yes	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::Forecast::Dataset	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::Forecast::DatasetGroup	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::FraudDetector::EntityType	No	No	No	No	No	No	No	No	Yes	Yes	No	No	No
AWS::FraudDetector::Label	No	No	No	No	No	No	No	No	Yes	Yes	No	No	No
AWS::FraudDetector::Outcome	No	No	No	No	No	No	No	No	Yes	Yes	No	No	No
AWS::FraudDetector::Variable	No	No	No	No	No	No	No	No	Yes	Yes	No	No	No
AWS::Glue::Classifier	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Glue::Job	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::Glue::MLTransform	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Grafana::Workspace	No	No	No	No	No	No	No	Yes	Yes	Yes	No	No	Yes
AWS::GreengrassV2::ComponentVersion	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::GroundStation::Config	No	No	No	No	No	No	No	Yes	Yes	Yes	No	No	No
AWS::GroundStation::DataflowEndpointGroup	No	No	No	No	No	No	No	Yes	Yes	Yes	No	No	No
AWS::GroundStation::MissionProfile	No	No	No	No	No	No	No	Yes	Yes	Yes	No	No	No
AWS::GuardDuty::Detector	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::GuardDuty::Filter	Yes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::GuardDuty::IPSet	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::GuardDuty::ThreatIntelSet	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::HealthLake::FHIRDatastore	No	No	No	No	No	Yes	No	No	No	No	No	No	No
AWS::IAM::Group	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::IAM::Policy	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::IAM::Role	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::IAM::User	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::IVS::Channel	No	No	No	No	No	Yes	No	Yes	No	No	No	No	Yes
AWS::IVS::PlaybackKeyPair	No	No	No	No	No	Yes	No	Yes	No	No	No	No	Yes
AWS::IVS::RecordingConfiguration	No	No	No	No	No	Yes	No	Yes	No	No	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::ImageBuilder::ContainerRecipe	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::ImageBuilder::DistributionConfiguration	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::ImageBuilder::ImagePipeline	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::ImageBuilder::ImageRecipe	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::ImageBuilder::InfrastructureConfiguration	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::InspectorV2::Activation	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::InspectorV2::Filter	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::IoT::AccountAuditConfiguration	Yes	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::IoT::Authorizer	Yes	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::IoT::CACertificate	Yes	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::IoT::CustomMetric	Yes	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::IoT::Dimension	Yes	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::IoT::FleetMetric	Yes	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::IoT::JobTemplate	Yes	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::IoT::MitigationAction	Yes	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::IoT::Policy	Yes	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::IoT::ProvisioningTemplate	Yes	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::IoT::RoleAlias	Yes	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::IoT::ScheduledAudit	Yes	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::IoT::SecurityProfile	Yes	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::IoTAnalytics::Channel	No	No	No	No	No	Yes	No	No	No	Yes	No	No	Yes
AWS::IoTAnalytics::Dataset	No	No	No	No	No	Yes	No	No	No	Yes	No	No	Yes
AWS::IoTAnalytics::Datastore	No	No	No	No	No	Yes	No	No	No	Yes	No	No	Yes
AWS::IoTAnalytics::Pipeline	No	No	No	No	No	Yes	No	No	No	Yes	No	No	Yes
AWS::IoTEvents::AlarmModel	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::IoTEvents::DetectorModel	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::IoTEvents::Input	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::IoTSiteWise::AssetModel	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::IoTSiteWise::Dashboard	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::IoTSiteWise::Gateway	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::IoTSiteWise::Portal	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::IoTSiteWise::Project	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::IoTTwinMaker::ComponentType	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::IoTTwinMaker::Entity	No	No	No	No	No	No	No	No	Yes	Yes	No	No	No
AWS::IoTTwinMaker::Scene	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::IoTTwinMaker::SyncJob	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::IoTTwinMaker::Workspace	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::IoTWireless::FuotaTask	No	No	No	No	No	No	No	No	No	Yes	No	No	Yes
AWS::IoTWireless::MulticastGroup	No	No	No	No	No	No	No	No	No	Yes	No	No	Yes
AWS::IoTWireless::ServiceProfile	No	No	No	No	No	No	No	No	No	Yes	No	No	Yes
AWS::KMS::Alias	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::KMS::Key	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::KafkaConnect::Connector	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::Kendra::Index	No	No	No	No	No	Yes	No	No	Yes	Yes	No	No	Yes
AWS::Kinesis::Stream	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::Kinesis::StreamConsumer	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::KinesisAnalyticsV2::Application	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::KinesisFirehose::DeliveryStream	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::KinesisVideo::SignalingChannel	Yes	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::KinesisVideo::Stream	Yes	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::Lambda::CodeSigningConfig	Yes	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::Lambda::Function	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Lex::Bot	No	No	No	No	No	No	No	Yes	Yes	Yes	No	No	Yes
AWS::Lex::BotAlias	No	No	No	No	No	No	No	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::Lightsail::Bucket	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::Lightsail::Certificate	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::Lightsail::Disk	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::Lightsail::StaticIp	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::Logs::Destination	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::LookoutMetrics::Alert	No	No	No	No	No	No	No	No	Yes	Yes	No	No	Yes
AWS::LookoutVision::Project	No	No	No	No	No	No	No	Yes	No	No	No	No	Yes
AWS::M2::Environment	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::MSK::BatchScramSecret	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::MSK::Cluster	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::MSK::ClusterPolicy	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::MSK::Configuration	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::MSK::VpcConnection	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Macie::Session	Yes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::MediaConnect::FlowEntitlement	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::MediaConnect::FlowSource	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::MediaConnect::FlowVpcInterface	Yes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::MediaConnect::Gateway	Yes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::MediaPackage::PackagingConfiguration	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::MediaPackage::PackagingGroup	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::MediaTailor::PlaybackConfiguration	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::MemoryDB::SubnetGroup	Yes	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::NetworkFirewall::Firewall	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
AWS::NetworkFirewall::FirewallPolicy	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
AWS::NetworkFirewall::RuleGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
AWS::NetworkFirewall::TLSInspectionConfiguration	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
AWS::NetworkFirewall::VpcEndpointAssociation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::OpenSearch::Domain	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::OpenSearchServerless::Collection	No	No	No	No	No	Yes	No	No	Yes	Yes	No	No	Yes
AWS::OpenSearchServerless::VpcEndpoint	No	No	No	No	No	Yes	No	No	Yes	Yes	No	No	Yes
AWS::Panorama::Package	No	No	No	No	No	No	No	No	Yes	Yes	No	No	No
AWS::Personalize::Dataset	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::Personalize::DatasetGroup	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::Personalize::Schema	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::Personalize::Solution	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::Pinpoint::App	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::Pinpoint::ApplicationSettings	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::Pinpoint::Campaign	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::Pinpoint::EmailChannel	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::Pinpoint::EmailTemplate	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::Pinpoint::EventStream	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::Pinpoint::InAppTemplate	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::Pinpoint::Segment	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::QLDB::Ledger	No	No	No	No	No	No	No	Yes	Yes	Yes	No	No	Yes
AWS::QuickSight::DataSource	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::QuickSight::Template	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::QuickSight::Theme	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::RDS::DBCluster	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::RDS::DBClusterSnapshot	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::RDS::DBInstance	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::RDS::DBSecurityGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::RDS::DBSnapshot	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::RDS::DBSubnetGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::RDS::EventSubscription	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::RDS::GlobalCluster	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::RDS::OptionGroup	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::RUM::AppMonitor	No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Redshift::Cluster	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Redshift::ClusterParameterGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Redshift::ClusterSecurityGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Redshift::ClusterSnapshot	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Redshift::ClusterSubnetGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Redshift::EndpointAccess	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::Redshift::EndpointAuthorization	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::Redshift::EventSubscription	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::Redshift::ScheduledAction	Yes	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::ResilienceHub::App	Yes	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::ResilienceHub::ResiliencyPolicy	Yes	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::ResourceExplorer2::Index	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::RoboMaker::RobotApplication	No	No	No	No	No	No	No	No	Yes	No	No	No	Yes
AWS::RoboMaker::RobotApplicationVersion	No	No	No	No	No	No	No	No	Yes	No	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::RoboMaker::SimulationApplication	No	No	No	No	No	No	No	No	Yes	No	No	No	Yes
AWS::Route53Profiles::Profile	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Route53Resolver::FirewallDomainList	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Route53Resolver::FirewallRuleGroup	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Route53Resolver::FirewallRuleGroupAssociation	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Route53Resolver::ResolverEndpoint	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::Route53Resolver::ResolverQueryLoggingConfig	Yes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	Yes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Route53Resolver::ResolverRule	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Route53Resolver::ResolverRuleAssociation	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::S3::AccessPoint	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::S3::AccountPublicAccessBlock	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::S3::Bucket	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::S3::StorageLens	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::S3::StorageLensGroup	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::S3Express::BucketPolicy	No	No	No	No	No	Yes	No	No	No	No	No	No	Yes
AWS::S3Express::DirectoryBucket	No	No	No	No	No	Yes	No	No	No	No	No	No	Yes
AWS::SES::ConfigurationSet	No	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::SES::ContactList	No	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::SES::ReceiptFilter	No	No	Yes	No	No	No	No	No	Yes	Yes	No	No	Yes
AWS::SES::ReceiptRuleSet	No	No	Yes	No	No	No	No	No	Yes	Yes	No	No	Yes
AWS::SES::Template	No	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::SNS::Topic	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::SQS::Queue	Yes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::SSM::AssociationCompliance	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No	Yes	Yes
AWS::SSM::Document	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::SSM::FileData	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No	Yes	Yes
AWS::SSM::ManagedInstanceInventory	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
AWS::SSM::PatchCompliance	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No	Yes	Yes
AWS::SageMaker::AppImageConfig	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::SageMaker::CodeRepository	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::SageMaker::Domain	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::SageMaker::EndpointConfig	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::SageMaker::FeatureGroup	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::SageMaker::Image	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::SageMaker::InferenceExperiment	Yes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::SageMaker::Model	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::SageMaker::NotebookInstance	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::SageMaker::NotebookInstanceLifecycleConfig	Yes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::SageMaker::Workteam	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::SecretsManager::Secret	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AWS::SecurityHub::Standard	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
AWS::ServiceCatalog::CloudFormationProduct	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::ServiceCatalog::Portfolio	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::ServiceDiscovery::HttpNamespace	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::ServiceDiscovery::Instance	Yes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::ServiceDiscovery::PublicDnsNamespace	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::ServiceDiscovery::Service	Yes	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::ShieldRegional::Protection	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Signer::SigningProfile	Yes	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::StepFunctions::Activity	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::StepFunctions::StateMachine	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Transfer::Agreement	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Transfer::Certificate	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Transfer::Connector	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::Transfer::Profile	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::Transfer::Workflow	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::WAFRegional::RateBasedRule	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::WAFRegional::Rule	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::WAFRegional::RuleGroup	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::WAFRegional::WebACL	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
AWS::WAFv2::IPSet	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
AWS::WAFv2::ManagedRuleSet	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
AWS::WAFv2::RegexPatternSet	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes

Resource type	Asia Pacific (Hong Kong)	Asia Pacific (Hyderabad)	Asia Pacific (Jakarta)	Asia Pacific (Malaysia)	Asia Pacific (Melbourne)	Asia Pacific (Mumbai)	Asia Pacific (Osaka)	Asia Pacific (Seoul)	Asia Pacific (Singapore)	Asia Pacific (Sydney)	Asia Pacific (Taipei)	Asia Pacific (Thailand)	Asia Pacific (Tokyo)
AWS::WAFv2::RuleGroup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
AWS::WAFv2::WebACL	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
AWS::WorkSpaces::ConnectionAlias	No	No	No	No	No	No	No	Yes	Yes	Yes	No	No	Yes
AWS::WorkSpaces::Workspace	No	No	No	No	No	Yes	No	Yes	Yes	Yes	No	No	Yes
AWS::XRay::EncryptionConfig	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes

China Regions

Resource type	China (Beijing)	China (Ningxia)
AWS::ACM::Certificate	Yes	Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::AmazonMQ::Broker	 Yes	 Yes
AWS::ApiGateway::RestApi	 Yes	 Yes
AWS::ApiGateway::Stage	 Yes	 Yes
AWS::ApiGatewayV2::Api	 Yes	 Yes
AWS::ApiGatewayV2::Stage	 Yes	 Yes
AWS::AppConfig::Application	 Yes	 Yes
AWS::AppConfig::ConfigurationProfile	 Yes	 Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::AppConfig::DeploymentStrategy	 Yes	 Yes
AWS::AppConfig::Environment	 Yes	 Yes
AWS::AppConfig::ExtensionAssociation	 Yes	 Yes
AWS::AppConfig::HostedConfigurationVersion	 Yes	 Yes
AWS::AppSync::ApiCache	 Yes	 Yes
AWS::AppSync::GraphQLApi	 Yes	 Yes
AWS::Athena::DataCatalog	 Yes	 Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::Athena::PreparedStatement	 Yes	 Yes
AWS::Athena::WorkGroup	 Yes	 Yes
AWS::AutoScaling::AutoScalingGroup	 Yes	 Yes
AWS::AutoScaling::LaunchConfiguration	 Yes	 Yes
AWS::AutoScaling::ScalingPolicy	 Yes	 Yes
AWS::AutoScaling::ScheduledAction	 Yes	 Yes
AWS::AutoScaling::WarmPool	 Yes	 Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::Backup::BackupPlan	 Yes	 Yes
AWS::Backup::BackupSelection	 Yes	 Yes
AWS::Backup::BackupVault	 Yes	 Yes
AWS::Backup::RecoveryPoint	 Yes	 Yes
AWS::Batch::ComputeEnvironment	 Yes	 Yes
AWS::Batch::JobQueue	 Yes	 Yes
AWS::Batch::SchedulingPolicy	 Yes	 Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::Cassandra::Keyspace	 Yes	 Yes
AWS::CloudFormation::Stack	 Yes	 Yes
AWS::CloudTrail::Trail	 Yes	 Yes
AWS::CloudWatch::Alarm	 Yes	 Yes
AWS::CloudWatch::MetricStream	 Yes	 Yes
AWS::CodeBuild::Project	 Yes	 Yes
AWS::CodeBuild::ReportGroup	 Yes	 Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::Cognito::IdentityPool	 Yes	 No
AWS::Config::ConfigurationRecorder	 Yes	 Yes
AWS::Config::ResourceCompliance	 Yes	 Yes
AWS::DMS::Certificate	 Yes	 Yes
AWS::DMS::Endpoint	 Yes	 Yes
AWS::DMS::EventSubscription	 Yes	 Yes
AWS::DMS::ReplicationInstance	 Yes	 Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::DMS::ReplicationSubnetGroup	 Yes	 Yes
AWS::DMS::ReplicationTask	 Yes	 Yes
AWS::DataSync::LocationEFS	 Yes	 Yes
AWS::DataSync::LocationHDFS	 Yes	 Yes
AWS::DataSync::LocationNFS	 Yes	 Yes
AWS::DataSync::LocationObjectStorage	 Yes	 Yes
AWS::DataSync::LocationS3	 Yes	 Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::DataSync::LocationSMB	Yes	Yes
AWS::DataSync::Task	Yes	Yes
AWS::DynamoDB::Table	Yes	Yes
AWS::EC2::CapacityReservation	Yes	Yes
AWS::EC2::DHCPOptions	Yes	Yes
AWS::EC2::EC2Fleet	Yes	Yes
AWS::EC2::EIP	Yes	Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::EC2::EIPAssociation	 Yes	 Yes
AWS::EC2::FlowLog	 Yes	 Yes
AWS::EC2::Host	 Yes	 Yes
AWS::EC2::Instance	 Yes	 Yes
AWS::EC2::InternetGateway	 Yes	 Yes
AWS::EC2::LaunchTemplate	 Yes	 Yes
AWS::EC2::NatGateway	 Yes	 Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::EC2::NetworkAcl	 Yes	 Yes
AWS::EC2::NetworkInterface	 Yes	 Yes
AWS::EC2::PrefixList	 Yes	 Yes
AWS::EC2::RouteTable	 Yes	 Yes
AWS::EC2::SecurityGroup	 Yes	 Yes
AWS::EC2::SnapshotBlockPublicAccess	 Yes	 Yes
AWS::EC2::SpotFleet	 Yes	 Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::EC2::Subnet	 Yes	 Yes
AWS::EC2::SubnetRouteTableAssociation	 Yes	 Yes
AWS::EC2::TrafficMirrorFilter	 Yes	 Yes
AWS::EC2::TrafficMirrorSession	 Yes	 Yes
AWS::EC2::TrafficMirrorTarget	 Yes	 Yes
AWS::EC2::TransitGateway	 Yes	 Yes
AWS::EC2::TransitGatewayAttachment	 Yes	 Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::EC2::TransitGatewayConnect	 Yes	 Yes
AWS::EC2::TransitGatewayMulticastDomain	 Yes	 Yes
AWS::EC2::TransitGatewayRouteTable	 Yes	 Yes
AWS::EC2::VPC	 Yes	 Yes
AWS::EC2::VPCBlockPublicAccessExclusion	 Yes	 Yes
AWS::EC2::VPCBlockPublicAccessOptions	 Yes	 Yes
AWS::EC2::VPCEndpoint	 Yes	 Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::EC2::VPCEndpointConnectionNotification	 Yes	 Yes
AWS::EC2::VPCEndpointService	 Yes	 Yes
AWS::EC2::VPCPeeringConnection	 Yes	 Yes
AWS::EC2::VPNGateway	 Yes	 No
AWS::EC2::Volume	 Yes	 Yes
AWS::ECR::Repository	 Yes	 Yes
AWS::ECS::CapacityProvider	 Yes	 Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::ECS::Cluster	 Yes	 Yes
AWS::ECS::Service	 Yes	 Yes
AWS::ECS::TaskDefinition	 Yes	 Yes
AWS::ECS::TaskSet	 Yes	 Yes
AWS::EFS::AccessPoint	 Yes	 Yes
AWS::EFS::FileSystem	 Yes	 Yes
AWS::EKS::Addon	 Yes	 Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::EKS::Cluster	 Yes	 Yes
AWS::EKS::FargateProfile	 Yes	 Yes
AWS::EKS::IdentityProviderConfig	 Yes	 Yes
AWS::EMR::SecurityConfiguration	 Yes	 Yes
AWS::ElasticBeanstalk::Application	 Yes	 Yes
AWS::ElasticBeanstalk::ApplicationVersion	 Yes	 Yes
AWS::ElasticBeanstalk::Environment	 Yes	 Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::ElasticLoadBalancing::LoadBalancer	 Yes	 Yes
AWS::ElasticLoadBalancingV2::Listener	 Yes	 Yes
AWS::ElasticLoadBalancingV2::LoadBalancer	 Yes	 Yes
AWS::Elasticsearch::Domain	 Yes	 Yes
AWS::Events::Archive	 Yes	 Yes
AWS::Events::EventBus	 Yes	 Yes
AWS::Events::Rule	 Yes	 Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::Glue::Classifier	Yes	Yes
AWS::Glue::Job	Yes	Yes
AWS::Glue::MLTransform	Yes	No
AWS::GreengrassV2::ComponentVersion	Yes	No
AWS::GuardDuty::Filter	Yes	Yes
AWS::GuardDuty::ThreatIntelSet	Yes	Yes
AWS::IAM::Group	Yes	Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::IAM::InstanceProfile	 Yes	 No
AWS::IAM::OIDCProvider	 Yes	 No
AWS::IAM::Policy	 Yes	 Yes
AWS::IAM::Role	 Yes	 Yes
AWS::IAM::SAMLProvider	 Yes	 No
AWS::IAM::ServerCertificate	 Yes	 No
AWS::IAM::User	 Yes	 Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::ImageBuilder::ContainerRecipe	 Yes	 Yes
AWS::ImageBuilder::DistributionConfiguration	 Yes	 Yes
AWS::ImageBuilder::ImagePipeline	 Yes	 Yes
AWS::ImageBuilder::ImageRecipe	 Yes	 Yes
AWS::ImageBuilder::InfrastructureConfiguration	 Yes	 Yes
AWS::InspectorV2::Activation	 Yes	 Yes
AWS::IoT::AccountAuditConfiguration	 Yes	 Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::IoT::Authorizer	 Yes	 Yes
AWS::IoT::CACertificate	 Yes	 Yes
AWS::IoT::CustomMetric	 Yes	 Yes
AWS::IoT::Dimension	 Yes	 Yes
AWS::IoT::FleetMetric	 Yes	 Yes
AWS::IoT::JobTemplate	 Yes	 Yes
AWS::IoT::MitigationAction	 Yes	 Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::IoT::Policy	 Yes	 Yes
AWS::IoT::ProvisioningTemplate	 Yes	 Yes
AWS::IoT::RoleAlias	 Yes	 Yes
AWS::IoT::ScheduledAudit	 Yes	 Yes
AWS::IoT::SecurityProfile	 Yes	 Yes
AWS::IoTAnalytics::Channel	 Yes	 No
AWS::IoTAnalytics::Dataset	 Yes	 No

Resource type	China (Beijing)	China (Ningxia)
AWS::IoTAnalytics::Datastore	 Yes	 No
AWS::IoTAnalytics::Pipeline	 Yes	 No
AWS::IoTEvents::AlarmModel	 Yes	 No
AWS::IoTEvents::DetectorModel	 Yes	 No
AWS::IoTEvents::Input	 Yes	 No
AWS::IoTSiteWise::AssetModel	 Yes	 No
AWS::IoTSiteWise::Dashboard	 Yes	 No

Resource type	China (Beijing)	China (Ningxia)
AWS::IoTSiteWise::Gateway	 Yes	 No
AWS::IoTSiteWise::Portal	 Yes	 No
AWS::IoTSiteWise::Project	 Yes	 No
AWS::KMS::Alias	 Yes	 Yes
AWS::KMS::Key	 Yes	 Yes
AWS::Kinesis::Stream	 Yes	 Yes
AWS::Kinesis::StreamConsumer	 Yes	 Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::KinesisAnalyticsV2::Application	 Yes	 Yes
AWS::KinesisFirehose::DeliveryStream	 Yes	 Yes
AWS::Lambda::Function	 Yes	 No
AWS::Logs::Destination	 Yes	 Yes
AWS::MSK::BatchScramSecret	 Yes	 Yes
AWS::MSK::Cluster	 Yes	 Yes
AWS::MSK::ClusterPolicy	 Yes	 Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::MSK::Configuration	Yes	Yes
AWS::MSK::VpcConnection	Yes	Yes
AWS::NetworkFirewall::Firewall	Yes	Yes
AWS::NetworkFirewall::FirewallPolicy	Yes	Yes
AWS::NetworkFirewall::RuleGroup	Yes	Yes
AWS::NetworkFirewall::TLSInspectionConfiguration	Yes	Yes
AWS::NetworkFirewall::VpcEndpointAssociation	Yes	Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::OpenSearch::Domain	 Yes	 Yes
AWS::Personalize::Dataset	 Yes	 No
AWS::Personalize::DatasetGroup	 Yes	 No
AWS::Personalize::Schema	 Yes	 No
AWS::Personalize::Solution	 Yes	 No
AWS::RDS::DBCluster	 No	 Yes
AWS::RDS::DBClusterSnapshot	 Yes	 Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::RDS::DBInstance	 Yes	 Yes
AWS::RDS::DBSecurityGroup	 Yes	 Yes
AWS::RDS::DBSnapshot	 Yes	 Yes
AWS::RDS::DBSubnetGroup	 Yes	 Yes
AWS::RDS::EventSubscription	 Yes	 Yes
AWS::RDS::OptionGroup	 Yes	 Yes
AWS::Redshift::Cluster	 Yes	 Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::Redshift::ClusterParameterGroup	 Yes	 Yes
AWS::Redshift::ClusterSecurityGroup	 Yes	 Yes
AWS::Redshift::ClusterSnapshot	 Yes	 Yes
AWS::Redshift::ClusterSubnetGroup	 Yes	 Yes
AWS::Redshift::EventSubscription	 Yes	 Yes
AWS::Route53Profiles::Profile	 Yes	 Yes
AWS::Route53Resolver::FirewallDomainList	 Yes	 Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::Route53Resolver::FirewallRuleGroupAssociation	Yes	Yes
AWS::Route53Resolver::ResolverEndpoint	Yes	Yes
AWS::Route53Resolver::ResolverQueryLoggingConfig	Yes	Yes
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	Yes	Yes
AWS::Route53Resolver::ResolverRule	Yes	Yes
AWS::Route53Resolver::ResolverRuleAssociation	Yes	Yes
AWS::S3::AccessPoint	Yes	Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::S3::AccountPublicAccessBlock	 Yes	 Yes
AWS::S3::Bucket	 Yes	 Yes
AWS::S3::StorageLensGroup	 Yes	 Yes
AWS::SES::ConfigurationSet	 No	 Yes
AWS::SES::ContactList	 No	 Yes
AWS::SES::Template	 No	 Yes
AWS::SNS::Topic	 Yes	 Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::SQS::Queue	 Yes	 Yes
AWS::SSM::AssociationCompliance	 Yes	 Yes
AWS::SSM::Document	 Yes	 Yes
AWS::SSM::FileData	 Yes	 Yes
AWS::SSM::ManagedInstanceInventory	 Yes	 Yes
AWS::SSM::PatchCompliance	 Yes	 Yes
AWS::SageMaker::AppImageConfig	 Yes	 Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::SageMaker::CodeRepository	 Yes	 Yes
AWS::SageMaker::Domain	 Yes	 Yes
AWS::SageMaker::EndpointConfig	 Yes	 Yes
AWS::SageMaker::FeatureGroup	 Yes	 Yes
AWS::SageMaker::Image	 Yes	 Yes
AWS::SageMaker::Model	 Yes	 Yes
AWS::SageMaker::NotebookInstance	 Yes	 Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::SageMaker::NotebookInstanceLifecycleConfig	 Yes	 Yes
AWS::SecretsManager::Secret	 Yes	 Yes
AWS::SecurityHub::Standard	 Yes	 Yes
AWS::ServiceCatalog::CloudFormationProduct	 Yes	 Yes
AWS::ServiceCatalog::CloudFormationProvisionedProduct	 Yes	 Yes
AWS::ServiceCatalog::Portfolio	 Yes	 Yes
AWS::ServiceDiscovery::HttpNamespace	 Yes	 Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::ServiceDiscovery::Instance	 Yes	 Yes
AWS::ServiceDiscovery::PublicDnsNamespace	 Yes	 Yes
AWS::ServiceDiscovery::Service	 Yes	 Yes
AWS::StepFunctions::Activity	 Yes	 No
AWS::StepFunctions::StateMachine	 Yes	 Yes
AWS::Transfer::Agreement	 Yes	 Yes
AWS::Transfer::Certificate	 Yes	 Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::Transfer::Connector	 Yes	 Yes
AWS::Transfer::Profile	 Yes	 Yes
AWS::Transfer::Workflow	 Yes	 Yes
AWS::WAFRegional::RateBasedRule	 Yes	 Yes
AWS::WAFRegional::Rule	 Yes	 Yes
AWS::WAFRegional::RuleGroup	 Yes	 Yes
AWS::WAFRegional::WebACL	 Yes	 Yes

Resource type	China (Beijing)	China (Ningxia)
AWS::WAFv2::IPSet	 Yes	 Yes
AWS::WAFv2::ManagedRuleSet	 Yes	 Yes
AWS::WAFv2::RegexPatternSet	 Yes	 Yes
AWS::WAFv2::RuleGroup	 Yes	 Yes
AWS::WAFv2::WebACL	 Yes	 Yes
AWS::WorkSpaces::Workspace	 No	 Yes

Africa and Middle East Regions

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::ACM::Certificate	 Yes	 Yes	 Yes	 Yes
AWS::ACMPCA::CertificateAuthority	 Yes	 Yes	 Yes	 Yes
AWS::ACMPCA::Certificateauthorityactivation	 Yes	 Yes	 Yes	 Yes
AWS::AccessAnalyzer::Analyzer	 Yes	 Yes	 Yes	 Yes
AWS::AmazonMQ::Broker	 Yes	 No	 Yes	 Yes
AWS::Amplify::App	 No	 No	 Yes	 No

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::Amplify::Branch	 No	 No	 Yes	 No
AWS::ApiGateway::RestApi	 Yes	 Yes	 Yes	 Yes
AWS::ApiGateway::Stage	 Yes	 Yes	 Yes	 Yes
AWS::ApiGatewayV2::Api	 Yes	 Yes	 Yes	 Yes
AWS::ApiGatewayV2::Stage	 Yes	 Yes	 Yes	 Yes
AWS::AppConfig::Application	 Yes	 Yes	 Yes	 No

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::AppConfig::ConfigurationProfile	 Yes	 Yes	 Yes	 No
AWS::AppConfig::DeploymentStrategy	 Yes	 Yes	 Yes	 Yes
AWS::AppConfig::Environment	 Yes	 Yes	 Yes	 No
AWS::AppConfig::ExtensionAssociation	 Yes	 Yes	 Yes	 Yes
AWS::AppConfig::HostedConfigurationVersion	 Yes	 Yes	 Yes	 No
AWS::AppFlow::Flow	 Yes	 No	 No	 No

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::AppIntegrations::Application	 Yes	 No	 No	 No
AWS::AppIntegrations::EventIntegration	 Yes	 No	 No	 No
AWS::AppMesh::GatewayRoute	 Yes	 Yes	 Yes	 No
AWS::AppMesh::Mesh	 Yes	 Yes	 Yes	 No
AWS::AppMesh::Route	 Yes	 Yes	 Yes	 No
AWS::AppMesh::VirtualGateway	 Yes	 Yes	 Yes	 No

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::AppMesh::VirtualNode	 Yes	 Yes	 Yes	 No
AWS::AppMesh::VirtualRouter	 Yes	 Yes	 Yes	 No
AWS::AppMesh::VirtualService	 Yes	 Yes	 Yes	 No
AWS::AppSync::ApiCache	 Yes	 Yes	 Yes	 Yes
AWS::AppSync::GraphQLApi	 Yes	 Yes	 Yes	 Yes
AWS::Athena::DataCatalog	 Yes	 Yes	 Yes	 Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::Athena::PreparedStatement	 Yes	 Yes	 Yes	 Yes
AWS::Athena::WorkGroup	 Yes	 Yes	 Yes	 Yes
AWS::AutoScaling::AutoScalingGroup	 Yes	 Yes	 Yes	 Yes
AWS::AutoScaling::LaunchConfiguration	 Yes	 Yes	 Yes	 Yes
AWS::AutoScaling::ScalingPolicy	 Yes	 Yes	 Yes	 Yes
AWS::AutoScaling::ScheduledAction	 Yes	 Yes	 Yes	 Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::AutoScaling::WarmPool	 Yes	 No	 Yes	 No
AWS::Backup::BackupPlan	 Yes	 Yes	 Yes	 Yes
AWS::Backup::BackupSelection	 Yes	 Yes	 Yes	 Yes
AWS::Backup::BackupVault	 Yes	 Yes	 Yes	 Yes
AWS::Backup::RecoveryPoint	 Yes	 Yes	 Yes	 Yes
AWS::Backup::ReportPlan	 Yes	 No	 Yes	 No

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::Batch::ComputeEnvironment	 Yes	 No	 Yes	 Yes
AWS::Batch::JobQueue	 Yes	 No	 Yes	 Yes
AWS::Batch::SchedulingPolicy	 Yes	 Yes	 Yes	 Yes
AWS::Cassandra::Keyspace	 No	 No	 Yes	 No
AWS::Cloud9::EnvironmentEC2	 Yes	 No	 Yes	 No
AWS::CloudFormation::Stack	 Yes	 No	 Yes	 No

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::CloudTrail::Trail	 Yes	 Yes	 Yes	 Yes
AWS::CloudWatch::Alarm	 Yes	 Yes	 Yes	 Yes
AWS::CloudWatch::MetricStream	 Yes	 Yes	 Yes	 Yes
AWS::CodeBuild::Project	 Yes	 Yes	 Yes	 Yes
AWS::CodeBuild::ReportGroup	 Yes	 Yes	 Yes	 Yes
AWS::CodeDeploy::Application	 Yes	 No	 Yes	 No

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::CodeDeploy::DeploymentConfig	 Yes	 No	 Yes	 No
AWS::CodeDeploy::DeploymentGroup	 Yes	 No	 Yes	 No
AWS::CodePipeline::Pipeline	 No	 Yes	 No	 Yes
AWS::Cognito::IdentityPool	 Yes	 Yes	 Yes	 Yes
AWS::Cognito::UserPool	 Yes	 Yes	 Yes	 Yes
AWS::Cognito::UserPoolClient	 Yes	 Yes	 Yes	 Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::Cognito::UserPoolGroup	Yes	Yes	Yes	Yes
AWS::Config::ConfigurationRecorder	Yes	Yes	Yes	Yes
AWS::Config::ConformancePackCompliance	Yes	Yes	Yes	Yes
AWS::Config::ResourceCompliance	Yes	Yes	Yes	Yes
AWS::Connect::Instance	Yes	No	No	No
AWS::Connect::PhoneNumber	Yes	No	No	No

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::Connect::QuickConnect	 Yes	 No	 No	 No
AWS::Connect::Rule	 Yes	 No	 No	 No
AWS::Connect::User	 Yes	 No	 No	 No
AWS::CustomerProfiles::Domain	 Yes	 No	 No	 No
AWS::CustomerProfiles::ObjectType	 Yes	 No	 No	 No
AWS::DMS::Certificate	 Yes	 No	 Yes	 No

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::DMS::Endpoint	 Yes	 No	 Yes	 No
AWS::DMS::EventSubscription	 Yes	 No	 Yes	 No
AWS::DMS::ReplicationInstance	 Yes	 No	 Yes	 No
AWS::DMS::ReplicationSubnetGroup	 Yes	 No	 Yes	 No
AWS::DMS::ReplicationTask	 Yes	 No	 Yes	 No
AWS::DataSync::LocationEFS	 Yes	 No	 Yes	 Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::DataSync::LocationFSxLustre	 Yes	 No	 Yes	 No
AWS::DataSync::LocationFSxWindows	 Yes	 No	 Yes	 No
AWS::DataSync::LocationHDFS	 Yes	 No	 Yes	 Yes
AWS::DataSync::LocationNFS	 Yes	 No	 Yes	 Yes
AWS::DataSync::LocationObjectStorage	 Yes	 No	 Yes	 Yes
AWS::DataSync::LocationS3	 Yes	 Yes	 Yes	 Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::DataSync::LocationSMB	 Yes	 No	 Yes	 Yes
AWS::DataSync::Task	 Yes	 Yes	 Yes	 Yes
AWS::Detective::Graph	 Yes	 Yes	 Yes	 No
AWS::DynamoDB::Table	 Yes	 Yes	 Yes	 Yes
AWS::EC2::CapacityReservation	 Yes	 Yes	 Yes	 Yes
AWS::EC2::ClientVpnEndpoint	 Yes	 No	 Yes	 No

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::EC2::ClientVpnTargetNetworkAssociation	 Yes	 Yes	 Yes	 No
AWS::EC2::CustomerGateway	 Yes	 Yes	 Yes	 Yes
AWS::EC2::DHCPOptions	 Yes	 Yes	 Yes	 Yes
AWS::EC2::EC2Fleet	 Yes	 No	 Yes	 Yes
AWS::EC2::EIP	 Yes	 Yes	 Yes	 Yes
AWS::EC2::EIPAssociation	 Yes	 Yes	 Yes	 Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::EC2::EgressOnlyInternetGateway	 Yes	 No	 Yes	 Yes
AWS::EC2::FlowLog	 Yes	 No	 Yes	 Yes
AWS::EC2::Host	 Yes	 Yes	 Yes	 Yes
AWS::EC2::IPAM	 Yes	 No	 Yes	 Yes
AWS::EC2::IPAMPool	 Yes	 No	 Yes	 Yes
AWS::EC2::IPAMResourceDiscovery	 Yes	 Yes	 Yes	 Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::EC2::IPAMResourceDiscoveryAssociation	 Yes	 Yes	 Yes	 Yes
AWS::EC2::IPAMScope	 Yes	 No	 Yes	 Yes
AWS::EC2::Instance	 Yes	 Yes	 Yes	 Yes
AWS::EC2::InstanceConnectEndpoint	 Yes	 Yes	 Yes	 Yes
AWS::EC2::InternetGateway	 Yes	 Yes	 Yes	 Yes
AWS::EC2::LaunchTemplate	 Yes	 No	 Yes	 No

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::EC2::NatGateway	 Yes	 No	 Yes	 Yes
AWS::EC2::NetworkAcl	 Yes	 Yes	 Yes	 Yes
AWS::EC2::NetworkInsightsAccessScope	 Yes	 No	 Yes	 No
AWS::EC2::NetworkInsightsAccessScopeAnalysis	 Yes	 No	 Yes	 No
AWS::EC2::NetworkInsightsAnalysis	 Yes	 No	 Yes	 No
AWS::EC2::NetworkInsightsPath	 Yes	 No	 Yes	 No

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::EC2::NetworkInterface	Yes	Yes	Yes	Yes
AWS::EC2::PrefixList	Yes	Yes	Yes	Yes
AWS::EC2::RouteTable	Yes	Yes	Yes	Yes
AWS::EC2::SecurityGroup	Yes	Yes	Yes	Yes
AWS::EC2::SnapshotBlockPublicAccess	Yes	Yes	Yes	Yes
AWS::EC2::SpotFleet	Yes	Yes	Yes	Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::EC2::Subnet	 Yes	 Yes	 Yes	 Yes
AWS::EC2::SubnetRouteTableAssociation	 Yes	 Yes	 Yes	 Yes
AWS::EC2::TrafficMirrorFilter	 Yes	 Yes	 Yes	 Yes
AWS::EC2::TrafficMirrorSession	 No	 No	 Yes	 No
AWS::EC2::TrafficMirrorTarget	 No	 No	 Yes	 No
AWS::EC2::TransitGateway	 Yes	 Yes	 Yes	 Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::EC2::TransitGatewayAttachment	 Yes	 No	 Yes	 Yes
AWS::EC2::TransitGatewayConnect	 Yes	 No	 Yes	 Yes
AWS::EC2::TransitGatewayMulticastDomain	 Yes	 Yes	 Yes	 Yes
AWS::EC2::TransitGatewayRouteTable	 Yes	 No	 Yes	 Yes
AWS::EC2::VPC	 Yes	 Yes	 Yes	 Yes
AWS::EC2::VPCBlockPublicAccessExclusion	 Yes	 Yes	 Yes	 Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::EC2::VPCBlockPublicAccessOptions	 Yes	 Yes	 Yes	 Yes
AWS::EC2::VPCEndpoint	 Yes	 Yes	 Yes	 Yes
AWS::EC2::VPCEndpointConnectionNotification	 Yes	 Yes	 Yes	 Yes
AWS::EC2::VPCEndpointService	 Yes	 Yes	 Yes	 Yes
AWS::EC2::VPCPeeringConnection	 Yes	 Yes	 Yes	 Yes
AWS::EC2::VPNConnection	 Yes	 Yes	 Yes	 Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::EC2::VPNConnectionRoute	 Yes	 Yes	 Yes	 Yes
AWS::EC2::VPNGateway	 Yes	 Yes	 Yes	 Yes
AWS::EC2::Volume	 Yes	 Yes	 Yes	 Yes
AWS::ECR::PullThroughCacheRule	 Yes	 Yes	 Yes	 Yes
AWS::ECR::RegistryPolicy	 Yes	 Yes	 Yes	 Yes
AWS::ECR::Repository	 Yes	 Yes	 Yes	 Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::ECS::CapacityProvider	 Yes	 Yes	 Yes	 Yes
AWS::ECS::Cluster	 Yes	 Yes	 Yes	 Yes
AWS::ECS::Service	 Yes	 Yes	 Yes	 Yes
AWS::ECS::TaskDefinition	 Yes	 Yes	 Yes	 Yes
AWS::ECS::TaskSet	 Yes	 No	 Yes	 Yes
AWS::EFS::AccessPoint	 Yes	 Yes	 Yes	 Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::EFS::FileSystem	 Yes	 Yes	 Yes	 Yes
AWS::EKS::Addon	 Yes	 No	 Yes	 Yes
AWS::EKS::Cluster	 Yes	 No	 Yes	 Yes
AWS::EKS::FargateProfile	 Yes	 Yes	 Yes	 Yes
AWS::EKS::IdentityProviderConfig	 Yes	 No	 Yes	 Yes
AWS::EMR::SecurityConfiguration	 Yes	 Yes	 Yes	 Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::ElasticBeanstalk::Application	 Yes	 No	 Yes	 Yes
AWS::ElasticBeanstalk::ApplicationVersion	 Yes	 No	 Yes	 Yes
AWS::ElasticBeanstalk::Environment	 Yes	 No	 Yes	 Yes
AWS::ElasticLoadBalancing::LoadBalancer	 Yes	 Yes	 Yes	 Yes
AWS::ElasticLoadBalancingV2::Listener	 Yes	 No	 Yes	 No
AWS::ElasticLoadBalancingV2::LoadBalancer	 Yes	 Yes	 Yes	 Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::Elasticsearch::Domain	 Yes	 Yes	 Yes	 Yes
AWS::EventSchemas::Discoverer	 Yes	 No	 Yes	 Yes
AWS::EventSchemas::Registry	 Yes	 No	 Yes	 Yes
AWS::EventSchemas::RegistryPolicy	 Yes	 No	 Yes	 Yes
AWS::EventSchemas::Schema	 Yes	 No	 Yes	 Yes
AWS::Events::ApiDestination	 Yes	 No	 Yes	 Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::Events::Archive	 Yes	 No	 Yes	 Yes
AWS::Events::Connection	 Yes	 No	 Yes	 Yes
AWS::Events::EventBus	 Yes	 Yes	 Yes	 Yes
AWS::Events::Rule	 Yes	 No	 Yes	 No
AWS::FIS::ExperimentTemplate	 Yes	 No	 Yes	 No
AWS::Glue::Classifier	 Yes	 Yes	 Yes	 Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::Glue::Job	 Yes	 Yes	 Yes	 Yes
AWS::Glue::MLTransform	 Yes	 Yes	 Yes	 Yes
AWS::GroundStation::Config	 Yes	 No	 Yes	 No
AWS::GroundStation ::DataflowEndpointGroup	 Yes	 No	 Yes	 No
AWS::GroundStation::MissionProfile	 Yes	 No	 Yes	 No
AWS::GuardDuty::Detector	 Yes	 Yes	 Yes	 Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::GuardDuty::Filter	 Yes	 No	 Yes	 No
AWS::GuardDuty::IPSet	 Yes	 No	 Yes	 Yes
AWS::GuardDuty::ThreatIntelSet	 Yes	 Yes	 Yes	 Yes
AWS::IAM::Group	 Yes	 No	 Yes	 No
AWS::IAM::Policy	 Yes	 No	 Yes	 No
AWS::IAM::Role	 Yes	 No	 Yes	 No

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::IAM::User	 Yes	 No	 Yes	 No
AWS::ImageBuilder::ContainerRecipe	 Yes	 Yes	 Yes	 Yes
AWS::ImageBuilder: :DistributionConfiguration	 Yes	 Yes	 Yes	 Yes
AWS::ImageBuilder::ImagePipeline	 Yes	 Yes	 Yes	 Yes
AWS::ImageBuilder::ImageRecipe	 Yes	 Yes	 Yes	 Yes
AWS::ImageBuilder::Infrastr uctureConfiguration	 Yes	 Yes	 Yes	 Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::InspectorV2::Activation	 Yes	 No	 Yes	 No
AWS::InspectorV2::Filter	 Yes	 No	 Yes	 No
AWS::IoT::AccountAuditConfiguration	 No	 No	 Yes	 Yes
AWS::IoT::Authorizer	 No	 No	 Yes	 Yes
AWS::IoT::CACertificate	 No	 No	 Yes	 Yes
AWS::IoT::CustomMetric	 No	 No	 Yes	 Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::IoT::Dimension	 No	 No	 Yes	 Yes
AWS::IoT::FleetMetric	 No	 No	 Yes	 Yes
AWS::IoT::JobTemplate	 No	 No	 Yes	 Yes
AWS::IoT::MitigationAction	 No	 No	 Yes	 Yes
AWS::IoT::Policy	 No	 No	 Yes	 Yes
AWS::IoT::ProvisioningTemplate	 No	 No	 Yes	 Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::IoT::RoleAlias	No	No	Yes	Yes
AWS::IoT::ScheduledAudit	No	No	Yes	Yes
AWS::IoT::SecurityProfile	No	No	Yes	Yes
AWS::KMS::Alias	Yes	No	Yes	Yes
AWS::KMS::Key	Yes	Yes	Yes	Yes
AWS::Kinesis::Stream	Yes	No	Yes	Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::Kinesis::StreamConsumer	 Yes	 Yes	 Yes	 Yes
AWS::KinesisAnalyticsV2::Application	 Yes	 Yes	 Yes	 Yes
AWS::KinesisFirehose::DeliveryStream	 Yes	 Yes	 Yes	 Yes
AWS::Lambda::CodeSigningConfig	 Yes	 No	 Yes	 No
AWS::Lambda::Function	 Yes	 Yes	 Yes	 Yes
AWS::Lex::Bot	 Yes	 No	 No	 No

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::Lex::BotAlias	 Yes	 No	 No	 No
AWS::Logs::Destination	 Yes	 Yes	 Yes	 Yes
AWS::MSK::BatchScramSecret	 Yes	 No	 Yes	 Yes
AWS::MSK::Cluster	 Yes	 No	 Yes	 Yes
AWS::MSK::ClusterPolicy	 Yes	 Yes	 Yes	 Yes
AWS::MSK::Configuration	 Yes	 Yes	 Yes	 Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::MSK::VpcConnection	Yes	Yes	Yes	Yes
AWS::Macie::Session	Yes	Yes	Yes	No
AWS::MediaConnect::FlowEntitlement	Yes	No	No	Yes
AWS::MediaConnect::FlowSource	Yes	No	No	Yes
AWS::MediaConnect::FlowVpcInterface	Yes	No	No	No
AWS::MediaConnect::Gateway	Yes	No	No	No

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::MediaTailor::PlaybackConfiguration	 Yes	 No	 No	 Yes
AWS::NetworkFirewall::Firewall	 Yes	 Yes	 Yes	 Yes
AWS::NetworkFirewall::FirewallPolicy	 Yes	 Yes	 Yes	 Yes
AWS::NetworkFirewall::RuleGroup	 Yes	 Yes	 Yes	 Yes
AWS::NetworkFirewall::TLSInspectionConfiguration	 Yes	 Yes	 Yes	 Yes
AWS::NetworkFirewall::VpcEndpointAssociation	 Yes	 Yes	 Yes	 Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::OpenSearch::Domain	Yes	No	Yes	No
AWS::RDS::DBCluster	Yes	Yes	Yes	Yes
AWS::RDS::DBClusterSnapshot	Yes	No	Yes	Yes
AWS::RDS::DBInstance	Yes	Yes	Yes	Yes
AWS::RDS::DBSecurityGroup	Yes	Yes	Yes	Yes
AWS::RDS::DBSnapshot	Yes	Yes	Yes	Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::RDS::DBSubnetGroup	 Yes	 Yes	 Yes	 Yes
AWS::RDS::EventSubscription	 Yes	 Yes	 Yes	 Yes
AWS::RDS::GlobalCluster	 Yes	 Yes	 Yes	 Yes
AWS::RDS::OptionGroup	 Yes	 Yes	 Yes	 Yes
AWS::RUM::AppMonitor	 No	 No	 Yes	 Yes
AWS::Redshift::Cluster	 Yes	 Yes	 Yes	 Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::Redshift::ClusterParameterGroup	 Yes	 Yes	 Yes	 Yes
AWS::Redshift::ClusterSecurityGroup	 Yes	 Yes	 Yes	 Yes
AWS::Redshift::ClusterSnapshot	 Yes	 Yes	 Yes	 Yes
AWS::Redshift::ClusterSubnetGroup	 Yes	 Yes	 Yes	 Yes
AWS::Redshift::EventSubscription	 Yes	 Yes	 Yes	 Yes
AWS::Redshift::ScheduledAction	 No	 No	 Yes	 No

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::ResilienceHub::App	 Yes	 No	 Yes	 No
AWS::ResilienceHub::ResiliencyPolicy	 Yes	 No	 Yes	 No
AWS::ResourceExplorer2::Index	 No	 No	 Yes	 Yes
AWS::Route53Profiles::Profile	 Yes	 Yes	 Yes	 Yes
AWS::Route53Resolver::FirewallDomainList	 Yes	 No	 Yes	 No
AWS::Route53Resolver::FirewallRuleGroup	 Yes	 No	 Yes	 No

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::Route53Resolver::FirewallRuleGroupAssociation	 Yes	 No	 Yes	 No
AWS::Route53Resolver::ResolverEndpoint	 Yes	 No	 Yes	 Yes
AWS::Route53Resolver::ResolverQueryLoggingConfig	 Yes	 No	 Yes	 No
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	 Yes	 No	 Yes	 No
AWS::Route53Resolver::ResolverRule	 Yes	 No	 Yes	 Yes
AWS::Route53Resolver::ResolverRuleAssociation	 Yes	 No	 Yes	 Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::S3::AccessPoint	 Yes	 Yes	 Yes	 Yes
AWS::S3::AccountPublicAccessBlock	 Yes	 No	 Yes	 Yes
AWS::S3::Bucket	 Yes	 Yes	 Yes	 Yes
AWS::SES::ConfigurationSet	 Yes	 Yes	 Yes	 No
AWS::SES::ContactList	 Yes	 Yes	 Yes	 No
AWS::SES::Template	 Yes	 Yes	 Yes	 No

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::SNS::Topic	 Yes	 Yes	 Yes	 Yes
AWS::SQS::Queue	 Yes	 No	 Yes	 No
AWS::SSM::AssociationCompliance	 Yes	 Yes	 Yes	 Yes
AWS::SSM::Document	 Yes	 Yes	 Yes	 Yes
AWS::SSM::FileData	 Yes	 Yes	 Yes	 Yes
AWS::SSM::ManagedInstanceInventory	 Yes	 Yes	 Yes	 Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::SSM::PatchCompliance	 Yes	 Yes	 Yes	 Yes
AWS::SageMaker::AppImageConfig	 Yes	 Yes	 Yes	 Yes
AWS::SageMaker::CodeRepository	 Yes	 No	 Yes	 No
AWS::SageMaker::Domain	 Yes	 No	 Yes	 No
AWS::SageMaker::EndpointConfig	 Yes	 No	 Yes	 No
AWS::SageMaker::FeatureGroup	 Yes	 Yes	 Yes	 No

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::SageMaker::Image	 Yes	 Yes	 Yes	 Yes
AWS::SageMaker::InferenceExperiment	 Yes	 No	 Yes	 No
AWS::SageMaker::Model	 Yes	 No	 Yes	 No
AWS::SageMaker::NotebookInstance	 Yes	 No	 Yes	 No
AWS::SageMaker::NotebookInstanceLifecycleConfig	 Yes	 No	 Yes	 No
AWS::SecretsManager::Secret	 Yes	 Yes	 Yes	 Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::SecurityHub::Standard	 Yes	 Yes	 Yes	 Yes
AWS::ServiceCatalog::CloudFormationProduct	 Yes	 No	 Yes	 Yes
AWS::ServiceCatalog::CloudFormationProvisionedProduct	 Yes	 No	 Yes	 Yes
AWS::ServiceCatalog::Portfolio	 Yes	 No	 Yes	 Yes
AWS::ServiceDiscovery::HttpNamespace	 Yes	 Yes	 Yes	 Yes
AWS::ServiceDiscovery::Instance	 Yes	 No	 Yes	 Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::ServiceDiscovery::PublicDnsNamespace	Yes	Yes	Yes	Yes
AWS::ServiceDiscovery::Service	Yes	No	Yes	Yes
AWS::ShieldRegional::Protection	Yes	No	Yes	Yes
AWS::Signer::SigningProfile	Yes	No	Yes	No
AWS::StepFunctions::Activity	Yes	Yes	Yes	Yes
AWS::StepFunctions::StateMachine	Yes	Yes	Yes	Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::Transfer::Agreement	 Yes	 No	 Yes	 Yes
AWS::Transfer::Certificate	 Yes	 Yes	 Yes	 Yes
AWS::Transfer::Connector	 Yes	 Yes	 Yes	 Yes
AWS::Transfer::Profile	 Yes	 Yes	 Yes	 Yes
AWS::Transfer::Workflow	 Yes	 Yes	 Yes	 Yes
AWS::WAFRegional::RateBasedRule	 Yes	 Yes	 Yes	 Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::WAFRegional::Rule	 Yes	 Yes	 Yes	 Yes
AWS::WAFRegional::RuleGroup	 Yes	 Yes	 Yes	 Yes
AWS::WAFRegional::WebACL	 Yes	 Yes	 Yes	 Yes
AWS::WAFv2::IPSet	 Yes	 Yes	 Yes	 Yes
AWS::WAFv2::ManagedRuleSet	 Yes	 Yes	 Yes	 Yes
AWS::WAFv2::RegexPatternSet	 Yes	 Yes	 Yes	 Yes

Resource type	Africa (Cape Town)	Israel (Tel Aviv)	Middle East (Bahrain)	Middle East (UAE)
AWS::WAFv2::RuleGroup	 Yes	 Yes	 Yes	 Yes
AWS::WAFv2::WebACL	 Yes	 Yes	 Yes	 Yes
AWS::WorkSpaces::Workspace	 Yes	 No	 No	 No
AWS::XRay::EncryptionConfig	 Yes	 Yes	 No	 Yes

GovCloud Regions

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::ACM::Certificate	 Yes	 Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::ACMPCA::CertificateAuthority	Yes	Yes
AWS::ACMPCA::CertificateAuthorityActivation	Yes	Yes
AWS::AccessAnalyzer::Analyzer	Yes	Yes
AWS::AmazonMQ::Broker	Yes	Yes
AWS::ApiGateway::RestApi	Yes	Yes
AWS::ApiGateway::Stage	Yes	Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::ApiGatewayV2::Api	Yes	Yes
AWS::ApiGatewayV2::Stage	Yes	Yes
AWS::AppConfig::Application	Yes	Yes
AWS::AppConfig::ConfigurationProfile	Yes	Yes
AWS::AppConfig::DeploymentStrategy	Yes	Yes
AWS::AppConfig::Environment	Yes	Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::AppConfig::ExtensionAssociation	 Yes	 Yes
AWS::AppConfig::HostedConfigurationVersion	 Yes	 Yes
AWS::AppStream::Application	 Yes	 Yes
AWS::AppStream::DirectoryConfig	 Yes	 No
AWS::AppStream::Fleet	 Yes	 No
AWS::AppStream::Stack	 Yes	 No

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::Athena::DataCatalog	 Yes	 Yes
AWS::Athena::WorkGroup	 Yes	 Yes
AWS::AutoScaling::AutoScalingGroup	 Yes	 Yes
AWS::AutoScaling::LaunchConfiguration	 Yes	 Yes
AWS::AutoScaling::ScalingPolicy	 Yes	 Yes
AWS::AutoScaling::ScheduledAction	 Yes	 Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::AutoScaling::WarmPool	 Yes	 Yes
AWS::Backup::BackupPlan	 Yes	 Yes
AWS::Backup::BackupSelection	 Yes	 Yes
AWS::Backup::BackupVault	 Yes	 Yes
AWS::Backup::RecoveryPoint	 Yes	 Yes
AWS::Batch::ComputeEnvironment	 Yes	 Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::Batch::JobQueue	Yes	Yes
AWS::Batch::SchedulingPolicy	Yes	Yes
AWS::Bedrock::Guardrail	Yes	Yes
AWS::Bedrock::KnowledgeBase	Yes	Yes
AWS::Cassandra::Keyspace	Yes	Yes
AWS::CloudFormation::Stack	Yes	Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::CloudTrail::Trail	 Yes	 Yes
AWS::CloudWatch::Alarm	 Yes	 Yes
AWS::CodeBuild::Project	 Yes	 Yes
AWS::CodeBuild::ReportGroup	 Yes	 Yes
AWS::Cognito::IdentityPool	 Yes	 No
AWS::Cognito::UserPoolGroup	 Yes	 No

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::Config::ConfigurationRecorder	 Yes	 Yes
AWS::Config::ConformancePackCompliance	 Yes	 Yes
AWS::Config::ResourceCompliance	 Yes	 Yes
AWS::Connect::Instance	 Yes	 No
AWS::Connect::QuickConnect	 Yes	 No
AWS::Connect::User	 Yes	 No

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::DMS::Certificate	 Yes	 Yes
AWS::DMS::Endpoint	 Yes	 Yes
AWS::DMS::EventSubscription	 Yes	 Yes
AWS::DMS::ReplicationInstance	 Yes	 Yes
AWS::DMS::ReplicationSubnetGroup	 Yes	 Yes
AWS::DMS::ReplicationTask	 Yes	 Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::DataSync::LocationEFS	 Yes	 Yes
AWS::DataSync::LocationFSxLustre	 Yes	 Yes
AWS::DataSync::LocationFSxWindows	 Yes	 Yes
AWS::DataSync::LocationHDFS	 Yes	 Yes
AWS::DataSync::LocationNFS	 Yes	 Yes
AWS::DataSync::LocationObjectStorage	 Yes	 Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::DataSync::LocationS3	Yes	Yes
AWS::DataSync::LocationSMB	Yes	Yes
AWS::DataSync::Task	Yes	Yes
AWS::Detective::Graph	Yes	Yes
AWS::DynamoDB::Table	Yes	Yes
AWS::EC2::CapacityReservation	Yes	Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::EC2::ClientVpnEndpoint	 Yes	 Yes
AWS::EC2::ClientVpnTargetNetworkAssociation	 Yes	 Yes
AWS::EC2::CustomerGateway	 Yes	 Yes
AWS::EC2::DHCPOptions	 Yes	 Yes
AWS::EC2::EC2Fleet	 Yes	 Yes
AWS::EC2::EIP	 Yes	 Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::EC2::EgressOnlyInternetGateway	 Yes	 Yes
AWS::EC2::FlowLog	 Yes	 Yes
AWS::EC2::Host	 Yes	 Yes
AWS::EC2::IPAM	 Yes	 Yes
AWS::EC2::IPAMPool	 Yes	 Yes
AWS::EC2::IPAMResourceDiscovery	 Yes	 Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::EC2::IPAMResourceDiscoveryAssociation	 Yes	 Yes
AWS::EC2::IPAMScope	 Yes	 Yes
AWS::EC2::Instance	 Yes	 Yes
AWS::EC2::InstanceConnectEndpoint	 Yes	 Yes
AWS::EC2::InternetGateway	 Yes	 Yes
AWS::EC2::LaunchTemplate	 Yes	 Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::EC2::NatGateway	 Yes	 Yes
AWS::EC2::NetworkAcl	 Yes	 Yes
AWS::EC2::NetworkInterface	 Yes	 Yes
AWS::EC2::PrefixList	 Yes	 Yes
AWS::EC2::RouteTable	 Yes	 Yes
AWS::EC2::SecurityGroup	 Yes	 Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::EC2::SnapshotBlockPublicAccess	 Yes	 Yes
AWS::EC2::SpotFleet	 Yes	 Yes
AWS::EC2::Subnet	 Yes	 Yes
AWS::EC2::SubnetRouteTableAssociation	 Yes	 Yes
AWS::EC2::TrafficMirrorFilter	 Yes	 Yes
AWS::EC2::TrafficMirrorSession	 Yes	 Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::EC2::TrafficMirrorTarget	 Yes	 Yes
AWS::EC2::TransitGateway	 Yes	 No
AWS::EC2::TransitGatewayAttachment	 Yes	 Yes
AWS::EC2::TransitGatewayConnect	 Yes	 Yes
AWS::EC2::TransitGatewayMulticastDomain	 Yes	 Yes
AWS::EC2::TransitGatewayRouteTable	 Yes	 Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::EC2::VPC	 Yes	 Yes
AWS::EC2::VPCBlockPublicAccessExclusion	 Yes	 Yes
AWS::EC2::VPCBlockPublicAccessOptions	 Yes	 Yes
AWS::EC2::VPCEndpoint	 Yes	 Yes
AWS::EC2::VPCEndpointConnectionNotification	 Yes	 Yes
AWS::EC2::VPCEndpointService	 Yes	 No

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::EC2::VPCPeeringConnection	 Yes	 Yes
AWS::EC2::VPNConnection	 Yes	 Yes
AWS::EC2::VPNConnectionRoute	 Yes	 Yes
AWS::EC2::VPNGateway	 Yes	 Yes
AWS::EC2::Volume	 Yes	 Yes
AWS::ECR::Repository	 Yes	 Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::ECS::CapacityProvider	 Yes	 Yes
AWS::ECS::Cluster	 Yes	 Yes
AWS::ECS::Service	 Yes	 Yes
AWS::ECS::TaskDefinition	 Yes	 Yes
AWS::ECS::TaskSet	 Yes	 Yes
AWS::EFS::AccessPoint	 Yes	 Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::EFS::FileSystem	 Yes	 Yes
AWS::EKS::Addon	 Yes	 Yes
AWS::EKS::Cluster	 Yes	 Yes
AWS::EKS::IdentityProviderConfig	 Yes	 Yes
AWS::EMR::SecurityConfiguration	 Yes	 Yes
AWS::ElasticBeanstalk::Application	 Yes	 Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::ElasticBeanstalk::ApplicationVersion	 Yes	 Yes
AWS::ElasticBeanstalk::Environment	 Yes	 Yes
AWS::ElasticLoadBalancing::LoadBalancer	 Yes	 Yes
AWS::ElasticLoadBalancingV2::Listener	 Yes	 Yes
AWS::ElasticLoadBalancingV2::LoadBalancer	 Yes	 Yes
AWS::Elasticsearch::Domain	 Yes	 Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::Events::EventBus	 Yes	 Yes
AWS::Events::Rule	 Yes	 Yes
AWS::FIS::ExperimentTemplate	 Yes	 Yes
AWS::Glue::Classifier	 Yes	 Yes
AWS::Glue::Job	 Yes	 Yes
AWS::Glue::MLTransform	 Yes	 No

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::GreengrassV2::ComponentVersion	 Yes	 Yes
AWS::GuardDuty::Detector	 Yes	 Yes
AWS::GuardDuty::Filter	 Yes	 Yes
AWS::GuardDuty::IPSet	 Yes	 Yes
AWS::GuardDuty::ThreatIntelSet	 Yes	 Yes
AWS::IAM::Group	 Yes	 Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::IAM::InstanceProfile	 No	 Yes
AWS::IAM::OIDCProvider	 No	 Yes
AWS::IAM::Policy	 Yes	 Yes
AWS::IAM::Role	 Yes	 Yes
AWS::IAM::SAMLProvider	 No	 Yes
AWS::IAM::ServerCertificate	 No	 Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::IAM::User	Yes	Yes
AWS::ImageBuilder::ContainerRecipe	Yes	Yes
AWS::ImageBuilder::DistributionConfiguration	Yes	Yes
AWS::ImageBuilder::ImagePipeline	Yes	Yes
AWS::ImageBuilder::ImageRecipe	Yes	Yes
AWS::ImageBuilder::InfrastructureConfiguration	Yes	Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::InspectorV2::Activation	 Yes	 Yes
AWS::IoT::AccountAuditConfiguration	 Yes	 Yes
AWS::IoT::Authorizer	 Yes	 Yes
AWS::IoT::CACertificate	 Yes	 Yes
AWS::IoT::CustomMetric	 Yes	 Yes
AWS::IoT::Dimension	 Yes	 Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::IoT::FleetMetric	 Yes	 Yes
AWS::IoT::JobTemplate	 Yes	 Yes
AWS::IoT::MitigationAction	 Yes	 Yes
AWS::IoT::Policy	 Yes	 Yes
AWS::IoT::ProvisioningTemplate	 Yes	 Yes
AWS::IoT::RoleAlias	 Yes	 Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::IoT::ScheduledAudit	 Yes	 Yes
AWS::IoT::SecurityProfile	 Yes	 Yes
AWS::IoTEvents::AlarmModel	 Yes	 No
AWS::IoTEvents::DetectorModel	 Yes	 No
AWS::IoTEvents::Input	 Yes	 No
AWS::IoTSiteWise::AssetModel	 Yes	 No

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::IoTSiteWise::Gateway	 Yes	 No
AWS::IoTSiteWise::Portal	 Yes	 No
AWS::IoTTwinMaker::ComponentType	 Yes	 No
AWS::IoTTwinMaker::Entity	 Yes	 No
AWS::IoTTwinMaker::Workspace	 Yes	 No
AWS::KMS::Alias	 Yes	 Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::KMS::Key	 Yes	 Yes
AWS::Kinesis::Stream	 Yes	 Yes
AWS::Kinesis::StreamConsumer	 Yes	 Yes
AWS::KinesisAnalyticsV2::Application	 Yes	 Yes
AWS::KinesisFirehose::DeliveryStream	 Yes	 Yes
AWS::Lambda::Function	 Yes	 Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::Logs::Destination	 Yes	 Yes
AWS::MSK::BatchScramSecret	 Yes	 Yes
AWS::MSK::Cluster	 Yes	 Yes
AWS::MSK::ClusterPolicy	 Yes	 Yes
AWS::MSK::Configuration	 Yes	 Yes
AWS::MSK::VpcConnection	 Yes	 Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::NetworkFirewall::Firewall	Yes	Yes
AWS::NetworkFirewall::FirewallPolicy	Yes	Yes
AWS::NetworkFirewall::RuleGroup	Yes	Yes
AWS::NetworkFirewall::VpcEndpointAssociation	Yes	Yes
AWS::NetworkManager::CustomerGatewayAssociation	Yes	No
AWS::NetworkManager::Device	Yes	No

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::NetworkManager::GlobalNetwork	 Yes	 No
AWS::NetworkManager::Link	 Yes	 No
AWS::NetworkManager::LinkAssociation	 Yes	 No
AWS::NetworkManager::Site	 Yes	 No
AWS::NetworkManager::TransitGatewayRegistration	 Yes	 No
AWS::OpenSearch::Domain	 Yes	 Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::Pinpoint::App	 Yes	 No
AWS::Pinpoint::ApplicationSettings	 Yes	 No
AWS::Pinpoint::Campaign	 Yes	 No
AWS::Pinpoint::EmailChannel	 Yes	 No
AWS::Pinpoint::EmailTemplate	 Yes	 No
AWS::Pinpoint::EventStream	 Yes	 No

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::Pinpoint::InAppTemplate	 Yes	 No
AWS::Pinpoint::Segment	 Yes	 No
AWS::QuickSight::Template	 Yes	 No
AWS::RDS::DBCluster	 Yes	 Yes
AWS::RDS::DBClusterSnapshot	 Yes	 Yes
AWS::RDS::DBInstance	 Yes	 Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::RDS::DBSecurityGroup	 Yes	 Yes
AWS::RDS::DBSnapshot	 Yes	 Yes
AWS::RDS::DBSubnetGroup	 Yes	 Yes
AWS::RDS::EventSubscription	 Yes	 Yes
AWS::RDS::OptionGroup	 Yes	 Yes
AWS::Redshift::Cluster	 Yes	 Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::Redshift::ClusterParameterGroup	 Yes	 Yes
AWS::Redshift::ClusterSecurityGroup	 Yes	 Yes
AWS::Redshift::ClusterSnapshot	 Yes	 Yes
AWS::Redshift::ClusterSubnetGroup	 Yes	 Yes
AWS::Redshift::EventSubscription	 Yes	 Yes
AWS::Redshift::ScheduledAction	 Yes	 Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::RoboMaker::RobotApplication	 Yes	 No
AWS::RoboMaker::RobotApplicationVersion	 Yes	 No
AWS::RoboMaker::SimulationApplication	 Yes	 No
AWS::Route53Profiles::Profile	 Yes	 Yes
AWS::Route53Resolver::FirewallDomainList	 Yes	 Yes
AWS::Route53Resolver::FirewallRuleGroup	 Yes	 Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::Route53Resolver::FirewallRuleGroupAssociation	Yes	Yes
AWS::Route53Resolver::ResolverEndpoint	Yes	Yes
AWS::Route53Resolver::ResolverQueryLoggingConfig	Yes	Yes
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	Yes	Yes
AWS::Route53Resolver::ResolverRule	Yes	Yes
AWS::Route53Resolver::ResolverRuleAssociation	Yes	Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::S3::AccessPoint	 Yes	 Yes
AWS::S3::AccountPublicAccessBlock	 Yes	 Yes
AWS::S3::Bucket	 Yes	 Yes
AWS::SES::ConfigurationSet	 Yes	 No
AWS::SES::ContactList	 Yes	 No
AWS::SES::Template	 Yes	 No

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::SNS::Topic	 Yes	 Yes
AWS::SQS::Queue	 Yes	 Yes
AWS::SSM::AssociationCompliance	 Yes	 Yes
AWS::SSM::Document	 Yes	 Yes
AWS::SSM::FileData	 Yes	 Yes
AWS::SSM::ManagedInstanceInventory	 Yes	 Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::SSM::PatchCompliance	 Yes	 Yes
AWS::SageMaker::Model	 Yes	 No
AWS::SageMaker::NotebookInstance	 Yes	 No
AWS::SageMaker::NotebookInstanceLifecycleConfig	 Yes	 No
AWS::SecretsManager::Secret	 Yes	 Yes
AWS::SecurityHub::Standard	 Yes	 Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::ServiceCatalog::CloudFormationProduct	 Yes	 Yes
AWS::ServiceCatalog::CloudFormationProvisionedProduct	 Yes	 Yes
AWS::ServiceCatalog::Portfolio	 Yes	 Yes
AWS::ServiceDiscovery::HttpNamespace	 Yes	 Yes
AWS::ServiceDiscovery::Instance	 Yes	 Yes
AWS::ServiceDiscovery::Service	 Yes	 Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::StepFunctions::StateMachine	Yes	Yes
AWS::Transfer::Agreement	Yes	Yes
AWS::Transfer::Certificate	Yes	Yes
AWS::Transfer::Connector	Yes	Yes
AWS::Transfer::Profile	Yes	Yes
AWS::Transfer::Workflow	Yes	Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::WAFRegional::RateBasedRule	Yes	Yes
AWS::WAFRegional::Rule	Yes	Yes
AWS::WAFRegional::RuleGroup	Yes	Yes
AWS::WAFRegional::WebACL	Yes	Yes
AWS::WAFv2::IPSet	Yes	Yes
AWS::WAFv2::ManagedRuleSet	Yes	Yes

Resource type	Amazon GovCloud (US-West)	Amazon GovCloud (US-East)
AWS::WAFv2::RegexPatternSet	 Yes	 Yes
AWS::WAFv2::RuleGroup	 Yes	 Yes
AWS::WAFv2::WebACL	 Yes	 Yes
AWS::WorkSpaces::Workspace	 Yes	 No

Recording Amazon Resources with Amazon Config

Amazon Config continuously detects when supported resource types are created, changed, or deleted. Amazon Config records these events as configuration items (CIs).

You can customize Amazon Config to record configuration changes for all supported resource types, or for only the supported resource types that are relevant to you. For a list of supported resource types that Amazon Config can record, see Supported Resource Types for Amazon Config.

Topics

- Considerations
- What are the differences between Regional and global resources?

- Amazon Config Rules and global resource types
- Recording frequency for Amazon Config
- Non-recorded resources
- Recording resources in the Amazon Config console
- Recording resources with the Amazon CLI
- Excluding resources from recording with Amazon Config
- Stopping Amazon Config from recording with the customer managed configuration recorder

Considerations

High Number of Amazon Config Evaluations

You might notice increased activity in your account during your initial month recording with Amazon Config when compared to subsequent months. During the initial bootstrapping process, Amazon Config runs evaluations on all the resources in your account that you have selected for Amazon Config to record.

If you are running ephemeral workloads, you may see increased activity from Amazon Config as it records configuration changes associated with creating and deleting these temporary resources. An *ephemeral workload* is a temporary use of computing resources that are loaded and run when needed. Examples include Amazon Elastic Compute Cloud (Amazon EC2) Spot Instances, Amazon EMR jobs, and Amazon Auto Scaling.

If you want to avoid the increased activity from running ephemeral workloads, you can set up the customer managed configuration recorder to exclude these resource types from being recorded, or run these types of workloads in a separate account with Amazon Config turned off to avoid increased configuration recording and rule evaluations.

Region availability

Before specifying a resource type for Amazon Config to track, check Resource Coverage by Region availability to see if the resource type is supported in the Amazon Region where you set up Amazon Config.

If a resource type is supported by Amazon Config in at least one Region, you can enable the recording of that resource type in all Regions supported by Amazon Config, even if the specified resource type is not supported in the Amazon Region where you set up Amazon Config.

What are the differences between Regional and global resources?

Regional resources

Regional resources are tied to a Region and can be used only in that Region. You create them in a specified Amazon Web Services Region, and then they exist in that Region. To see or interact with those resources, you must direct your operations to that Region. For example, to create an Amazon EC2 instance with the Amazon Web Services Management Console, you choose the Amazon Web Services Region that you want to create the instance in. If you use the Amazon Command Line Interface (Amazon CLI) to create the instance, then you include the `--region` parameter. The Amazon SDKs each have their own equivalent mechanism to specify the Region that the operation uses.

There are several reasons for using Regional resources. One reason is to ensure that the resources, and the service endpoints that you use to access them, are as close to the customer as possible. This improves performance by minimizing latency. Another reason is to provide an isolation boundary. This lets you create independent copies of resources in multiple Regions to distribute the load and improve scalability. At the same time, it isolates the resources from each other to improve availability.

If you specify a different Amazon Web Services Region in the console or in an Amazon CLI command, then you can no longer see or interact with the resources you could see in the previous Region.

When you look at the Amazon Resource Name (ARN) for a Regional resource, the Region that contains the resource is specified as the fourth field in the ARN. For example, an Amazon EC2 instance is a Regional resource. The following is an example of an ARN for a Amazon EC2 instance that exists in the `us-east-1` Region.

```
arn:aws-cn:ec2:us-east-1:123456789012:instance/i-0a6f30921424d3eee
```

Global resources

Some Amazon services resources are *global resources*, meaning that you can use the resource from ***anywhere***. You don't specify an Amazon Web Services Region in a global service's console. To access a global resource, you don't specify a `--region` parameter when using the service's Amazon CLI and Amazon SDK operations.

Global resources support cases where it is critical that only one instance of a particular resource can exist at a time. In these scenarios, replication or synchronization between copies in different

Regions is not adequate. Having to access a single global endpoint, with the possible increase in latency, is considered acceptable to ensure that any changes are instantaneously visible to consumers of the resource.

For example, Amazon Aurora global clusters (`AWS::RDS::GlobalCluster`) are global resources, and therefore not tied to a Region. This means that you can create a global cluster without relying on a regional endpoint. The benefit is that, while the Amazon Relational Database Service (Amazon RDS) itself is organized by Regions, the specific Region where a global cluster originates doesn't impact the global cluster. It appears as a single, continuous global cluster across all Regions.

The Amazon Resource Name (ARN) for a global resource doesn't include a Region. The fourth field is empty, such as in the following example of an ARN for a global cluster.

```
arn:aws-cn:rds::123456789012:global-cluster:test-global-cluster
```

Important

Global resource types onboarded to Amazon Config after February 2022 will only be recorded in the service's home Region for the commercial partition and Amazon GovCloud (US-West) for the GovCloud partition. You can view the configuration items (CIs) for these new global resource types only in their home Region and Amazon GovCloud (US-West).
Global resource types onboarded before February 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy`, `AWS::IAM::Role`, and `AWS::IAM::User`) remain unchanged. You can enable the recording of these global IAM resources in all Regions where Amazon Config was supported before February 2022. These global IAM resources cannot be recorded in Regions supported by Amazon Config after February 2022.

Global resource types | IAM resources

The following IAM resource types are global resources: IAM users, groups, roles, and customer managed policies. These resource types can be recorded by Amazon Config in Regions where Amazon Config was available before February 2022. This list where you cannot record the global IAM resource types includes the following Regions: Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Asia Pacific (Thailand), Canada

West (Calgary), Europe (Spain), Europe (Zurich), Israel (Tel Aviv), Mexico (Central), and Middle East (UAE).

To prevent duplicate configuration items (CIs), you should consider only recording the global IAM resource types one time in one of the supported Regions. This can also help you avoid unneccessary evaluations and API throttling.

Global resource types | Home Region Only

Global resources for the following services are only recorded by Amazon Config in the home Region of the global resource type: Amazon Elastic Container Registry Public, Amazon Global Accelerator, Amazon Route 53, Amazon CloudFront, and Amazon WAF. For these global resources, the same instance of the resource type can be used in multiple Amazon Regions, but the configuration items (CIs) are only recorded in the home Region for the commercial partition or Amazon GovCloud (US-West) for the Amazon GovCloud (US) partition.

Home Regions for Global Resource Types

Amazon Service	Resource Type Value	Home Region
Amazon Elastic Container Registry Public	`AWS::ECR::PublicRepository`	US East (N. Virginia) Region
Amazon Global Accelerator	`AWS::GlobalAccelerator::Listener`	US West (Oregon) Region
	`AWS::GlobalAccelerator::EndpointGroup`	US West (Oregon) Region
	`AWS::GlobalAccelerator::Accelerator`	US West (Oregon) Region
Amazon Route 53	`AWS::Route53::HostedZone`	US East (N. Virginia) Region
	`AWS::Route53::HealthCheck`	US East (N. Virginia) Region

Amazon Service	Resource Type Value	Home Region
Amazon CloudFront	`AWS::CloudFront::Distribution`	US East (N. Virginia) Region
Amazon WAF	`AWS::WAFv2::WebACL`	US East (N. Virginia) Region

Global resource types | Aurora global clusters

`AWS::RDS::GlobalCluster` is a global resource that is recorded in all supported Amazon Config Regions where the customer managed configuration recorder is enabled. This global resource type is unique in that if you enable the recording of this resource in one Region, Amazon Config will record configuration items (CIs) for this resource type in all your enabled Regions.

If you do not want to record `AWS::RDS::GlobalCluster` in all enabled Regions, use one of the following recording strategies for the Amazon Config console:

- **Record all resource types with customizable overrides**, choose "Amazon RDS GlobalCluster", and choose the override "Exclude from recording"
- **Record specific resource types**.

If you do not want to record `AWS::RDS::GlobalCluster` in all enabled Regions, use one of the following recording strategies for the API/CLI:

- **Record all current and future resource types with exclusions** (`EXCLUSION_BY_RESOURCE_TYPES`)
- **Record specific resource types** (`INCLUSION_BY_RESOURCE_TYPES`).

Amazon Config Rules and global resource types

The global IAM resource types onboarded before February 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy`, `AWS::IAM::Role`, and `AWS::IAM::User`) can only be recorded by Amazon Config in Regions where Amazon Config was available before February 2022. These global IAM resource types cannot be recorded in Regions supported by Amazon Config after February 2022. For a list of those Regions, see Recording Amazon Resources | Global Resources.

If you record a global IAM resource type in at least one Region, periodic rules that report compliance on the global IAM resource type will run evaluations in all Regions where the periodic

rule is added, even if you have not enabled the recording of the global IAM resource type in the Region where the periodic rule was added.

Best Practices for reporting compliance on global resources onboarded before February 2022

To avoid unnecessary evaluations, you should only deploy Amazon Config rules and conformance packs that have these global resources in scope to one of the supported Regions. For a list of which managed rules are supported in which Regions, see List of Amazon Config Managed Rules by Region Availability. This applies to Amazon Config rules, organizational Amazon Config rules, and also rules created by other Amazon services, such as Amazon Security Hub and Amazon Control Tower.

If you are not recording global resource types onboarded before February 2022, it is recommended that you do not enable the following periodic rules to avoid unnecessary evaluations:

- access-keys-rotated
- account-part-of-organizations
- iam-password-policy
- iam-policy-in-use
- iam-root-access-key-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- mfa-enabled-for-iam-console-access
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled

Best Practices for reporting compliance on global resources onboarded after February 2022

Global resource types onboarded to Amazon Config recording after February 2022 will be recorded only in the service's home Region for the commercial partition and Amazon GovCloud (US-West) for the Amazon GovCloud (US) partition. You should deploy Amazon Config rules and conformance packs that have these global resources in scope only to the resource type's home Region. For more information, see Home Regions for Global Resource Types.

Recording frequency for Amazon Config

Amazon Config supports *Continuous recording* and *Daily recording*. Continuous recording allows you to record configuration changes continuously whenever a change occurs. Daily recording allows you to receive a configuration item (CI) representing the most recent state of your resources over the last 24-hour period, only if it's different from the previous CI recorded. For steps on how to change the recording frequency, see Changing Recording Frequency.

Continuous recording

Some benefits of continuous recording include:

- **Real-time Monitoring**: Continuous recording can provide immediate detection for unauthorized changes or unexpected alterations, which can enhance your security and compliance efforts.
- **Detailed Analysis**: Continuous recording can allow you to perfom in-depth analysis of configuration changes to your resources as they occur, which can allow you to identify patterns and trends in the moment.

Daily recording

Some benefits of daily recording include:

- **Minimal Disruption**: Daily recording can provide you with a more mangeable flow of information, which can reduce the frequency of notifications and alert fatigue.
- **Cost Efficiency**: Daily recording can provide you with the flexibility to record changes to your resources at at a lower frequency, which can reduce costs related to the number of configuration changes recorded.

> **Note**
>
> Amazon Firewall Manager depends on continuous recording to monitor your resources. If you are using Firewall Manager, it is recommended that you set the recording frequency to Continuous.

Non-recorded resources

If a resource is not recorded, Amazon Config captures only the creation and deletion of that resource, and no other details, at no cost to you. When a non-recorded resource is created or deleted, Amazon Config sends a notification, and it displays the event on the resource details page. The details page for a non-recorded resource provides null values for most configuration details, and it does not provide information about relationships and configuration changes.

The relationship information that Amazon Config provides for recorded resources is not limited because of missing data for non-recorded resources. If a recorded resource is related to a non-recorded resource, that relationship is provided in the details page of the recorded resource.

IAM resource type considerations

The `AWS::IAM::User`, `AWS::IAM::Policy`, `AWS::IAM::Group`, `AWS::IAM::Role` resource types will only capture the creation (`ResourceNotRecorded`) and deletion (`ResourceDeletedNotRecorded`) states if the resource is, or previously was, selected as a resource to record in the customer managed configuration recorder .

CI recording schedule for non-recorded resources

The configuration items (CIs) for `ResourceNotRecorded` and `ResourceDeletedNotRecorded` do not follow the typical recording time for resource types. These resource types are only recorded during the periodic baselining process for the customer managed configuration recorder, which is at a less frequent cadance than that for the other resource types. This means that create and delete notifications are not sent upon creation or deletion, but during the baselining process.

CI delivery and service-linked recorder scope

For service-linked configuration recorders, the recording scope determines if you receive configuration items (CIs) in the delivery channel. The recording scope is set by the service that is linked to the configuration recorder. If the recording scope is internal, you will not receive CIs in the delivery channel.

Recording resources in the Amazon Config console

You can use the Amazon Config console to select the types of resources that Amazon Config records with the customer managed configuration recorder.

To select resources

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. Choose **Settings** in the left navigation pane.
3. On the **Customer managed recorder** tab, choose **Edit**.
4. In the **Recording method** section, choose a recording strategy. You can specify the Amazon resources that you want Amazon Config to record.

   All resource types with customizable overrides

   Set up Amazon Config to record configuration changes for all current and future supported resource types in this Region. You can override the recording frequency for specific resource types or exclude specific resource types from recording. For more information, see Supported Resource Types.

   - **Default settings**

     Configure the default recording frequency for all current and future supported resource types. For more information see, Recording Frequency.

     - Continuous recording – Amazon Config will record configuration changes continuously whenever a change occurs.
     - Daily recording – You will receive a configuration item (CI) representing the most recent state of your resources over the last 24-hour period, only if it's different from the previous CI recorded.

     > **Note**
     >
     > Amazon Firewall Manager depends on continuous recording to monitor your resources. If you are using Firewall Manager, it is recommended that you set the recording frequency to Continuous.

   - **Override settings**

     Override the recording frequency for specific resource types, or exclude specific resource types from recording. If you change the recording frequency for a resource type or stop recording a resource type, the configuration items that were already recorded will remain unchanged.

Specific resource types

Set up Amazon Config to record configuration changes for only the resource types that you specify.

- **Specific resource types**

  Choose a resource type to record and its frequency. For more information see, Recording Frequency.

  - Continuous recording – Amazon Config will record configuration changes continuously whenever a change occurs.
  - Daily recording – You will receive a configuration item (CI) representing the most recent state of your resources over the last 24-hour period, only if it's different from the previous CI recorded.

  > **Note**
  >
  > Amazon Firewall Manager depends on continuous recording to monitor your resources. If you are using Firewall Manager, it is recommended that you set the recording frequency to Continuous.

  If you change the recording frequency for a resource type or stop recording a resource type, the configuration items that were already recorded will remain unchanged.

5. Choose **Save** to save your changes.

Considerations When Recording Resources

High Number of Amazon Config Evaluations

You might notice increased activity in your account during your initial month recording with Amazon Config when compared to subsequent months. During the initial bootstrapping process, Amazon Config runs evaluations on all the resources in your account that you have selected for Amazon Config to record.

If you are running ephemeral workloads, you may see increased activity from Amazon Config as it records configuration changes associated with creating and deleting these temporary resources.

An *ephemeral workload* is a temporary use of computing resources that are loaded and run when needed. Examples include Amazon Elastic Compute Cloud (Amazon EC2) Spot Instances, Amazon EMR jobs, and Amazon Auto Scaling. . If you want to avoid the increased activity from running ephemeral workloads, you can set up the customer managed configuration recorder to exclude these resource types from being recorded, or run these types of workloads in a separate account with Amazon Config turned off to avoid increased configuration recording and rule evaluations.

Considerations: All resource types with customizable overrides

Globally recorded resource types | Aurora global clusters are initially included in recording

The `AWS::RDS::GlobalCluster` resource type will be recorded in all supported Amazon Config Regions where the customer managed configuration recorder is enabled.

If you do not want to record `AWS::RDS::GlobalCluster` in all enabled Regions, choose "Amazon RDS GlobalCluster", and choose the override "Exclude from recording".

Global resource types | IAM resource types are initially excluded from recording

The global IAM resource types are initially excluded from recording to help you reduce costs. This bundle includes IAM users, groups, roles, and customer managed policies. Choose **Remove** to remove the override and include these resources in your recording.

Additionally, the global IAM resource types (`AWS::IAM::User`, `AWS::IAM::Group`, `AWS::IAM::Role`, and `AWS::IAM::Policy`) cannot be recorded in Regions supported by Amazon Config after February 2022. For a list of those Regions, see Recording Amazon Resources | Global Resources.

Limits

You can add up to 100 frequency overrides and 600 exclusion overrides.

Daily recording is not supported for the following resource types:

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

Considerations: Specific resource types

Region Availability

Before specifying a resource type for Amazon Config to track, check Resource Coverage by Region Availability to see if the resource type is supported in the Amazon Region where you set up Amazon Config. If a resource type is supported by Amazon Config in at least one Region, you can enable the recording of that resource type in all Regions supported by Amazon Config, even if the specified resource type is not supported in the Amazon Region where you set up Amazon Config.

Limits

No limits if all resource types have the same frequency. You can add up to 100 resource types with Daily frequency if at least one resource type is set to Continuous.

The Daily frequency is not supported for the following resource types:

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

Recording resources with the Amazon CLI

You can use the Amazon CLI to select the types of resources that you want Amazon Config to record. You do this by creating a customer managed configuration recorder, which records the types of resources that you specify in a recording group. In the recording group, you specify whether you want to record all supported resource types, or to include or exclude specific types of resources.

Record all current and future supported resource types

Set up Amazon Config to record configuration changes for all current and future supported resource types in this Region. For a list of supported resources types, see Supported Resource Types.

1. Use the `put-configuration-recorder` command:

   This command uses the `--configuration-recorder` and `---recording-group` fields.

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

The `configuration-recorder` field

The `configurationRecorder.json` file specifies `name` and `roleArn` as well as the default recording frequency for the configuration recorder (`recordingMode`).

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include
 in the override ]
        }
    ]
  }
}
```

The `recording-group` field

The `recordingGroup.json` file specifies which resource types are recorded.

```
{
    "allSupported": true,
    "recordingStrategy": {
        "useOnly": "ALL_SUPPORTED_RESOURCE_TYPES"
    },
    "includeGlobalResourceTypes": true
}
```

For more information about these fields, see `put-configuration-recorder` in the *Amazon CLI Command Reference*.

2. (Optional) To verify that your customer managed configuration recorder has the settings that you want, use the following `describe-configuration-recorders` command.

```
$ aws configservice describe-configuration-recorders
```

The following is an example response.

```
{
    "ConfigurationRecorders": [
        {
            "name": "default"
            "recordingGroup": {
                "allSupported": true,
                "exclusionByResourceTypes": {
                     "resourceTypes": []
                },
                "includeGlobalResourceTypes": true,
                "recordingStrategy": {
                    "useOnly": "ALL_SUPPORTED_RESOURCE_TYPES"
                },
                "resourceTypes": [],
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types
 to include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

Record all current and future supported resources types excluding the types you specify

Set up Amazon Config to record configuration changes for all current and future supported resource types, including global resource types, except the resource types that you specify to exclude from recording.

If you choose to stop recording for a resource type, the configuration items that were already recorded will remain unchanged. For a list of supported resources types, see Supported Resource Types.

1. Use the `put-configuration-recorder` command:

   This command uses the `--configuration-recorder` and `---recording-group` fields.

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

The `configuration-recorder` field

The `configurationRecorder.json` file specifies `name` and `roleArn` as well as the default recording frequency for the configuration recorder (`recordingMode`).

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include
 in the override ]
        }
    ]
  }
}
```

The `recording-group` field

The `recordingGroup.json` file specifies which types of resources Amazon Config will record. Pass one or more resource types to exclude in the `resourceTypes` field of `exclusionByResourceTypes`, as shown in the following example.

```
{
    "allSupported": false,
```

```
    "exclusionByResourceTypes": {
        "resourceTypes": [
            "AWS::Redshift::ClusterSnapshot",
            "AWS::RDS::DBClusterSnapshot",
            "AWS::CloudFront::StreamingDistribution"
        ]
    },
   "includeGlobalResourceTypes": false,
   "recordingStrategy": {
       "useOnly": "EXCLUSION_BY_RESOURCE_TYPES"
    },

}
```

For more information about these fields, see put-configuration-recorder in the *Amazon CLI Command Reference*.

2. (Optional) To verify that your customer managed configuration recorder has the settings that you want, use the following describe-configuration-recorders command.

```
$ aws configservice describe-configuration-recorders
```

The following is an example response.

```
{
    "ConfigurationRecorders": [
        {
            "name": "default",
            "recordingGroup": {
                "allSupported": false,
                "exclusionByResourceTypes": {
                    "resourceTypes": [
                        "AWS::Redshift::ClusterSnapshot",
                        "AWS::RDS::DBClusterSnapshot",
                        "AWS::CloudFront::StreamingDistribution"
                    ]
                },
                "includeGlobalResourceTypes": false,
                "recordingStrategy": {
                    "useOnly": "EXCLUSION_BY_RESOURCE_TYPES"
                },
                "resourceTypes": [],
```

```
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types to
 include in the override]
                 }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

Record specific resource types

Set up Amazon Config to record configuration changes for only the resource types that you specify.

If you choose to stop recording for a resource type, the configuration items that were already recorded will remain unchanged. For a list of supported resources types, see Supported Resource Types.

1. Use the `put-configuration-recorder` command:

   This command uses the `--configuration-recorder` and `---recording-group` fields.

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

   The `configuration-recorder` field

   The `configurationRecorder.json` file specifies `name` and `roleArn` as well as the default recording frequency for the configuration recorder (`recordingMode`).

```
{
  "name": "default",
```

```
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include
 in the override ]
        }
    ]
  }
}
```

The `recording-group` field

The `recordingGroup.json` file specifies which types of resources Amazon Config will record. Pass one or more resource types to exclude in the `resourceTypes` field as shown in the following example.

```
{
    "allSupported": false,
    "recordingStrategy": {
        "useOnly": "INCLUSION_BY_RESOURCE_TYPES"
    },
    "includeGlobalResourceTypes": false,
    "resourceTypes": [
        "AWS::EC2::EIP",
        "AWS::EC2::Instance",
        "AWS::EC2::NetworkAcl",
        "AWS::EC2::SecurityGroup",
        "AWS::CloudTrail::Trail",
        "AWS::EC2::Volume",
        "AWS::EC2::VPC",
        "AWS::IAM::User",
        "AWS::IAM::Policy"
  ]
}
```

For more information about these fields, see `put-configuration-recorder` in the *Amazon CLI Command Reference*.

2. (Optional) To verify that your customer managed configuration recorder has the settings that you want, use the following describe-configuration-recorders command.

```
$ aws configservice describe-configuration-recorders
```

The following is an example response.

```
{
    "ConfigurationRecorders": [
        {
            "name": "default",
            "recordingGroup": {
                "allSupported": false,
                "exclusionByResourceTypes": {
                    "resourceTypes": []
                },
                "includeGlobalResourceTypes": false
                "recordingStrategy": {
                    "useOnly": "INCLUSION_BY_RESOURCE_TYPES"
                },
                "resourceTypes": [
                    "AWS::EC2::EIP",
                    "AWS::EC2::Instance",
                    "AWS::EC2::NetworkAcl",
                    "AWS::EC2::SecurityGroup",
                    "AWS::CloudTrail::Trail",
                    "AWS::EC2::Volume",
                    "AWS::EC2::VPC",
                    "AWS::IAM::User",
                    "AWS::IAM::Policy"
                ]
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types to
 include in the override]
                }
              ]
```

```
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

Excluding resources from recording with Amazon Config

Amazon Config allows you to exclude specific types of Amazon resources from inventory tracking and compliance monitoring while still tracking all other supported resource types currently available in Amazon Config, including those that will be added in the future. You can use this feature to concentrate on critical resources that are subject to your compliance and governance standards.

Excluding resources (Console)

If you do not want to record an Amazon resource type, use one of the following recording strategies for the Amazon Config console:

- **Record all resource types with customizable overrides**, choose the resource type you want to exclude, and choose the override "Exclude from recording"
- **Record specific resource types**.

For more detailed steps, see Recording resources (Console).

Excluding resources (Amazon CLI)

If you do not want to record an Amazon resource type, use one of the following recording strategies for the API/CLI:

- **Record all current and future resource types with exclusions** (`EXCLUSION_BY_RESOURCE_TYPES`)
- **Record specific resource types** (`INCLUSION_BY_RESOURCE_TYPES`).

For more detailed steps, see Recording Resources (Amazon CLI).

Stopping Amazon Config from recording with the customer managed configuration recorder

You can stop Amazon Config from recording with the customer managed configuration recorder any time. After Amazon Config stops recording a resource, it retains the configuration information that was previously captured, and you can continue to access this information.

For steps on how to stop recording, see Stopping the customer managed configuration recorder.

Recording Configurations with Amazon Config for Third-Party Resources using the Amazon CLI

Record configurations for third-party resources or custom resource types such as on premise servers, SAAS monitoring tools, and version control systems (like GitHub).

You can publish the configuration data of third-party resources into Amazon Config and view and monitor the resource inventory and configuration history using the Amazon Config console and APIs. You can use Amazon Config to manage all your resources and evaluate resource configuration for compliance against best practices using Amazon Config rules. You can also create Amazon Config rules or conformance packs to evaluate these third-party resources against best practices, internal policies, and regulatory policies.

> **Note**
>
> If you have configured Amazon Config to record all resource types, then third-party resources that are managed (created, updated, or deleted) through Amazon CloudFormation are automatically tracked in Amazon Config as configuration items.

Prerequisite: The third-party resources or custom resource type must be registered using Amazon CloudFormation.

Topics

- Adding Third-Party Resources to Amazon Config
- Record Configuration Items with Amazon Config for Third-Party Resources using the Amazon CLI
- Read Configuration Items with Amazon Config for Third-Party Resources using the Amazon CLI

- Delete Third-Party Resources from Amazon Config using the Amazon CLI

Adding Third-Party Resources to Amazon Config

Follow these steps to add a third-party resource to Amazon Config.

Topics

- Step 1: Setup Your Development Environment
- Step 2: Model Your Resource
- Step 3: Generate Artifacts
- Step 4: Register Your Resource
- Step 5: Publish Resource Configuration

Step 1: Setup Your Development Environment

Install and configure the Amazon CloudFormation Amazon CLI. The Amazon CLI allows you to model and register your custom resources. For more information, see Custom Resources and What Is the CloudFormation Command Line Interface?.

Step 2: Model Your Resource

Create a resource provider schema that conforms to and validates the configuration of the resource type.

1. Use the `init` command to create your resource provider project and generate the files it requires.

   ```
   $ cfn init
   Initializing new project
   ```

2. The `init` command launches a wizard that walks you through setting up the project, including specifying the resource name. For this walkthrough, specify `MyCustomNamespace::Testing::WordPress`.

   ```
   Enter resource type identifier (Organization::Service::Resource):
    MyCustomNamespace::Testing::WordPress
   ```

3. Enter a package name for your resource.

```
Enter a package name (empty for default 'com.custom.testing.wordpress'):
 com.custom.testing.wordpress
Initialized a new project in /workplace/user/custom-testing-wordpress
```

> **Note**
>
> In order to guarantee that any project dependencies are correctly resolved, you can import the generated project into your IDE with Maven support.
> For example, if you are using IntelliJ IDEA, you would need to do the following:
>
> - From the **File** menu, choose **New**, then choose **Project From Existing Sources**.
> - Navigate to the project directory
> - In the **Import Project** dialog box, choose **Import project from external model** and then choose **Maven**.
> - Choose **Next** and accept any defaults to complete importing the project.

4. Open the `mycustomnamespace-testing-wordpress.json` file that contains the schema for your resource. Copy and paste the following schema into `mycustomnamespace-testing-wordpress.json`.

```
{
  "typeName": "MyCustomNamespace::Testing::WordPress",
  "description": "An example resource that creates a website based on WordPress
 5.2.2.",
  "properties": {
    "Name": {
      "description": "A name associated with the website.",
      "type": "string",
      "pattern": "^[a-zA-Z0-9]{1,219}\\Z",
      "minLength": 1, "maxLength": 219
    },
    "SubnetId": {
      "description": "A subnet in which to host the website.",
      "pattern": "^(subnet-[a-f0-9]{13})|(subnet-[a-f0-9]{8})\\Z",
      "type": "string"
    },
    "InstanceId": {
      "description": "The ID of the instance that backs the WordPress site.",
```

```
      "type": "string"
    },
    "PublicIp": {
      "description": "The public IP for the WordPress site.",
      "type": "string"
    }
  },
  "required": [ "Name", "SubnetId" ],
  "primaryIdentifier": [ "/properties/PublicIp", "/properties/InstanceId" ],
  "readOnlyProperties": [ "/properties/PublicIp", "/properties/InstanceId" ],
  "additionalProperties": false
}
```

5. Validate the schema.

```
$ cfn validate
```

6. Update the auto-generated files in the resource provider package to view the resource provider schema updates. Upon initiation of the resource provider project, the Amazon CLI generates supporting files and code for the resource provider. Regenerate the code to see the updated schema.

```
$ cfn generate
```

> **Note**
>
> When using Maven, as part of the build process the `generate` command is automatically run before the code is compiled. So your changes will never get out of sync with the generated code.
> Be aware the CloudFormation CLI must be in a location Maven/the system can find. For more information, see Setting up your environment for developing extensions.

For more information on the whole process, see Modeling Resource Providers for Use in Amazon CloudFormation.

Step 3: Generate Artifacts

Run the following command to generate artifacts for `cfn submit`.

```
$ mvn package
```

Step 4: Register Your Resource

Amazon Config does not require resource provider handlers to perform configuration tracking for your resource. Run the following command to register your resource.

```
$ cfn submit
```

For more information, see Registering Resource Providers for Use in Amazon CloudFormation Templates.

Step 5: Publish Resource Configuration

Determine the configuration for MyCustomNamespace::Testing::WordPress.

```
{
  "Name": "MyWordPressSite",
  "SubnetId": "subnet-abcd0123",
  "InstanceId": "i-01234567",
  "PublicIp": "my-wordpress-site.com"
}
```

Determine the schema version id from Amazon CloudFormation `DescribeType`.

In Amazon Config, you can see see if this resource configuration is accepted. To evaluate compliance you can write Amazon Config rules using this resource.

(Optional) To automate recording of configuration, implement periodic or change-based configuration collectors.

Record Configuration Items with Amazon Config for Third-Party Resources using the Amazon CLI

Record a configuration item for a third-party resource or a custom resource type using the following procedure:

Ensure you register the resource type `MyCustomNamespace::Testing::WordPress` with its matching schema.

1. Open a command prompt or a terminal window.

2. Enter the following command:

```
aws configservice put-resource-config --resource-type
 MyCustomNamespace::Testing::WordPress --resource-id resource-001 --schema-version-
id 00000001 --configuration  '{
  "Id": "resource-001",
  "Name": "My example custom resource.",
  "PublicAccess": false
}'
```

Note

As defined in the type schema, `writeOnlyProperties` will be removed from the configuration prior to being recorded by Amazon Config. This means that these values will not be present when the configuration is obtained from read APIs. For more information on `writeOnlyProperties`, see Resource type schema.

Read Configuration Items with Amazon Config for Third-Party Resources using the Amazon CLI

Read a configuration item for a third-party resource or a custom resource type using the following procedure:

1. Open a command prompt or a terminal window.
2. Enter the following command:

```
aws configservice list-discovered-resources --resource-type
 MyCustomNamespace::Testing::WordPress
```

3. Press Enter.

   You should see output similar to the following:

```
{
    "resourceIdentifiers": [
        {
            "resourceType": "MyCustomNamespace::Testing::WordPress",
            "resourceId": "resource-001"
```

```
        }
    ]
}
```

4. Enter the following command:

```
aws configservice batch-get-resource-config --resource-keys '[ { "resourceType":
 "MyCustomNamespace::Testing::WordPress", "resourceId": "resource-001" } ]'
```

5. Press Enter.

   You should see output similar to the following:

```
{
    "unprocessedResourceKeys": [],
    "baseConfigurationItems": [
        {
            "configurationItemCaptureTime": 1569605832.673,
            "resourceType": "MyCustomNamespace::Testing::WordPress",
            "resourceId": "resource-001",
            "configurationStateId": "1569605832673",
            "awsRegion": "us-west-2",
            "version": "1.3",
            "supplementaryConfiguration": {},
            "configuration": "{\"Id\":\"resource-001\",\"Name\":\"My example custom
 resource.\",\"PublicAccess\":false}",
            "configurationItemStatus": "ResourceDiscovered",
            "accountId": "AccountId"
        }
    ]
}
```

Delete Third-Party Resources from Amazon Config using the Amazon CLI

Enter the following command to delete a third-party resource:

```
aws configservice delete-resource-config --resource-type
 MyCustomNamespace::Testing::WordPress --resource-id resource-002
```

If successful, the command executes with no additional output.

Recording Software Configuration for Managed Instances with Amazon Config

You can use Amazon Config to record software inventory changes on Amazon EC2 instances and on-premises servers. This enables you to see the historical changes to software configuration. For example, when a new Windows update is installed on a managed Windows instance, Amazon Config records the changes and then sends the changes to your delivery channel, so that you are notified about the change. With Amazon Config, you can see the history of when Windows updates were installed for the managed instance and how they changed over time.

Topics

- Prerequisites
- Recording Software Configurations

Prerequisites

You must complete the following steps to record software configuration changes:

- Turn on recording for the managed instance inventory resource type in Amazon Config.
- Configure EC2 and on-premises servers as *managed instances* in Amazon Systems Manager. A managed instance is a machine that has been configured for use with Systems Manager.
- Initiate collection of software inventory from your managed instances using the Systems Manager Inventory capability.

> **Note**
>
> **Systems Manager now supports creating configuration items for *unmanaged instances***
> Configuration item for unmanaged instances will have supplementary configuration with `Key: "InstanceStatus"` and `Value: "Unmanaged"`.
> **Configuration items for unmanaged instances won't receive additional updates**
> To receive additional updates, the configuration item must be a managed instance.

You can also use Amazon Config rules to monitor software configuration changes and be notified whether the changes are compliant or noncompliant against your rules. For example, if you create a rule that checks whether your managed instances have a specified application, and an instance doesn't have that application installed, Amazon Config flags that instance as noncompliant against your rule. For a list of Amazon Config managed rules, see List of Amazon Config Managed Rules.

Recording Software Configurations

To enable recording of software configuration changes in Amazon Config:

1. Turn on recording for all supported resource types or selectively record the managed instance inventory resource type in Amazon Config. For more information, see Recording Amazon Resources with Amazon Config.
2. Launch an Amazon EC2 instance with an instance profile for Systems Manager that includes the **AmazonSSMManagedInstanceCore** managed policy. This Amazon managed policy enables an instance to use Systems Manager service core functionality.

   For information about other policies you can add to the instance profile for Systems Manager, see Create an IAM Instance Profile for Systems Manager in the *Amazon Systems Manager User Guide*.

   Important

   SSM Agent is Amazon software that must be installed on a managed instance in order to communicate with the Systems Manager in the cloud. If your EC2 instance was created from an AMI for one of the following operating systems, the agent is preinstalled:

   - Windows Server 2003-2012 R2 AMIs published in November 2016 or later
   - Windows Server 2016 and 2019
   - Amazon Linux
   - Amazon Linux 2
   - Ubuntu Server 16.04
   - Ubuntu Server 18.04

On EC2 instances that were not created from an AMI with the agent preinstalled, you must install the agent manually. For information, see the following topics in the *Amazon Systems Manager User Guide*:

- Installing and configuring SSM Agent on EC2 instances for Windows Server
- Installing and configuring SSM Agent on EC2 instances for Linux

3. Initiate inventory collection as described in Configuring Inventory Collection in the *Amazon Systems Manager User Guide*. The procedures are the same for Linux and Windows instances.

   Amazon Config can record configuration changes for the following inventory types:

   - **Applications** – A list of applications for managed instances, such as antivirus software.
   - **Amazon components** – A list of Amazon components for managed instances, such as the Amazon CLI and SDKs.
   - **Instance information** – Instance information such as OS name and version, domain, and firewall status.
   - **Network configuration** – Configuration information such as IP address, gateway, and subnet mask.
   - **Windows Updates** – A list of Windows updates for managed instances (Windows instances only).

   Note

   Amazon Config doesn't support recording the custom inventory type at this time.

Inventory collection is one of many Systems Manager capabilities, which are grouped in the categories *Operations Management*, *Actions & Change*, *Instances & Nodes*, and *Shared Resources*. For more information, see What is Systems Manager? and Systems Manager Capabilities in the *Amazon Systems Manager User Guide*.

Looking Up Resources That Are Discovered by Amazon Config

You can use the Amazon Config console, Amazon CLI, and Amazon Config API to look up the resources that Amazon Config has taken an inventory of, or *discovered*, including deleted resources and resources that Amazon Config is not currently recording. Amazon Config discovers supported resource types only. For more information, see Supported Resource Types for Amazon Config.

Looking Up Resources (Console)

You can use resource types or tag information to look up resources in the Amazon Config console.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. On the **Resource inventory** page, specify the search options for the resources that you want to look up:
   - **Resource category** – Choose all resource categories or narrow results to only Amazon Resources.
   - **Resource type** – Choose all resource types or select which resource(s) to filter by.
   - **Compliance** – Choose to filter by any compliance status, compliant, or noncompliant.
3. Amazon Config lists the resources that match your search options. You can see the following information about the resources:
   - **Resource identifier** – The resource identifier might be a resource ID or a resource name, if applicable. Choose the resource identifier link to view the resource details page.
   - **Resource type** – The type of the resource is listed.
   - **Compliance** – The status of the resource that Amazon Config evaluated against your rule.

Looking Up Resources (Amazon CLI)

You can use the Amazon CLI to list resources that Amazon Config has discovered.

Use the **Amazon Configservice** **`list-discovered-resources`** command:

```
$ aws configservice list-discovered-resources --resource-type "AWS::EC2::Instance"
        {
            "resourceIdentifiers": [
```

```
            {
                "resourceType": "AWS::EC2::Instance",
                "resourceId": "i-nnnnnnnn"
            }
        ]
    }
```

To view the configuration details of a resource that is listed in the response, use the `get-resource-config-history` command, and specify the resource type and ID. For an example of this command and the response from Amazon Config, see Viewing Configuration History.

Looking up Resources (API)

You specify a resource type, and Amazon Config returns a list of resource identifiers for resources of that type. For more information, see ResourceIdentifier in the *Amazon Config API Reference*.

Use the ListDiscoveredResources action.

To get the configuration details of a resource that is listed in the response, use the GetResourceConfigHistory action, and specify the resource type and ID.

Viewing Compliance Information and Evaluation Results for your Amazon Resources with Amazon Config

Important

For accurate reporting on the compliance status, you must record the `AWS::Config::ResourceCompliance` resource type. For more information, see Recording Amazon Resources.

You can use the Amazon Config console or Amazon SDKs to view the compliance information and the evaluation results of your resources.

Topics

- Viewing compliance (Console)
- Viewing compliance (Amazon SDKs)

Viewing compliance (Console)

To view compliance (Console)

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. In the Amazon Web Services Management Console menu, verify that the region selector is set to a region that supports Amazon Config rules. For the list of supported regions, see Amazon Config Regions and Endpoints in the *Amazon Web Services General Reference*.
3. In the navigation pane, choose **Resources**. On the Resource inventory page, you can filter by resource category, resource type, and compliance status. Choose **Include deleted resources** if appropriate. The table displays the resource identifier for the resource type and the resource compliance status for that resource. The resource identifier might be a resource ID or a resource name.
4. Choose a resource from the resource identifier column.
5. Choose the **Resource Timeline** button. You can filter by Configuration events, Compliance events, or CloudTrail Events.

> **Note**
>
> Alternatively, on the Resource inventory page, you can directly choose the resource name. To access the resource timeline from the resource details page, choose the **Resource Timeline** button.

You can also view the compliance of your resources by looking them up on the **Resource inventory** page. For more information, see Looking Up Resources That Are Discovered by Amazon Config.

Viewing compliance (Amazon SDKs)

To get compliance information for your Amazon resources

The following code examples show how to use `DescribeComplianceByResource`.

CLI

Amazon CLI

To get compliance information for your Amazon resources

The following command returns compliance information for each EC2 instance that is recorded by Amazon Config and that violates one or more rules:

```
aws configservice describe-compliance-by-resource --resource-
type AWS::EC2::Instance --compliance-types NON_COMPLIANT
```

In the output, the value for each `CappedCount` attribute indicates how many rules the resource violates. For example, the following output indicates that instance `i-1a2b3c4d` violates 2 rules.

Output:

```
{
    "ComplianceByResources": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-1a2b3c4d",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 2,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        },
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-2a2b3c4d ",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        }
    ]
}
```

- For API details, see DescribeComplianceByResource in *Amazon CLI Command Reference*.

PowerShell

Tools for PowerShell V4

Example 1: This example checks the `AWS::SSM::ManagedInstanceInventory` resource type for 'COMPLIANT' compliance type.

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

Output:

```
Compliance                              ResourceId          ResourceType
----------                              ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- For API details, see DescribeComplianceByResource in *Amazon Tools for PowerShell Cmdlet Reference (V4)*.

Tools for PowerShell V5

Example 1: This example checks the `AWS::SSM::ManagedInstanceInventory` resource type for 'COMPLIANT' compliance type.

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

Output:

```
Compliance                              ResourceId          ResourceType
----------                              ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- For API details, see DescribeComplianceByResource in *Amazon Tools for PowerShell Cmdlet Reference (V5)*.

To get the compliance summary of your Amazon resources

The following code examples show how to use `GetComplianceSummaryByResourceType`.

CLI

Amazon CLI

To get the compliance summary for all resource types

The following command returns the number of Amazon resources that are noncompliant and the number that are compliant:

```
aws configservice get-compliance-summary-by-resource-type
```

In the output, the value for each `CappedCount` attribute indicates how many resources are compliant or noncompliant.

Output:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 16,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1453237464.543,
                "CompliantResourceCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

To get the compliance summary for a specific resource type

The following command returns the number of EC2 instances that are noncompliant and the number that are compliant:

```
aws configservice get-compliance-summary-by-resource-type --resource-
types AWS::EC2::Instance
```

In the output, the value for each CappedCount attribute indicates how many resources are compliant or noncompliant.

Output:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1452204923.518,
                "CompliantResourceCount": {
                    "CappedCount": 7,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

- For API details, see GetComplianceSummaryByResourceType in *Amazon CLI Command Reference*.

PowerShell

Tools for PowerShell V4

Example 1: This sample returns the number of resources that are compliant or noncompliant and converts the output to json.

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
```

```
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- For API details, see GetComplianceSummaryByResourceType in *Amazon Tools for PowerShell Cmdlet Reference (V4)*.

Tools for PowerShell V5

Example 1: This sample returns the number of resources that are compliant or noncompliant and converts the output to json.

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- For API details, see GetComplianceSummaryByResourceType in *Amazon Tools for PowerShell Cmdlet Reference (V5)*.

To get the evaluation results for an Amazon resource

The following code examples show how to use `GetComplianceDetailsByResource`.

CLI

Amazon CLI

To get the evaluation results for an Amazon resource

The following command returns the evaluation results for each rule with which the EC2 instance `i-1a2b3c4d` does not comply:

```
aws configservice get-compliance-details-by-resource --resource-
type AWS::EC2::Instance --resource-id i-1a2b3c4d --compliance-types NON_COMPLIANT
```

Output:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.288,
            "ConfigRuleInvokedTime": 1450314643.034,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "RequiredTagForEC2Instances"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
```

```
}
```

- For API details, see GetComplianceDetailsByResource in *Amazon CLI Command Reference*.

PowerShell

Tools for PowerShell V4

Example 1: This example evaulation results for the given resource.

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

Output:

```
Annotation                :
ComplianceType            : COMPLIANT
ConfigRuleInvokedTime     : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime        : 8/25/2019 11:34:56 PM
ResultToken               :
```

- For API details, see GetComplianceDetailsByResource in *Amazon Tools for PowerShell Cmdlet Reference (V4)*.

Tools for PowerShell V5

Example 1: This example evaulation results for the given resource.

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

Output:

```
Annotation                :
ComplianceType            : COMPLIANT
ConfigRuleInvokedTime     : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
```

```
ResultRecordedTime          : 8/25/2019 11:34:56 PM
ResultToken                 :
```

- For API details, see GetComplianceDetailsByResource in *Amazon Tools for PowerShell Cmdlet Reference (V5)*.

Viewing Compliance History for your Amazon Resources with Amazon Config

> **Important**
>
> For accurate reporting on the compliance status, you must record the `AWS::Config::ResourceCompliance` resource type. For more information, see Recording Amazon Resources.

You can view the configuration, relationships, and number of changes made to a resource in the Amazon Config console. You can view the configuration history for a resource using Amazon CLI.

Topics

- Viewing Compliance History (Console)
- Viewing Compliance History (Amazon CLI)
- Viewing Compliance History Timeline for Resources and Rules

Viewing Compliance History (Console)

Viewing Compliance History Using the Console

When you look up resources on the **Resource inventory** page, choose the resource name or ID in the resource identifier column to view the resource's details page. The details page provides information about the configuration, relationships, and number of changes made to that resource.

To access the resource timeline from the resource details page, choose the **Resource Timeline** button. The Resource timeline captures changes as `ConfigurationItems` over a period of time for a specific resource. You can filter by Configuration events, Compliance events, or CloudTrail Events.

Viewing Compliance History (Amazon CLI)

Viewing Compliance History Using the Amazon CLI

The configuration items that Amazon Config records are delivered to the specified delivery channel on demand as a configuration snapshot and as a configuration stream. You can use the Amazon CLI to view history of configuration items for each resource.

Viewing Configuration History

Enter the `get-resource-config-history` command and specify the resource type and the resource ID, for example:

```
$ aws configservice get-resource-config-history --resource-type AWS::EC2::SecurityGroup
 --resource-id sg-6fbb3807
{
    "configurationItems": [
        {
            "configurationItemCaptureTime": 1414708529.9219999,
            "relationships": [
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-7a3b232a",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-8b6eb2ab",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-c478efe5",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-e4cbe38d",
                    "relationshipName": "Is associated with Instance"
                }
            ],
            "availabilityZone": "Not Applicable",
            "tags": {},
```

```
            "resourceType": "AWS::EC2::SecurityGroup",
            "resourceId": "sg-6fbb3807",
            "configurationStateId": "1",
            "relatedEvents": [],
            "arn": "arn:aws:ec2:us-east-2:012345678912:security-group/default",
            "version": "1.0",
            "configurationItemMD5Hash": "860aa81fc3869e186b2ee00bc638a01a",
            "configuration": "{\"ownerId\":\"605053316265\",\"groupName\":\"default
\",\"groupId\":\"sg-6fbb3807\",\"description\":\"default group\",\"ipPermissions
\":[{\"ipProtocol\":\"tcp\",\"fromPort\":80,\"toPort\":80,\"userIdGroupPairs\":
[{\"userId\":\"amazon-elb\",\"groupName\":\"amazon-elb-sg\",\"groupId\":\"sg-843f59ed
\"}],\"ipRanges\":[\"0.0.0.0/0\"]},{\"ipProtocol\":\"tcp\",\"fromPort\":0,\"toPort
\":65535,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",\"groupName\":\"default
\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol\":\"udp\",\"fromPort
\":0,\"toPort\":65535,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",\"groupName
\":\"default\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol\":\"icmp
\",\"fromPort\":-1,\"toPort\":-1,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",
\"groupName\":\"default\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol
\":\"tcp\",\"fromPort\":1433,\"toPort\":1433,\"userIdGroupPairs\":[],\"ipRanges
\":[\"0.0.0.0/0\"]},{\"ipProtocol\":\"tcp\",\"fromPort\":3389,\"toPort\":3389,
\"userIdGroupPairs\":[],\"ipRanges\":[\"207.171.160.0/19\"]}],\"ipPermissionsEgress\":
[],\"vpcId\":null,\"tags\":[]}",
            "configurationItemStatus": "ResourceDiscovered",
            "accountId": "605053316265"
        }
    ],
    "nextToken":
     ..........
```


For detailed explanation of the response fields, see Components of a Configuration Item and Supported Resource Types for Amazon Config.

Example Amazon EBS Configuration History from Amazon Config

Amazon Config generates a set of files that each represent a resource type and lists all configuration changes for the resources of that type that Amazon Config is recording. Amazon Config exports this resource-centric configuration history as an object in the Amazon S3 bucket that you specified when you enabled Amazon Config. The configuration history file for each resource type contains the changes that were detected for the resources of that type since the last history file was delivered. The history files are typically delivered every six hours.

The following is an example of the contents of the Amazon S3 object that describes the configuration history of all the Amazon Elastic Block Store volumes in the current region for your

Amazon Web Services account. The volumes in this account include `vol-ce676ccc` and `vol-cia007c`. Volume `vol-ce676ccc` had two configuration changes since the previous history file was delivered while volume `vol-cia007c` had one change.


```
{
    "fileVersion": "1.0",
    "requestId": "asudf8ow-4e34-4f32-afeb-0ace5bf3trye",
    "configurationItems": [
        {
            "snapshotVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
            "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
```

```
                    "state": "attached",
                    "attachTime": "2014-03-07T23:46:28.0000+0000",
                    "deleteOnTermination": false
                }
            ],
            "tags": [
                {
                    "tagName": "environment",
                    "tagValue": "PROD"
                },
                {
                    "tagName": "name",
                    "tagValue": "DataVolume1"
                }
            ],
            "volumeType": "standard"
        }
    },
    {
        "configurationItemVersion": "1.0",
        "resourceId": "vol-ce676ccc",
        "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
        "accountId": "12345678910",
        "configurationItemCaptureTime": "2014-03-07T21:47:08.918Z",
        "configurationItemState": "3e660fdf-4e34-4f32-sseb-0ace5bf3d63a",
        "configurationItemStatus": "OK",
        "relatedEvents": [
            "06c12a39-eb35-11de-ae07-ad229edbb1e4",
            "c376e30d-71a2-4694-89b7-a5a04w292281"
        ],
        "availibilityZone": "us-west-2b",
        "resourceType": "AWS::EC2::Volume",
        "resourceCreationTime": "2014-02-27T21:43:53.885Z",
        "tags": {},
        "relationships": [
            {
                "resourceId": "i-344c463d",
                "resourceType": "AWS::EC2::Instance",
                "name": "Attached to Instance"
            }
        ],
        "configuration": {
            "volumeId": "vol-ce676ccc",
            "size": 1,
```

```
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume1"
                    }
                ],
                "volumeType": "standard"
            }
        },
        {
            "configurationItemVersion": "1.0",
            "resourceId": "vol-cia007c",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-cia007c",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T20:47:08.918Z",
            "configurationItemState": "3e660fdf-4e34-4f88-sseb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adjhk8edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a67u292281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T20:43:53.885Z",
            "tags": {},
            "relationships": [
```

```
                {
                    "resourceId": "i-344e563d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-cia007c",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T20:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-cia007c",
                        "instanceId": "i-344e563d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume2"
                    }
                ],
                "volumeType": "standard"
            }
        }
    ]
}
```

Viewing Compliance History Timeline for Resources and Rules

Amazon Config supports storing compliance state changes of resources as evaluated by Amazon Config Rules. The resource compliance history is presented in the form of a timeline. The timeline

captures changes as `ConfigurationItems` over a period of time for a specific resource. For information on the contents of `ConfigurationItem`, see ConfigurationItem in the Amazon Config API Reference.

You can opt in or out to record all resource types in Amazon Config. If you have opted to record all resource types, Amazon Config automatically begins recording the resource compliance history as evaluated by Amazon Config Rules. By default, Amazon Config records the configuration changes for all supported resources. You can also select only the specific resource compliance history resource type: `AWS::Config::ResourceCompliance`. For more information, see Recording Amazon Records.

Viewing Resource Timeline Using Resources

Access the resource timeline by selecting a specific resource from the Resource inventory page.

1. Choose the **Resources** from the left navigation.
2. On the Resource inventory page, you can filter by resource category, resource type, and compliance status. Choose **Include deleted resources** if appropriate.

   The table displays the resource identifier for the resource type and the resource compliance status for that resource. The resource identifier might be a resource ID or a resource name.
3. Choose a resource from the resource identifier column.
4. Choose the **Resource Timeline** button. You can filter by Configuration events, Compliance events, or CloudTrail Events.

> **Note**
>
> Alternatively, on the Resource inventory page, you can directly choose the resource name. To access the resource timeline from the resource details page, choose the **Resource Timeline** button.

Viewing Resource Timeline Using Rules

Access the resource timeline by selecting a specific rule from the Rule page.

1. Select the **Rules** from the left navigation.
2. On the Rule page, choose a rule evaluating your relevant resources. If no rules are displayed on the screen, add rules using the **Add rule** button.

3. On the Rule details page, select the resources from the Resources evaluated table.
4. Select the **Resource Timeline** button. The resource timeline is displayed.

Querying Compliance History for your Amazon Resources

Query the resource compliance history using get-resource-config-history using the resource type `AWS::Config::ResourceCompliance`.

```
aws configservice get-resource-config-history --resource-type
 AWS::Config::ResourceCompliance --resource-id AWS::S3::Bucket/configrules-bucket
```

You should see output similar to the following:

```
{
 "configurationItems": [
  {
   "configurationItemCaptureTime": 1539799966.921,
   "relationships": [
    {
     "resourceType": "AWS::S3::Bucket",
     "resourceId": "configrules-bucket",
     "relationshipName": "Is associated with "
    }
   ]
   "tags": {},
   "resourceType": "AWS::Config::ResourceCompliance",
   "resourceId": "AWS::S3::Bucket/configrules-bucket",
   "ConfigurationStateId": "1539799966921",
   "relatedEvents": [];
   "awsRegion": "us-west-2",
   "version": "1.3",
   "configurationItemMD5Hash": "",
   "supplementaryConfiguration": {},
   "configuration": "{\"complianceType\":\"COMPLIANT\",\"targetResourceId\":
\"configrules-bucket\",\"targetResourceType\":\"AWS::S3::Bucket\",\configRuleList"\":
[{\"configRuleArn\":\"arn:aws:config:us-west-2:AccountID:config-rule/config-rule-w1gogw
\",\"configRuleId\":\"config-rule-w1gogw\",\"configRuleName\":\"s3-bucket-logging-
enabled\",\"complianceType\":\"COMPLIANT\"}]}",

   "configurationItemStatus": "ResourceDiscovered",
   "accountId": "AccountID"
```

```
  }
 ]
}
```

Tagging Your Amazon Config Resources

A tag is a label that you assign to an Amazon resource. Each tag consists of a *key* and an optional *value*, both of which you define. Tags make it easier to manage, search for, and filter resources.

Tags enable you to categorize your Amazon resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type—you can quickly identify a specific resource based on the tags you've assigned to it. You can assign one or more tags to your Amazon resources. Each tag has an associated value.

We recommend that you devise a set of tag keys that meets your needs for each resource type. Using a consistent set of tag keys makes it easier for you to manage your Amazon resources. You can search and filter the resources based on the tags you add.

Tags are interpreted strictly as a string of characters and are not automatically assigned to your resources. You can edit tag keys and values, and you can remove tags from a resource at any time. You can set the value of a tag to an empty string, but you can't set the value of a tag to null. If you add a tag that has the same key as an existing tag on that resource, the new value overwrites the old value. If you delete a resource, any tags for the resource are also deleted.

You can work with tags using the Amazon Command Line Interface (Amazon CLI) and the Amazon Config API reference.

Restrictions Related to Tagging

The following basic restrictions apply to tags.

Restriction	Description
Maximum number of tags per resource	50
Maximum key length	128 Unicode characters in UTF-8
Maximum value length	256 Unicode characters in UTF-8

Restriction	Description
Prefix restriction	Do not use the `aws:` prefix in your tag names or values because it is reserved for Amazon use. You can't edit or delete tag names or values with this prefix. Tags with this prefix do not count against your tags per resource limit.
Character restrictions	Tags may only contain Unicode letters, digits, whitespace, or these symbols: `_ . : / = + - @`

Managing Tags with Amazon Config API Actions

Tag based access controls are available for three resources `ConfigurationAggregator`, `AggregationAuthorization`, and `ConfigRule`. Use the following to add, update, list, and delete the tags for your resources.

- ListTagsForResource
- TagResource
- UntagResource

> **Note**
>
> `TagResource` and `UntagResource` require certain Amazon Identity and Access Management (IAM) permissions to control access. For more information, see Controlling access based on tag keys in the IAM User Guide.

Evaluating Resources with Amazon Config Rules

Use Amazon Config to evaluate the configuration settings of your Amazon resources. You do this by creating Amazon Config rules, which represent your ideal configuration settings. Amazon Config provides customizable, predefined rules called managed rules to help you get started.

Topics

- Considerations
- Region Support
- Components of an Amazon Config Rule
- Amazon Config Managed Rules
- Amazon Config Custom Rules
- Service-Linked Amazon Config Rules
- Adding Amazon Config Rules
- Updating Amazon Config Rules
- Deleting Amazon Config Rules
- Viewing Details and Compliance Information for your Amazon Config Rules
- Turning on Proactive Evaluation for Amazon Config Rules
- Sending Rule Evaluations to Security Hub
- Evaluating Your Resources with Amazon Config Rules
- Deleting Evaluation Results from Amazon Config Rules
- Troubleshooting for Amazon Config rules

Considerations

Cost Considerations

For details about the costs associated with resource recording, see Amazon Config pricing.

Recommendation: Consider excluding the `AWS::Config::ResourceCompliance` resource type from recording before deleting rules

Deleting rules creates configuration items (CIs) for `AWS::Config::ResourceCompliance` that can affect your costs for the configuration recorder. If you are deleting rules which evaluate a large number of resource types, this can lead to a spike in the number of CIs recorded.

To avoid the associated costs, you can opt to disable recording for the `AWS::Config::ResourceCompliance` resource type before deleting rules, and re-enable recording after the rules have been deleted.

However, since deleting rules is an asynchronous process, it might take an hour or more to complete. During the time when recording is disabled for `AWS::Config::ResourceCompliance`, rule evaluations will not be recorded in the associated resource's history.

Amazon Config recommends that you weigh these factors on a case-by-case basis before deciding how to proceed with deleting rules.

Recommendation: Add logic to handle the evaluation of deleted resources for custom lambda rules

When creating Amazon Config custom lambda rules, it is highly recommended that you add logic to handle the evaluation of deleted resources.

When evaluation results are marked as `NOT_APPLICABLE`, they will be marked for deletion and cleaned up. If they're NOT marked as `NOT_APPLICABLE`, the evaluation results will remain unchanged until the rule is deleted, which can cause an unexpected spike in the creation of CIs for `AWS::Config::ResourceCompliance` upon rule deletion.

For information on how to set Amazon Config custom lambda rules to return `NOT_APPLICABLE` for deleted resources, see Managing deleted resources with Amazon Config custom lambda rules.

Recommendation: Provide the resources in scope for custom lambda rules

Amazon Config Custom Lambda Rules can cause a high number of Lambda function invocations if the rule is not scoped to one or more resource types. To avoid increased activity associated with your account, it is highly recommended to provide resources in scope for your Custom Lambda rules. If no resource types are selected, the rule will invoke the Lambda function for all resources in the account.

Other considerations

Defaut Values for Managed Rules

The default values specified for managed rules are pre-populated only when using the Amazon console. Default values are not supplied for the API, CLI, or SDK.

Configuration Item Recording Delays

Amazon Config usually records configuration changes to your resources right after a change is detected, or at the frequency that you specify. However, this is on a best effort basis and can take longer at times. For example, a resource type with known delays is `AWS::SecretsManager::Secret`. This resource type is an example, and this list is non-exhaustive.

Policies and compliance results

IAM policies and other policies managed in Amazon Organizations can impact whether Amazon Config has permissions to record configuration changes for your resources. Additionally, rules directly evaluate the configuration of a resource and rules don't take into account these policies when running evaluations. Make sure that the policies in effect align with how you intend to use Amazon Config.

Tagging support for resource types

If a resource type does not support tagging or does not include tag information in its describe API response, Amazon Config won't capture tag data in the configuration items (CIs) for that resource type. Amazon Config will still record these resources. However, any functionality that relies on tag data won't work. This affects tag-based filtering, grouping, or compliance evaluation that relies on tag data.

Directory Buckets Are Not Supported

Managed rules only support general purpose buckets when evaluating Amazon Simple Storage Service (Amazon S3) resources. For more information on general purpose buckets and directory buckets, see Buckets overview and Directory buckets in the Amazon S3 User Guide.

Managed Rules and Global IAM Resource Types

The global IAM resource types onboarded before February 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy`, `AWS::IAM::Role`, and `AWS::IAM::User`) can only be recorded by Amazon Config in Amazon Regions where Amazon Config was available before February 2022. These resource types cannot be recorded in Regions supported by Amazon Config after February 2022. For a list of those Regions, see Recording Amazon Resources | Global Resources.

If you record a global IAM resource type in at least one Region, periodic rules that report compliance on the global IAM resource type will run evaluations in all Regions where the periodic rule is added, even if you have not enabled the recording of the global IAM resource type in the Region where the periodic rule was added.

To avoid unnecessary evaluations, you should only deploy periodic rules that report compliance on a global IAM resource type to one of the supported Regions. For a list of which managed rules are supported in which Regions, see List of Amazon Config Managed Rules by Region Availability.

Region Support

Currently, the Amazon Config Rule feature is supported in the following Amazon regions. For a list of which individual Amazon Config rules are supported in which Regions, see List of Amazon Config Managed Rules by Region Availability.

Region Name	Region	Endpoint	Protocol
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com config-fips.us-east-2.amazonaws.com	HTTPS HTTPS
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com config-fips.us-east-1.amazonaws.com	HTTPS HTTPS
US West (N. California)	us-west-1	config.us-west-1.amazonaws.com config-fips.us-west-1.amazonaws.com	HTTPS HTTPS
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com config-fips.us-west-2.amazonaws.com	HTTPS HTTPS

Region Name	Region	Endpoint	Protocol	
Africa (Cape Town)	af-south-1	config.af-south-1.amazonaws.com	HTTPS	
Asia Pacific (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS	
Asia Pacific (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS	
Asia Pacific (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS	
Asia Pacific (Malaysia)	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS	
Asia Pacific (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS	
Asia Pacific (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS	
Asia Pacific (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS	

Region Name	Region	Endpoint	Protocol	
Asia Pacific (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS	
Asia Pacific (Singapore)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS	
Asia Pacific (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS	
Asia Pacific (Taipei)	ap-east-2	config.ap-east-2.amazonaws.com	HTTPS	
Asia Pacific (Thailand)	ap-southeast-7	config.ap-southeast-7.amazonaws.com	HTTPS	
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS	
Canada (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS	
Canada West (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS	
China (Beijing)	cn-north-1	config.cn-north-1.amazonaws.com.cn	HTTPS	

Region Name	Region	Endpoint	Protocol	
China (Ningxia)	cn-northwest-1	config.cn-northwest-1.amazonaws.com.cn	HTTPS	
Europe (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS	
Europe (Ireland)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS	
Europe (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS	
Europe (Milan)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS	
Europe (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS	
Europe (Spain)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS	
Europe (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS	
Europe (Zurich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS	
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS	
Mexico (Central)	mx-central-1	config.mx-central-1.amazonaws.com	HTTPS	

Region Name	Region	Endpoint	Protocol	
Middle East (Bahrain)	me-south-1	config.me-south-1.amazonaws.com	HTTPS	
Middle East (UAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS	
South America (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS	

Deploying Amazon Config Rules across member accounts in an Amazon Organization is supported in the following Regions.

Region Name	Region	Endpoint	Protocol	
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS	
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS	
US West (N. California)	us-west-1	config.us-west-1.amazonaws.com	HTTPS	
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS	

Region Name	Region	Endpoint	Protocol	
Africa (Cape Town)	af-south-1	config.af-south-1.amazonaws.com	HTTPS	
Asia Pacific (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS	
Asia Pacific (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS	
Asia Pacific (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS	
Asia Pacific (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS	
Asia Pacific (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS	
Asia Pacific (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS	
Asia Pacific (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS	

Region Name	Region	Endpoint	Protocol	
Asia Pacific (Singapore)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS	
Asia Pacific (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS	
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS	
Canada (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS	
Canada West (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS	
Europe (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS	
Europe (Ireland)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS	
Europe (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS	
Europe (Milan)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS	
Europe (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS	

Region Name	Region	Endpoint	Protocol	
Europe (Spain)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS	
Europe (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS	
Europe (Zurich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS	
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS	
Middle East (Bahrain)	me-south-1	config.me-south-1.amazonaws.com	HTTPS	
Middle East (UAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS	
South America (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS	

Components of an Amazon Config Rule

Amazon Config rules evaluate the configuration settings of your Amazon resources. This page discusses the components of a rule.

Topics

- How Amazon Config Rules Work
- Trigger Types

- Evaluation Modes
- Amazon Config Rule Metadata

How Amazon Config Rules Work

While Amazon Config continuously tracks the configuration changes that occur among your resources, it checks whether these changes do not comply with the conditions in your rules. If a resource does not comply with rule, Amazon Config flags the resource and the rule as *noncompliant*.

There are four possible evaluation results for an Amazon Config rule.

Evaluation result	Description
`COMPLIANT`	The rule passes the conditions of the compliance check.
`NON_COMPLIANT`	The rule fails the conditions of the compliance check.
`ERROR`	The one of the required/optional parameter s is not valid, not of the correct type, or is formatted incorrectly.
`NOT_APPLICABLE`	Used to filter out resources that the logic of the rule cannot be applied to. For example, the alb-desync-mode-check rule only checks Application Load Balancers, and ignores Network Load Balancers and Gateway Load Balancers.

For example, when an EC2 volume is created, Amazon Config can evaluate the volume against a rule that requires volumes to be encrypted. If the volume is not encrypted, Amazon Config flags the volume and the rule as noncompliant. Amazon Config can also check all of your resources for account-wide requirements. For example, Amazon Config can check whether the number of EC2 volumes in an account stays within a desired total, or whether an account uses Amazon CloudTrail for logging.

Trigger Types

After you add a rule to your account, Amazon Config compares your resources to the conditions of the rule. After this initial evaluation, Amazon Config continues to run evaluations each time one is triggered. The evaluation triggers are defined as part of the rule, and they can include the following types.

Trigger type	Description
Configuration changes	Amazon Config runs evaluations for the rule when there is a resource that matches the rule's scope and there is a change in configura tion of the resource. The evaluation runs after Amazon Config sends a configuration item change notification. You choose which resources initiate the evaluation by defining the rule's *scope*. The scope can include the following: • One or more resource types • A combination of a resource type and a resource ID • A combination of a tag key and value • When any recorded resource is created, updated, or deleted Amazon Config runs the evaluation when it detects a change to a resource that matches the rule's scope. You can use the scope to define which resources initiate evaluations.
Periodic	Amazon Config runs evaluations for the rule at a frequency that you choose; for example, every 24 hours.

Trigger type	Description
Hybrid	Some rules have both configuration change and periodic triggers. For these rules, Amazon Config evaluates your resources when it detects a configuration change and also at the frequency that you specify.

Evaluation Modes

There are two evaluation modes for Amazon Config rules.

Evaluation mode	Description
Proactive	Use proactive evaluation to evaluate resources before they have been deployed. This allows you to evaluate whether a set of resource properties, if used to define an Amazon resource, would be COMPLIANT or NON_COMPLIANT given the set of proactive rules that you have in your account in your Region.
Detective	Use detective evaluation to evaluate resources that have already been deployed. This allows you to evaluate the configuration settings of your existing resources.

> **Note**
>
> Proactive rules do not remediate resources that are flagged as NON_COMPLIANT or prevent them from being deployed.

For more information, see Turning on Proactive Evaluation for Amazon Config Rules.

List of managed rules with proactive evaluation

For a list of managed rules that support proactive evaluation, see List of Amazon Config Managed Rules by Evaluation Mode.

List of supported resource types for proactive evaluation

The following is a list of resource types that are supported for proactive evaluation:

- `AWS::ApiGateway::Stage`
- `AWS::AutoScaling::AutoScalingGroup`
- `AWS::EC2::EIP`
- `AWS::EC2::Instance`
- `AWS::EC2::Subnet`
- `AWS::Elasticsearch::Domain`
- `AWS::Lambda::Function`
- `AWS::RDS::DBInstance`
- `AWS::Redshift::Cluster`
- `AWS::S3::Bucket`
- `AWS::SNS::Topic`

Amazon Config Rule Metadata

Amazon Config rules can contain the following mutable metadata:

defaultName

The defaultName is the name that instances of a rule will get by default.

description

The rule description provides context for what the rule evaluates. The Amazon Config Console has a limit of 256 characters. As a best practice, the rule description should begin with “Checks if” and include a description of the NON_COMPLIANT scenario. Service Names should be written in full beginning with Amazon or Amazon when first mentioned in the rule description. For example, Amazon CloudTrail or Amazon CloudWatch instead of CloudTrail or CloudWatch for first use. Services names can be abbreviated after subsequent reference.

scope

The scope determines which resource types the rule targets. For a list of supported resource types, see Supported Resource Types.

compulsoryInputParameterDetails

The compulsoryInputParameterDetails are used for parameters that are required for a rule to do its evaluation. For example, the `access-keys-rotated` managed rule includes `maxAccessKeyAge` as a required parameter. If a parameter is required, it will not be marked as (Optional). For each parameter, a type must be specified. Type can be one of "String", "int", "double", "CSV", "boolean" and "StringMap".

optionalInputParameterDetails

The optionalInputParameterDetails are used for parameters that are optional for a rule to do its evaluation. For example, the `elasticsearch-logs-to-cloudwatch` managed rule includes `logTypes` as an optional parameter. For each parameter, a type must be specified. Type can be one of "String", "int", "double", "CSV", "boolean" and "StringMap".

supportedEvaluationModes

The supportedEvaluationModes determines when resources will be evaluated, either before a resource has been deployed or after a resource has been deployed.

`DETECTIVE` is used to evaluate resources which have already been deployed. This allows you to evaluate the configuration settings of your existing resources. `PROACTIVE` is used to evaluate resources before they have been deployed.

This allows you to evaluate whether a set of resource properties, if used to define an Amazon resource, would be COMPLIANT or NON_COMPLIANT given the set of proactive rules that you have in your account in your Region.

You can specify the supportedEvaluationModes to `DETECTIVE`, `PROACTIVE`, or both `DETECTIVE` and `PROACTIVE`. You must specify an evaluation mode and this field cannot remain empty.

> **Note**
>
> Proactive rules do not remediate resources that are flagged as NON_COMPLIANT or prevent them from being deployed.

Amazon Config Managed Rules

Amazon Config provides *Amazon managed rules*, which are predefined, customizable rules that Amazon Config uses to evaluate whether your Amazon resources comply with common best practices. For example, you could use a managed rule to quickly start assessing whether your Amazon Elastic Block Store (Amazon EBS) volumes are encrypted or whether specific tags are applied to your resources.

The Amazon Config console guides you through the process of configuring and activating a managed rule. You can also use the Amazon Command Line Interface or Amazon Config API to pass the JSON code that defines your configuration of a managed rule.

You can customize the behavior of a managed rule to suit your needs. For example, you can define the rule's scope to constrain which resources trigger an evaluation for the rule, such as EC2 instances or volumes.

You can customize the rule's parameters to define attributes that your resources must have to comply with the rule. For example, you can customize a parameter to specify that your security group should block incoming traffic to a specific port number.

Before using managed rules, see Considerations.

Topics

- List of Amazon Config Managed Rules
- List of Amazon Config Managed Rules by Evaluation Mode
- List of Amazon Config Managed Rules by Trigger Type
- List of Amazon Config Managed Rules by Region Availability
- Creating Amazon Config Managed Rules With Amazon CloudFormation Templates

List of Amazon Config Managed Rules

Amazon Config currently supports the following managed rules. Before using these rules, see Considerations.

Topics

- access-keys-rotated
- acm-certificate-expiration-check

- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- athena-workgroup-logging-enabled
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check

- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloudtrail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-logging-enabled
- dax-encryption-enabled
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type

- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-encrypted-in-transit
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-systems-manager
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check

- ec2-managedinstance-platform-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit

- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-ontap-deployment-type-check
- fsx-openzfs-deployment-type-check
- glue-job-logging-enabled
- glue-spark-job-supported-version
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check

- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- restricted-ssh
- ec2-instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloudtrail-enabled
- nacl-no-unrestricted-ssh-rdp

- no-unrestricted-route-to-igw
- opensearch-update-check
- rabbit-mq-supported-version
- rds-automatic-minor-version-upgrade-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled

- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- required-tags
- restricted-common-ports
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check

- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- transfer-connector-logging-enabled
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports

- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

access-keys-rotated

Checks if active IAM access keys are rotated (changed) within the number of days specified in `maxAccessKeyAge`. The rule is NON_COMPLIANT if access keys are not rotated within the specified time period. The default value is 90 days.

Warning

Do not provide your access keys to unauthorized parties, even to help find your account identifiers. By doing this, you might give someone permanent access to your account. The security best practice is to remove passwords and access keys when users no longer need them.

Note

Resource Type Marked as Noncompliant in the Console
If this rule finds that any of your access keys are noncompliant, the `AWS::IAM::User` resource type will also be marked as noncompliant in the Amazon console.
Managed Rules and Global IAM Resource Types
The global IAM resource types onboarded before February 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy`, `AWS::IAM::Role`, and `AWS::IAM::User`) can only be recorded by Amazon Config in Amazon Regions where Amazon Config was available before February 2022. These resource types cannot be recorded in Regions supported by Amazon Config after February 2022. For a list of those Regions, see Recording Amazon Resources | Global Resources.
If you record a global IAM resource type in at least one Region, periodic rules that report compliance on the global IAM resource type will run evaluations in all Regions where the periodic rule is added, even if you have not enabled the recording of the global IAM resource type in the Region where the periodic rule was added.

To avoid unnecessary evaluations, you should only deploy periodic rules that report compliance on a global IAM resource type to one of the supported Regions. For a list of which managed rules are supported in which Regions, see List of Amazon Config Managed Rules by Region Availability.

Limitations

This rule does not apply to Amazon account root user access keys. To delete or rotate your root user access keys, use your root user credentials to sign in to the My Security Credentials page in the Amazon Web Services Management Console at https://aws.amazon.com/console/.

Identifier: ACCESS_KEYS_ROTATED

Resource Types: AWS::IAM::User

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

maxAccessKeyAge, Type: int, Default: 90

Maximum number of days without rotation. Default 90.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

acm-certificate-expiration-check

Checks if Amazon Certificate Manager Certificates in your account are marked for expiration within the specified number of days. Certificates provided by ACM are automatically renewed. ACM does not automatically renew certificates that you import. The rule is NON_COMPLIANT if your certificates are about to expire.

Identifier: ACM_CERTIFICATE_EXPIRATION_CHECK

Resource Types: AWS::ACM::Certificate

Trigger type: Configuration changes and Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Osaka) Region

Parameters:

daysToExpiration (Optional), Type: int, Default: 14

Specify the number of days before the rule flags the ACM Certificate as noncompliant.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

active-mq-supported-version

Checks if an Amazon MQ ActiveMQ broker is running on a specified minimum supported engine version. The rule is NON_COMPLIANT if the ActiveMQ broker is not running on the minimum supported engine version that you specify.

Identifier: ACTIVE_MQ_SUPPORTED_VERSION

Resource Types: AWS::AmazonMQ::Broker

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

supportedEngineVersion, Type: String

String value for the rule to check the minimum supported engine version for the ActiveMQ broker. ActiveMQ brokers use semantic versioning specification: X.Y.Z. X denotes the major version, Y represents the minor version, and Z denotes the patch version.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

alb-desync-mode-check

Checks if an Application Load Balancer (ALB) is configured with a user defined desync mitigation mode. The rule is NON_COMPLIANT if ALB desync mitigation mode does not match with the user defined desync mitigation mode.

Identifier: ALB_DESYNC_MODE_CHECK

Resource Types: AWS::ElasticLoadBalancingV2::LoadBalancer

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

desyncMode, Type: CSV

> Comma-separated list, in which customers can choose max 2 values among - 'defensive', 'strictest', and 'monitor'.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

alb-http-drop-invalid-header-enabled

Checks if rule evaluates Amazon Application Load Balancers (ALB) to ensure they are configured to drop http headers. The rule is NON_COMPLIANT if the value of routing.http.drop_invalid_header_fields.enabled is set to false.

Identifier: ALB_HTTP_DROP_INVALID_HEADER_ENABLED

Resource Types: AWS::ElasticLoadBalancingV2::LoadBalancer

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Osaka) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

alb-http-to-https-redirection-check

Checks if HTTP to HTTPS redirection is configured on all HTTP listeners of Application Load Balancers. The rule is NON_COMPLIANT if one or more HTTP listeners of Application Load Balancer do not have HTTP to HTTPS redirection configured. The rule is also NON_COMPLIANT if one of more HTTP listeners have forwarding to an HTTP listener instead of redirection.

Identifier: ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK

Resource Types: AWS::ElasticLoadBalancingV2::LoadBalancer

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Osaka) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

alb-waf-enabled

Checks if Amazon WAF is enabled on Application Load Balancers (ALBs). The rule is NON_COMPLIANT if key: waf.enabled is set to false.

Identifier: ALB_WAF_ENABLED

Resource Types: AWS::ElasticLoadBalancingV2::LoadBalancer

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Osaka) Region

Parameters:

wafWebAclIds (Optional), Type: CSV

Comma separated list of web ACL ID (for WAF) or web ACL ARN (for WAFV2) checking for ALB association.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

api-gwv2-access-logs-enabled

Checks if Amazon API Gateway V2 stages have access logging enabled. The rule is NON_COMPLIANT if 'accessLogSettings' is not present in Stage configuration.

Identifier: API_GWV2_ACCESS_LOGS_ENABLED

Resource Types: AWS::ApiGatewayV2::Stage

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

api-gwv2-authorization-type-configured

Checks if Amazon API Gatewayv2 API routes have an authorization type set. This rule is NON_COMPLIANT if the authorization type is NONE.

Identifier: API_GWV2_AUTHORIZATION_TYPE_CONFIGURED

Resource Types: AWS::ApiGatewayV2::Route

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

authorizationType (Optional), Type: String

> Parameter to check API routes' authorization types against. String parameters matching CUSTOM, Amazon_IAM, JWT are valid.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

api-gw-associated-with-waf

Checks if an Amazon API Gateway API stage is using an Amazon WAF web access control list (web ACL). The rule is NON_COMPLIANT if an Amazon WAF Web ACL is not used or if a used Amazon Web ACL does not match what is listed in the rule parameter.

Identifier: API_GW_ASSOCIATED_WITH_WAF

Resource Types: AWS::ApiGateway::Stage

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Mexico (Central), Asia Pacific (Taipei) Region

Parameters:

WebAclArns (Optional), Type: CSV

Comma-separated list of web ACL Amazon Resource Names (ARNs).

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

api-gw-cache-enabled-and-encrypted

Checks if all methods in Amazon API Gateway stages have cache enabled and cache encrypted. The rule is NON_COMPLIANT if any method in an Amazon API Gateway stage is not configured to cache or the cache is not encrypted.

Identifier: API_GW_CACHE_ENABLED_AND_ENCRYPTED

Resource Types: AWS::ApiGateway::Stage

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Mexico (Central), Asia Pacific (Taipei) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

api-gw-endpoint-type-check

Checks if Amazon API Gateway APIs are of the type specified in the rule parameter `endpointConfigurationType`. The rule returns NON_COMPLIANT if the REST API does not match the endpoint type configured in the rule parameter.

Identifier: API_GW_ENDPOINT_TYPE_CHECK

Resource Types: AWS::ApiGateway::RestApi

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Mexico (Central), Asia Pacific (Taipei) Region

Parameters:

endpointConfigurationTypes, Type: String

Comma-separated list of allowed endpointConfigurationTypes. Allowed values are REGIONAL, PRIVATE and EDGE.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

api-gw-execution-logging-enabled

Checks if all methods in Amazon API Gateway stages have logging enabled. The rule is NON_COMPLIANT if logging is not enabled, or if `loggingLevel` is neither ERROR nor INFO.

Identifier: API_GW_EXECUTION_LOGGING_ENABLED

Resource Types: AWS::ApiGateway::Stage, AWS::ApiGatewayV2::Stage

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Mexico (Central), Asia Pacific (Taipei) Region

Parameters:

loggingLevel (Optional), Type: String, Default: ERROR,INFO

Comma-separated list of specific logging levels (for example, ERROR, INFO or ERROR,INFO).

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

api-gw-ssl-enabled

Checks if a REST API stage uses an SSL certificate. The rule is NON_COMPLIANT if the REST API stage does not have an associated SSL certificate.

> **Note**
>
> This rule returns `NOT_APPLICABLE` if the GetIntegration API returns `AWS` as type.

Identifier: API_GW_SSL_ENABLED

Resource Types: AWS::ApiGateway::Stage

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Mexico (Central), Asia Pacific (Taipei) Region

Parameters:

CertificateIDs (Optional), Type: CSV

Comma-separated list of client certificate IDs configured on a REST API stage.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

api-gw-xray-enabled

Checks if Amazon X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise.

Identifier: API_GW_XRAY_ENABLED

Resource Types: AWS::ApiGateway::Stage

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Mexico (Central), Asia Pacific (Taipei) Region

Parameters:

None

Proactive Evaluation

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with Amazon Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
   "TracingEnabled": BOOLEAN,
   "RestApiId": "my-rest-api-Id",
}
...
```

For more information on proactive evaluation, see Evaluation Mode.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

approved-amis-by-id

Checks if EC2 instances are using specified Amazon Machine Images (AMIs). Specify a list of approved AMI IDs. Running instances with AMIs that are not on this list are NON_COMPLIANT.

Identifier: APPROVED_AMIS_BY_ID

Resource Types: AWS::EC2::Instance

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

amiIds, Type: CSV

Comma-separated list of up to 21 AMI IDs. There is a 1024 characters limit.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

approved-amis-by-tag

Checks if EC2 instances are using specified Amazon Machine Images (AMIs). Specify the tags that identify the AMIs. Running instances with AMIs that don't have at least one of the specified tags are NON_COMPLIANT.

Identifier: APPROVED_AMIS_BY_TAG

Resource Types: AWS::EC2::Instance

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

amisByTagKeyAndValue, Type: StringMap, Default: tag-key:tag-value,other-tag-key

Comma-separated list of up to 10 AMIs tags (tag-key:tag-value). For example, tag-key1 matches AMIs with tag-key1; tag-key2:value2 matches tag-key2 with the value 2.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

appsync-associated-with-waf

Checks if Amazon AppSync APIs are associated with Amazon WAFv2 web access control lists (ACLs). The rule is NON_COMPLIANT for an Amazon AppSync API if it is not associated with a web ACL.

Identifier: APPSYNC_ASSOCIATED_WITH_WAF

Resource Types: AWS::AppSync::GraphQLApi

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

wafWebAclARNs (Optional), Type: CSV

Comma-separated list of Amazon Resource Names (ARNs) for authorized web ACLs.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

appsync-authorization-check

Checks if an Amazon AppSync API is using allowed authorization mechanisms. The rule is NON_COMPLIANT if an unapproved authorization mechanism is being used.

Identifier: APPSYNC_AUTHORIZATION_CHECK

Resource Types: AWS::AppSync::GraphQLApi

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary) Region

Parameters:

AllowedAuthorizationTypes, Type: CSV

Comma-separated list of allowed Amazon AppSync authorization mechanisms. Allowed values are: 'API_KEY', 'Amazon_LAMBDA', 'Amazon_IAM', 'OPENID_CONNECT', 'AMAZON_COGNITO_USER_POOLS'.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

appsync-logging-enabled

Checks if an Amazon AppSync API has logging enabled. The rule is NON_COMPLIANT if logging is not enabled, or if the field logging levels for the Amazon AppSync API do not match the values specified in the '`fieldLoggingLevel`' rule parameter.

Identifier: APPSYNC_LOGGING_ENABLED

Resource Types: AWS::AppSync::GraphQLApi

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary) Region

Parameters:

fieldLoggingLevel (Optional), Type: CSV

Comma-separated list of field logging levels for the rule to check. For example, "ERROR, INFO".

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

athena-workgroup-encrypted-at-rest

Checks if an Amazon Athena workgroup is encrypted at rest. The rule is NON_COMPLIANT if encryption of data at rest is not enabled for an Athena workgroup.

Identifier: ATHENA_WORKGROUP_ENCRYPTED_AT_REST

Resource Types: AWS::Athena::WorkGroup

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

athena-workgroup-logging-enabled

Checks if Amazon Athena WorkGroup publishes usage metrics to Amazon CloudWatch. The rule is NON_COMPLIANT if an Amazon Athena WorkGroup 'PublishCloudWatchMetricsEnabled' is set to false.

Identifier: ATHENA_WORKGROUP_LOGGING_ENABLED

Resource Types: AWS::Athena::WorkGroup

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

autoscaling-group-elb-healthcheck-required

Checks if your Amazon EC2 Auto Scaling groups that are associated with an Elastic Load Balancer use Elastic Load Balancing health checks. The rule is NON_COMPLIANT if the Amazon EC2 Auto Scaling groups are not using Elastic Load Balancing health checks.

Identifier: AUTOSCALING_GROUP_ELB_HEALTHCHECK_REQUIRED

Resource Types: AWS::AutoScaling::AutoScalingGroup

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Middle East (UAE), Asia Pacific (Taipei) Region

Parameters:

None

Proactive Evaluation

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with Amazon Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
   "LoadBalancerNames": "[my-load-balancer-1, my-load-balancer-2, my-load-balancer-3, ...]",
   "HealthCheckType": HealthCheckType*"
}
...
```

*The valid values are EC2 (default), ELB, and VPC_LATTICE. The VPC_LATTICE health check type is reserved for use with VPC Lattice, which is in preview release and is subject to change. For more information, see Health checks for Auto Scaling instances in the Amazon EC2 Auto Scaling User Guide.

For more information on proactive evaluation, see Evaluation Mode.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

autoscaling-launchconfig-requires-imdsv2

Checks whether only IMDSv2 is enabled. This rule is NON_COMPLIANT if the Metadata version is not included in the launch configuration or if both Metadata V1 and V2 are enabled.

Identifier: AUTOSCALING_LAUNCHCONFIG_REQUIRES_IMDSV2

Resource Types: AWS::AutoScaling::LaunchConfiguration

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

autoscaling-launch-config-hop-limit

Checks the number of network hops that the metadata token can travel. This rule is NON_COMPLIANT if the Metadata response hop limit is greater than 1.

Identifier: AUTOSCALING_LAUNCH_CONFIG_HOP_LIMIT

Resource Types: AWS::AutoScaling::LaunchConfiguration

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Asia Pacific (Malaysia), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

autoscaling-launch-config-public-ip-disabled

Checks if Amazon EC2 Auto Scaling groups have public IP addresses enabled through Launch Configurations. The rule is NON_COMPLIANT if the Launch Configuration for an Amazon EC2 Auto Scaling group has AssociatePublicIpAddress set to 'true'.

Identifier: AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED

Resource Types: AWS::AutoScaling::LaunchConfiguration

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Taipei) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

autoscaling-launch-template

Checks if an Amazon Elastic Compute Cloud (EC2) Auto Scaling group is created from an EC2 launch template. The rule is NON_COMPLIANT if the scaling group is not created from an EC2 launch template.

Identifier: AUTOSCALING_LAUNCH_TEMPLATE

Resource Types: AWS::AutoScaling::AutoScalingGroup

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

autoscaling-multiple-az

Checks if the Auto Scaling group spans multiple Availability Zones. The rule is NON_COMPLIANT if the Auto Scaling group does not span multiple Availability Zones.

Identifier: AUTOSCALING_MULTIPLE_AZ

Resource Types: AWS::AutoScaling::AutoScalingGroup

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Canada West (Calgary) Region

Parameters:

minAvailabilityZones (Optional), Type: int

Minimum number of expected Availability zones.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

autoscaling-multiple-instance-types

Checks if an Amazon EC2 Auto Scaling group uses multiple instance types. The rule is NON_COMPLIANT if the Amazon EC2 Auto Scaling group has only one instance type defined. This rule does not evaluate attribute-based instance types.

Identifier: AUTOSCALING_MULTIPLE_INSTANCE_TYPES

Resource Types: AWS::AutoScaling::AutoScalingGroup

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

beanstalk-enhanced-health-reporting-enabled

Checks if an Amazon Elastic Beanstalk environment is configured for enhanced health reporting. The rule is COMPLIANT if the environment is configured for enhanced health reporting. The rule is NON_COMPLIANT if the environment is configured for basic health reporting.

Identifier: BEANSTALK_ENHANCED_HEALTH_REPORTING_ENABLED

Resource Types: AWS::ElasticBeanstalk::Environment

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

clb-desync-mode-check

Checks if Classic Load Balancers (CLB) are configured with a user defined Desync mitigation mode. The rule is NON_COMPLIANT if CLB Desync mitigation mode does not match with user defined Desync mitigation mode.

Identifier: CLB_DESYNC_MODE_CHECK

Resource Types: AWS::ElasticLoadBalancing::LoadBalancer

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

desyncMode, Type: CSV

> Comma-separated list of values. You can select a max of two. Valid values include 'Defensive', 'Strictest', and 'Monitor'.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

clb-multiple-az

Checks if a Classic Load Balancer spans multiple Availability Zones (AZs). The rule is NON_COMPLIANT if a Classic Load Balancer spans less than 2 AZs or does not span number of AZs mentioned in the `minAvailabilityZones` parameter (if provided).

Identifier: CLB_MULTIPLE_AZ

Resource Types: AWS::ElasticLoadBalancing::LoadBalancer

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Canada West (Calgary) Region

Parameters:

minAvailabilityZones (Optional), Type: int

Desired minimum number of expected AZs. Valid values are between 2 and 10, both inclusive. Default value is 2 if parameter is not specified.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

cloudformation-stack-drift-detection-check

Checks if the actual configuration of a Amazon CloudFormation (Amazon CloudFormation) stack differs, or has drifted, from the expected configuration. A stack is considered to have drifted if one or more of its resources differ from their expected configuration. The rule and the stack are COMPLIANT when the stack drift status is IN_SYNC. The rule is NON_COMPLIANT if the stack drift status is DRIFTED.

Note

This rule performs the DetectStackDrift operation on each stack in your account. The DetectStackDrift operation can take up to several minutes, depending on the number of resources contained within the stack. Given that the maximum execution time of this rule is limited to 15 mins, it is possible that the rule times out before it completes the evaluation of all the stacks in your account.
If you encounter this issue, it is suggested that you to restrict the number of stacks in-scope for the rule, using tags. You can do the following:

1. Divide your stacks into groups, each with a different tag.

2. Apply the same tag to all the stacks in that group.
3. Have multiple instances of this rule in your account, each scoped by a different tag. This allows each instance of the rule to only process the stacks which have the corresponding tag mentioned in its scope.

Identifier: CLOUDFORMATION_STACK_DRIFT_DETECTION_CHECK

Resource Types: AWS::CloudFormation::Stack

Trigger type: Configuration changes and Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Melbourne), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

cloudformationRoleArn, Type: String

The Amazon Resource Name (ARN) of the IAM role with policy permissions to detect drift for Amazon CloudFormation stacks. For information on required IAM permissions for the role, see Detecting unmanaged configuration changes to stacks and resources | Considerations when detecting drift in the *Amazon CloudFormation User Guide*.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

cloudformation-stack-notification-check

Checks if your CloudFormation stacks send event notifications to an Amazon SNS topic. Optionally checks if specified Amazon SNS topics are used. The rule is NON_COMPLIANT if CloudFormation stacks do not send notifications.

Identifier: CLOUDFORMATION_STACK_NOTIFICATION_CHECK

Resource Types: AWS::CloudFormation::Stack

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

snsTopic1 (Optional), Type: String

SNS Topic ARN.

snsTopic2 (Optional), Type: String

SNS Topic ARN.

snsTopic3 (Optional), Type: String

SNS Topic ARN.

snsTopic4 (Optional), Type: String

SNS Topic ARN.

snsTopic5 (Optional), Type: String

SNS Topic ARN.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

cloudtrail-s3-bucket-access-logging

Checks if the S3 bucket configurations for your Amazon CloudTrail logs have Amazon S3 server access logging enabled. The rule is NON_COMPLIANT if at least one S3 bucket for a CloudTrail trail does not have S3 server access logging enabled.

Identifier: CLOUDTRAIL_S3_BUCKET_ACCESS_LOGGING

Resource Types: AWS::CloudTrail::Trail

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

cloudtrail-s3-bucket-public-access-prohibited

Checks if the S3 bucket configurations for your Amazon CloudTrail logs block public access. The rule is NON_COMPLIANT if at least one S3 bucket for a CloudTrail trail is publicly accessible.

Identifier: CLOUDTRAIL_S3_BUCKET_PUBLIC_ACCESS_PROHIBITED

Resource Types: AWS::CloudTrail::Trail

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

cloudtrail-s3-dataevents-enabled

Checks if at least one Amazon CloudTrail trail is logging Amazon Simple Storage Service (Amazon S3) data events for all S3 buckets. The rule is NON_COMPLIANT if there are trails or if no trails record S3 data events.

Identifier: CLOUDTRAIL_S3_DATAEVENTS_ENABLED

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Taipei) Region

Parameters:

S3BucketNames (Optional), Type: String

Comma-separated list of S3 bucket names for which data events logging should be enabled. Default behavior checks for all S3 buckets.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

cloudtrail-security-trail-enabled

Checks that there is at least one Amazon CloudTrail trail defined with security best practices. This rule is COMPLIANT if there is at least one trail that meets all of the following:

- records global service events
- is a multi-region trail
- has Log file validation enabled
- encrypted with a KMS key
- records events for reads and writes
- records management events
- does not exclude any management events

This rule is NON_COMPLIANT if no trails meet all of the criteria mentioned above.

Identifier: CLOUDTRAIL_SECURITY_TRAIL_ENABLED

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

cloudwatch-alarm-action-check

Checks if CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally checks if any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter.

Identifier: CLOUDWATCH_ALARM_ACTION_CHECK

Resource Types: AWS::CloudWatch::Alarm

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

alarmActionRequired, Type: String, Default: true

Alarms have at least one action.

insufficientDataActionRequired, Type: String, Default: true

Alarms have at least one action when the alarm transitions to the INSUFFICIENT_DATA state from any other state.

okActionRequired, Type: String, Default: false

Alarms have at least one action when the alarm transitions to an OK state from any other state.

action1 (Optional), Type: String

The action to execute, specified as an ARN.

action2 (Optional), Type: String

The action to execute, specified as an ARN.

action3 (Optional), Type: String

The action to execute, specified as an ARN.

action4 (Optional), Type: String

The action to execute, specified as an ARN.

action5 (Optional), Type: String

The action to execute, specified as an ARN.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

cloudwatch-alarm-action-enabled-check

Checks if Amazon CloudWatch alarms actions are in enabled state. The rule is NON_COMPLIANT if the CloudWatch alarms actions are not in enabled state.

Identifier: CLOUDWATCH_ALARM_ACTION_ENABLED_CHECK

Resource Types: AWS::CloudWatch::Alarm

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

cloudwatch-alarm-resource-check

Checks if a resource type has a CloudWatch alarm for the named metric. For resource type, you can specify EBS volumes, EC2 instances, Amazon RDS clusters, or S3 buckets. The rule is COMPLIANT if the named metric has a resource ID and CloudWatch alarm.

Identifier: CLOUDWATCH_ALARM_RESOURCE_CHECK

Resource Types: AWS::EC2::Instance, AWS::RDS::DBCluster, AWS::S3::Bucket, AWS::EC2::Volume

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions

Parameters:

resourceType, Type: String

Amazon resource type. The value can be one of the following: AWS::EC2::Volume, AWS::EC2::Instance, AWS::RDS::DBCluster, or AWS::S3::Bucket.

metricName, Type: String

The name for the metric associated with the alarm (for example, 'CPUUtilization' for EC2 instances).

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

cloudwatch-alarm-settings-check

Checks whether CloudWatch alarms with the given metric name have the specified settings.

Identifier: CLOUDWATCH_ALARM_SETTINGS_CHECK

Resource Types: AWS::CloudWatch::Alarm

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

metricName, Type: String

The name for the metric associated with the alarm.

threshold (Optional), Type: int

The value against which the specified statistic is compared.

evaluationPeriods (Optional), Type: int

The number of periods over which data is compared to the specified threshold.

period (Optional), Type: int, Default: 300

The period, in seconds, during which the specified statistic is applied.

comparisonOperator (Optional), Type: String

The operation for comparing the specified statistic and threshold (for example, 'GreaterThanThreshold').

statistic (Optional), Type: String

The statistic for the metric associated with the alarm (for example, 'Average' or 'Sum').

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

cloudwatch-log-group-encrypted

Checks if Amazon CloudWatch Log Groups are encrypted with any Amazon KMS key or a specified Amazon KMS key Id. The rule is NON_COMPLIANT if a CloudWatch Log Group is not encrypted with a KMS key or is encrypted with a KMS key not supplied in the rule parameter.

Identifier: CLOUDWATCH_LOG_GROUP_ENCRYPTED

Resource Types: AWS::Logs::LogGroup

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Middle East (UAE), Asia Pacific (Taipei) Region

Parameters:

KmsKeyId (Optional), Type: String

Amazon Resource Name (ARN) of the ID for the KMS key that is used to encrypt the log group.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

cloud-trail-cloud-watch-logs-enabled

Checks if Amazon CloudTrail trails are configured to send logs to CloudWatch logs. The trail is NON_COMPLIANT if the CloudWatchLogsLogGroupArn property of the trail is empty.

Identifier: CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED

Resource Types: AWS::CloudTrail::Trail

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions

Parameters:

expectedDeliveryWindowAge (Optional), Type: int

Maximum age in hours of the most recent delivery to CloudWatch logs that satisfies compliance.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

cloudtrail-enabled

Important

For this rule, the rule identifier (CLOUD_TRAIL_ENABLED) and rule name (cloudtrail-enabled) are different.

Checks if an Amazon CloudTrail trail is enabled in your Amazon account. The rule is NON_COMPLIANT if a trail is not enabled. Optionally, the rule checks a specific S3 bucket, Amazon Simple Notification Service (Amazon SNS) topic, and CloudWatch log group.

Identifier: CLOUD_TRAIL_ENABLED

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions

Parameters:

s3BucketName (Optional), Type: String

Name of S3 bucket for CloudTrail to deliver log files to.

snsTopicArn (Optional), Type: String

SNS topic ARN for CloudTrail to use for notifications.

cloudWatchLogsLogGroupArn (Optional), Type: String

CloudWatch log group ARN for CloudTrail to send data to.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

cloud-trail-encryption-enabled

Checks if Amazon CloudTrail is configured to use the server side encryption (SSE) Amazon Key Management Service (Amazon KMS) encryption. The rule is COMPLIANT if the KmsKeyId is defined.

Identifier: CLOUD_TRAIL_ENCRYPTION_ENABLED

Resource Types: AWS::CloudTrail::Trail

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

cloud-trail-log-file-validation-enabled

Checks if Amazon CloudTrail creates a signed digest file with logs. Amazon recommends that the file validation must be enabled on all trails. The rule is NON_COMPLIANT if the validation is not enabled.

Identifier: CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED

Resource Types: AWS::CloudTrail::Trail

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

cmk-backing-key-rotation-enabled

Checks if automatic key rotation is enabled for each key and matches to the key ID of the customer created Amazon KMS key. The rule is NON_COMPLIANT if the Amazon Config recorder role for a resource does not have the kms:DescribeKey permission.

> **Note**
>
> Automatic key rotation is not supported for asymmetric KMS keys, HMAC KMS keys, KMS keys with imported key material, or KMS keys in custom key stores.

Identifier: CMK_BACKING_KEY_ROTATION_ENABLED

Resource Types: AWS::KMS::Key

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Middle East (UAE) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

codebuild-project-environment-privileged-check

Checks if an Amazon CodeBuild project environment has privileged mode enabled. The rule is NON_COMPLIANT for a CodeBuild project if 'privilegedMode' is set to 'true'.

Identifier: CODEBUILD_PROJECT_ENVIRONMENT_PRIVILEGED_CHECK

Resource Types: AWS::CodeBuild::Project

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

exemptedProjects (Optional), Type: CSV

> Comma-separated list of CodeBuild project names that are allowed to have 'privilegedMode' with value 'true'.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

codebuild-project-envvar-awscred-check

Checks if the project contains environment variables Amazon_ACCESS_KEY_ID and Amazon_SECRET_ACCESS_KEY. The rule is NON_COMPLIANT when the project environment variables contains plaintext credentials.

Identifier: CODEBUILD_PROJECT_ENVVAR_AWSCRED_CHECK

Resource Types: AWS::CodeBuild::Project

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

codebuild-project-logging-enabled

Checks if an Amazon CodeBuild project environment has at least one log option enabled. The rule is NON_COMPLIANT if the status of all present log configurations is set to 'DISABLED'.

Identifier: CODEBUILD_PROJECT_LOGGING_ENABLED

Resource Types: AWS::CodeBuild::Project

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

s3BucketNames (Optional), Type: String

Comma-separated list of Amazon S3 bucket names that logs should be sent to if S3 logs are configured.

cloudWatchGroupNames (Optional), Type: String

Comma-separated list of Amazon CloudWatch log group names that logs should be be sent to if CloudWatch logs are configured.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

codebuild-project-s3-logs-encrypted

Checks if a Amazon CodeBuild project configured with Amazon S3 Logs has encryption enabled for its logs. The rule is NON_COMPLIANT if 'encryptionDisabled' is set to 'true' in a S3LogsConfig of a CodeBuild project.

Identifier: CODEBUILD_PROJECT_S3_LOGS_ENCRYPTED

Resource Types: AWS::CodeBuild::Project

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

exemptedProjects (Optional), Type: CSV

Comma-separated list of CodeBuild project names that are allowed to output unencrypted logs.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

codebuild-project-source-repo-url-check

Checks if the Bitbucket source repository URL contains sign-in credentials or not. The rule is NON_COMPLIANT if the URL contains any sign-in information and COMPLIANT if it doesn't.

Identifier: CODEBUILD_PROJECT_SOURCE_REPO_URL_CHECK

Resource Types: AWS::CodeBuild::Project

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

codebuild-report-group-encrypted-at-rest

Checks if an Amazon CodeBuild report group has encryption at rest setting enabled. The rule is NON_COMPLIANT if 'EncryptionDisabled' is 'true'.

Identifier: CODEBUILD_REPORT_GROUP_ENCRYPTED_AT_REST

Resource Types: AWS::CodeBuild::ReportGroup

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

custom-eventbus-policy-attached

Checks if Amazon EventBridge custom event buses have a resource-based policy attached. The rule is NON_COMPLIANT if a custom event bus policy does not have an attached resource-based policy.

Identifier: CUSTOM_EVENTBUS_POLICY_ATTACHED

Resource Types: AWS::Events::EventBus

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

cw-loggroup-retention-period-check

Checks if an Amazon CloudWatch LogGroup retention period is set to greater than 365 days or else a specified retention period. The rule is NON_COMPLIANT if the retention period is less than `MinRetentionTime`, if specified, or else 365 days.

> **Note**
>
> If the retention setting is "Never expire" for a log group, the rule is marked as COMPLIANT.

Identifier: CW_LOGGROUP_RETENTION_PERIOD_CHECK

Resource Types: AWS::Logs::LogGroup

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Middle East (UAE) Region

Parameters:

LogGroupNames (Optional), Type: CSV

A comma-separated list of Log Group names to check the retention period.

MinRetentionTime (Optional), Type: int

Specify the retention time in days. Valid values are: 1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365, 400, 545, 731, 1827, and 3653. The default retention period is 365 days.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

datasync-task-logging-enabled

Checks if an Amazon DataSync task has Amazon CloudWatch logging enabled. The rule is NON_COMPLIANT if an Amazon DataSync task does not have Amazon CloudWatch logging enabled or if the logging level is not equivalent to the logging level that you specify.

Identifier: DATASYNC_TASK_LOGGING_ENABLED

Resource Types: AWS::DataSync::Task

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

logLevel (Optional), Type: String

String value for the logging level. Valid values include: 'BASIC' and 'TRANSFER'. If not specified, the default value is 'BASIC'.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

dax-encryption-enabled

Checks if Amazon DynamoDB Accelerator (DAX) clusters are encrypted. The rule is NON_COMPLIANT if a DAX cluster is not encrypted.

Identifier: DAX_ENCRYPTION_ENABLED

Resource Types: AWS::DAX::Cluster

Trigger type: Periodic

Amazon Web Services Region: Only available in Europe (Stockholm), China (Beijing), Asia Pacific (Mumbai), Europe (Paris), US East (Ohio), Europe (Ireland), Europe (Frankfurt), South America (Sao Paulo), US East (N. Virginia), Europe (London), Asia Pacific (Tokyo), US West (Oregon), US West (N. California), Asia Pacific (Singapore), Asia Pacific (Sydney), Europe (Spain), China (Ningxia) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

db-instance-backup-enabled

Checks if RDS DB instances have backups enabled. Optionally, the rule checks the backup retention period and the backup window.

Identifier: DB_INSTANCE_BACKUP_ENABLED

Resource Types: AWS::RDS::DBInstance

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

backupRetentionPeriod (Optional), Type: int

Retention period for backups.

backupRetentionMinimum (Optional), Type: int

Minimum retention period for backups.

preferredBackupWindow (Optional), Type: String

Time range in which backups are created.

checkReadReplicas (Optional), Type: boolean

Checks whether RDS DB instances have backups enabled for read replicas.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

desired-instance-tenancy

Checks EC2 instances for a 'tenancy' value. Also checks if AMI IDs are specified to be launched from those AMIs or if Host IDs are launched on those Dedicated Hosts. The rule is COMPLIANT if the instance matches a host and an AMI, if specified, in a list.

Identifier: DESIRED_INSTANCE_TENANCY

Resource Types: AWS::EC2::Instance

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

tenancy, Type: String

Desired tenancy of the instances. Valid values are DEDICATED, HOST and DEFAULT.

imageId (Optional), Type: CSV

The rule evaluates instances launched only from AMIs with the specified IDs. Separate multiple AMI IDs with commas.

hostId (Optional), Type: CSV

The IDs of the EC2 Dedicated Hosts on which the instances are meant to be launched. Separate multiple Host IDs with commas.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

desired-instance-type

Checks if your EC2 instances are of a specific instance type. The rule is NON_COMPLIANT if an EC2 instance is not specified in the parameter list. For a list of supported EC2 instance types, see Instance types in the EC2 User Guide for Linux Instances.

Identifier: DESIRED_INSTANCE_TYPE

Resource Types: AWS::EC2::Instance

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

instanceType, Type: CSV

Comma-separated list of EC2 instance types (for example, "t2.small, m4.large, i2.xlarge").

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

dms-auto-minor-version-upgrade-check

Checks if an Amazon Database Migration Service (Amazon DMS) replication instance has automatic minor version upgrades enabled. The rule is NON_COMPLIANT if an Amazon DMS replication instance is not configured with automatic minor version upgrades.

Identifier: DMS_AUTO_MINOR_VERSION_UPGRADE_CHECK

Resource Types: AWS::DMS::ReplicationInstance

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

dms-endpoint-ssl-configured

Checks if Amazon Database Migration Service (Amazon DMS) endpoints are configured with an SSL connection. The rule is NON_COMPLIANT if Amazon DMS does not have an SSL connection configured.

Context: SSL/TLS connections provide one layer of security by encrypting data that moves between your client and a DB instance. Using server certificate provides an extra layer of security by validating that the connection is being made to an Amazon RDS DB instance. It does so by checking the server certificate that is automatically installed on all DB instances that you provision. By enabling SSL connection on Amazon DMS, you protect the confidentiality of the data during the migration.

To configure SSL connection for Amazon DMS, see Using SSL/TLS to encrypt a connection to a DB instance or cluster in the *Amazon Relational Database Service User Guide*.

Identifier: DMS_ENDPOINT_SSL_CONFIGURED

Resource Types: AWS::DMS::Endpoint

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific

(Melbourne), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

dms-replication-not-public

Checks if Amazon Database Migration Service (Amazon DMS) replication instances are public. The rule is NON_COMPLIANT if PubliclyAccessible field is set to true.

Identifier: DMS_REPLICATION_NOT_PUBLIC

Resource Types: AWS::DMS::ReplicationInstance

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Taipei) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

dms-replication-task-sourcedb-logging

Checks if logging is enabled with a valid severity level for Amazon DMS replication tasks of a source database. The rule is NON_COMPLIANT if logging is not enabled or logs for DMS replication tasks of a source database have a severity level that is not valid.

Identifier: DMS_REPLICATION_TASK_SOURCEDB_LOGGING

Resource Types: AWS::DMS::ReplicationTask

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

dms-replication-task-targetdb-logging

Checks if logging is enabled with a valid severity level for Amazon DMS replication task events of a target database. The rule is NON_COMPLIANT if logging is not enabled or replication task logging of a target database has a severity level that is not valid.

Identifier: DMS_REPLICATION_TASK_TARGETDB_LOGGING

Resource Types: AWS::DMS::ReplicationTask

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

docdb-cluster-encrypted-in-transit

Checks if connections to Amazon DocumentDB clusters are configured to use encryption in transit. The rule is NON_COMPLIANT if the parameter group is not "in-sync", or the TLS parameter is set to either "disabled" or a value in `excludeTlsParameters`.

Identifier: DOCDB_CLUSTER_ENCRYPTED_IN_TRANSIT

Resource Types: AWS::RDS::DBCluster

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Europe (Stockholm), Middle East (Bahrain), Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), US West (N. California), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

excludeTlsParameters (Optional), Type: CSV

> Comma-separated list of TLS cluster parameters for the rule to NOT check. Default value: 'disabled'.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

dynamodb-autoscaling-enabled

Checks if Amazon DynamoDB tables or global secondary indexes can process read/write capacity using on-demand mode or provisioned mode with auto scaling enabled. The rule is NON_COMPLIANT if either mode is used without auto scaling enabled

Identifier: DYNAMODB_AUTOSCALING_ENABLED

Resource Types: AWS::DynamoDB::Table

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions

Parameters:

minProvisionedReadCapacity (Optional), Type: int

The minimum number of units that should be provisioned with read capacity in the Auto Scaling group.

maxProvisionedReadCapacity (Optional), Type: int

The maximum number of units that should be provisioned with read capacity in the Auto Scaling group.

targetReadUtilization (Optional), Type: double

The target utilization percentage for read capacity. Target utilization is expressed in terms of the ratio of consumed capacity to provisioned capacity.

minProvisionedWriteCapacity (Optional), Type: int

The minimum number of units that should be provisioned with write capacity in the Auto Scaling group.

maxProvisionedWriteCapacity (Optional), Type: int

The maximum number of units that should be provisioned with write capacity in the Auto Scaling group.

targetWriteUtilization (Optional), Type: double

The target utilization percentage for write capacity. Target utilization is expressed in terms of the ratio of consumed capacity to provisioned capacity.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

dynamodb-in-backup-plan

Checks whether Amazon DynamoDB table is present in Amazon Backup Plans. The rule is NON_COMPLIANT if Amazon DynamoDB tables are not present in any Amazon Backup plan.

Identifier: DYNAMODB_IN_BACKUP_PLAN

Resource Types: AWS::DynamoDB::Table

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Taipei) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

dynamodb-pitr-enabled

Checks if point-in-time recovery (PITR) is enabled for Amazon DynamoDB tables. The rule is NON_COMPLIANT if PITR is not enabled for DynamoDB tables.

Identifier: DYNAMODB_PITR_ENABLED

Resource Types: AWS::DynamoDB::Table

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

dynamodb-table-deletion-protection-enabled

Checks if an Amazon DynamoDB table have deletion protection set to enabled. The rule is NON_COMPLIANT if the table have deletion protection set to disabled.

Identifier: DYNAMODB_TABLE_DELETION_PROTECTION_ENABLED

Resource Types: AWS::DynamoDB::Table

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

dynamodb-table-encrypted-kms

Checks if Amazon DynamoDB table is encrypted with Amazon Key Management Service (KMS). The rule is NON_COMPLIANT if Amazon DynamoDB table is not encrypted with Amazon KMS. The rule is also NON_COMPLIANT if the encrypted Amazon KMS key is not present in `kmsKeyArns` input parameter.

Identifier: DYNAMODB_TABLE_ENCRYPTED_KMS

Resource Types: AWS::DynamoDB::Table

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Taipei) Region

Parameters:

kmsKeyArns (Optional), Type: CSV

> Comma separated list of Amazon KMS key ARNs allowed for encrypting Amazon DynamoDB Tables.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

dynamodb-throughput-limit-check

Checks if provisioned DynamoDB throughput is approaching the maximum limit for your account. By default, the rule checks if provisioned throughput exceeds a threshold of 80 percent of your account limits.

Identifier: DYNAMODB_THROUGHPUT_LIMIT_CHECK

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Taipei) Region

Parameters:

accountRCUThresholdPercentage (Optional), Type: int, Default: 80

Percentage of provisioned read capacity units for your account. When this value is reached, the rule is marked as noncompliant.

accountWCUThresholdPercentage (Optional), Type: int, Default: 80

Percentage of provisioned write capacity units for your account. When this value is reached, the rule is marked as noncompliant.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ebs-in-backup-plan

Check if Amazon Elastic Block Store (Amazon EBS) volumes are added in backup plans of Amazon Backup. The rule is NON_COMPLIANT if Amazon EBS volumes are not included in backup plans.

Identifier: EBS_IN_BACKUP_PLAN

Resource Types: AWS::EC2::Volume

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Melbourne), Asia Pacific (Taipei), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ebs-optimized-instance

Checks if Amazon EBS optimization is enabled for your Amazon Elastic Compute Cloud (Amazon EC2) instances that can be Amazon EBS-optimized. The rule is NON_COMPLIANT if EBS optimization is not enabled for an Amazon EC2 instance that can be EBS-optimized.

> **Note**
>
> EC2 instances which are EBS-optimized by default always result in rule evaluations returning `COMPLIANT`.

Identifier: EBS_OPTIMIZED_INSTANCE

Resource Types: AWS::EC2::Instance

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ebs-snapshot-public-restorable-check

Checks if Amazon Elastic Block Store (Amazon EBS) snapshots are not publicly restorable. The rule is NON_COMPLIANT if one or more snapshots with RestorableByUserIds field are set to all, that is, Amazon EBS snapshots are public.

Identifier: EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Europe (Spain) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ec2-ebs-encryption-by-default

Checks if Amazon Elastic Block Store (EBS) encryption is enabled by default. The rule is NON_COMPLIANT if the encryption is not enabled.

Identifier: EC2_EBS_ENCRYPTION_BY_DEFAULT

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ec2-imdsv2-check

Checks if your Amazon Elastic Compute Cloud (Amazon EC2) instance metadata version is configured with Instance Metadata Service Version 2 (IMDSv2). The rule is NON_COMPLIANT if the HttpTokens is set to optional.

Identifier: EC2_IMDSV2_CHECK

Resource Types: AWS::EC2::Instance

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ec2-instance-detailed-monitoring-enabled

Checks if detailed monitoring is enabled for EC2 instances. The rule is NON_COMPLIANT if detailed monitoring is not enabled.

Identifier: EC2_INSTANCE_DETAILED_MONITORING_ENABLED

Resource Types: AWS::EC2::Instance

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ec2-instance-launched-with-allowed-ami

Checks if running or stopped EC2 instances were launched with Amazon Machine Images (AMIs) that meet your Allowed AMIs criteria. The rule is NON_COMPLIANT if an AMI doesn't meet the Allowed AMIs criteria and the Allowed AMIs settings isn't disabled.

Identifier: EC2_INSTANCE_LAUNCHED_WITH_ALLOWED_AMI

Resource Types: AWS::EC2::Instance

Trigger type: Configuration changes and Periodic

Amazon Web Services Region: All supported Amazon regions

Parameters:

InstanceStateNameList (Optional), Type: CSV

> Comma-separate list of Amazon EC2 instance states for the rule to check. Valid values are "running" and "stopped".

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ec2-instance-managed-by-systems-manager

> **Important**
>
> For this rule, the rule identifier (EC2_INSTANCE_MANAGED_BY_SSM) and rule name (ec2-instance-managed-by-systems-manager) are different.

Checks if your Amazon EC2 instances are managed by Amazon Systems Manager Agent (SSM Agent). The rule is NON_COMPLIANT if an EC2 instance is running and the SSM Agent is stopped, or if an EC2 instance is running and the SSM Agent is terminated.

> **Note**
>
> The rule will not return NON_COMPLIANT if an EC2 instance is stopped and the SSM Agent is running.

Identifier: EC2_INSTANCE_MANAGED_BY_SSM

Resource Types: AWS::EC2::Instance, AWS::SSM::ManagedInstanceInventory

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Middle East (UAE), Asia Pacific (Taipei) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ec2-instance-multiple-eni-check

Checks if Amazon Elastic Compute Cloud (Amazon EC2) uses multiple Elastic Network Interfaces (ENIs) or Elastic Fabric Adapters (EFAs). The rule is NON_COMPLIANT an Amazon EC2 instance use multiple network interfaces.

Identifier: EC2_INSTANCE_MULTIPLE_ENI_CHECK

Resource Types: AWS::EC2::Instance

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

NetworkInterfaceIds (Optional), Type: CSV

Comma-separated list of network instance IDs

Proactive Evaluation

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with Amazon Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
   "NetworkInterfaces": "[NetworkInterfaceId-1, NetworkInterfaceId-2,
 NetworkInterfaceId-3, ...]"
}
...
```

For more information on proactive evaluation, see Evaluation Mode.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ec2-instance-no-public-ip

Checks if EC2 instances have a public IP association. The rule is NON_COMPLIANT if the publicIp field is present in the EC2 instance configuration item. The rule applies only to IPv4.

Context: Public IP addresses can make EC2 instances directly accessible from the internet, which might not always be desirable from a security or compliance standpoint:

- **Security**: In many cases, you might not want your EC2 instances to have public IP addresses unless they need to be publicly accessible. Having a public IP address can expose your EC2 instance to potential security risks, such as unauthorized access or attacks.
- **Compliance**: Various compliance standards such as PCI, DSS, or HIPAA have specific requirements regarding network segmentation and access controls. Ensuring that EC2 instances do not have unnecessary public IP addresses can help ensure compliance with these requirements.
- **Cost Management**: Public IP addresses can incur additional costs, especially if there are EC2 instances continuously associated with them. By identifying EC2 instances with public IPs which do not need them, you can potentially reduce costs.

Identifier: EC2_INSTANCE_NO_PUBLIC_IP

Resource Types: AWS::EC2::Instance

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ec2-instance-profile-attached

Checks if an EC2 instance has an Amazon Identity and Access Management (IAM) profile attached to it. The rule is NON_COMPLIANT if no IAM profile is attached to the EC2 instance.

Identifier: EC2_INSTANCE_PROFILE_ATTACHED

Resource Types: AWS::EC2::Instance

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Taipei), Canada West (Calgary) Region

Parameters:

IamInstanceProfileArnList (Optional), Type: CSV

> Comma-separated list of IAM profile Amazon Resource Names (ARNs) that can be attached to Amazon EC2 instances.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ec2-launch-template-imdsv2-check

Checks if the currently set default version of an Amazon EC2 Launch Template requires new launched instances to use V2 of the Amazon EC2 Instance Metadata Service (IMDSv2). The rule is NON_COMPLIANT if 'Metadata version' is not specified as V2 (IMDSv2).

Identifier: EC2_LAUNCH_TEMPLATE_IMDSV2_CHECK

Resource Types: AWS::EC2::LaunchTemplate

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ec2-launch-template-public-ip-disabled

Checks if Amazon EC2 Launch Templates are set to assign public IP addresses to Network Interfaces. The rule is NON_COMPLIANT if the default version of an EC2 Launch Template has at least 1 Network Interface with 'AssociatePublicIpAddress' set to 'true'.

Identifier: EC2_LAUNCH_TEMPLATE_PUBLIC_IP_DISABLED

Resource Types: AWS::EC2::LaunchTemplate

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

exemptedLaunchTemplates (Optional), Type: CSV

Comma-separated list of exempted EC2 Launch Template IDs that are allowed to have Network Interfaces with the AssociatePublicIpAddress value set to 'true'.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ec2-managedinstance-applications-blacklisted

Checks if none of the specified applications are installed on the instance. Optionally, specify the version. Newer versions will not be denylisted. Optionally, specify the platform to apply the rule only to instances running that platform.

Identifier: EC2_MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED

Resource Types: AWS::SSM::ManagedInstanceInventory

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Taipei), Canada West (Calgary) Region

Parameters:

applicationNames, Type: CSV

Comma-separated list of application names. Optionally, specify versions appended with ':' (for example, 'Chrome:0.5.3, Firefox').

> **Note**
>
> The application names must be an exact match. For example, use **`firefox`** on Linux or **`firefox-compat`** on Amazon Linux. In addition, Amazon Config does not currently support wildcards for the *applicationNames* parameter (for example, **`firefox*`**).

platformType (Optional), Type: String

Platform type (for example, 'Linux' or 'Windows').

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ec2-managedinstance-applications-required

Checks if all of the specified applications are installed on the instance. Optionally, specify the minimum acceptable version. You can also specify the platform to apply the rule only to instances running that platform.

> **Note**
>
> Ensure that SSM agent is running on the EC2 instance and an association to gather application software inventory is created. The rule returns `NOT_APPLICABLE` if SSM agent is not installed or an association is not yet created or running.

Identifier: EC2_MANAGEDINSTANCE_APPLICATIONS_REQUIRED

Resource Types: AWS::SSM::ManagedInstanceInventory

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Taipei), Canada West (Calgary) Region

Parameters:

applicationNames, Type: CSV

Comma-separated list of application names. Optionally, specify versions appended with ':' (for example, 'Chrome:0.5.3, Firefox').

> **Note**
>
> The application names must be an exact match. For example, use **`firefox`** on Linux or **`firefox-compat`** on Amazon Linux. In addition, Amazon Config does not currently support wildcards for the *applicationNames* parameter (for example, **`firefox*`**).

platformType (Optional), Type: String

Platform type (for example, 'Linux' or 'Windows').

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ec2-managedinstance-association-compliance-status-check

Checks if the status of the Amazon Systems Manager association compliance is COMPLIANT or NON_COMPLIANT after the association execution on the instance. The rule is compliant if the field status is COMPLIANT. For more information about associations, see What is an association?.

Identifier: EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK

Resource Types: AWS::SSM::AssociationCompliance

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Europe (Milan), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ec2-managedinstance-inventory-blacklisted

Checks whether instances managed by Amazon EC2 Systems Manager are configured to collect blacklisted inventory types.

Identifier: EC2_MANAGEDINSTANCE_INVENTORY_BLACKLISTED

Resource Types: AWS::SSM::ManagedInstanceInventory

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Taipei), Canada West (Calgary) Region

Parameters:

inventoryNames, Type: CSV

Comma separated list of Systems Manager inventory types (for example, 'Amazon:Network, Amazon:WindowsUpdate').

platformType (Optional), Type: String

Platform type (for example, 'Linux').

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ec2-managedinstance-patch-compliance-status-check

Checks if the compliance status of the Amazon Systems Manager patch compliance is COMPLIANT or NON_COMPLIANT after the patch installation on the instance. The rule is compliant if the field status is COMPLIANT.

Identifier: EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK

Resource Types: AWS::SSM::PatchCompliance

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Osaka), Europe (Milan), Asia Pacific (Taipei), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ec2-managedinstance-platform-check

Checks whether EC2 managed instances have the desired configurations.

Identifier: EC2_MANAGEDINSTANCE_PLATFORM_CHECK

Resource Types: AWS::SSM::ManagedInstanceInventory

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Taipei), Canada West (Calgary) Region

Parameters:

platformType, Type: String

Platform type (for example, 'Linux').

platformVersion (Optional), Type: String

Platform version (for example, '2016.09').

agentVersion (Optional), Type: String

Agent version (for example, '2.0.433.0').

platformName (Optional), Type: String

The version of the platform (for example, '2016.09')

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ec2-security-group-attached-to-eni

Checks if non-default security groups are attached to elastic network interfaces. The rule is NON_COMPLIANT if the security group is not associated with a network interface.

Identifier: EC2_SECURITY_GROUP_ATTACHED_TO_ENI

Resource Types: AWS::EC2::SecurityGroup

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Middle East (UAE), Asia Pacific (Taipei), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ec2-stopped-instance

Checks if there are Amazon Elastic Compute Cloud (Amazon EC2) instances stopped for more than the allowed number of days. The rule is NON_COMPLIANT if the state of an Amazon EC2 instance has been stopped for longer than the allowed number of days, or if the amount of time cannot be determined.

Identifier: EC2_STOPPED_INSTANCE

Resource Types: AWS::EC2::Instance

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Africa (Cape Town), Middle East (UAE), Asia Pacific (Osaka), Asia Pacific (Melbourne), Europe (Milan), Canada West (Calgary) Region

Parameters:

AllowedDays (Optional), Type: int, Default: 30

The number of days an Amazon EC2 instance can be stopped before the rule is NON_COMPLIANT. The default number of days is 30.

> **Note**
>
> The number of days selected needs to be less than the configured retention period since this rule relies on the historical data collected. For more information about historical data retention, see Deleting Amazon Config Data.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ec2-volume-inuse-check

Checks if EBS volumes are attached to EC2 instances. Optionally checks if EBS volumes are marked for deletion when an instance is terminated.

The rule is COMPLIANT if an EBS volume is attached to a running EC2 instance. In this case, it is COMPLIANT when the EBS volume is actively in use by an EC2 instance.

The rule is NON_COMPLIANT if an EBS volume is not attached to any EC2 instance or is attached to a stopped or terminated EC2 instance. In this case, it is NON_COMPLIANT when the EBS volume is not actively in use by an EC2 instance.

Identifier: EC2_VOLUME_INUSE_CHECK

Resource Types: AWS::EC2::Volume

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Taipei), Canada West (Calgary) Region

Parameters:

deleteOnTermination (Optional), Type: boolean

EBS volumes are marked for deletion when an instance is terminated. Possible values: True or False (other input values are marked as NON_COMPLIANT). If set to `True`, the rule is NON_COMPLIANT if a terminated EBS volume is not marked for deletion.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ecr-private-lifecycle-policy-configured

Checks if a private Amazon Elastic Container Registry (ECR) repository has at least one lifecycle policy configured. The rule is NON_COMPLIANT if no lifecycle policy is configured for the ECR private repository.

Identifier: ECR_PRIVATE_LIFECYCLE_POLICY_CONFIGURED

Resource Types: AWS::ECR::Repository

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ecr-private-tag-immutability-enabled

Checks if a private Amazon Elastic Container Registry (ECR) repository has tag immutability enabled. This rule is NON_COMPLIANT if tag immutability is not enabled for the private ECR repository.

Identifier: ECR_PRIVATE_TAG_IMMUTABILITY_ENABLED

Resource Types: AWS::ECR::Repository

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ecr-repository-cmk-encryption-enabled

Checks if ECR repository is encrypted at rest using customer-managed KMS key. This rule is NON_COMPLIANT if the repository is encrypted using AES256 or the default KMS key ('aws/ecr').

Identifier: ECR_REPOSITORY_CMK_ENCRYPTION_ENABLED

Resource Types: AWS::ECR::Repository

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Middle East (Bahrain), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary) Region

Parameters:

kmsKeyArns (Optional), Type: CSV

Comma-separated list of KMS key Amazon Resource Names (ARNs) intended to encrypt the ECR repository.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ecs-containers-nonprivileged

Checks if the privileged parameter in the container definition of ECSTaskDefinitions is set to 'true'. The rule is NON_COMPLIANT if the privileged parameter is 'true'.

> **Note**
>
> This rule only evaluates the latest active revision of an Amazon ECS task definition.

Identifier: ECS_CONTAINERS_NONPRIVILEGED

Resource Types: AWS::ECS::TaskDefinition

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ecs-containers-readonly-access

Checks if Amazon Elastic Container Service (Amazon ECS) Containers only have read-only access to its root filesystems. The rule is NON_COMPLIANT if the readonlyRootFilesystem parameter in the container definition of ECSTaskDefinitions is set to 'false'.

> **Note**
>
> This rule only evaluates the latest active revision of an Amazon ECS task definition.

Identifier: ECS_CONTAINERS_READONLY_ACCESS

Resource Types: AWS::ECS::TaskDefinition

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ecs-container-insights-enabled

Checks if Amazon Elastic Container Service clusters have container insights enabled. The rule is NON_COMPLIANT if container insights are not enabled.

Identifier: ECS_CONTAINER_INSIGHTS_ENABLED

Resource Types: AWS::ECS::Cluster

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ecs-fargate-latest-platform-version

Checks if ECS Fargate services is set to the latest platform version. The rule is NON_COMPLIANT if PlatformVersion for the Fargate launch type is not set to LATEST, or if neither latestLinuxVersion nor `latestWindowsVersion` are provided as parameters.

Identifier: ECS_FARGATE_LATEST_PLATFORM_VERSION

Resource Types: AWS::ECS::Service

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

latestLinuxVersion (Optional), Type: String

> Latest Linux supported 'PlatformVersion' in semantic versioning (SemVer) format. Parameter may be needed if Fargate was deployed and the 'PlatformVersion' was explicitly specified or CodeDeploy is used as the 'DeploymentController'

latestWindowsVersion (Optional), Type: String

> Latest Windows supported 'PlatformVersion' in semantic versioning (SemVer) format. Parameter may be needed if Fargate was deployed and the 'PlatformVersion' was explicitly specified or CodeDeploy is used as the 'DeploymentController'

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ecs-no-environment-secrets

Checks if secrets are passed as container environment variables. The rule is NON_COMPLIANT if 1 or more environment variable key matches a key listed in the '`secretKeys`' parameter (excluding environmental variables from other locations such as Amazon S3).

> **Note**
>
> This rule only evaluates the latest active revision of an Amazon ECS task definition.

Identifier: ECS_NO_ENVIRONMENT_SECRETS

Resource Types: AWS::ECS::TaskDefinition

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Canada West (Calgary) Region

Parameters:

secretKeys, Type: CSV

Comma-separated list of key names to search for in the environment variables of container definitions within Task Definitions. Extra spaces will be removed.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ecs-task-definition-log-configuration

Checks if logConfiguration is set on active ECS Task Definitions. This rule is NON_COMPLIANT if an active ECSTaskDefinition does not have the logConfiguration resource defined or the value for logConfiguration is null in at least one container definition.

> **Note**
>
> This rule only evaluates the latest active revision of an Amazon ECS task definition.

Identifier: ECS_TASK_DEFINITION_LOG_CONFIGURATION

Resource Types: AWS::ECS::TaskDefinition

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ecs-task-definition-network-mode-not-host

Checks if the latest active revision of Amazon ECS task definitions use host network mode. The rule is NON_COMPLIANT if the latest active revision of the ECS task definition uses host network mode.

Identifier: ECS_TASK_DEFINITION_NETWORK_MODE_NOT_HOST

Resource Types: AWS::ECS::TaskDefinition

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Middle East (Bahrain), Asia Pacific (Thailand), Mexico (Central) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ecs-task-definition-pid-mode-check

Checks if ECSTaskDefinitions are configured to share a host's process namespace with its Amazon Elastic Container Service (Amazon ECS) containers. The rule is NON_COMPLIANT if the pidMode parameter is set to 'host'.

> **Note**
>
> This rule only evaluates the latest active revision of an Amazon ECS task definition.

Identifier: ECS_TASK_DEFINITION_PID_MODE_CHECK

Resource Types: AWS::ECS::TaskDefinition

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ecs-task-definition-user-for-host-mode-check

Checks if Amazon ECS task definitions with host network mode have privileged OR nonroot in the container definition. The rule is NON_COMPLIANT if the latest active revision of a task definition has privileged=false (or is null) AND user=root (or is null).

Important

Only one condition needs to be met for the rule to return compliant
The rule is COMPLIANT in any of following scenarios:

- If the network mode is not set to host,
- If the latest active revision of a task definition has privileged=true,
- If the latest active revision of a task definition has a user that is not the root.

This means that only one of these conditions need to be met for the rule to return compliant. To check specifically if a task definition has privileged=true, see ecs-containers-nonprivileged. To check specifically if a task definition has a user that is not the root, see ecs-task-definition-nonroot-user.

Identifier: ECS_TASK_DEFINITION_USER_FOR_HOST_MODE_CHECK

Resource Types: AWS::ECS::TaskDefinition

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Middle East (UAE), Asia Pacific (Taipei) Region

Parameters:

SkipInactiveTaskDefinitions (Optional), Type: boolean

Boolean flag to not check INACTIVE Amazon EC2 task definitions. If set to 'true', the rule won't evaluate INACTIVE Amazon EC2 task definitions. If set to 'false', the rule will evaluate the latest revision of INACTIVE Amazon EC2 task definitions.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

efs-automatic-backups-enabled

Checks if an Amazon Elastic File System (Amazon EFS) file system has automatic backups enabled. The rule is NON_COMPLIANT if `BackupPolicy.Status` is set to DISABLED.

Identifier: EFS_AUTOMATIC_BACKUPS_ENABLED

Resource Types: AWS::EFS::FileSystem

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

efs-encrypted-check

Checks if Amazon Elastic File System (Amazon EFS) is configured to encrypt the file data using Amazon Key Management Service (Amazon KMS). The rule is NON_COMPLIANT if the encrypted key is set to false on `DescribeFileSystems` or if the `KmsKeyId` key on `DescribeFileSystems` does not match the `KmsKeyId` parameter.

Identifier: EFS_ENCRYPTED_CHECK

Resource Types: AWS::EFS::FileSystem

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Taipei) Region

Parameters:

KmsKeyId (Optional), Type: String

Amazon Resource Name (ARN) of the KMS key that is used to encrypt the EFS file system.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

efs-filesystem-ct-encrypted

Checks if Amazon Elastic File System (Amazon EFS) encrypts data with Amazon Key Management Service (Amazon KMS). The rule is NON_COMPLIANT if a file system is not encrypted. Optionally, you can check if a file system is not encrypted with specified KMS keys.

Identifier: EFS_FILESYSTEM_CT_ENCRYPTED

Resource Types: AWS::EFS::FileSystem

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary) Region

Parameters:

kmsKeyArns (Optional), Type: String

(Optional) Comma-separated list of Amazon Resource Names (ARNs) for Amazon KMS keys. If provided, the rule checks if the specified KMS keys do not encrypt an Amazon EFS file system.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

efs-in-backup-plan

Checks if Amazon Elastic File System (Amazon EFS) file systems are added in the backup plans of Amazon Backup. The rule is NON_COMPLIANT if EFS file systems are not included in the backup plans.

Identifier: EFS_IN_BACKUP_PLAN

Resource Types: AWS::EFS::FileSystem

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Taipei) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

eip-attached

Checks if all Elastic IP addresses that are allocated to an Amazon account are attached to EC2 instances or in-use elastic network interfaces. The rule is NON_COMPLIANT if the 'AssociationId' is null for the Elastic IP address.

> **Note**
>
> Results might take up to 6 hours to become available after an evaluation occurs.

Identifier: EIP_ATTACHED

Resource Types: AWS::EC2::EIP

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Middle East (UAE) Region

Parameters:

None

Proactive Evaluation

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with Amazon Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
   "InstanceId": "my-instance-Id"
}
...
```

For more information on proactive evaluation, see Evaluation Mode.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

eks-cluster-log-enabled

Checks if an Amazon Elastic Kubernetes Service (Amazon EKS) cluster is configured with logging enabled. The rule is NON_COMPLIANT if logging for Amazon EKS clusters is not enabled or if logging is not enabled with the log type mentioned.

Identifier: EKS_CLUSTER_LOG_ENABLED

Resource Types: AWS::EKS::Cluster

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary) Region

Parameters:

logTypes (Optional), Type: CSV

> Comma-separated list of EKS Cluster control plane log types for the rule to check. Valid values: "api", "audit", "authenticator", "controllerManager", "scheduler

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

eks-cluster-supported-version

Checks if an Amazon Elastic Kubernetes Service (EKS) cluster is running a supported Kubernetes version. This rule is NON_COMPLIANT if an EKS cluster is running an unsupported version (less than the parameter '`oldestVersionSupported`').

Identifier: EKS_CLUSTER_SUPPORTED_VERSION

Resource Types: AWS::EKS::Cluster

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary) Region

Parameters:

oldestVersionSupported, Type: String

Value of the oldest version of Kubernetes supported on Amazon.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

eks-endpoint-no-public-access

Checks if the Amazon Elastic Kubernetes Service (Amazon EKS) endpoint is not publicly accessible. The rule is NON_COMPLIANT if the endpoint is publicly accessible.

Identifier: EKS_ENDPOINT_NO_PUBLIC_ACCESS

Resource Types: AWS::EKS::Cluster

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Taipei) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

eks-secrets-encrypted

Checks if Amazon Elastic Kubernetes Service clusters are configured to have Kubernetes secrets encrypted using Amazon Key Management Service (KMS) keys.

- This rule is COMPLIANT if an EKS cluster has an encryptionConfig with secrets as one of the resources.
- This rule is also COMPLIANT if the key used to encrypt EKS secrets matches with the parameter.
- This rule is NON_COMPLIANT if an EKS cluster does not have an encryptionConfig or if the encryptionConfig resources do not include secrets.
- This rule is also NON_COMPLIANT if the key used to encrypt EKS secrets does not match with the parameter.

Identifier: EKS_SECRETS_ENCRYPTED

Resource Types: AWS::EKS::Cluster

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Taipei) Region

Parameters:

kmsKeyArns (Optional), Type: CSV

> Comma separated list of Amazon Resource Name (ARN) of the KMS key that should be used for encrypted secrets in an EKS cluster.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

elasticache-auto-minor-version-upgrade-check

Checks if Amazon ElastiCache clusters have auto minor version upgrades enabled. The rule is NON_COMPLIANT for an ElastiCache cluster if it is using the Redis or Valkey engine and 'AutoMinorVersionUpgrade' is not set to 'true'.

Identifier: ELASTICACHE_AUTO_MINOR_VERSION_UPGRADE_CHECK

Resource Types: AWS::ElastiCache::CacheCluster

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

elasticache-redis-cluster-automatic-backup-check

Check if the Amazon ElastiCache Redis clusters have automatic backup turned on. The rule is NON_COMPLIANT if the SnapshotRetentionLimit for Redis cluster is less than the SnapshotRetentionPeriod parameter. For example: If the parameter is 15 then the rule is non-compliant if the snapshotRetentionPeriod is between 0-15.

Identifier: ELASTICACHE_REDIS_CLUSTER_AUTOMATIC_BACKUP_CHECK

Resource Types: AWS::ElastiCache::CacheCluster, AWS::ElastiCache::ReplicationGroup

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Taipei) Region

Parameters:

snapshotRetentionPeriod (Optional), Type: int, Default: 15

Minimum snapshot retention period in days for Redis cluster. Default is 15 days.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

elasticache-repl-grp-auto-failover-enabled

Checks if Amazon ElastiCache Redis replication groups have automatic failover enabled. The rule is NON_COMPLIANT for an ElastiCache replication group if 'AutomaticFailover' is not set to 'enabled'.

Identifier: ELASTICACHE_REPL_GRP_AUTO_FAILOVER_ENABLED

Resource Types: AWS::ElastiCache::ReplicationGroup

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

elasticache-repl-grp-encrypted-at-rest

Checks if Amazon ElastiCache replication groups have encryption-at-rest enabled. The rule is NON_COMPLIANT for an ElastiCache replication group if 'AtRestEncryptionEnabled' is disabled or if the KMS key ARN does not match the approvedKMSKeyArns parameter.

Identifier: ELASTICACHE_REPL_GRP_ENCRYPTED_AT_REST

Resource Types: AWS::ElastiCache::ReplicationGroup

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary) Region

Parameters:

approvedKMSKeyIds (Optional), Type: CSV

Comma-separated list of KMS Key IDs that are approved for ElastiCache usage.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

elasticache-repl-grp-encrypted-in-transit

Checks if Amazon ElastiCache replication groups have encryption-in-transit enabled. The rule is NON_COMPLIANT for an ElastiCache replication group if 'TransitEncryptionEnabled' is set to 'false'.

Identifier: ELASTICACHE_REPL_GRP_ENCRYPTED_IN_TRANSIT

Resource Types: AWS::ElastiCache::ReplicationGroup

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

elasticache-repl-grp-redis-auth-enabled

Checks if Amazon ElastiCache replication groups have Redis AUTH enabled. The rule is NON_COMPLIANT for an ElastiCache replication group if the Redis version of its nodes is below 6 (Version 6+ use Redis ACLs) and 'AuthToken' is missing or is empty/null.

Identifier: ELASTICACHE_REPL_GRP_REDIS_AUTH_ENABLED

Resource Types: AWS::ElastiCache::ReplicationGroup

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

elasticache-subnet-group-check

Checks if Amazon ElastiCache clusters are configured with a custom subnet group. The rule is NON_COMPLIANT for an ElastiCache cluster if it is using a default subnet group.

Identifier: ELASTICACHE_SUBNET_GROUP_CHECK

Resource Types: AWS::ElastiCache::CacheCluster

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

elasticsearch-encrypted-at-rest

Checks if Amazon OpenSearch Service (previously called Elasticsearch) domains have encryption at rest configuration enabled. The rule is NON_COMPLIANT if the EncryptionAtRestOptions field is not enabled.

Identifier: ELASTICSEARCH_ENCRYPTED_AT_REST

Resource Types: AWS::Elasticsearch::Domain

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Taipei) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

elasticsearch-in-vpc-only

Checks if Amazon OpenSearch Service (previously called Elasticsearch) domains are in Amazon Virtual Private Cloud (Amazon VPC). The rule is NON_COMPLIANT if an OpenSearch Service domain endpoint is public.

Identifier: ELASTICSEARCH_IN_VPC_ONLY

Resource Types: AWS::Elasticsearch::Domain

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Taipei) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

elasticsearch-logs-to-cloudwatch

Checks if Amazon OpenSearch Service domains are configured to send logs to Amazon CloudWatch Logs. The rule is COMPLIANT if a log is enabled for an Amazon ES domain. This rule is NON_COMPLIANT if logging is not configured.

Identifier: ELASTICSEARCH_LOGS_TO_CLOUDWATCH

Resource Types: AWS::Elasticsearch::Domain

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Taipei) Region

Parameters:

logTypes (Optional), Type: CSV

Comma-separated list of logs that are enabled. Valid values are 'search', 'index', 'error'.

Proactive Evaluation

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with Amazon Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
   "LogPublishingOptions": "{Key : Value, ...}"*
}
```

```
...
```

*An object with one or more of the following keys: `SEARCH_SLOW_LOGS`, `ES_APPLICATION_LOGS`, `INDEX_SLOW_LOGS`, `AUDIT_LOGS`, depending on the types of logs you want to publish. Each key needs a valid `LogPublishingOption` value.

For more information on proactive evaluation, see Evaluation Mode.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

elasticsearch-node-to-node-encryption-check

Check if OpenSearch Service (previously called Elasticsearch) nodes are encrypted end to end. The rule is NON_COMPLIANT if the node-to-node encryption is not enabled on the domain.

Identifier: ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK

Resource Types: AWS::Elasticsearch::Domain

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Taipei) Region

Parameters:

None

Proactive Evaluation

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with Amazon Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
   "NodeToNodeEncryptionOptions": BOOLEAN
}
```

```
...
```

For more information on proactive evaluation, see Evaluation Mode.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

elastic-beanstalk-managed-updates-enabled

Checks if managed platform updates in an Amazon Elastic Beanstalk environment is enabled. The rule is COMPLIANT if the value for `ManagedActionsEnabled` is set to true. The rule is NON_COMPLIANT if the value for `ManagedActionsEnabled` is set to false, or if a parameter is provided and its value does not match the existing configurations.

Identifier: ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED

Resource Types: AWS::ElasticBeanstalk::Environment

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

UpdateLevel (Optional), Type: String

Indicates whether update levels are set to 'minor' version updates or a 'patch' version updates.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

elbv2-acm-certificate-required

Checks if Application Load Balancers and Network Load Balancers have listeners that are configured to use certificates from Amazon Certificate Manager (ACM). This rule is

NON_COMPLIANT if at least 1 load balancer has at least 1 listener that is configured without a certificate from ACM or is configured with a certificate different from an ACM certificate.

Identifier: ELBV2_ACM_CERTIFICATE_REQUIRED

Resource Types: AWS::ElasticLoadBalancingV2::LoadBalancer

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

AcmCertificatesAllowed (Optional), Type: CSV

Comma-separated list of certificate Amazon Resource Names (ARNs).

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

elbv2-listener-encryption-in-transit

Checks if listeners for the load balancers are configured with HTTPS or TLS termination. The rule is NON_COMPLIANT if listeners are not configured with HTTPS or TLS termination.

Identifier: ELBV2_LISTENER_ENCRYPTION_IN_TRANSIT

Resource Types: AWS::ElasticLoadBalancingV2::Listener

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Seoul), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

elbv2-multiple-az

Checks if an Elastic Load Balancer V2 (Application, Network, or Gateway Load Balancer) is mapped to multiple Availability Zones (AZs). The rule is NON_COMPLIANT if an Elastic Load Balancer V2 is mapped to less than 2 AZs. For more information, see Availability Zones for your Application Load Balancer.

Identifier: ELBV2_MULTIPLE_AZ

Resource Types: AWS::ElasticLoadBalancingV2::LoadBalancer

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Canada West (Calgary) Region

Parameters:

minAvailabilityZones (Optional), Type: int

Minimum number of expected AZs (between 2 and 10 inclusive).

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

elb-acm-certificate-required

Checks if the Classic Load Balancers use SSL certificates provided by Amazon Certificate Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. This rule is only

applicable to Classic Load Balancers. This rule does not check Application Load Balancers and Network Load Balancers.

Identifier: ELB_ACM_CERTIFICATE_REQUIRED

Resource Types: AWS::ElasticLoadBalancing::LoadBalancer

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Africa (Cape Town), Asia Pacific (Osaka), Europe (Milan), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

elb-cross-zone-load-balancing-enabled

Checks if cross-zone load balancing is enabled for Classic Load Balancers. The rule is NON_COMPLIANT if cross-zone load balancing is not enabled for Classic Load Balancers.

Identifier: ELB_CROSS_ZONE_LOAD_BALANCING_ENABLED

Resource Types: AWS::ElasticLoadBalancing::LoadBalancer

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

elb-custom-security-policy-ssl-check

Checks whether your Classic Load Balancer SSL listeners are using a custom policy. The rule is only applicable if there are SSL listeners for the Classic Load Balancer.

Identifier: ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK

Resource Types: AWS::ElasticLoadBalancing::LoadBalancer

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Jakarta), Asia Pacific (Osaka), Asia Pacific (Melbourne), Asia Pacific (Taipei) Region

Parameters:

sslProtocolsAndCiphers, Type: String

Comma separated list of ciphers and protocols.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

elb-deletion-protection-enabled

Checks if an Elastic Load Balancer has deletion protection enabled. The rule is NON_COMPLIANT if deletion_protection.enabled is false.

Identifier: ELB_DELETION_PROTECTION_ENABLED

Resource Types: AWS::ElasticLoadBalancingV2::LoadBalancer

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Osaka) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

elb-logging-enabled

Checks if the Application Load Balancer and the Classic Load Balancer have logging enabled. The rule is NON_COMPLIANT if the `access_logs.s3.enabled` is false or `access_logs.S3.bucket` is not equal to the s3BucketName that you provided.

> **Note**
>
> The rule does not apply to Network Load Balancers or Gateway Load Balancers.

Identifier: ELB_LOGGING_ENABLED

Resource Types: AWS::ElasticLoadBalancing::LoadBalancer, AWS::ElasticLoadBalancingV2::LoadBalancer

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

s3BucketNames (Optional), Type: CSV

Comma-separated list of Amazon S3 bucket names for Amazon ELB to deliver the log files.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

elb-predefined-security-policy-ssl-check

Checks if your Classic Load Balancer SSL listeners use a predefined policy. The rule is NON_COMPLIANT if the Classic Load Balancer HTTPS/SSL listener's policy does not equal the value of the parameter '`predefinedPolicyName`'.

Identifier: ELB_PREDEFINED_SECURITY_POLICY_SSL_CHECK

Resource Types: AWS::ElasticLoadBalancing::LoadBalancer

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Osaka) Region

Parameters:

predefinedPolicyName, Type: String

Name of the predefined policy.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

elb-tls-https-listeners-only

Checks if your Classic Load Balancer is configured with SSL or HTTPS listeners. The rule is NON_COMPLIANT if a listener is not configured with SSL or HTTPS.

- If the Classic Load Balancer does not have a listener configured, then the rule returns `NOT_APPLICABLE`.
- The rule is COMPLIANT if the Classic Load Balancer listeners are configured with SSL or HTTPS.
- The rule is NON_COMPLIANT if a listener is not configured with SSL or HTTPS.

Identifier: ELB_TLS_HTTPS_LISTENERS_ONLY

Resource Types: AWS::ElasticLoadBalancing::LoadBalancer

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Middle East (UAE), Asia Pacific (Osaka) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

emr-kerberos-enabled

Checks if Amazon EMR clusters have Kerberos enabled. The rule is NON_COMPLIANT if a security configuration is not attached to the cluster or the security configuration does not satisfy the specified rule parameters.

Identifier: EMR_KERBEROS_ENABLED

Resource Types: AWS::EMR::Cluster

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Taipei), Canada West (Calgary) Region

Parameters:

TicketLifetimeInHours (Optional), Type: int

Period for which Kerberos ticket issued by cluster's KDC is valid.

Realm (Optional), Type: String

Kereberos realm name of the other realm in the trust relationship.

Domain (Optional), Type: String

Domain name of the other realm in the trust relationship.

AdminServer (Optional), Type: String

Fully qualified domain of the admin server in the other realm of the trust relationship.

KdcServer (Optional), Type: String

Fully qualified domain of the KDC server in the other realm of the trust relationship.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

emr-master-no-public-ip

Checks if Amazon EMR clusters' master nodes have public IPs. The rule is NON_COMPLIANT if the master node has a public IP.

> **Note**
>
> This rule checks clusters that are in RUNNING or WAITING state. This rule requires you to enable recording for the `AWS::EC2::Instance` resource type in order to have an accurate evaluation.

Identifier: EMR_MASTER_NO_PUBLIC_IP

Resource Types: AWS::EMR::Cluster, AWS::EC2::Instance

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Osaka), Asia Pacific (Melbourne), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

encrypted-volumes

Checks if attached Amazon EBS volumes are encrypted and optionally are encrypted with a specified KMS key. The rule is NON_COMPLIANT if attached EBS volumes are unencrypted or are encrypted with a KMS key not in the supplied parameters.

Identifier: ENCRYPTED_VOLUMES

Resource Types: AWS::EC2::Volume

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

kmsId (Optional), Type: String

ID or ARN of the KMS key that is used to encrypt the volume.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

fms-webacl-resource-policy-check

Checks if the web ACL is associated with an Application Load Balancer, API Gateway stage, or Amazon CloudFront distributions. When Amazon Firewall Manager creates this rule, the FMS policy owner specifies the `WebACLId` in the FMS policy and can optionally enable remediation.

Identifier: FMS_WEBACL_RESOURCE_POLICY_CHECK

Resource Types: AWS::CloudFront::Distribution, AWS::ApiGateway::Stage, AWS::ElasticLoadBalancingV2::LoadBalancer, AWS::WAFRegional::WebACL

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

Parameters:

webACLId, Type: String

The WebACLId of the web ACL.

resourceTags (Optional), Type: String

The resource tags (ApplicationLoadBalancer, ApiGatewayStage and CloudFront distributions) that the rule should be associated with. (for example, { "tagKey1" : ["tagValue1"], "tagKey2" : ["tagValue2", "tagValue3"] })

excludeResourceTags (Optional), Type: boolean

If true, exclude resources that match resourceTags.

fmsManagedToken (Optional), Type: String

A token generated by Amazon Firewall Manager when creating the rule in customer account. Amazon Config ignores this parameter when customer creates this rule.

fmsRemediationEnabled (Optional), Type: boolean

If true, Amazon Firewall Manager will update non-compliant resources according to FMS policy. Amazon Config ignores this parameter when customer creates this rule.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

fms-webacl-rulegroup-association-check

Checks if the rule groups associate with the web ACL at the correct priority. The correct priority is decided by the rank of the rule groups in the ruleGroups parameter. When Amazon Firewall Manager creates this rule, it assigns the highest priority 0 followed by 1, 2, and so on. The FMS policy owner specifies the `ruleGroups` rank in the FMS policy and can optionally enable remediation.

Identifier: FMS_WEBACL_RULEGROUP_ASSOCIATION_CHECK

Resource Types: AWS::WAF::WebACL, AWS::WAFRegional::WebACL

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

Parameters:

ruleGroups, Type: String

Comma-separated list of RuleGroupIds and WafOverrideAction pairs. (for example, ruleGroupId-1:NONE, ruleGroupId2:COUNT)

fmsManagedToken (Optional), Type: String

A token generated by Amazon Firewall Manager when creating the rule in customer account. Amazon Config ignores this parameter when customer creates this rule.

fmsRemediationEnabled (Optional), Type: boolean

If true, Amazon Firewall Manager will update non-compliant resources according to FMS policy. Amazon Config ignores this parameter when customer creates this rule.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

fsx-ontap-deployment-type-check

Checks if Amazon FSx for NetApp ONTAP file systems are configured with certain deployment types. The rule is NON_COMPLIANT if the Amazon FSx for NetApp ONTAP file systems are not configured with the deployment types you specify.

Identifier: FSX_ONTAP_DEPLOYMENT_TYPE_CHECK

Resource Types: AWS::FSx::FileSystem

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Middle East (Bahrain), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

deploymentTypes, Type: CSV

Comma-separated list of allowed Deployment types for the rule to check.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

fsx-openzfs-deployment-type-check

Checks if the Amazon FSx for OpenZFS file systems are configured with certain deployment types. The rule is NON_COMPLIANT if FSx for OpenZFS file systems are not configured with the deployment types you specify.

Identifier: FSX_OPENZFS_DEPLOYMENT_TYPE_CHECK

Resource Types: AWS::FSx::FileSystem

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Middle East (Bahrain), Asia Pacific (Thailand), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Canada West (Calgary) Region

Parameters:

deploymentTypes, Type: CSV

Comma-separated list of allowed Deployment types for the rule to check.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

glue-job-logging-enabled

Checks if an Amazon Glue job has logging enabled. The rule is NON_COMPLIANT if an Amazon Glue job does not have Amazon CloudWatch logs enabled.

Identifier: GLUE_JOB_LOGGING_ENABLED

Resource Types: AWS::Glue::Job

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

glue-spark-job-supported-version

Checks if an Amazon Glue Spark job is running on the specified minimum supported Amazon Glue version. The rule is NON_COMPLIANT if the Amazon Glue Spark job is not running on the minimum supported Amazon Glue version that you specify.

Identifier: GLUE_SPARK_JOB_SUPPORTED_VERSION

Resource Types: AWS::Glue::Job

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Middle East (Bahrain), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

minimumSupportedGlueVersion, Type: String

> String value you must specify of the minimum supported Amazon Glue version for the rule to check.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

guardduty-enabled-centralized

Checks if Amazon GuardDuty is enabled in your Amazon account and Amazon Region. If you provide an Amazon account for centralization, the rule evaluates the GuardDuty results in the centralized account. The rule is COMPLIANT when GuardDuty is enabled.

Identifier: GUARDDUTY_ENABLED_CENTRALIZED

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Mexico (Central), Asia Pacific (Taipei) Region

Parameters:

CentralMonitoringAccount (Optional), Type: String

Comma separated list of Amazon Accounts (12-digit) where Amazon GuardDuty results are allowed to be centralized.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

guardduty-non-archived-findings

Checks if Amazon GuardDuty has findings that are non-archived. The rule is NON_COMPLIANT if GuardDuty has non-archived low/medium/high severity findings older than the specified number in the daysLowSev/daysMediumSev/`daysHighSev` parameter.

Identifier: GUARDDUTY_NON_ARCHIVED_FINDINGS

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Mexico (Central), Asia Pacific (Taipei) Region

Parameters:

daysLowSev (Optional), Type: int, Default: 30

The number of days Amazon GuardDuty low severity findings are allowed to stay non archived. The default is 30 days.

daysMediumSev (Optional), Type: int, Default: 7

The number of days Amazon GuardDuty medium severity findings are allowed to stay non archived. The default is 7 days.

daysHighSev (Optional), Type: int, Default: 1

The number of days Amazon GuardDuty high severity findings are allowed to stay non archived. The default is 1 day.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

iam-customer-policy-blocked-kms-actions

Checks if the managed Amazon Identity and Access Management (IAM) policies that you create do not allow blocked KMS actions on all Amazon KMS key resources. The rule is NON_COMPLIANT if any blocked action is allowed on all Amazon KMS keys by the managed IAM policy.

> **Note**
>
> To be considered non-public, an IAM policy must grant access only to fixed values. This means values that don't contain a wildcard or the following IAM policy element: Variables.

Identifier: IAM_CUSTOMER_POLICY_BLOCKED_KMS_ACTIONS

Resource Types: AWS::IAM::Policy

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

blockedActionsPatterns, Type: CSV

Comma-separated list of blocked KMS action patterns for the rule to check. The rule is NON_COMPLIANT if IAM customer managed policies allow wildcard access to all resources for the actions you specify.

excludePermissionBoundaryPolicy (Optional), Type: boolean

Boolean flag to exclude the evaluation of IAM policies used as permissions boundaries. If set to 'true', the rule will not include permissions boundaries in the evaluation. Otherwise, all IAM policies in scope are evaluated when value is set to 'false.' Default value is 'false'.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

iam-group-has-users-check

Checks whether IAM groups have at least one IAM user.

Identifier: IAM_GROUP_HAS_USERS_CHECK

Resource Types: AWS::IAM::Group

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

iam-inline-policy-blocked-kms-actions

Checks if the inline policies attached to your IAM users, roles, and groups do not allow blocked actions on all Amazon KMS keys. The rule is NON_COMPLIANT if any blocked action is allowed on all Amazon KMS keys in an inline policy.

Identifier: IAM_INLINE_POLICY_BLOCKED_KMS_ACTIONS

Resource Types: AWS::IAM::Group, AWS::IAM::Role, AWS::IAM::User

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

blockedActionsPatterns, Type: CSV

Comma-separated list of blocked KMS action patterns, for example, kms:*, kms:Decrypt, kms:ReEncrypt*.

excludeRoleByManagementAccount (Optional), Type: boolean

Exclude a role if it is only assumable by organization management account.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

iam-no-inline-policy-check

Checks if the inline policy feature is not in use. The rule is NON_COMPLIANT if an Amazon Identity and Access Management (IAM) user, IAM role or IAM group has any inline policy.

Identifier: IAM_NO_INLINE_POLICY_CHECK

Resource Types: AWS::IAM::User, AWS::IAM::Role, AWS::IAM::Group

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

iam-password-policy

Checks if the account password policy for Amazon Identity and Access Management (IAM) users meets the specified requirements indicated in the parameters. The rule is NON_COMPLIANT if the account password policy does not meet the specified requirements.

Important

The `true` and `false` values for the rule parameters are case-sensitive. If `true` is not provided in lowercase, it will be treated as `false`.

Note

Evaluation Result for the Default IAM Password Policy
This rule is marked as NON_COMPLIANT when the default IAM password policy is used.
Managed Rules and Global IAM Resource Types
The global IAM resource types onboarded before February 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy`, `AWS::IAM::Role`, and `AWS::IAM::User`) can only be recorded by Amazon Config in Amazon Regions where Amazon Config was available before February 2022. These resource types cannot be recorded in Regions supported by Amazon Config after February 2022. For a list of those Regions, see Recording Amazon Resources | Global Resources.
If you record a global IAM resource type in at least one Region, periodic rules that report compliance on the global IAM resource type will run evaluations in all Regions where the periodic rule is added, even if you have not enabled the recording of the global IAM resource type in the Region where the periodic rule was added.
To avoid unnecessary evaluations, you should only deploy periodic rules that report compliance on a global IAM resource type to one of the supported Regions. For a list of

which managed rules are supported in which Regions, see List of Amazon Config Managed Rules by Region Availability.

Identifier: IAM_PASSWORD_POLICY

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary) Region

Parameters:

RequireUppercaseCharacters (Optional), Type: boolean, Default: true

Require at least one uppercase character in password.

RequireLowercaseCharacters (Optional), Type: boolean, Default: true

Require at least one lowercase character in password.

RequireSymbols (Optional), Type: boolean, Default: true

Require at least one symbol in password.

RequireNumbers (Optional), Type: boolean, Default: true

Require at least one number in password.

MinimumPasswordLength (Optional), Type: int, Default: 14

Password minimum length.

PasswordReusePrevention (Optional), Type: int, Default: 24

Number of passwords before allowing reuse.

MaxPasswordAge (Optional), Type: int, Default: 90

Number of days before password expiration.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

iam-policy-blacklisted-check

Checks in each Amazon Identity and Access Management (IAM) resource, if a policy Amazon Resource Name (ARN) in the input parameter is attached to the IAM resource. The rule is NON_COMPLIANT if the policy ARN is attached to the IAM resource.

Identifier: IAM_POLICY_BLACKLISTED_CHECK

Resource Types: AWS::IAM::User, AWS::IAM::Group, AWS::IAM::Role

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

policyArns, Type: CSV, Default: arn:aws:iam::aws:policy/AdministratorAccess

Comma separated list of IAM policy arns which should not be attached to any IAM entity.

exceptionList (Optional), Type: CSV

Comma separated list of resourcetypes and list of resource name pairs. For example, users:[user1;user2], groups:[group1;group2], roles:[role1;role2;role3].

> **Note**
>
> For the exception list, specify the name of the resource and not the full ARN. Not valid: `arn:aws:iam::444455556666:role/Admin`. Valid: `Admin`.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

iam-policy-in-use

Checks whether the IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity.

Note

Managed Rules and Global IAM Resource Types
The global IAM resource types onboarded before February 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy`, `AWS::IAM::Role`, and `AWS::IAM::User`) can only be recorded by Amazon Config in Amazon Regions where Amazon Config was available before February 2022. These resource types cannot be recorded in Regions supported by Amazon Config after February 2022. For a list of those Regions, see Recording Amazon Resources | Global Resources.
If you record a global IAM resource type in at least one Region, periodic rules that report compliance on the global IAM resource type will run evaluations in all Regions where the periodic rule is added, even if you have not enabled the recording of the global IAM resource type in the Region where the periodic rule was added.
To avoid unnecessary evaluations, you should only deploy periodic rules that report compliance on a global IAM resource type to one of the supported Regions. For a list of which managed rules are supported in which Regions, see List of Amazon Config Managed Rules by Region Availability.

Identifier: IAM_POLICY_IN_USE

Resource Types: AWS::IAM::Policy

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

policyARN, Type: String

An IAM policy ARN to be checked.

policyUsageType (Optional), Type: String

Specify whether you expect the policy to be attached to an IAM user, group or role. Valid values are IAM_USER, IAM_GROUP, IAM_ROLE, or ANY. Default value is ANY.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

iam-policy-no-statements-with-admin-access

Checks if Amazon Identity and Access Management (IAM) policies that you create have Allow statements that grant permissions to all actions on all resources. The rule is NON_COMPLIANT if any customer managed IAM policy statement includes "Effect": "Allow" with "Action": "*" over "Resource": "*".

> **Note**
>
> This rule only evaluates customer managed policies. This rule does NOT evaluate inline policies or Amazon managed policies. For more information on the difference, see Managed policies and inline policies in the *IAM User Guide*.

The following policy is NON_COMPLIANT:

```
"Statement": [
{
"Sid": "VisualEditor",
"Effect": "Allow",
"Action": "*",
"Resource": "*"
}
```

The following policy is COMPLIANT:

```
"Statement": [
{
"Sid": "VisualEditor",
"Effect": "Allow",
"Action": "service:*",
"Resource": "*"
}
```

Identifier: IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS

Resource Types: AWS::IAM::Policy

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

excludePermissionBoundaryPolicy (Optional), Type: boolean

> Boolean flag to exclude the evaluation of IAM policies used as permissions boundaries. If set to 'true', the rule will not include permissions boundaries in the evaluation. Otherwise, all IAM policies in scope are evaluated when value is set to 'false.' Default value is 'false'.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

iam-policy-no-statements-with-full-access

Checks if Amazon Identity and Access Management (IAM) policies that you create grant permissions to all actions on individual Amazon resources. The rule is NON_COMPLIANT if any customer managed IAM policy allows full access to at least 1 Amazon service.

Context: Following the principle of least privilege, it is recommended to limit the permitted actions in your IAM policies when granting permissions to Amazon services. This approach helps ensure that you only grant the necessary permissions by specifying the exact actions required, avoiding the use of unrestricted wildcards for a service, such as `ec2:*`.

In some cases, you might want to permit multiple actions with a similar prefix, such as DescribeFlowLogs and DescribeAvailabilityZones. In these cases, you can add a suffixed wildcard to the common prefix (for example, `ec2:Describe*`). Grouping related actions can help avoid hitting IAM policy size limits.

This rule will return COMPLIANT if you use prefixed actions with a suffixed wildcard (for example, `ec2:Describe*`). This rule will only return NON_COMPLIANT if you use unrestricted wildcards (for example, `ec2:*`).

> **Note**
>
> This rule only evaluates customer managed policies. This rule does NOT evaluate inline policies or Amazon managed policies. For more information on the difference, see Managed policies and inline policies in the *IAM User Guide*.

Identifier: IAM_POLICY_NO_STATEMENTS_WITH_FULL_ACCESS

Resource Types: AWS::IAM::Policy

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

excludePermissionBoundaryPolicy (Optional), Type: boolean

Boolean flag to exclude the evaluation of IAM policies used as permissions boundaries. If set to 'true', the rule will not include permissions boundaries in the evaluation. Otherwise, all IAM policies in scope are evaluated when value is set to 'false.' Default value is 'false'.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

iam-role-managed-policy-check

Checks if all managed policies specified in the list of managed policies are attached to the Amazon Identity and Access Management (IAM) role. The rule is NON_COMPLIANT if a managed policy is not attached to the IAM role.

Identifier: IAM_ROLE_MANAGED_POLICY_CHECK

Resource Types: AWS::IAM::Role

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

managedPolicyArns, Type: CSV

Comma-separated list of Amazon managed policy Amazon Resource Names (ARNs). For more information, see Amazon Resource Names (ARNs) and Amazon managed policies in the *IAM User Guide*.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

iam-root-access-key-check

Checks if the root user access key is available. The rule is COMPLIANT if the user access key does not exist. Otherwise, NON_COMPLIANT.

Note

Managed Rules and Global IAM Resource Types
The global IAM resource types onboarded before February 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy`, `AWS::IAM::Role`, and `AWS::IAM::User`) can only be recorded by Amazon Config in Amazon Regions where Amazon Config was available before February 2022. These resource types cannot be recorded in Regions supported by Amazon Config after February 2022. For a list of those Regions, see Recording Amazon Resources | Global Resources.
If you record a global IAM resource type in at least one Region, periodic rules that report compliance on the global IAM resource type will run evaluations in all Regions where the periodic rule is added, even if you have not enabled the recording of the global IAM resource type in the Region where the periodic rule was added.
To avoid unnecessary evaluations, you should only deploy periodic rules that report compliance on a global IAM resource type to one of the supported Regions. For a list of

which managed rules are supported in which Regions, see List of Amazon Config Managed Rules by Region Availability.

Identifier: IAM_ROOT_ACCESS_KEY_CHECK

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

iam-user-group-membership-check

Checks whether IAM users are members of at least one IAM group.

Identifier: IAM_USER_GROUP_MEMBERSHIP_CHECK

Resource Types: AWS::IAM::User

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

groupNames (Optional), Type: String

Comma-separated list of IAM groups in which IAM users must be members.

> **Note**
>
> This rule does not support group names with commas.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

iam-user-mfa-enabled

Checks if the Amazon Identity and Access Management (IAM) users have multi-factor authentication (MFA) enabled. The rule is NON_COMPLIANT if MFA is not enabled for at least one IAM user.

> **Note**
>
> **Managed Rules and Global IAM Resource Types**
> The global IAM resource types onboarded before February 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy`, `AWS::IAM::Role`, and `AWS::IAM::User`) can only be recorded by Amazon Config in Amazon Regions where Amazon Config was available before February 2022. These resource types cannot be recorded in Regions supported by Amazon Config after February 2022. For a list of those Regions, see Recording Amazon Resources | Global Resources.
> If you record a global IAM resource type in at least one Region, periodic rules that report compliance on the global IAM resource type will run evaluations in all Regions where the periodic rule is added, even if you have not enabled the recording of the global IAM resource type in the Region where the periodic rule was added.
> To avoid unnecessary evaluations, you should only deploy periodic rules that report compliance on a global IAM resource type to one of the supported Regions. For a list of which managed rules are supported in which Regions, see List of Amazon Config Managed Rules by Region Availability.

Identifier: IAM_USER_MFA_ENABLED

Resource Types: AWS::IAM::User

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

iam-user-no-policies-check

Checks if none of your Amazon Identity and Access Management (IAM) users have policies attached. IAM users must inherit permissions from IAM groups or roles. The rule is NON_COMPLIANT if there is at least one policy that is attached to the IAM user.

Identifier: IAM_USER_NO_POLICIES_CHECK

Resource Types: AWS::IAM::User

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

iam-user-unused-credentials-check

Checks if your Amazon Identity and Access Management (IAM) users have passwords or active access keys that have not been used within the specified number of days you provided. The rule is NON_COMPLIANT if there are inactive accounts not recently used.

> **Note**
>
> **Re-evaluation Timeline**
> Re-evaluating this rule within 4 hours of the first evaluation will have no effect on the results.
> **Managed Rules and Global IAM Resource Types**
> The global IAM resource types onboarded before February 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy`, `AWS::IAM::Role`, and `AWS::IAM::User`) can only be recorded by Amazon Config in Amazon Regions where Amazon Config was available before February 2022. These resource types cannot be recorded in Regions supported by Amazon Config after February 2022. For a list of those Regions, see Recording Amazon Resources | Global Resources.
> If you record a global IAM resource type in at least one Region, periodic rules that report compliance on the global IAM resource type will run evaluations in all Regions where the periodic rule is added, even if you have not enabled the recording of the global IAM resource type in the Region where the periodic rule was added.
> To avoid unnecessary evaluations, you should only deploy periodic rules that report compliance on a global IAM resource type to one of the supported Regions. For a list of which managed rules are supported in which Regions, see List of Amazon Config Managed Rules by Region Availability.

Identifier: IAM_USER_UNUSED_CREDENTIALS_CHECK

Resource Types: AWS::IAM::User

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

maxCredentialUsageAge, Type: int, Default: 90

Maximum number of days a credential cannot be used. The default value is 90 days.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

restricted-ssh

> **Important**
>
> For this rule, the rule identifier (INCOMING_SSH_DISABLED) and rule name (restricted-ssh) are different.

Checks if the incoming SSH traffic for the security groups is accessible. The rule is COMPLIANT if the IP addresses of the incoming SSH traffic in the security groups are restricted (CIDR other than 0.0.0.0/0 or ::/0). Otherwise, NON_COMPLIANT.

Identifier: INCOMING_SSH_DISABLED

Resource Types: AWS::EC2::SecurityGroup

Trigger type: Configuration changes and Periodic

Amazon Web Services Region: All supported Amazon regions

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ec2-instances-in-vpc

> **Important**
>
> For this rule, the rule identifier (INSTANCES_IN_VPC) and rule name (ec2-instances-in-vpc) are different.

Checks if your EC2 instances belong to a virtual private cloud (VPC). Optionally, you can specify the VPC ID to associate with your instances.

Identifier: INSTANCES_IN_VPC

Resource Types: AWS::EC2::Instance

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

vpcId (Optional), Type: String

VPC ID that contains these EC2 instances.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

internet-gateway-authorized-vpc-only

Checks if internet gateways are attached to an authorized virtual private cloud (Amazon VPC). The rule is NON_COMPLIANT if internet gateways are attached to an unauthorized VPC.

Identifier: INTERNET_GATEWAY_AUTHORIZED_VPC_ONLY

Resource Types: AWS::EC2::InternetGateway

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Taipei), Canada West (Calgary) Region

Parameters:

AuthorizedVpcIds (Optional), Type: String

Comma-separated list of the authorized VPC IDs with attached IGWs. If parameter is not provided all attached IGWs will be NON_COMPLIANT.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

kinesis-stream-backup-retention-check

Checks if an Amazon Kinesis Data Stream has its data record retention period set to a specific number of hours. The rule is NON_COMPLIANT if the property `RetentionPeriodHours` is set to a value less than the value specified by the parameter.

Identifier: KINESIS_STREAM_BACKUP_RETENTION_CHECK

Resource Types: AWS::Kinesis::Stream

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary) Region

Parameters:

minimumBackupRetentionPeriod (Optional), Type: String

Minimum hours data records should be retained. Valid values are 24 to 8760, default value is 168.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

kinesis-stream-encrypted

Checks if Amazon Kinesis streams are encrypted at rest with server-side encryption. The rule is NON_COMPLIANT for a Kinesis stream if 'StreamEncryption' is not present.

Context: Server-side encryption is a feature in Amazon Kinesis Data Streams that automatically encrypts data before it's at rest by using an Amazon KMS Key. Data is encrypted before it's written to the Kinesis stream storage layer, and decrypted after it's retrieved from storage. As a result, your data is encrypted at rest within the Kinesis Data Streams service. This can help you to meet regulatory requirements and enhance the security of your data. For more information, Data Protection in Amazon Kinesis Data Streams.

Identifier: KINESIS_STREAM_ENCRYPTED

Resource Types: AWS::Kinesis::Stream

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

kms-cmk-not-scheduled-for-deletion

Checks if Amazon Key Management Service (Amazon KMS) keys are not scheduled for deletion in Amazon KMS. The rule is NON_COMPLIANT if KMS keys are scheduled for deletion.

Identifier: KMS_CMK_NOT_SCHEDULED_FOR_DELETION

Resource Types: AWS::KMS::Key

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Europe (Milan), Asia Pacific (Taipei) Region

Parameters:

kmsKeyIds (Optional), Type: String

(Optional) Comma-separated list of specific customer managed key IDs not to be scheduled for deletion. If you do not specify any keys, the rule checks all the keys.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

kms-key-policy-no-public-access

Checks if the Amazon KMS key policy allows public access. The rule is NON_COMPLIANT if the KMS key policy allows public access to the KMS key.

> **Note**
>
> To be considered non-public, a KMS key policy must grant access only to fixed values. This means values that don't contain a wildcard or the following IAM policy element: Variables.

Identifier: KMS_KEY_POLICY_NO_PUBLIC_ACCESS

Resource Types: AWS::KMS::Key

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

mfa-enabled-for-iam-console-access

Checks if Amazon multi-factor authentication (MFA) is enabled for all Amazon Identity and Access Management (IAM) users that use a console password. The rule is COMPLIANT if MFA is enabled.

> **Note**
>
> **Re-evaluation Timeline**
> Re-evaluating this rule within 4 hours of the first evaluation will have no effect on the results.
> **Managed Rules and Global IAM Resource Types**
> The global IAM resource types onboarded before February 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy`, `AWS::IAM::Role`, and `AWS::IAM::User`) can only be recorded by Amazon Config in Amazon Regions where Amazon Config was available before February 2022. These resource types cannot be recorded in Regions supported by Amazon Config after February 2022. For a list of those Regions, see Recording Amazon Resources | Global Resources.
> If you record a global IAM resource type in at least one Region, periodic rules that report compliance on the global IAM resource type will run evaluations in all Regions where the periodic rule is added, even if you have not enabled the recording of the global IAM resource type in the Region where the periodic rule was added.
> To avoid unnecessary evaluations, you should only deploy periodic rules that report compliance on a global IAM resource type to one of the supported Regions. For a list of which managed rules are supported in which Regions, see List of Amazon Config Managed Rules by Region Availability.

Identifier: MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS

Resource Types: AWS::IAM::User

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

mq-active-deployment-mode

Checks the deployment mode configured for Amazon MQ ActiveMQ broker engine. The rule is NON_COMPLIANT if the default single-instance broker mode is being used.

Identifier: MQ_ACTIVE_DEPLOYMENT_MODE

Resource Types: AWS::AmazonMQ::Broker

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

mq-auto-minor-version-upgrade-enabled

Checks if automatic minor version upgrades are enabled for Amazon MQ brokers. The rule is NON_COMPLIANT if the 'AutoMinorVersionUpgrade' field is not enabled for an Amazon MQ broker.

Identifier: MQ_AUTO_MINOR_VERSION_UPGRADE_ENABLED

Resource Types: AWS::AmazonMQ::Broker

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

mq-rabbit-deployment-mode

Checks the deployment mode configured for the Amazon MQ RabbitMQ broker engine. The rule is NON_COMPLIANT if the default single-instance broker mode is being used.

Identifier: MQ_RABBIT_DEPLOYMENT_MODE

Resource Types: AWS::AmazonMQ::Broker

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

msk-cluster-public-access-disabled

Checks if public access is disabled on Amazon MSK clusters. The rule is NON_COMPLIANT if public access on an Amazon MSK cluster is not disabled.

Identifier: MSK_CLUSTER_PUBLIC_ACCESS_DISABLED

Resource Types: AWS::MSK::Cluster

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Seoul), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

msk-enhanced-monitoring-enabled

Checks if enhanced monitoring is enabled for an Amazon MSK cluster set to PER_TOPIC_PER_BROKER or PER_TOPIC_PER_PARTITION. The rule is NON_COMPLIANT if enhanced monitoring is enabled and set to DEFAULT or PER_BROKER.

Identifier: MSK_ENHANCED_MONITORING_ENABLED

Resource Types: AWS::MSK::Cluster

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

msk-in-cluster-node-require-tls

Checks if an Amazon MSK cluster enforces encryption in transit using HTTPS (TLS) with the broker nodes of the cluster. The rule is NON_COMPLIANT if plain text communication is enabled for in-cluster broker node connections.

Identifier: MSK_IN_CLUSTER_NODE_REQUIRE_TLS

Resource Types: AWS::MSK::Cluster

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

msk-unrestricted-access-check

Checks if an Amazon MSK Cluster has unauthenticated access disabled. The rule is NON_COMPLIANT if Amazon MSK Cluster has unauthenticated access enabled.

Identifier: MSK_UNRESTRICTED_ACCESS_CHECK

Resource Types: AWS::MSK::Cluster

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Seoul), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

multi-region-cloudtrail-enabled

> **Important**
>
> For this rule, the rule identifier (MULTI_REGION_CLOUD_TRAIL_ENABLED) and rule name (multi-region-cloudtrail-enabled) are different.

Checks if there is at least one multi-region Amazon CloudTrail. The rule is NON_COMPLIANT if the trails do not match input parameters. The rule is NON_COMPLIANT if the `ExcludeManagementEventSources` field is not empty or if Amazon CloudTrail is configured to exclude management events such as Amazon KMS events or Amazon RDS Data API events.

Identifier: MULTI_REGION_CLOUD_TRAIL_ENABLED

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions

Parameters:

s3BucketName (Optional), Type: String

Name of Amazon S3 bucket for Amazon CloudTrail to deliver log files to.

snsTopicArn (Optional), Type: String

Amazon SNS topic ARN for Amazon CloudTrail to use for notifications.

cloudWatchLogsLogGroupArn (Optional), Type: String

Amazon CloudWatch log group ARN for Amazon CloudTrail to send data to.

includeManagementEvents (Optional), Type: boolean

Event selector to include management events for the Amazon CloudTrail.

readWriteType (Optional), Type: String

Type of events to record. Valid values are ReadOnly, WriteOnly and ALL.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

nacl-no-unrestricted-ssh-rdp

Checks if default ports for SSH/RDP ingress traffic for network access control lists (NACLs) is unrestricted. The rule is NON_COMPLIANT if a NACL inbound entry allows a source TCP or UDP CIDR block for ports 22 or 3389.

Identifier: NACL_NO_UNRESTRICTED_SSH_RDP

Resource Types: AWS::EC2::NetworkAcl

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

no-unrestricted-route-to-igw

Checks if there are public routes in the route table to an Internet gateway (IGW). The rule is NON_COMPLIANT if a route to an IGW has a destination CIDR block of '0.0.0.0/0' or '::/0' or if a destination CIDR block does not match the rule parameter.

Identifier: NO_UNRESTRICTED_ROUTE_TO_IGW

Resource Types: AWS::EC2::RouteTable

Trigger type: Configuration changes and Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Taipei), Canada West (Calgary) Region

Parameters:

routeTableIds (Optional), Type: CSV

> Comma-separated list of route table IDs that can have routes to an Internet Gateway with a destination CIDR block of '0.0.0.0/0' or '::/0'.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

opensearch-update-check

Checks if Amazon OpenSearch Service version updates are available but not installed. The rule is NON_COMPLIANT for an OpenSearch domain if the latest software updates are not installed.

Identifier: OPENSEARCH_UPDATE_CHECK

Resource Types: AWS::OpenSearch::Domain

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

rabbit-mq-supported-version

Checks if an Amazon MQ RabbitMQ broker is running on a specified minimum supported engine version. The rule is NON_COMPLIANT if the RabbitMQ broker is not running on the minimum supported engine version that you specify.

Identifier: RABBIT_MQ_SUPPORTED_VERSION

Resource Types: AWS::AmazonMQ::Broker

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

supportedEngineVersion, Type: String

> String value for the rule to check the minimum supported engine version for the RabbitMQ broker. RabbitMQ brokers use semantic versioning specification: X.Y.Z. X denotes the major version, Y represents the minor version, and Z denotes the patch version.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

rds-automatic-minor-version-upgrade-enabled

Checks if Amazon Relational Database Service (Amazon RDS) database instances are configured for automatic minor version upgrades. The rule is NON_COMPLIANT if the value of 'autoMinorVersionUpgrade' is false.

Identifier: RDS_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED

Resource Types: AWS::RDS::DBInstance

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

None

Proactive Evaluation

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with Amazon Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
    "AutoMinorVersionUpgrade": BOOLEAN*,
    "Engine": String*
}
...
```

*For more information on valid values for these inputs, see AutoMinorVersionUpgrade and Engine in the Amazon CloudFormation User Guide.

For more information on proactive evaluation, see Evaluation Mode.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

rds-enhanced-monitoring-enabled

Checks if enhanced monitoring is enabled for Amazon RDS instances. This rule is NON_COMPLIANT if '`monitoringInterval`' is '0' in the configuration item of the RDS instance, or if '`monitoringInterval`' does not match the rule parameter value.

Identifier: RDS_ENHANCED_MONITORING_ENABLED

Resource Types: AWS::RDS::DBInstance

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

monitoringInterval (Optional), Type: int

An integer value in seconds between points when enhanced monitoring metrics are collected for the database instance. The valid values are 1, 5, 10, 15, 30, and 60.

Proactive Evaluation

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with Amazon Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
    "MonitoringInterval": Integer*,
    "Engine": String*
}
...
```

*For more information on valid values for these inputs, see MonitoringInterval and Engine in the Amazon CloudFormation User Guide.

For more information on proactive evaluation, see Evaluation Mode.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

rds-instance-deletion-protection-enabled

Checks if an Amazon Relational Database Service (Amazon RDS) instance has deletion protection enabled. The rule is NON_COMPLIANT if an Amazon RDS instance does not have deletion protection enabled; for example, deletionProtection is set to false.

> **Warning**
>
> Some RDS DB instances within a Cluster (Aurora/DocumentDB) will show as non-compliant.

Identifier: RDS_INSTANCE_DELETION_PROTECTION_ENABLED

Resource Types: AWS::RDS::DBInstance

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

databaseEngines (Optional), Type: CSV

Comma-separated list of RDS database engines to include in the evaluation of the rule. For example, 'mysql, postgres, mariadb'.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

rds-instance-iam-authentication-enabled

Checks if an Amazon Relational Database Service (Amazon RDS) instance has Amazon Identity and Access Management (IAM) authentication enabled. The rule is NON_COMPLIANT if an Amazon RDS instance does not have IAM authentication enabled.

> **Note**
>
> The DB Engine should be one of 'mysql', 'postgres', 'aurora', 'aurora-mysql', or 'aurora-postgresql'. The DB instance status should be one of 'available', 'backing-up', 'storage-optimization', or 'storage-full'.

Identifier: RDS_INSTANCE_IAM_AUTHENTICATION_ENABLED

Resource Types: AWS::RDS::DBInstance

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

rds-instance-public-access-check

Checks if the Amazon Relational Database Service (Amazon RDS) instances are not publicly accessible. The rule is NON_COMPLIANT if the publiclyAccessible field is true in the instance configuration item.

Identifier: RDS_INSTANCE_PUBLIC_ACCESS_CHECK

Resource Types: AWS::RDS::DBInstance

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

None

Proactive Evaluation

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with Amazon Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
   "PubliclyAccessible": BOOLEAN
}
...
```

For more information on proactive evaluation, see Evaluation Mode.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

rds-instance-subnet-igw-check

Checks if RDS DB instances are deployed in a public subnet with a route to the internet gateway. The rule is NON_COMPLIANT if RDS DB instances is deployed in a public subnet

Identifier: RDS_INSTANCE_SUBNET_IGW_CHECK

Resource Types: AWS::RDS::DBInstance

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Middle East (Bahrain), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

rds-in-backup-plan

Checks if Amazon Relational Database Service (Amazon RDS) databases are present in Amazon Backup plans. The rule is NON_COMPLIANT if Amazon RDS databases are not included in any Amazon Backup plan.

> **Note**
>
> The rule only applies to Amazon Aurora DB instances. DB clusters are not supported.

Identifier: RDS_IN_BACKUP_PLAN

Resource Types: AWS::RDS::DBInstance

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Taipei), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

rds-logging-enabled

Checks if respective logs of Amazon Relational Database Service (Amazon RDS) are enabled. The rule is NON_COMPLIANT if any log types are not enabled.

> **Note**
>
> DB Instances that are not in 'available', 'backing-up', 'storage-optimization', or 'storage-full' status evaluate as `NOT_APPLICABLE`.

Identifier: RDS_LOGGING_ENABLED

Resource Types: AWS::RDS::DBInstance

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

additionalLogs (Optional), Type: StringMap

Comma-separated list of engine names and log type names. For example, "additionalLogs": "oracle: general, slowquery ; aurora: alert, slowquery"

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

rds-multi-az-support

Checks whether high availability is enabled for your RDS DB instances.

In a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. For more information, see High Availability (Multi-AZ) in the *Amazon RDS User Guide*.

> **Note**
>
> This rule does not evaluate Amazon Aurora DB, Amazon DocumentDB, and Amazon Neptune DB instances.

Identifier: RDS_MULTI_AZ_SUPPORT

Resource Types: AWS::RDS::DBInstance

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

None

Proactive Evaluation

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with Amazon Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
    "MultiAZ": BOOLEAN*,
    "Engine": String*
}
...
```

*For more information on valid values for these inputs, see MultiAZ and Engine in the Amazon CloudFormation User Guide.

For more information on proactive evaluation, see Evaluation Mode.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

rds-mysql-instance-encrypted-in-transit

Checks if connections to Amazon RDS for MySQL database instances are configured to use encryption in transit. The rule is NON_COMPLIANT if the associated database parameter group is not in-sync or if the require_secure_transport parameter is not set to 1.

> **Note**
>
> The rule returns `NOT_APPLICABLE` if the Amazon RDS instance is part of an RDS cluster.

Identifier: RDS_MYSQL_INSTANCE_ENCRYPTED_IN_TRANSIT

Resource Types: AWS::RDS::DBInstance

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

rds-postgresql-logs-to-cloudwatch

Checks if an Amazon PostgreSQL DB instance is configured to publish logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if the DB instance is not configured to publish logs to Amazon CloudWatch Logs.

Identifier: RDS_POSTGRESQL_LOGS_TO_CLOUDWATCH

Resource Types: AWS::RDS::DBInstance

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

logTypes (Optional), Type: CSV

> Comma-separated list of log types to be published to CloudWatch Logs. Valid values are: 'postgresql', 'upgrade'. Default value is 'postgresql'.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

rds-postgres-instance-encrypted-in-transit

Checks if connections to Amazon RDS PostgreSQL database instances are configured to use encryption in transit. The rule is NON_COMPLIANT if the associated database parameter group is not in-sync or if the rds.force_ssl parameter is not set to 1.

> **Note**
>
> The rule returns `NOT_APPLICABLE` if the Amazon RDS instance is part of an RDS cluster.

Identifier: RDS_POSTGRES_INSTANCE_ENCRYPTED_IN_TRANSIT

Resource Types: AWS::RDS::DBInstance

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

rds-snapshots-public-prohibited

Checks if Amazon Relational Database Service (Amazon RDS) snapshots are public. The rule is NON_COMPLIANT if any existing and new Amazon RDS snapshots are public.

> **Note**
>
> It can take up to 12 hours for compliance results to be captured.

Identifier: RDS_SNAPSHOTS_PUBLIC_PROHIBITED

Resource Types: AWS::RDS::DBSnapshot, AWS::RDS::DBClusterSnapshot

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Africa (Cape Town), Asia Pacific (Melbourne), Europe (Milan), Israel (Tel Aviv), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

rds-snapshot-encrypted

Checks if Amazon Relational Database Service (Amazon RDS) DB snapshots are encrypted. The rule is NON_COMPLIANT if the Amazon RDS DB snapshots are not encrypted.

Identifier: RDS_SNAPSHOT_ENCRYPTED

Resource Types: AWS::RDS::DBSnapshot, AWS::RDS::DBClusterSnapshot

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

rds-sqlserver-encrypted-in-transit

Checks if connections to Amazon RDS SQL server database instances are configured to use encryption in transit. The rule is NON_COMPLIANT if the DB parameter force_ssl for the parameter group is not set to 1 or the ApplyStatus parameter is not 'in-sync'.

Identifier: RDS_SQLSERVER_ENCRYPTED_IN_TRANSIT

Resource Types: AWS::RDS::DBInstance

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Middle East (Bahrain), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

rds-sql-server-logs-to-cloudwatch

Checks if an Amazon SQL Server DB instance is configured to publish logs to Amazon CloudWatch Logs. This rule is NON_COMPLIANT if the DB instance is not configured to publish logs to Amazon CloudWatch Logs.

Identifier: RDS_SQL_SERVER_LOGS_TO_CLOUDWATCH

Resource Types: AWS::RDS::DBInstance

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

logTypes (Optional), Type: CSV

> logTypes - (Optional): Comma-separated list of log types to be published to CloudWatch Logs. Valid values are: 'error', 'agent'. Default value is 'error', 'agent'.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

rds-storage-encrypted

Checks if storage encryption is enabled for your Amazon Relational Database Service (Amazon RDS) DB instances. The rule is NON_COMPLIANT if storage encryption is not enabled.

Identifier: RDS_STORAGE_ENCRYPTED

Resource Types: AWS::RDS::DBInstance

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

kmsKeyId (Optional), Type: String

KMS key ID or Amazon Resource Name (ARN) used to encrypt the storage.

Proactive Evaluation

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with Amazon Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
   "StorageEncrypted": BOOLEAN
}
...
```

For more information on proactive evaluation, see Evaluation Mode.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

redshift-backup-enabled

Checks that Amazon Redshift automated snapshots are enabled for clusters. The rule is NON_COMPLIANT if the value for `automatedSnapshotRetentionPeriod` is greater than `MaxRetentionPeriod` or less than `MinRetentionPeriod` or the value is 0.

Identifier: REDSHIFT_BACKUP_ENABLED

Resource Types: AWS::Redshift::Cluster

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary) Region

Parameters:

MinRetentionPeriod (Optional), Type: int

Minimum value for the retention period. Minimum value is 1.

MaxRetentionPeriod (Optional), Type: int

Maximum value for the retention period. Maximum value is 35.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

redshift-cluster-configuration-check

Checks if Amazon Redshift clusters have the specified settings. The rule is NON_COMPLIANT if the Amazon Redshift cluster is not encrypted or encrypted with another key, or if a cluster does not have audit logging enabled.

Identifier: REDSHIFT_CLUSTER_CONFIGURATION_CHECK

Resource Types: AWS::Redshift::Cluster

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain) Region

Parameters:

clusterDbEncrypted, Type: boolean, Default: true

Database encryption is enabled.

loggingEnabled, Type: boolean, Default: true

Audit logging is enabled.

nodeTypes (Optional), Type: CSV, Default: dc1.large

Specify node type.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

redshift-cluster-kms-enabled

Checks if Amazon Redshift clusters are using a specified Amazon Key Management Service (Amazon KMS) key for encryption. The rule is COMPLIANT if encryption is enabled and the cluster is encrypted with the key provided in the `kmsKeyArn` parameter. The rule is NON_COMPLIANT if the cluster is not encrypted or encrypted with another key.

Identifier: REDSHIFT_CLUSTER_KMS_ENABLED

Resource Types: AWS::Redshift::Cluster

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Mexico (Central), Asia Pacific (Taipei) Region

Parameters:

kmsKeyArns (Optional), Type: CSV

Comma-separated list of Amazon KMS key Amazon Resource Names (ARNs) used in Amazon Redshift clusters for encryption.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

redshift-cluster-maintenancesettings-check

Checks if Amazon Redshift clusters have the specified maintenance settings. The rule is NON_COMPLIANT if the automatic upgrades to major version is disabled.

Identifier: REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK

Resource Types: AWS::Redshift::Cluster

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Mexico (Central), Asia Pacific (Taipei) Region

Parameters:

allowVersionUpgrade, Type: boolean, Default: true

Allow version upgrade is enabled.

preferredMaintenanceWindow (Optional), Type: String

Scheduled maintenance window for clusters (for example, Mon:09:30-Mon:10:00).

automatedSnapshotRetentionPeriod (Optional), Type: int, Default: 1

Number of days to retain automated snapshots.

Proactive Evaluation

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with Amazon Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration

schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
    "AutomatedSnapshotRetentionPeriod": Integer*,
    "PreferredMaintenanceWindow": String*,
    "AllowVersionUpgrade": BOOLEAN*
}
...
```

*For more information on valid values for these inputs, see AutomatedSnapshotRetentionPeriod, PreferredMaintenanceWindow, and AllowVersionUpgrade in the Amazon CloudFormation User Guide.

For more information on proactive evaluation, see Evaluation Mode.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

redshift-cluster-multi-az-enabled

Checks if an Amazon Redshift cluster has multiple Availability Zones deployments enabled. This rule is NON_COMPLIANT if Amazon Redshift cluster does not have multiple Availability Zones deployments enabled.

Identifier: REDSHIFT_CLUSTER_MULTI_AZ_ENABLED

Resource Types: AWS::Redshift::Cluster

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Seoul), Asia Pacific (Malaysia), Mexico (Central), US West (N. California), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

redshift-cluster-public-access-check

Checks if Amazon Redshift clusters are not publicly accessible. The rule is NON_COMPLIANT if the publiclyAccessible field is True in the cluster configuration item.

Identifier: REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK

Resource Types: AWS::Redshift::Cluster

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Mexico (Central), Asia Pacific (Taipei) Region

Parameters:

None

Proactive Evaluation

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with Amazon Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
   "PubliclyAccessible": BOOLEAN
}
...
```

For more information on proactive evaluation, see Evaluation Mode.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

redshift-cluster-subnet-group-multi-az

Checks If Amazon Redshift subnet groups contain subnets from more than one Availability Zone. The rule is NON_COMPLIANT if an Amazon Redshift subnet group does not contain subnets from at least two different Availability Zones.

Identifier: REDSHIFT_CLUSTER_SUBNET_GROUP_MULTI_AZ

Resource Types: AWS::Redshift::ClusterSubnetGroup

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

redshift-default-admin-check

Checks if an Amazon Redshift cluster has changed the admin username from its default value. The rule is NON_COMPLIANT if the admin username for a Redshift cluster is set to “awsuser” or if the username does not match what is listed in parameter.

Identifier: REDSHIFT_DEFAULT_ADMIN_CHECK

Resource Types: AWS::Redshift::Cluster

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary) Region

Parameters:

validAdminUserNames (Optional), Type: CSV

Comma-separated list of admin username(s) for Redshift clusters to use. Note: 'awsuser' is the default and not accepted.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

redshift-default-db-name-check

Checks if a Redshift cluster has changed its database name from the default value. The rule is NON_COMPLIANT if the database name for a Redshift cluster is set to “dev”, or if the optional parameter is provided and the database name does not match.

Identifier: REDSHIFT_DEFAULT_DB_NAME_CHECK

Resource Types: AWS::Redshift::Cluster

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary) Region

Parameters:

validDatabaseNames (Optional), Type: CSV

Comma-separated list of database name(s) for Redshift clusters.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

redshift-enhanced-vpc-routing-enabled

Checks if Amazon Redshift cluster has 'enhancedVpcRouting' enabled. The rule is NON_COMPLIANT if 'enhancedVpcRouting' is not enabled or if the configuration.enhancedVpcRouting field is 'false'.

Identifier: REDSHIFT_ENHANCED_VPC_ROUTING_ENABLED

Resource Types: AWS::Redshift::Cluster

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Mexico (Central), Asia Pacific (Taipei) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

redshift-require-tls-ssl

Checks if Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. The rule is NON_COMPLIANT if any Amazon Redshift cluster has parameter require_SSL not set to true.

Identifier: REDSHIFT_REQUIRE_TLS_SSL

Resource Types: AWS::Redshift::Cluster, AWS::Redshift::ClusterParameterGroup

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Mexico (Central), Asia Pacific (Taipei) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

redshift-serverless-default-admin-check

Checks if an Amazon Redshift Serverless Namespace has changed the admin username from its default value. The rule is NON_COMPLIANT if the admin username for a Redshift Serverless Namespace is set to “admin”.

Identifier: REDSHIFT_SERVERLESS_DEFAULT_ADMIN_CHECK

Resource Types: AWS::RedshiftServerless::Namespace

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Middle East (Bahrain), Asia Pacific (Thailand), Africa (Cape Town), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Europe (Milan), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

redshift-serverless-default-db-name-check

Checks if an Amazon Redshift Serverless namespace has changed its database name from the default value. The rule is NON_COMPLIANT if the database name for an Amazon Redshift Serverless namespace is set to `dev`.

Identifier: REDSHIFT_SERVERLESS_DEFAULT_DB_NAME_CHECK

Resource Types: AWS::RedshiftServerless::Namespace

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Middle East (Bahrain), Asia Pacific (Thailand), Africa (Cape Town), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Europe (Milan), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

redshift-serverless-namespace-cmk-encryption

Checks if Amazon Redshift Serverless namespaces are encrypted by customer managed Amazon KMS keys. The rule is NON_COMPLIANT if a namespace is not encrypted by a customer managed key. Optionally, you can specify a list of KMS keys for rule to check.

Identifier: REDSHIFT_SERVERLESS_NAMESPACE_CMK_ENCRYPTION

Resource Types: AWS::RedshiftServerless::Namespace

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Middle East (Bahrain), Asia Pacific (Thailand), Africa (Cape Town), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Europe (Milan), Mexico (Central), Canada West (Calgary) Region

Parameters:

kmsKeyArns (Optional), Type: CSV

> Comma-separated list of Amazon Resource Names (ARNs) of customer managed keys for the rule to check. If provided, the rule is NON_COMPLIANT if an Amazon Redshift Serverless namespace is not encrypted with one of these KMS keys.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

redshift-serverless-publish-logs-to-cloudwatch

Checks if Amazon Redshift Serverless Namespace is configured to publish the following logs to Amazon CloudWatch Logs. This rule is NON_COMPLIANT if the Namespace is not configured to publish the following logs to Amazon CloudWatch Logs.

Identifier: REDSHIFT_SERVERLESS_PUBLISH_LOGS_TO_CLOUDWATCH

Resource Types: AWS::RedshiftServerless::Namespace

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Middle East (Bahrain), Asia Pacific (Thailand), Africa (Cape Town), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Europe (Milan), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Canada West (Calgary) Region

Parameters:

logType (Optional), Type: CSV

> Comma-separated list of log types to be published to CloudWatch Logs. Valid values are 'connectionlog', 'userlog' Default value is 'connectionlog', 'userlog'.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

required-tags

Checks if your resources have the tags that you specify. For example, you can check whether your Amazon EC2 instances have the `CostCenter` tag, while also checking if all your RDS instance have one set of Keys tag. Separate multiple values with commas. You can check up to 6 tags at a time.

The Amazon-managed Amazon Systems Manager automation document `AWS-SetRequiredTags` does not work as a remediation with this rule. You will need to create your own custom Systems Manager automation documentation for remediation.

Context: Amazon allows you to assign metadata to Amazon resources in the form of tags. Each tag is a label consisting of a key and an optional value to store information about the resource or data retained on that resource. For more information see, Building your tagging strategy.

You can use this rule to find resources in your account that were not launched with your desired configurations by specifying which resources should have tags and the expected value for each tag. You can also run remediation actions to fix tagging mistakes. However, this rule does not prevent you from creating resources with incorrect tags.

> **Note**
>
> Amazon Config does not support recording associated tags for all resource types. To verify if Amazon Config records tags in the configuration item (CI) for a specific resource type:
>
> - Check that Amazon Config correctly records the current configuration for the resource, excluding tags.
> - Check that Amazon Config refreshes the recorded configuration when a change is made to the resource.

Identifier: REQUIRED_TAGS

Resource Types: AWS::ACM::Certificate, AWS::AutoScaling::AutoScalingGroup, AWS::CloudFormation::Stack, AWS::CodeBuild::Project, AWS::DynamoDB::Table, AWS::EC2::CustomerGateway, AWS::EC2::Instance, AWS::EC2::InternetGateway, AWS::EC2::NetworkAcl, AWS::EC2::NetworkInterface, AWS::EC2::RouteTable, AWS::EC2::SecurityGroup, AWS::EC2::Subnet, AWS::EC2::Volume, AWS::EC2::VPC, AWS::EC2::VPNConnection, AWS::EC2::VPNGateway, AWS::ElasticLoadBalancing::LoadBalancer, AWS::ElasticLoadBalancingV2::LoadBalancer, AWS::RDS::DBInstance, AWS::RDS::DBSecurityGroup, AWS::RDS::DBSnapshot, AWS::RDS::DBSubnetGroup, AWS::RDS::EventSubscription, AWS::Redshift::Cluster, AWS::Redshift::ClusterParameterGroup, AWS::Redshift::ClusterSecurityGroup, AWS::Redshift::ClusterSnapshot, AWS::Redshift::ClusterSubnetGroup, AWS::S3::Bucket

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

tag1Key, Type: String, Default: CostCenter

Key of the required tag.

tag1Value (Optional), Type: CSV

Optional value of the required tag. Separate multiple values with commas.

tag2Key (Optional), Type: String

Key of a second required tag.

tag2Value (Optional), Type: CSV

Optional value of the second required tag. Separate multiple values with commas.

tag3Key (Optional), Type: String

Key of a third required tag.

tag3Value (Optional), Type: CSV

Optional value of the third required tag. Separate multiple values with commas.

tag4Key (Optional), Type: String

Key of a fourth required tag.

tag4Value (Optional), Type: CSV

Optional value of the fourth required tag. Separate multiple values with commas.

tag5Key (Optional), Type: String

Key of a fifth required tag.

tag5Value (Optional), Type: CSV

Optional value of the fifth required tag. Separate multiple values with commas.

tag6Key (Optional), Type: String

Key of a sixth required tag.

tag6Value (Optional), Type: CSV

Optional value of the sixth required tag. Separate multiple values with commas.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

restricted-common-ports

> **Important**
>
> For this rule, the rule identifier (RESTRICTED_INCOMING_TRAFFIC) and rule name (restricted-common-ports) are different.

Checks if the security groups in use do not allow unrestricted incoming Transmission Control Protocol (TCP) traffic to specified ports. The rule is COMPLIANT if:

- Port access is blocked to all TCP traffic.
- Port access is open to TCP traffic through Inbound rules, where the source is either a single IPv4 address or a range of IPv4 addresses in CIDR notation which does not cover all IPv4 addresses ("0.0.0.0/0").
- Port access is open to TCP traffic through Inbound rules, where the source is either a single IPv6 address or a range of IPv6 addresses in CIDR notation which does not cover all IPv6 addresses ("::/0)").

The rule is NON_COMPLIANT if IP addresses for inbound TCP connections are not restricted to specified ports.

Identifier: RESTRICTED_INCOMING_TRAFFIC

Resource Types: AWS::EC2::SecurityGroup

Trigger type: Configuration changes and Periodic

Amazon Web Services Region: All supported Amazon regions

Parameters:

blockedPort1 (Optional), Type: int, Default: 20

Blocked TCP port number. The default of 20 corresponds to File Transfer Protocol (FTP) Data Transfer.

blockedPort2 (Optional), Type: int, Default: 21

Blocked TCP port number. The default of 21 corresponds to File Transfer Protocol (FTP) Command Control.

blockedPort3 (Optional), Type: int, Default: 3389

Blocked TCP port number. The default of 3389 corresponds to Remote Desktop Protocol (RDP).

blockedPort4 (Optional), Type: int, Default: 3306

Blocked TCP port number. The default of 3306 corresponds to MySQL protocol.

blockedPort5 (Optional), Type: int, Default: 4333

Blocked TCP port number. The default of 4333 corresponds to MySQL protocol.

blockedPorts (Optional), Type: CSV

Comma-separated list of blocked TCP port numbers. For example, 20, 21, 3306, 3389, and 4333.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

s3-access-point-in-vpc-only

Checks if an Amazon S3 access point does not allow access from the internet (NetworkOrigin is VPC). The rule is NON_COMPLIANT if NetworkOrigin is Internet.

Identifier: S3_ACCESS_POINT_IN_VPC_ONLY

Resource Types: AWS::S3::AccessPoint

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

s3-access-point-public-access-blocks

Checks if Amazon S3 access points have block public access settings enabled. The rule is NON_COMPLIANT if block public access settings are not enabled for S3 access points.

Identifier: S3_ACCESS_POINT_PUBLIC_ACCESS_BLOCKS

Resource Types: AWS::S3::AccessPoint

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

excludedAccessPoints (Optional), Type: CSV

Comma-separated list of names for allowed public Amazon S3 access points.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

s3-account-level-public-access-blocks

Checks if the required public access block settings are configured from account level. The rule is only NON_COMPLIANT when the fields set below do not match the corresponding fields in the configuration item.

> **Note**
>
> If you are using this rule, ensure that S3 Block Public Access is enabled. The rule is change-triggered, so it will not be invoked unless S3 Block Public Access is enabled. If S3 Block Public Access is not enabled the rule returns INSUFFICIENT_DATA. This means that you still might have some public buckets. For more information about setting up S3 Block Public Access, see Blocking public access to your Amazon S3 storage.

Identifier: S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS

Resource Types: AWS::S3::AccountPublicAccessBlock

Trigger type: Configuration changes (current status not checked, only evaluated when changes generate new events)

> **Note**
>
> This rule is only triggered by configuration changes for the specific region where the S3 endpoint is located. In all other regions, the rule is checked periodically. If a change was made in another region, there could be a delay before the rule returns NON_COMPLIANT.

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary) Region

Parameters:

IgnorePublicAcls (Optional), Type: String, Default: True

IgnorePublicAcls is enforced or not, default True

BlockPublicPolicy (Optional), Type: String, Default: True

BlockPublicPolicy is enforced or not, default True

BlockPublicAcls (Optional), Type: String, Default: True

BlockPublicAcls is enforced or not, default True

RestrictPublicBuckets (Optional), Type: String, Default: True

RestrictPublicBuckets is enforced or not, default True

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

s3-account-level-public-access-blocks-periodic

Checks if the required public access block settings are configured at the account level. The rule is NON_COMPLIANT if the configuration item does not match one or more settings from parameters (or default).

Identifier: S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC

Resource Types: AWS::::Account

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions

Parameters:

IgnorePublicAcls (Optional), Type: String

IgnorePublicAcls is enforced or not, default True

BlockPublicPolicy (Optional), Type: String

BlockPublicPolicy is enforced or not, default True

BlockPublicAcls (Optional), Type: String

BlockPublicAcls is enforced or not, default True

RestrictPublicBuckets (Optional), Type: String

RestrictPublicBuckets is enforced or not, default True

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

s3-bucket-acl-prohibited

Checks if Amazon Simple Storage Service (Amazon S3) Buckets allow user permissions through access control lists (ACLs). The rule is NON_COMPLIANT if ACLs are configured for user access in Amazon S3 Buckets.

Identifier: S3_BUCKET_ACL_PROHIBITED

Resource Types: AWS::S3::Bucket

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

s3-bucket-blacklisted-actions-prohibited

Checks if an Amazon Simple Storage Service (Amazon S3) bucket policy does not allow blocklisted bucket-level and object-level actions on resources in the bucket for principals from other Amazon accounts. For example, the rule checks that the Amazon S3 bucket policy does not allow another Amazon account to perform any `s3:GetBucket*` actions and `s3:DeleteObject` on any object in the bucket. The rule is NON_COMPLIANT if any blocklisted actions are allowed by the Amazon S3 bucket policy.

> **Note**
>
> The rule will only check for entities in the Principal property and does not take into account any conditionals under the Condition property in a policy

Identifier: S3_BUCKET_BLACKLISTED_ACTIONS_PROHIBITED

Resource Types: AWS::S3::Bucket

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Hyderabad), Europe (Spain) Region

Parameters:

blacklistedActionPattern, Type: CSV

Comma-separated list of blacklisted action patterns, for example, s3:GetBucket* and s3:DeleteObject.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

s3-bucket-cross-region-replication-enabled

Checks if you have enabled S3 Cross-Region Replication for your Amazon S3 buckets. The rule is NON_COMPLIANT if there are no replication rules enabled for Cross-Region Replication.

Identifier: S3_BUCKET_CROSS_REGION_REPLICATION_ENABLED

Resource Types: AWS::S3::Bucket

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

s3-bucket-default-lock-enabled

Checks if the S3 bucket has lock enabled, by default. The rule is NON_COMPLIANT if the lock is not enabled.

Identifier: S3_BUCKET_DEFAULT_LOCK_ENABLED

Resource Types: AWS::S3::Bucket

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

mode (Optional), Type: String

mode: (optional): A mode parameter with valid values of GOVERNANCE or COMPLIANCE.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

s3-bucket-level-public-access-prohibited

Checks if S3 buckets are publicly accessible. The rule is NON_COMPLIANT if an S3 bucket is not listed in the `excludedPublicBuckets` parameter and bucket level settings are public.

Identifier: S3_BUCKET_LEVEL_PUBLIC_ACCESS_PROHIBITED

Resource Types: AWS::S3::Bucket

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

excludedPublicBuckets (Optional), Type: CSV

Comma-separated list of known allowed public Amazon S3 bucket names.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

s3-bucket-logging-enabled

Checks if logging is enabled for your S3 buckets. The rule is NON_COMPLIANT if logging is not enabled.

Identifier: S3_BUCKET_LOGGING_ENABLED

Resource Types: AWS::S3::Bucket

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

targetBucket (Optional), Type: String

Target S3 bucket for storing server access logs.

targetPrefix (Optional), Type: String

Prefix of the S3 bucket for storing server access logs.

Proactive Evaluation

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with Amazon Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
   "BucketName": "amzn-s3-demo-bucket",
   "LoggingConfiguration": {
         "DestinationBucketName": "amzn-s3-demo-destination-bucket",
         "LogFilePrefix":"my-log"
   }
}
...
```

For more information on proactive evaluation, see Evaluation Mode.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

s3-bucket-mfa-delete-enabled

Checks if MFA Delete is enabled in the Amazon Simple Storage Service (Amazon S3) bucket versioning configuration. The rule is NON_COMPLIANT if MFA Delete is not enabled.

Identifier: S3_BUCKET_MFA_DELETE_ENABLED

Resource Types: AWS::S3::Bucket

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

s3-bucket-policy-grantee-check

Checks that the access granted by the Amazon S3 bucket is restricted by any of the Amazon principals, federated users, service principals, IP addresses, or VPCs that you provide. The rule is COMPLIANT if a bucket policy is not present.

For example, if the input parameter to the rule is the list of two principals: 111122223333 and 444455556666 and the bucket policy specifies that only 111122223333 can access the bucket, then the rule is COMPLIANT. With the same input parameters: If the bucket policy specifies that 111122223333 and 444455556666 can access the bucket, it is also COMPLIANT.

However, if the bucket policy specifies that 999900009999 can access the bucket, the rule is NON_COMPLIANT.

> **Note**
>
> If a bucket policy contains more than one statement, each statement in the bucket policy is evaluated against this rule.

Identifier: S3_BUCKET_POLICY_GRANTEE_CHECK

Resource Types: AWS::S3::Bucket

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Taipei) Region

Parameters:

awsPrincipals (Optional), Type: CSV

Comma-separated list of principals such as IAM User ARNs, IAM Role ARNs, and Amazon accounts. You must provide the full ARN or use partial matching. For example, "arn:aws:iam::*AccountID*:role/*role_name*" or "arn:aws:iam::*AccountID*:role/*". If the provided value is not an exact match with the principal ARN specified in the bucket policy, the rule is NON_COMPLIANT.

servicePrincipals (Optional), Type: CSV

Comma-separated list of service principals, for example 'cloudtrail.amazonaws.com, lambda.amazonaws.com'.

federatedUsers (Optional), Type: CSV

Comma-separated list of identity providers for web identity federation such as Amazon Cognito and SAML identity providers. For example 'cognito-identity.amazonaws.com, arn:aws:iam::111122223333:saml-provider/my-provider'.

ipAddresses (Optional), Type: CSV

Comma-separated list of CIDR formatted IP addresses, for example '10.0.0.1, 192.168.1.0/24, 2001:db8::/32'.

vpcIds (Optional), Type: CSV

Comma-separated list of Amazon Virtual Private Clouds (Amazon VPC) IDs, for example 'vpc-1234abc0, vpc-ab1234c0'.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

s3-bucket-policy-not-more-permissive

Checks if your Amazon Simple Storage Service bucket policies do not allow other inter-account permissions than the control Amazon S3 bucket policy that you provide.

> **Note**
>
> If you provide an invalid parameter value, you will see the following error: Value for controlPolicy parameter must be an Amazon S3 bucket policy.

Identifier: S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE

Resource Types: AWS::S3::Bucket

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Taipei) Region

Parameters:

controlPolicy, Type: String

Amazon S3 bucket policy that defines an upper bound on the permissions of your S3 buckets. The policy can be a maximum of 1024 characters long.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

s3-bucket-public-read-prohibited

Checks if your Amazon S3 buckets do not allow public read access. The rule checks the Block Public Access settings, the bucket policy, and the bucket access control list (ACL).

The rule is compliant when both of the following are true:

- The Block Public Access setting restricts public policies or the bucket policy does not allow public read access.
- The Block Public Access setting restricts public ACLs or the bucket ACL does not allow public read access.

The rule is noncompliant when:

- If the Block Public Access setting does not restrict public policies, Amazon Config evaluates whether the policy allows public read access. If the policy allows public read access, the rule is noncompliant.
- If the Block Public Access setting does not restrict public bucket ACLs, Amazon Config evaluates whether the bucket ACL allows public read access. If the bucket ACL allows public read access, the rule is noncompliant.

> **Note**
>
> To be considered non-public, an S3 bucket policy must grant access only to fixed values. This means values that don't contain a wildcard or the following IAM policy element: Variables.

Identifier: S3_BUCKET_PUBLIC_READ_PROHIBITED

Resource Types: AWS::S3::Bucket

Trigger type: Configuration changes and Periodic

Amazon Web Services Region: All supported Amazon regions

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

s3-bucket-public-write-prohibited

Checks if your Amazon S3 buckets do not allow public write access. The rule checks the Block Public Access settings, the bucket policy, and the bucket access control list (ACL).

The rule is compliant when both of the following are true:

- The Block Public Access setting restricts public policies or the bucket policy does not allow public write access.

- The Block Public Access setting restricts public ACLs or the bucket ACL does not allow public write access.

The rule is noncompliant when:

- If the Block Public Access setting does not restrict public policies, Amazon Config evaluates whether the policy allows public write access. If the policy allows public write access, the rule is noncompliant.
- If the Block Public Access setting does not restrict public bucket ACLs, Amazon Config evaluates whether the bucket ACL allows public write access. If the bucket ACL allows public write access, the rule is noncompliant.

Note

This rule does not evaluate changes to account level public block access. To check if the required public access block settings are configured from the account level, see s3-account-level-public-access-blocks and s3-account-level-public-access-blocks-periodic.

Note

To be considered non-public, an S3 bucket policy must grant access only to fixed values. This means values that don't contain a wildcard or the following IAM policy element: Variables.

Identifier: S3_BUCKET_PUBLIC_WRITE_PROHIBITED

Resource Types: AWS::S3::Bucket

Trigger type: Configuration changes and Periodic

Amazon Web Services Region: All supported Amazon regions

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

s3-bucket-replication-enabled

Checks if S3 buckets have replication rules enabled. The rule is NON_COMPLIANT if an S3 bucket does not have a replication rule or has a replication rule that is not enabled.

Identifier: S3_BUCKET_REPLICATION_ENABLED

Resource Types: AWS::S3::Bucket

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

ReplicationType (Optional), Type: String

> Accepted values: 'CROSS-REGION' and 'SAME-REGION'. Enter 'CROSS-REGION' for the rule to check that all buckets have only Cross-Region Replication enabled. Enter 'SAME-REGION' for the rule to check that all buckets have only Same-Region Replication enabled.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

s3-bucket-server-side-encryption-enabled

Checks if your Amazon S3 bucket either has the Amazon S3 default encryption enabled or that the Amazon S3 bucket policy explicitly denies `put-object` requests without server side encryption that uses AES-256 or Amazon Key Management Service. The rule is NON_COMPLIANT if your Amazon S3 bucket is not encrypted by default.

Identifier: S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED

Resource Types: AWS::S3::Bucket

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Europe (Spain) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

s3-bucket-ssl-requests-only

Checks if S3 buckets have policies that require requests to use SSL/TLS. The rule is NON_COMPLIANT if any S3 bucket has policies allowing HTTP requests.

Identifier: S3_BUCKET_SSL_REQUESTS_ONLY

Resource Types: AWS::S3::Bucket

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

s3-bucket-versioning-enabled

Checks if versioning is enabled for your S3 buckets. Optionally, the rule checks if MFA delete is enabled for your S3 buckets.

Identifier: S3_BUCKET_VERSIONING_ENABLED

Resource Types: AWS::S3::Bucket

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

isMfaDeleteEnabled (Optional), Type: String

MFA delete is enabled for your S3 buckets.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

s3-default-encryption-kms

Checks if the S3 buckets are encrypted with Amazon Key Management Service (Amazon KMS). The rule is NON_COMPLIANT if the S3 bucket is not encrypted with an Amazon KMS key.

Identifier: S3_DEFAULT_ENCRYPTION_KMS

Resource Types: AWS::S3::Bucket, AWS::KMS::Key

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Taipei) Region

Parameters:

kmsKeyArns (Optional), Type: CSV

Comma separated list of Amazon KMS key ARNs allowed for encrypting Amazon S3 Buckets.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

s3-event-notifications-enabled

Checks if Amazon S3 Events Notifications are enabled on an S3 bucket. The rule is NON_COMPLIANT if S3 Events Notifications are not set on a bucket, or if the event type or destination do not match the `eventTypes` and destinationArn parameters.

Identifier: S3_EVENT_NOTIFICATIONS_ENABLED

Resource Types: AWS::S3::Bucket

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

destinationArn (Optional), Type: String

The Amazon Resource Name (ARN) of the destination for the event notification (Amazon SNS topic, Amazon Lambda, Amazon SQS Queue).

eventTypes (Optional), Type: CSV

Comma-separated list of the preferred Amazon S3 event types

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

s3-lifecycle-policy-check

Checks if a lifecycle rule is configured for an Amazon Simple Storage Service (Amazon S3) bucket. The rule is NON_COMPLIANT if there is no active lifecycle configuration rules or the configuration does not match with the parameter values.

Identifier: S3_LIFECYCLE_POLICY_CHECK

Resource Types: AWS::S3::Bucket

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

targetTransitionDays (Optional), Type: int

Number of days after object creation when objects are transitioned to a specified storage class (for example, 30 days).

targetExpirationDays (Optional), Type: int

Number of days after object creation when objects are deleted (for example, 395 days).

targetTransitionStorageClass (Optional), Type: String

Destination storage class type. For example, Amazon S3 Standard-Infrequent Access (S3 Standard-IA). For more information, see Understanding and managing Amazon S3 storage classes.

targetPrefix (Optional), Type: String

Amazon S3 Object prefix to identify one or more objects.

bucketNames (Optional), Type: CSV

Comma-separated list of Amazon S3 bucket names that have lifecycle policy enabled.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

s3-version-lifecycle-policy-check

Checks if Amazon Simple Storage Service (Amazon S3) version enabled buckets have lifecycle policy configured. The rule is NON_COMPLIANT if Amazon S3 lifecycle policy is not enabled.

Identifier: S3_VERSION_LIFECYCLE_POLICY_CHECK

Resource Types: AWS::S3::Bucket

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Canada West (Calgary) Region

Parameters:

bucketNames (Optional), Type: CSV

Comma-separated list of Amazon S3 bucket names that have lifecycle policy enabled.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

sagemaker-endpoint-configuration-kms-key-configured

Checks if Amazon Key Management Service (Amazon KMS) key is configured for an Amazon SageMaker endpoint configuration. The rule is NON_COMPLIANT if 'KmsKeyId' is not specified for the Amazon SageMaker endpoint configuration.

Identifier: SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED

Resource Types: AWS::SageMaker::EndpointConfig

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Asia Pacific (Taipei) Region

Parameters:

kmsKeyArns (Optional), Type: String

Comma-separated list of specific Amazon KMS key ARNs allowed for an Amazon SageMaker endpoint configuration.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

sagemaker-notebook-instance-inside-vpc

Checks if an Amazon SageMaker notebook instance is launched within a VPC or within a list of approved subnets. The rule is NON_COMPLIANT if a notebook instance is not launched within a VPC or if its subnet ID is not included in the parameter list.

Identifier: SAGEMAKER_NOTEBOOK_INSTANCE_INSIDE_VPC

Resource Types: AWS::SageMaker::NotebookInstance

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

SubnetIds (Optional), Type: CSV

Comma-separated list of subnet IDs that notebook instances can be launched in.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

sagemaker-notebook-instance-kms-key-configured

Checks if an Amazon Key Management Service (Amazon KMS) key is configured for an Amazon SageMaker notebook instance. The rule is NON_COMPLIANT if 'KmsKeyId' is not specified for the SageMaker notebook instance.

Identifier: SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED

Resource Types: AWS::SageMaker::NotebookInstance

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Asia Pacific (Taipei) Region

Parameters:

kmsKeyArns (Optional), Type: String

Comma-separated list of Amazon KMS key ARNs allowed for an Amazon SageMaker notebook instance.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

sagemaker-notebook-instance-platform-version

Checks if a Sagemaker Notebook Instance is configured to use a supported platform identifier version. The rule is NON_COMPLIANT if a Notebook Instance is not using the specified supported platform identifier version as specified in the parameter.

Identifier: SAGEMAKER_NOTEBOOK_INSTANCE_PLATFORM_VERSION

Resource Types: AWS::SageMaker::NotebookInstance

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Middle East (Bahrain), Asia Pacific (Thailand), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Canada West (Calgary) Region

Parameters:

supportedPlatformIdentifierVersions, Type: CSV

Comma-separated list of the supported platform identifier version for the rule to check.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

sagemaker-notebook-instance-root-access-check

Checks if the Amazon SageMaker RootAccess setting is enabled for Amazon SageMaker notebook instances. The rule is NON_COMPLIANT if the RootAccess setting is set to ‘Enabled’ for an Amazon SageMaker notebook instance.

Identifier: SAGEMAKER_NOTEBOOK_INSTANCE_ROOT_ACCESS_CHECK

Resource Types: AWS::SageMaker::NotebookInstance

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

sagemaker-notebook-no-direct-internet-access

Checks if direct internet access is disabled for an Amazon SageMaker notebook instance. The rule is NON_COMPLIANT if a SageMaker notebook instance is internet-enabled.

Identifier: SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS

Resource Types: AWS::SageMaker::NotebookInstance

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Asia Pacific (Taipei) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

secretsmanager-rotation-enabled-check

Checks if Amazon Secrets Manager secret has rotation enabled. The rule also checks an optional `maximumAllowedRotationFrequency` parameter. If the parameter is specified,

the rotation frequency of the secret is compared with the maximum allowed frequency. The rule is NON_COMPLIANT if the secret is not scheduled for rotation. The rule is also NON_COMPLIANT if the rotation frequency is higher than the number specified in the maximumAllowedRotationFrequency parameter.

> **Note**
>
> Re-evaluating this rule within 4 hours of the first evaluation will have no effect on the results.

Identifier: SECRETSMANAGER_ROTATION_ENABLED_CHECK

Resource Types: AWS::SecretsManager::Secret

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Mexico (Central), Asia Pacific (Taipei) Region

Parameters:

maximumAllowedRotationFrequency (Optional), Type: int

Maximum allowed rotation frequency of the secret in days.

maximumAllowedRotationFrequencyInHours (Optional), Type: int

Maximum allowed rotation frequency of the secret in hours.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

secretsmanager-scheduled-rotation-success-check

Checks if Amazon Secrets Manager secrets rotated successfully according to the rotation schedule. Secrets Manager calculates the date the rotation should happen. The rule is NON_COMPLIANT if the date passes and the secret isn't rotated.

> **Note**
>
> **Recording delays**
> Evaluation results for this rule can be delayed for up to 2 days from a missed rotation date. For more immediate monitoring, see Monitor Amazon Secrets Manager with Amazon CloudWatch in the *Secrets Manager User Guide*.
> **Secrets without rotation**
> The rule returns `NOT_APPLICABLE` for secrets that aren't configured for rotation.

Identifier: SECRETSMANAGER_SCHEDULED_ROTATION_SUCCESS_CHECK

Resource Types: AWS::SecretsManager::Secret

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Mexico (Central), Asia Pacific (Taipei) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

secretsmanager-secret-periodic-rotation

Checks if Amazon Secrets Manager secrets have been rotated in the past specified number of days. The rule is NON_COMPLIANT if a secret has not been rotated for more than maxDaysSinceRotation number of days. The default value is 90 days.

Identifier: SECRETSMANAGER_SECRET_PERIODIC_ROTATION

Resource Types: AWS::SecretsManager::Secret

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Mexico (Central), Asia Pacific (Taipei) Region

Parameters:

maxDaysSinceRotation (Optional), Type: int

Maximum number of days in which a secret can remain unchanged. The default value is 90 days.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

secretsmanager-secret-unused

Checks if Amazon Secrets Manager secrets have been accessed within a specified number of days. The rule is NON_COMPLIANT if a secret has not been accessed in 'unusedForDays' number of days. The default value is 90 days.

Context: It is recommended to routinely delete unused secrets. Unused secrets can be misused by former users who no longer need access to these secrets. Additionally, as more users gain access to a secret, it becomes increasingly possible that someone has misused a secret or has granted access to an unauthorized entity. Deleting unused secrets helps revoke secret access from users who no longer need it, and can reduce your cost of using Amazon Secrets Manager.

Identifier: SECRETSMANAGER_SECRET_UNUSED

Resource Types: AWS::SecretsManager::Secret

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Mexico (Central), Asia Pacific (Taipei) Region

Parameters:

unusedForDays (Optional), Type: int

The number of days in which a secret can remain unused. The default value is 90 days.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

secretsmanager-using-cmk

Checks if all secrets in Amazon Secrets Manager are encrypted using the Amazon managed key (`aws/secretsmanager`) or a customer managed key that was created in Amazon Key Management Service (Amazon KMS). The rule is COMPLIANT if a secret is encrypted using a customer managed key. This rule is NON_COMPLIANT if a secret is encrypted using `aws/secretsmanager`.

> **Note**
>
> This rule does not have access to cross-account customer managed keys and evaluates secrets as NON_COMPLIANT when a cross-account key is used.

Identifier: SECRETSMANAGER_USING_CMK

Resource Types: AWS::SecretsManager::Secret

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Taipei) Region

Parameters:

kmsKeyArns (Optional), Type: CSV

Comma-separated list of KMS key Amazon Resource Names (ARNs) to check if the keys are used in the encryption.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

securityhub-enabled

Checks if Amazon Security Hub is enabled for an Amazon Account. The rule is NON_COMPLIANT if Amazon Security Hub is not enabled.

Identifier: SECURITYHUB_ENABLED

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Taipei) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

security-account-information-provided

Checks if you have provided security contact information for your Amazon account contacts. The rule is NON_COMPLIANT if security contact information within the account is not provided.

Identifier: SECURITY_ACCOUNT_INFORMATION_PROVIDED

Resource Types: AWS::::Account

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

service-vpc-endpoint-enabled

Checks if Service Endpoint for the service provided in rule parameter is created for each Amazon Virtual Private Cloud (Amazon VPC). The rule is NON_COMPLIANT if an Amazon VPC doesn't have an Amazon VPC endpoint created for the service.

Identifier: SERVICE_VPC_ENDPOINT_ENABLED

Resource Types: AWS::EC2::VPC

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions

Parameters:

serviceName, Type: String

The short name or suffix for the service. Note: To get a list of available service names or valid suffix list, use DescribeVpcEndpointServices.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

sns-encrypted-kms

Checks if SNS topics are encrypted with Amazon Key Management Service (Amazon KMS). The rule is NON_COMPLIANT if an SNS topic is not encrypted with Amazon KMS. Optionally, specify the key ARNs, the alias ARNs, the alias name, or the key IDs for the rule to check.

Identifier: SNS_ENCRYPTED_KMS

Resource Types: AWS::SNS::Topic

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

kmsKeyIds (Optional), Type: CSV

Comma-separated list of Amazon KMS key Amazon Resource Names (ARNs), KMS alias ARNs, KMS alias names, or KMS key IDs for the rule to check.

Proactive Evaluation

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with Amazon Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
   "KmsMasterKeyId": "my-kms-key-Id"
}
...
```

For more information on proactive evaluation, see Evaluation Mode.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

sns-topic-message-delivery-notification-enabled

Checks if Amazon Simple Notification Service (SNS) logging is enabled for the delivery status of notification messages sent to a topic for the endpoints. The rule is NON_COMPLIANT if the delivery status notification for messages is not enabled.

Identifier: SNS_TOPIC_MESSAGE_DELIVERY_NOTIFICATION_ENABLED

Resource Types: AWS::SNS::Topic

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

sns-topic-no-public-access

Checks if the SNS topic access policy allows public access. The rule is NON_COMPLIANT if the SNS topic access policy allows public access.

> **Note**
>
> To be considered non-public, an SNS policy must grant access only to fixed values. This means values that don't contain a wildcard or the following IAM policy element: Variables.

Identifier: SNS_TOPIC_NO_PUBLIC_ACCESS

Resource Types: AWS::SNS::Topic

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

sqs-queue-no-public-access

Checks if the SQS queue access policy allows public access. The rule is NON_COMPLIANT if the SQS queue access policy allows public access.

> **Note**
>
> To be considered non-public, an SQS policy must grant access only to fixed values. This means values that don't contain a wildcard or the following IAM policy element: Variables.

Identifier: SQS_QUEUE_NO_PUBLIC_ACCESS

Resource Types: AWS::SQS::Queue

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Middle East (Bahrain), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ssm-automation-block-public-sharing

Checks if Amazon Systems Manager Automation has block public sharing enabled. The rule is NON_COMPLIANT if Systems Manager Automation has block public sharing disabled.

Identifier: SSM_AUTOMATION_BLOCK_PUBLIC_SHARING

Resource Types: AWS::::Account

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Seoul), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ssm-automation-logging-enabled

Checks if Amazon Systems Manager Automation has Amazon CloudWatch logging enabled. The rule returns NON_COMPLIANT if Systems Manager Automation doesn't have CloudWatch logging enabled.

Identifier: SSM_AUTOMATION_LOGGING_ENABLED

Resource Types: AWS::::Account

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Seoul), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

ssm-document-not-public

Checks if Amazon Systems Manager documents owned by the account are public. The rule is NON_COMPLIANT if Systems Manager documents with the owner 'Self' are public.

Identifier: SSM_DOCUMENT_NOT_PUBLIC

Resource Types: AWS::SSM::Document

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Taipei), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

step-functions-state-machine-logging-enabled

Checks if Amazon Step Functions machine has logging enabled. The rule is NON_COMPLIANT if a state machine does not have logging enabled or the logging configuration is not at the minimum level provided.

Identifier: STEP_FUNCTIONS_STATE_MACHINE_LOGGING_ENABLED

Resource Types: AWS::StepFunctions::StateMachine

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary) Region

Parameters:

cloudWatchLogGroupArns (Optional), Type: CSV

Comma-separated list of Amazon Resource Names (ARNs) for Amazon CloudWatch Logs log groups. The rule checks if the specified log groups are configured for your state machine logs.

logLevel (Optional), Type: String

The minimum log level for your state machine. Valid values include: ALL, ERROR, FATAL.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

subnet-auto-assign-public-ip-disabled

Checks if Amazon Virtual Private Cloud (Amazon VPC) subnets are assigned a public IP address. The rule is COMPLIANT if Amazon VPC does not have subnets that are assigned a public IP address. The rule is NON_COMPLIANT if Amazon VPC has subnets that are assigned a public IP address.

Identifier: SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED

Resource Types: AWS::EC2::Subnet

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

None

Proactive Evaluation

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with Amazon Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
   "MapPublicIpOnLaunch": BOOLEAN
}
...
```

For more information on proactive evaluation, see Evaluation Mode.

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

transfer-connector-logging-enabled

Checks if Amazon Transfer Family Connector publishes logs to Amazon CloudWatch. The rule is NON_COMPLIANT if a Connector does not have a LoggingRole assigned.

Identifier: TRANSFER_CONNECTOR_LOGGING_ENABLED

Resource Types: AWS::Transfer::Connector

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Middle East (Bahrain), Asia Pacific (Thailand), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

vpc-default-security-group-closed

Checks if the default security group of any Amazon Virtual Private Cloud (Amazon VPC) does not allow inbound or outbound traffic. The rule is NON_COMPLIANT if the default security group has one or more inbound or outbound traffic rules.

> **Note**
>
> There may be a delay between when Amazon Config records the deletion of related resources such as default security groups, which are deleted as part of the Amazon VPC deletion. As a result, even if all default security groups or other related resources have been deleted or remediated, the rule may report NON_COMPLIANT until the next account baselining process.

Identifier: VPC_DEFAULT_SECURITY_GROUP_CLOSED

Resource Types: AWS::EC2::SecurityGroup

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

vpc-endpoint-enabled

Checks if each service specified in the parameter has an Amazon VPC endpoint. The rule is NON_COMPLIANT if Amazon VPC does not have a VPC endpoint created for each specified service. Optionally, you can specify certain VPCs for the rule to check.

Identifier: VPC_ENDPOINT_ENABLED

Resource Types: AWS::EC2::VPC

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Osaka), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Canada West (Calgary) Region

Parameters:

serviceNames, Type: CSV

> Comma-separated list of service names or endpoints. Example: "access-analyzer, appconfig, cloudtrail" or "com.amazonaws.region.access-analyzer". Use DescribeVpcEndpointServices for available names.

vpcIds (Optional), Type: CSV

> Comma-separated list of Amazon VPC IDs for VPC endpoints. If provided, the rule is NON_COMPLIANT if the services specified in the serviceName parameter do not have one of these VPC endpoints.

scopeConfigResourceTypes (Optional), Type: CSV

Comma-separated list of Amazon Config resource types for the rule to check. If specified, the rule returns a compliance status only if at least one specified resource is recorded in the account. For example: "AWS::SNS::Topic".

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

vpc-flow-logs-enabled

Checks if Amazon Virtual Private Cloud (Amazon VPC) flow logs are found and enabled for all Amazon VPCs. The rule is NON_COMPLIANT if flow logs are not enabled for at least one Amazon VPC.

Identifier: VPC_FLOW_LOGS_ENABLED

Resource Types: AWS::EC2::VPC

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions

Parameters:

trafficType (Optional), Type: String

TrafficType of flow logs

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

vpc-network-acl-unused-check

Checks if there are unused network access control lists (network ACLs). The rule is COMPLIANT if each network ACL is associated with a subnet. The rule is NON_COMPLIANT if a network ACL is not associated with a subnet.

Identifier: VPC_NETWORK_ACL_UNUSED_CHECK

Resource Types: AWS::EC2::NetworkAcl

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

vpc-sg-open-only-to-authorized-ports

Checks if security groups allowing unrestricted incoming traffic ('0.0.0.0/0' or '::/0') only allow inbound TCP or UDP connections on authorized ports. The rule is NON_COMPLIANT if such security groups do not have ports specified in the rule parameters.

> **Note**
>
> This rule evaluates Amazon EC2 security groups with ingress rule set to IPv4='0.0.0.0/0' or IPv6='::/'. If the security group does not have one of those destinations, this rule returns `NOT_APPLICABLE`.

Identifier: VPC_SG_OPEN_ONLY_TO_AUTHORIZED_PORTS

Resource Types: AWS::EC2::SecurityGroup

Trigger type: Configuration changes and Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Melbourne) Region

Parameters:

authorizedTcpPorts (Optional), Type: String

Comma-separated list of TCP ports authorized to be open to 0.0.0.0/0 or ::/0. Ranges are defined by dash, for example, "443,1020-1025".

authorizedUdpPorts (Optional), Type: String

Comma-separated list of UDP ports authorized to be open to 0.0.0.0/0 or ::/0. Ranges are defined by dash, for example, "500,1020-1025".

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

wafv2-logging-enabled

Checks if logging is enabled on Amazon WAFv2 regional and global web access control lists (web ACLs). The rule is NON_COMPLIANT if the logging is enabled but the logging destination does not match the value of the parameter.

> **Note**
>
> **Amazon Security Lake Exception**
> This rule does not check logging done with Security Lake for Amazon WAFV2 web ACLs.

Identifier: WAFV2_LOGGING_ENABLED

Resource Types: AWS::WAFv2::WebACL

Trigger type: Periodic

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Mexico (Central), Asia Pacific (Taipei) Region

Parameters:

KinesisFirehoseDeliveryStreamArns (Optional), Type: CSV

Comma separated list of Kinesis Firehose delivery stream ARNs

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

wafv2-rulegroup-logging-enabled

Checks if Amazon CloudWatch security metrics collection on Amazon WAFv2 rule groups is enabled. The rule is NON_COMPLIANT if the 'VisibilityConfig.CloudWatchMetricsEnabled' field is set to false.

Context: Amazon WAFV2 (Web Application Firewall version 2) allows you to create Amazon WAF rules to protect your web applications from common web exploits and vulnerabilities. An Amazon WAF rule group is a collection of Amazon WAF rules that you can associate with a web ACL (Access Control List) to define the desired behavior for your web application traffic. For more information, see Amazon WAF rules and Rule groups in the *Amazon WAF Developer Guide*.

By configuring CloudWatch security metrics collection on Amazon WAFV2 rules group, you can monitor security metrics such as successful or failed Distributed denial of service (DDoS), SQL injection, and Cross-site scripting (XSS) attacks. The security metrics collected can help you simplify your investigations.

> **Note**
>
> If there are no Amazon WAF rules in the Amazon WAFV2 rule group for the Amazon Config managed rule to check, the Amazon Config managed rule returns `NOT_APPLICABLE`.

Identifier: WAFV2_RULEGROUP_LOGGING_ENABLED

Resource Types: AWS::WAFv2::RuleGroup

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

wafv2-webacl-not-empty

Checks if a WAFv2 Web ACL contains any WAF rules or WAF rule groups. This rule is NON_COMPLIANT if a Web ACL does not contain any WAF rules or WAF rule groups.

Identifier: WAFV2_WEBACL_NOT_EMPTY

Resource Types: AWS::WAFv2::WebACL

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

waf-regional-rule-not-empty

Checks whether WAF regional rule contains conditions. This rule is COMPLIANT if the regional rule contains at least one condition and NON_COMPLIANT otherwise.

Identifier: WAF_REGIONAL_RULE_NOT_EMPTY

Resource Types: AWS::WAFRegional::Rule

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

waf-regional-webacl-not-empty

Checks if a WAF regional Web ACL contains any WAF rules or rule groups. The rule is NON_COMPLIANT if there are no WAF rules or rule groups present within a Web ACL.

Identifier: WAF_REGIONAL_WEBACL_NOT_EMPTY

Resource Types: AWS::WAFRegional::WebACL

Trigger type: Configuration changes

Amazon Web Services Region: All supported Amazon regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Amazon GovCloud (US-East), Amazon GovCloud (US-West), Mexico (Central), Canada West (Calgary) Region

Parameters:

None

Amazon CloudFormation template

To create Amazon Config managed rules with Amazon CloudFormation templates, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.

List of Amazon Config Managed Rules by Evaluation Mode

Amazon Config currently supports the following managed rules. Before using these rules, see Considerations.

Proactive Evaluation

Proactive rules are rules that support the proactive evaluation mode for resources that have not been deployed. This allows you to evaluate whether a set of resource properties, if used to define an Amazon resource, would be COMPLIANT or NON_COMPLIANT given the set of proactive rules that you have in your account in your Region. For more information, see Evaluation modes.

> **Note**
>
> Proactive rules do not remediate resources that are flagged as NON_COMPLIANT or prevent them from being deployed.

Proactive Evaluation

- api-gw-xray-enabled
- autoscaling-group-elb-healthcheck-required
- ec2-instance-multiple-eni-check
- eip-attached
- elasticsearch-node-to-node-encryption-check
- lambda-function-settings-check
- lambda-inside-vpc
- rds-automatic-minor-version-upgrade-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-public-access-check
- rds-multi-az-support
- rds-storage-encrypted
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- s3-bucket-logging-enabled
- sns-encrypted-kms
- subnet-auto-assign-public-ip-disabled

Detective Evaluation

Detective rules are rules that support the detective evaluation mode for resource that have already been deployed. This allows you to evaluate the configuration settings of your existing resources.

> **Note**
>
> Currently, all Amazon Config rules support detective evaluation.

Detective Evaluation

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf

- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged

- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-at-rest
- appsync-cache-ct-encryption-in-transit
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required

- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled

- cloudfront-origin-failover-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-s3-origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-ssl-policy-check
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check

- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged

- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check

- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged

- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version

- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled

- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit

- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest

- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-oidc-provider-tagged
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-saml-provider-tagged
- iam-server-certificate-expiration-check
- iam-server-certificate-tagged
- iam-user-group-membership-check
- iam-user-mfa-enabled

- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged

- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled

- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled

- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target

- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access

- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-query-logging-enabled
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled

- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled

- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed

- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-empty
- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

List of Amazon Config Managed Rules by Trigger Type

Amazon Config currently supports the following managed rules. Before using these rules, see Considerations.

Configuration Changes

Change-triggered rules are rules that Amazon Config evaluates in response to configuration changes.

Configuration Changes

- acmpca-certificate-authority-tagged

- acm-certificate-rsa-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description

- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-authorization-check
- appsync-cache-ct-encryption-at-rest
- appsync-cache-ct-encryption-in-transit
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description

- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-mysql-backtracking-enabled
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-notification-check

- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-ssl-policy-check
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-settings-check
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegurureviewer-repository-association-tagged

- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-pitr-enabled

- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- ebs-optimized-instance
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-dhcp-options-tagged
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair

- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-security-group-attached-to-eni
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check

- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-filesystem-ct-encrypted
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-supported-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- evidently-launch-description

- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-oidc-provider-tagged
- iam-policy-blacklisted-check
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-saml-provider-tagged
- iam-server-certificate-tagged

- iam-user-group-membership-check
- iam-user-no-policies-check
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check

- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited

- netfw-deletion-protection-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled

- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-multi-az-support
- rds-postgresql-logs-to-cloudwatch
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- required-tags
- route53-query-logging-enabled
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only

- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check

- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-using-cmk
- service-catalog-shared-within-organization
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-closed
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-global-rulegroup-not-empty
- waf-global-rule-not-empty
- waf-global-webacl-not-empty

- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

Periodic

Periodic rules are rules that Amazon Config evaluates periodicially at a frequency that you specify; for example, every 24 hours.

Periodic

- access-keys-rotated
- account-part-of-organizations
- acm-pca-root-ca-disabled
- alb-http-to-https-redirection-check
- api-gwv2-authorization-type-configured
- appsync-associated-with-waf
- appsync-cache-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- cloudfront-s3-origin-non-existent-bucket
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled

- cloudwatch-alarm-resource-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- dms-replication-not-public
- docdb-cluster-encrypted-in-transit
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-resources-protected-by-backup-plan
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-last-backup-recovery-point-created
- ec2-meets-restore-time-target
- ec2-resources-in-logically-air-gapped-vault

- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ecr-private-image-scanning-enabled
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eks-cluster-logging-enabled
- eks-cluster-secrets-encrypted
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elbv2-acm-certificate-required
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip

- event-data-store-cmk-encryption-enabled
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-enabled
- iam-password-policy
- iam-policy-in-use
- iam-root-access-key-check
- iam-server-certificate-expiration-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled

- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- kinesis-firehose-delivery-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-automatic-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-no-public-access
- multi-region-cloud-trail-enabled
- netfw-logging-enabled
- nlb-logging-enabled
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-mysql-instance-encrypted-in-transit
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-sqlserver-encrypted-in-transit
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access

- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-account-level-public-access-blocks-periodic
- s3-last-backup-recovery-point-created
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created

- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-sg-port-restriction-check
- wafv2-logging-enabled
- waf-classic-logging-enabled

Hybrid

Hybrid rules are rules that Amazon Config evaluates both in response to configuration changes and periodicially.

Hybrid

- acm-certificate-expiration-check
- cloudformation-stack-drift-detection-check
- ec2-instance-launched-with-allowed-ami
- incoming-ssh-disabled
- no-unrestricted-route-to-igw
- restricted-incoming-traffic
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- vpc-sg-open-only-to-authorized-ports

List of Amazon Config Managed Rules by Region Availability

Amazon Config currently supports the following managed rules. Before using these rules, see Considerations.

US East (Ohio) Region

US East (Ohio)

- access-keys-rotated

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description

- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest

- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled

- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled

- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled

- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged

- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair

- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit

- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled

- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description

- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled

- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled

- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access

- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets

- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled

- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az

- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive

- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access

- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged

- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

US East (N. Virginia) Region

US East (N. Virginia)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version

- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description

- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-at-rest
- appsync-cache-ct-encryption-in-transit
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description

- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template

- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-s3-origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-ssl-policy-check
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check

- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged

- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created

- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached

- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged

- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible

- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit

- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged

- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions

- iam-no-inline-policy-check
- iam-oidc-provider-tagged
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-saml-provider-tagged
- iam-server-certificate-expiration-check
- iam-server-certificate-tagged
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged

- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check

- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled

- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest

- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check

- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-query-logging-enabled
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled

- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled

- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled

- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-empty
- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty

- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

US West (N. California) Region

US West (N. California)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check

- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf

- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed

- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check

- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled

- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled

- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance

- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity

- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest

- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups

- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check

- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check

- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled

- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled

- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check

- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive

- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access

- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged

- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

US West (Oregon) Region

US West (Oregon)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version

- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description

- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description

- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged

- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled

- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled

- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged

- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check

- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration

- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit

- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled

- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled

- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled

- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check

- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp

- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check

- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan

- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled

- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged

- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled

- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled

- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

Africa (Cape Town) Region

Africa (Cape Town)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled

- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check

- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged

- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check

- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan

- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created

- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged

- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access

- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access

- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled

- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted

- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled

- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled

- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled

- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive

- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check

- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description

- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

Asia Pacific (Hong Kong) Region

Asia Pacific (Hong Kong)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled

- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage

- appconfig-hosted-configuration-version-description
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault

- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging

- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached

- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled

- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required

- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled

- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version

- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check

- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled

- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iot-authorizer-token-signing-enabled

- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check

- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only

- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption

- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-no-public-access
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only

- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured

- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created

- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty

- waf-regional-webacl-not-empty

Asia Pacific (Hyderabad) Region

Asia Pacific (Hyderabad)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-extension-association-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description

- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check

- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type

- dms-replication-not-public
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami

- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled

- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only

- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glue-job-logging-enabled

- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-enabled
- iam-password-policy
- iam-root-access-key-check
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check

- mariadb-publish-logs-to-cloudwatch-logs
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan

- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled

- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version

- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-access
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check

- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Asia Pacific (Jakarta) Region

Asia Pacific (Jakarta)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged

- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration

- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging

- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-report-group-encrypted-at-rest
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled

- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted

- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity

- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch

- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled

- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc

- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled

- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled

- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check

- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-no-public-access
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled

- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled

- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up

- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Asia Pacific (Malaysia) Region

Asia Pacific (Malaysia)

- account-part-of-organizations
- acm-certificate-expiration-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-mysql-backtracking-enabled
- autoscaling-group-elb-healthcheck-required
- autoscaling-launch-config-public-ip-disabled
- cloudformation-stack-drift-detection-check
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted

- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check

- ec2-managedinstance-platform-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-user-for-host-mode-check
- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-password-policy
- incoming-ssh-disabled

- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled
- no-unrestricted-route-to-igw
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- required-tags

- restricted-incoming-traffic
- s3-account-level-public-access-blocks-periodic
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up

- wafv2-logging-enabled

Asia Pacific (Melbourne) Region

Asia Pacific (Melbourne)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage

- appconfig-hosted-configuration-version-description
- approved-amis-by-id
- approved-amis-by-tag
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging

- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled

- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created

- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration

- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled

- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-deployment-type-check
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled

- guardduty-s3-protection-enabled
- iam-external-access-analyzer-enabled
- iam-password-policy
- iam-root-access-key-check
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mariadb-publish-logs-to-cloudwatch-logs
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-log-enabled
- msk-cluster-public-access-disabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check

- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target

- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks

- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk

- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-access
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty

- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Asia Pacific (Mumbai) Region

Asia Pacific (Mumbai)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled

- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled

- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted

- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled

- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type

- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance

- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged

- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version

- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled

- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit

- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled

- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged

- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iot-authorizer-token-signing-enabled
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access

- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets

- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled

- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az

- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive

- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access

- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged

- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

Asia Pacific (Osaka) Region

Asia Pacific (Osaka)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled

- active-mq-supported-version
- alb-desync-mode-check
- alb-internal-scheme-check
- alb-listener-tagged
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding

- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing

- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check

- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type

- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-tagged
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged

- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description

- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached

- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-cross-zone-load-balancing-enabled
- elb-logging-enabled
- emr-block-public-access
- emr-kerberos-enabled
- emr-security-configuration-encryption-rest

- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled

- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check

- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted

- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch

- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled

- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive

- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access

- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged

- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Asia Pacific (Seoul) Region

Asia Pacific (Seoul)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check

- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged

- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging

- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check

- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged

- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan

- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached

- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled

- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault

- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check

- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled

- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check

- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iot-authorizer-token-signing-enabled
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check

- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted

- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch

- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled

- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled

- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc

- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged

- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

Asia Pacific (Singapore) Region

Asia Pacific (Singapore)

- access-keys-rotated

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description

- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf

- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed

- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check

- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy

- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target

- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target

- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access

- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled

- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip

- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled

- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check

- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check

- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled

- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version

- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit

- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks

- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count

- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault

- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

Asia Pacific (Sydney) Region

Asia Pacific (Sydney)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled

- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc

- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types

- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled

- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled

- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled

- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged

- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled

- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled

- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check

- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check

- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access

- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged

- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode

- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled

- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit

- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit

- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created

- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms

- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check

- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

Asia Pacific (Taipei) Region

Asia Pacific (Taipei)

- acm-certificate-expiration-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-mysql-backtracking-enabled
- cloudformation-stack-drift-detection-check
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled

- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-encryption-enabled
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-stopped-instance
- eip-attached
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- encrypted-volumes
- incoming-ssh-disabled
- instances-in-vpc
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled

- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- required-tags
- restricted-incoming-traffic
- s3-account-level-public-access-blocks-periodic
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed

- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up

Asia Pacific (Thailand) Region

Asia Pacific (Thailand)

- account-part-of-organizations
- acm-certificate-expiration-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-mysql-backtracking-enabled
- autoscaling-group-elb-healthcheck-required
- autoscaling-launch-config-public-ip-disabled
- cloudformation-stack-drift-detection-check
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted

- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check

- ec2-managedinstance-platform-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-task-definition-user-for-host-mode-check
- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check

- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled
- no-unrestricted-route-to-igw
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- required-tags
- restricted-incoming-traffic
- s3-account-level-public-access-blocks-periodic
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited

- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up

Asia Pacific (Tokyo) Region

Asia Pacific (Tokyo)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check

- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged

- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description

- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template

- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check

- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged

- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check

- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged

- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets

- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest

- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes

- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled

- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only

- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled

- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled

- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled

- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch

- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks

- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count

- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault

- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

Canada (Central) Region

Canada (Central)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled

- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag

- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check

- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled

- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check

- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault

- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged

- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version

- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled

- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit

- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled

- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged

- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled

- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled

- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled

- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch

- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled

- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled

- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check

- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

Canada West (Calgary) Region

Canada West (Calgary)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled

- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- approved-amis-by-id
- approved-amis-by-tag
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- autoscaling-group-elb-healthcheck-required
- autoscaling-launch-config-public-ip-disabled
- batch-scheduling-policy-tagged
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cognito-user-pool-tagged
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type

- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-prefix-list-tagged
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-multicast-domain-tagged
- ecr-repository-tagged
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-user-for-host-mode-check
- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check

- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- incoming-ssh-disabled
- instances-in-vpc
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled
- nlb-internal-scheme-check
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled

- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- required-tags
- restricted-incoming-traffic
- s3-account-level-public-access-blocks-periodic
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled

- s3-default-encryption-kms
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-tagged
- subnet-auto-assign-public-ip-disabled
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

China (Beijing) Region

China (Beijing)

- access-keys-rotated

- acm-certificate-expiration-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- athena-workgroup-logging-enabled
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check

- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudfront-s3-origin-non-existent-bucket
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-logging-enabled
- dax-encryption-enabled
- db-instance-backup-enabled
- desired-instance-tenancy

- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-encrypted-in-transit
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check

- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-paravirtual-instance-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted

- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-ontap-deployment-type-check
- fsx-openzfs-deployment-type-check

- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited

- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-update-check
- rabbit-mq-supported-version
- rds-automatic-minor-version-upgrade-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit

- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled

- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms

- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- transfer-connector-logging-enabled
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

China (Ningxia) Region

China (Ningxia)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check

- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- athena-workgroup-logging-enabled
- aurora-mysql-backtracking-enabled
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check

- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-logging-enabled
- dax-encryption-enabled
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured

- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required

- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-security-group-attached-to-eni
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check

- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-ontap-deployment-type-check
- fsx-openzfs-deployment-type-check
- glue-job-logging-enabled
- glue-spark-job-supported-version

- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-enhanced-monitoring-enabled

- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- no-unrestricted-route-to-igw
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-logging-enabled

- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic

- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk

- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- transfer-connector-logging-enabled
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

Europe (Frankfurt) Region

Europe (Frankfurt)

- access-keys-rotated

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description

- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf

- appsync-authorization-check
- appsync-cache-ct-encryption-at-rest
- appsync-cache-ct-encryption-in-transit
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check

- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled

- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption

- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan

- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted

- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged

- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access

- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only

- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled

- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled

- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted

- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls

- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required

- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit

- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic

- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check

- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled

- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled

- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

Europe (Ireland) Region

Europe (Ireland)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured

- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged

- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled

- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check

- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled

- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled

- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged

- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled

- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled

- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled

- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target

- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use

- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged

- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled

- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled

- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check

- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl

- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled

- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused

- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created

- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

Europe (London) Region

Europe (London)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check

- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged

- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration

- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged

- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update

- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public

- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged

- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan

- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check

- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description

- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check

- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions

- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check

- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check

- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance

- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted

- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks

- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured

- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created

- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty

- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

Europe (Milan) Region

Europe (Milan)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled

- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest

- appsync-logging-enabled
- athena-data-catalog-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template

- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest

- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted

- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm

- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled

- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled

- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check

- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled

- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled

- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls

- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled

- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check

- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited

- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation

- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created

- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Europe (Paris) Region

Europe (Paris)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check

- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding

- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target

- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check

- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check

- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited

- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm

- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description

- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target

- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required

- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured

- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled

- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode

- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated

- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled

- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check

- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled

- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation

- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created

- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Europe (Spain) Region

Europe (Spain)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-waf-enabled

- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-extension-association-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az

- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled

- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault

- ebs-resources-protected-by-backup-plan
- ec2-capacity-reservation-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled

- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access

- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elbv2-multiple-az
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created

- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-enabled
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted

- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mariadb-publish-logs-to-cloudwatch-logs
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled

- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled

- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged

- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-access
- ssm-document-not-public
- ssm-document-tagged

- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Europe (Stockholm) Region

Europe (Stockholm)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check

- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged

- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target

- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check

- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check

- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled

- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required

- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled

- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version

- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check

- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled

- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check

- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs

- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty

- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled

- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled

- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled

- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation

- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created

- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Europe (Zurich) Region

Europe (Zurich)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-waf-enabled

- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-extension-association-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template

- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled

- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance

- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-traffic-mirror-filter-description

- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created

- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elbv2-multiple-az
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest

- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-enabled

- iam-password-policy
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mariadb-publish-logs-to-cloudwatch-logs
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty

- netfw-subnet-change-protection-enabled
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshot-encrypted

- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic

- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check

- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-access
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up

- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Israel (Tel Aviv) Region

Israel (Tel Aviv)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description

- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-mysql-cluster-audit-logging
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template

- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- custom-eventbus-policy-attached

- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required

- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-prefix-list-tagged
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-in-backup-plan
- efs-mount-target-public-accessible
- eip-attached
- eks-cluster-secrets-encrypted
- eks-endpoint-no-public-access
- eks-secrets-encrypted

- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elbv2-multiple-az
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-windows-deployment-type-check
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled

- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- macie-auto-sensitive-data-discovery-check
- mariadb-publish-logs-to-cloudwatch-logs
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted

- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-multi-az-support

- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-no-public-access
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled

- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused

- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-access
- ssm-document-not-public
- ssm-document-tagged
- subnet-auto-assign-public-ip-disabled
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Mexico (Central) Region

Mexico (Central)

- account-part-of-organizations

- acm-certificate-expiration-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-mysql-backtracking-enabled
- autoscaling-group-elb-healthcheck-required
- autoscaling-launch-config-public-ip-disabled
- cloudformation-stack-drift-detection-check
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-encrypted-kms

- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-task-definition-user-for-host-mode-check
- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch

- elasticsearch-node-to-node-encryption-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled
- no-unrestricted-route-to-igw
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled

- rds-instance-public-access-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- required-tags
- restricted-incoming-traffic
- s3-account-level-public-access-blocks-periodic
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- secretsmanager-using-cmk
- securityhub-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed

- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up

Middle East (Bahrain) Region

Middle East (Bahrain)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted

- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf

- appsync-authorization-check
- appsync-cache-ct-encryption-at-rest
- appsync-cache-ct-encryption-in-transit
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed

- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check

- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged

- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check

- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged

- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan

- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elb-acm-certificate-required

- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- glb-listener-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled

- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted

- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled

- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version

- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check

- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited

- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation

- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan

- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Middle East (UAE) Region

Middle East (UAE)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-waf

- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-extension-association-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check

- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check

- codebuild-report-group-encrypted-at-rest
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created

- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged

- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access

- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan

- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-enabled
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited

- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mariadb-publish-logs-to-cloudwatch-logs
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated

- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption

- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-no-public-access
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited

- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check

- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-access
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled

- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

South America (São Paulo) Region

South America (São Paulo)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged

- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged

- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-at-rest
- appsync-cache-ct-encryption-in-transit
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types

- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled

- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled

- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created

- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check

- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged

- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check

- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled

- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled

- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged

- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled

- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest

- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit

- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-no-public-access
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic

- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check

- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled

- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled

- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

Amazon GovCloud (US-East) Region

Amazon GovCloud (US-East)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-mysql-cluster-audit-logging
- aurora-resources-protected-by-backup-plan

- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-public-ip-disabled
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled

- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- cw-loggroup-retention-period-check
- datasync-task-logging-enabled
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- docdb-cluster-encrypted-in-transit
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled

- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-user-identity

- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-mount-target-public-accessible
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elbv2-listener-encryption-in-transit
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes

- event-data-store-cmk-encryption-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-ontap-deployment-type-check
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-deployment-type-check
- glue-job-logging-enabled
- glue-spark-job-supported-version
- guardduty-eks-protection-audit-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-non-archived-findings
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check

- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-cloudwatch-audit-log-enabled
- msk-cluster-public-access-disabled
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-primary-node-fault-tolerance

- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled

- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled

- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-connector-logging-enabled
- transfer-family-server-no-ftp

- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

Amazon GovCloud (US-West) Region

Amazon GovCloud (US-West)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- athena-workgroup-logging-enabled

- aurora-last-backup-recovery-point-created
- aurora-mysql-cluster-audit-logging
- aurora-resources-protected-by-backup-plan
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-public-ip-disabled
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled

- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- cognito-identity-pool-unauth-access-check
- connect-instance-logging-enabled
- cw-loggroup-retention-period-check
- datasync-task-logging-enabled
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- docdb-cluster-encrypted-in-transit
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-optimized-instance

- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access

- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-mount-target-public-accessible
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elbv2-listener-encryption-in-transit
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled

- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-ontap-deployment-type-check
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-deployment-type-check
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-eks-protection-audit-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-non-archived-findings
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access

- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-server-certificate-expiration-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-cloudwatch-audit-log-enabled
- msk-cluster-public-access-disabled
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled

- nacl-no-unrestricted-ssh-rdp
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited

- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled

- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-automation-block-public-sharing

- ssm-automation-logging-enabled
- ssm-document-not-public
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-connector-logging-enabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

Creating Amazon Config Managed Rules With Amazon CloudFormation Templates

> **Important**
>
> You must first create and start the Amazon Config configuration recorder in order to create Amazon Config managed rules with Amazon CloudFormation. For more information, see Managing the Configuration Recorder.

For supported Amazon Config managed rules, you can use the Amazon CloudFormation templates to create the rule for your account or update an existing Amazon CloudFormation stack. A stack is

a collection of related resources that you provision and update as a single unit. When you launch a stack with a template, the Amazon Config managed rule is created for you. The templates create only the rule, and don't create additional Amazon resources.

> **Note**
>
> When Amazon Config managed rules are updated, the templates are updated for the latest changes. To save a specific version of a template for a rule, download the template, and upload it to your S3 bucket.

For more information about working with Amazon CloudFormation templates, see Getting Started with Amazon CloudFormation in the *Amazon CloudFormation User Guide*.

To launch an Amazon CloudFormation stack for an Amazon Config managed rule

1. Go to the CloudFormation console and create a new stack.
2. For **Specify template**:
   - If you downloaded the template, choose **Upload a template file**, and then **Choose file** to upload the template.
   - You can also choose **Amazon S3 URL**, and enter the template URL `http://s3.amazonaws.com/aws-configservice-us-east-1/cloudformation-templates-for-managed-rules/THE_RULE_IDENTIFIER.template`.

   > **Note**
   >
   > The rule identifier should be written in ALL_CAPS_WITH_UNDERSCORES. For example, CLOUDWATCH_LOG_GROUP_ENCRYPTED instead of cloudwatch-log-group-encrypted. For some rules, the rule identifier is different from the rule name. Make sure to use the rule identifier. For example, the rule identifier for restricted-ssh is INCOMING_SSH_DISABLED.
3. Choose **Next**.
4. For **Specify stack details**, type a stack name and enter parameter values for the Amazon Config rule. For example, if you are using the `DESIRED_INSTANCE_TYPE` managed rule template, you can specify the instance type such as "m4.large".

5. Choose **Next**.
6. For **Options**, you can create tags or configure other advanced options. These are not required.
7. Choose **Next**.
8. For **Review**, verify that the template, parameters, and other options are correct.
9. Choose **Create**. The stack is created in a few minutes. You can view the created rule in the Amazon Config console.

You can use the templates to create a single stack for Amazon Config managed rules or update an existing stack in your account. If you delete a stack, the managed rules created from that stack are also deleted. For more information, see Working with Stacks in the *Amazon CloudFormation User Guide*.

Amazon Config Custom Rules

Amazon Config Custom Rules are rules that you create from scratch. There are two ways to create Amazon Config custom rules: with Lambda functions (Amazon Lambda Developer Guide) and with Guard (Guard GitHub Repository), a policy-as-code language.

Amazon Config custom rules created with Lambda are called *Amazon Config Custom Lambda Rules* and Amazon Config custom rules created with Guard are called *Amazon Config Custom Policy Rules*.

Before using custom rules, see Considerations.

Amazon Config Custom Policy Rules

Rules written using Guard can be created from the Amazon Config console or by using the Amazon Config rule APIs. Amazon Config Custom Policy rules allow you to create Amazon Config Custom rules without needing to use Java or Python to develop Lambda functions to manage your custom rules. Amazon Config Custom Policy rules are initiated by configuration changes. For more information about Guard, see the Guard GitHub Repository.

Amazon Config Custom Lambda Rules

Custom Lambda rules provide you with the option to use Java or Python to create a Lambda function for a Amazon Config Custom rule. A *Lambda function* is custom code that you upload to Amazon Lambda, and it is invoked by events that are published to it by an event source. If the Lambda function is associated with an Amazon Config rule, Amazon Config invokes it when the

rule is initiated. The Lambda function then evaluates the configuration information that is sent by Amazon Config, and it returns the evaluation results. For more information about Lambda functions, see Function and Event Sources in the *Amazon Lambda Developer Guide*.

Format differences for Amazon Config Custom Rules

The following table displays the format differences in the fields for the ConfigurationItem data type and for Amazon Config Custom Rules.

ConfigurationItem	Amazon Config Custom Rule
`version`	`configurationItemVersion`
`accountId`	`awsAccountId`
`arn`	`ARN`
`configurationItemMD5Hash`	`configurationStateMd5Hash`

Topics

- Creating Amazon Config Custom Policy Rules
- Creating Amazon Config Custom Lambda Rules
- Managing Deleted Resources for Amazon Config Custom Lambda Rules

Creating Amazon Config Custom Policy Rules

You can create Amazon Config Custom Policy rules from the Amazon Web Services Management Console, Amazon CLI, or Amazon Config API.

Adding Amazon Config Custom Policy rules

Using the console

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. In the Amazon Web Services Management Console menu, verify that the Region selector is set to an Amazon Region that supports Amazon Config rules. For the list of supported

Regions, see Amazon Config Regions and Endpoints in the *Amazon Web Services General Reference*.

3. In the left navigation, choose **Rules**.
4. On the **Rules** page, choose **Add rule**.
5. On the **Specify rule type** page, choose **Create custom rule using Guard**.
6. On the **Configure rule** page, create your rule by completing the following steps:

   a. For **Rule name**, type a unique name for the rule.

   b. For **Description**, type a description for the rule.

   c. For **Guard runtime version**, choose the runtime system for your Amazon Config Custom Policy rule.

   d. For **Rule Content**, you can populate it with the Guard Custom policy for your rule.

   e. For **Evaluation mode**, choose when in the resource creation and management process you want Amazon Config to evaluate your resources. Depending on the rule, Amazon Config can evaluate your resource configurations before a resource has been provisioned, after a resource has been provisoned, or both.

      i. Choose **Turn on proactive evaluation** to allow you to run evaluations on the configuration settings of your resources before they are deployed.

      After you have turned on proactive evaluation, you can use the StartResourceEvaluation API and GetResourceEvaluationSummary API to check if the resources you specify in these commands would be flagged as NON_COMPLIANT by the proactive rules in your account in your Region.

      For more information on using this commands, see Evaluating Your Resources with Amazon Config Rules. For a list of managed rules that support proactive evaluation, see List of Amazon Config Managed Rules by Evaluation Mode.

      ii. Choose **Turn on detective evaluation** to evaluate the configuration settings of your existing resources.

      For detective evaluation, Amazon Config Custom Policy rules are initiated by **Configuration changes**. This option will be pre-selected.

      - **Resources** – When a resource that matches the specified resource type, or the type plus identifier, is created, changed, or deleted.

- **Tags** – When a resource with the specified tag is created, changed, or deleted.
- **All changes** – When a resource recorded by Amazon Config is created, changed, or deleted.

Amazon Config runs the evaluation when it detects a change to a resource that matches the rule's scope. You can use the scope to constrain which resources initiate evaluations. Otherwise, evaluations are initiated when there is a change to a post-provisioned resource.

f. For **Parameters**, you can customize the values for the provided keys if your rule includes parameters. A parameter is an attribute that your resources must adhere to before they are considered compliant with the rule.

7. On the **Review and create** page, review all your selections before adding the rule to your Amazon Web Services account.
8. When you finish reviewing your rules, choose **Add rule**.

Using the Amazon CLI

Use the `put-config-rule` command.

The `Owner` field should be `CUSTOM_POLICY`. The following additional fields are required for Amazon Config Custom Policy rules:

- `Runtime`: The runtime system for your Amazon Config Custom Policy rules.
- `PolicyText`: The policy definition containing the logic for your Amazon Config Custom Policy rules.
- `EnableDebugLogDelivery`: The Boolean expression for enabling debug logging for your Amazon Config Custom Policy rule. The default value is `false`.

Using the API Reference

Use the PutConfigRule action.

The `Owner` field should be `CUSTOM_POLICY`. The following additional fields are required for Amazon Config Custom Policy rules:

- `Runtime`: The runtime system for your Amazon Config Custom Policy rules.

- `PolicyText`: The policy definition containing the logic for your Amazon Config Custom Policy rules.
- `EnableDebugLogDelivery`: The Boolean expression for enabling debug logging for your Amazon Config Custom Policy rule. The default value is `false`.

Writing rule content for Amazon Config Custom Policy rules

With Amazon Config Custom Policy rules, you can use Amazon CloudFormation Guard's domain-specific language (DSL) to evaluate resource configurations. This topic provides patterns and best practices for writing custom policy rules.

For more information on how to write rules with Guard, see Writing Guard rules in the Amazon CloudFormation Guard User Guide and Amazon CloudFormation Guard 2.0's Modes of Operation in the Guard GitHub Repository.

Basic rule structure

Use the following basic format to create rules:

```
# Basic rule format
rule <rule_name> when
    resourceType == "<AWS::Service::Resource>" {
    # Evaluation clauses
}

# Example with filtering
let resources_of_type = Resources.*[ Type == 'AWS::Service::Resource' ]
rule check_resources when %resources_of_type !empty {
    %resources_of_type.configuration.property == expected_value
}
```

Key components

configuration

Contains the contents for the resource configuration.

supplementaryConfiguration

Contains additional contents for the resource configuration. Amazon Config returns this field for certain resource types to supplement the information returned for the configuration field.

resourceType

Amazon resource type being evaluated.

resourceId

The ID of the resource (for example, `sg-xxxxxx`).

accountId

The 12-digit Amazon Web Services account ID associated with the resource.

Common patterns

Status checks

```
let allowed_status = ['ACTIVE', 'RUNNING']
rule check_resource_status when
    resourceType == "AWS::Service::Resource" {
    configuration.status IN %allowed_status
}
```

Required properties

```
rule check_required_properties when
    resourceType == "AWS::Service::Resource" {
    configuration.propertyName exists
    configuration.propertyName is_string  # or is_list, is_struct
}
```

Query blocks

```
configuration.Properties {
    property1 exists
    property2 is_string
    property3 IN [allowed_value1, allowed_value2]
}
```

Conditional evaluation

```
when configuration.feature_enabled == true {
    configuration.feature_settings exists
    configuration.feature_settings is_struct
```

```
}
```

Custom messages

```
rule check_compliance when
    resourceType == "AWS::Service::Resource" {
    configuration.property == expected_value <<Custom error message explaining the
 requirement>>
}}
```

Advanced features

Range checks

```
rule check_numeric_limits {
    # Inclusive range (lower_limit <= value <= upper_limit)
    configuration.value IN r[minimum_value, maximum_value]

    # Exclusive range (lower_limit < value < upper_limit)
    configuration.value IN r(exclusive_min, exclusive_max)

    # Left inclusive, right exclusive (lower_limit <= value < upper_limit)
    configuration.value IN r[minimum_value, exclusive_max)

    # Left exclusive, right inclusive (lower_limit < value <= upper_limit)
    configuration.value IN r(exclusive_min, maximum_value]
}
```

Combining conditions

```
# AND conditions (implicit through new lines)
condition_1
condition_2

# OR conditions (explicit)
condition_3 OR
condition_4
```

Chaining rules

```
rule check_prerequisites {
```

```
    configuration.required_setting exists
}

rule check_details when check_prerequisites {
    configuration.required_setting == expected_value
}
```

Best practices

- Use variables with `let` statements for improved readability.
- Group related checks using named rule blocks.
- Include descriptive comments.
- Use appropriate operators (`exists`, `is_string`, `is_list`).
- Use regex patterns with case-insensitive matching.

Example: dynamodb-pitr-enabled

The following example shows the policy definition for an Amazon Config Custom Policy rule version of the Amazon Config Managed rule dynamodb-pitr-enabled. This rule checks if DynamoDB tables have Point-in-Time Recovery enabled.

```
# Check if DynamoDB tables have Point-in-Time Recovery enabled
let status = ['ACTIVE']

rule tableisactive when
    resourceType == "AWS::DynamoDB::Table" {
    configuration.tableStatus == %status
}

rule checkcompliance when
    resourceType == "AWS::DynamoDB::Table"
    tableisactive {
    let pitr =
 supplementaryConfiguration.ContinuousBackupsDescription.pointInTimeRecoveryDescription.pointIn
    %pitr == "ENABLED" <<DynamoDB tables must have Point-in-Time Recovery enabled>>
}
```

Creating Amazon Config Custom Lambda Rules

You can develop custom rules and add them to Amazon Config with Amazon Lambda functions.

You associate each custom rule with an Lambda function, which contains the logic that evaluates whether your Amazon resources comply with the rule. You associate this function with your rule, and the rule invokes the function either in response to configuration changes or periodically. The function then evaluates whether your resources comply with your rule, and sends its evaluation results to Amazon Config.

Amazon Rule Development Kit (RDK)

The Amazon Rule Development Kit (RDK) is designed to support a "Compliance-as-Code" workflow that is intuitive and productive. It abstracts away much of the undifferentiated heavy lifting associated with deploying Amazon Config rules backed by custom Lambda functions, and provides a streamlined develop-deploy-monitor iterative process.

For step-by-step instruction, see the Amazon Rule Development Kit (RDK) Documentation.

Example Amazon Lambda Functions for Amazon Config Rules (Node.js)

Amazon Lambda executes functions in response to events that are published by Amazon services. The function for an Amazon Config Custom Lambda rule receives an event that is published by Amazon Config, and the function then uses data that it receives from the event and that it retrieves from the Amazon Config API to evaluate the compliance of the rule. The operations in a function for a Config rule differ depending on whether it performs an evaluation that is triggered by configuration changes or triggered periodically.

For information about common patterns within Amazon Lambda functions, see Programming Model in the *Amazon Lambda Developer Guide*.

Example Function for Evaluations Triggered by Configuration Changes

Amazon Config will invoke a function like the following example when it detects a configuration change for a resource that is within a custom rule's scope.

If you use the Amazon Config console to create a rule that is associated with a function like this example, choose **Configuration changes** as the trigger type. If you use the Amazon Config API or Amazon CLI to create the rule, set the `MessageType` attribute to `ConfigurationItemChangeNotification` and

`OversizedConfigurationItemChangeNotification`. These settings enable your rule to be triggered whenever Amazon Config generates a configuration item or an oversized configuration item as a result of a resource change.

This example evaluates your resources and checks whether the instances match the resource type, `AWS::EC2::Instance`. The rule is triggered when Amazon Config generates a configuration item or an oversized configuration item notification.

```
'use strict';

import { ConfigServiceClient, GetResourceConfigHistoryCommand,
 PutEvaluationsCommand } from "@aws-sdk/client-config-service";

const configClient = new ConfigServiceClient({});

// Helper function used to validate input
function checkDefined(reference, referenceName) {
    if (!reference) {
        throw new Error(`Error: ${referenceName} is not defined`);
    }
    return reference;
}

// Check whether the message type is OversizedConfigurationItemChangeNotification,
function isOverSizedChangeNotification(messageType) {
    checkDefined(messageType, 'messageType');
    return messageType === 'OversizedConfigurationItemChangeNotification';
}

// Get the configurationItem for the resource using the getResourceConfigHistory
 API.
async function getConfiguration(resourceType, resourceId, configurationCaptureTime,
 callback) {
    const input = { resourceType, resourceId, laterTime: new
 Date(configurationCaptureTime), limit: 1 };
    const command = new GetResourceConfigHistoryCommand(input);
    await configClient.send(command).then(
        (data) => {
            callback(null, data.configurationItems[0]);
        },
        (error) => {
            callback(error, null);
        }
```

```
    );

}

// Convert the oversized configuration item from the API model to the original
 invocation model.
function convertApiConfiguration(apiConfiguration) {
    apiConfiguration.awsAccountId = apiConfiguration.accountId;
    apiConfiguration.ARN = apiConfiguration.arn;
    apiConfiguration.configurationStateMd5Hash =
 apiConfiguration.configurationItemMD5Hash;
    apiConfiguration.configurationItemVersion = apiConfiguration.version;
    apiConfiguration.configuration = JSON.parse(apiConfiguration.configuration);
    if ({}.hasOwnProperty.call(apiConfiguration, 'relationships')) {
        for (let i = 0; i < apiConfiguration.relationships.length; i++) {
            apiConfiguration.relationships[i].name =
 apiConfiguration.relationships[i].relationshipName;
        }
    }
    return apiConfiguration;
}

// Based on the message type, get the configuration item either from the
 configurationItem object in the invoking event or with the getResourceConfigHistory
 API in the getConfiguration function.
async function getConfigurationItem(invokingEvent, callback) {
    checkDefined(invokingEvent, 'invokingEvent');
    if (isOverSizedChangeNotification(invokingEvent.messageType)) {
        const configurationItemSummary =
 checkDefined(invokingEvent.configurationItemSummary, 'configurationItemSummary');
        await getConfiguration(configurationItemSummary.resourceType,
 configurationItemSummary.resourceId,
 configurationItemSummary.configurationItemCaptureTime, (err, apiConfigurationItem)
 => {
            if (err) {
                callback(err);
            }
            const configurationItem = convertApiConfiguration(apiConfigurationItem);
            callback(null, configurationItem);
        });
    } else {
        checkDefined(invokingEvent.configurationItem, 'configurationItem');
        callback(null, invokingEvent.configurationItem);
    }
```

```
}

// Check whether the resource has been deleted. If the resource was deleted, then
 the evaluation returns not applicable.
function isApplicable(configurationItem, event) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(event, 'event');
    const status = configurationItem.configurationItemStatus;
    const eventLeftScope = event.eventLeftScope;
    return (status === 'OK' || status === 'ResourceDiscovered') && eventLeftScope
 === false;
}

// In this example, the resource is compliant if it is an instance and its type
 matches the type specified as the desired type.
// If the resource is not an instance, then this resource is not applicable.
function evaluateChangeNotificationCompliance(configurationItem, ruleParameters) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(configurationItem.configuration,
 'configurationItem.configuration');
    checkDefined(ruleParameters, 'ruleParameters');

    if (configurationItem.resourceType !== 'AWS::EC2::Instance') {
        return 'NOT_APPLICABLE';
    } else if (ruleParameters.desiredInstanceType ===
 configurationItem.configuration.instanceType) {
        return 'COMPLIANT';
    }
    return 'NON_COMPLIANT';
}

// Receives the event and context from AWS Lambda.
export const handler = async (event, context) => {
    checkDefined(event, 'event');
    const invokingEvent = JSON.parse(event.invokingEvent);
    const ruleParameters = JSON.parse(event.ruleParameters);
    await getConfigurationItem(invokingEvent, async (err, configurationItem) => {

        let compliance = 'NOT_APPLICABLE';
        let annotation = '';
        const putEvaluationsRequest = {};
        if (isApplicable(configurationItem, event)) {
            // Invoke the compliance checking function.
```

```
            compliance = evaluateChangeNotificationCompliance(configurationItem,
 ruleParameters);
            if (compliance === "NON_COMPLIANT") {
                annotation = "This is an annotation describing why the resource is
 not compliant.";
            }
        }
        // Initializes the request that contains the evaluation results.
        if (annotation) {
            putEvaluationsRequest.Evaluations = [
                {
                    ComplianceResourceType: configurationItem.resourceType,
                    ComplianceResourceId: configurationItem.resourceId,
                    ComplianceType: compliance,
                    OrderingTimestamp: new
 Date(configurationItem.configurationItemCaptureTime),
                    Annotation: annotation
                },
            ];
        } else {
            putEvaluationsRequest.Evaluations = [
                {
                    ComplianceResourceType: configurationItem.resourceType,
                    ComplianceResourceId: configurationItem.resourceId,
                    ComplianceType: compliance,
                    OrderingTimestamp: new
 Date(configurationItem.configurationItemCaptureTime),
                },
            ];
        }
        putEvaluationsRequest.ResultToken = event.resultToken;

        // Sends the evaluation results to AWS Config.
        await configClient.send(new PutEvaluationsCommand(putEvaluationsRequest));
    });
};
```

Function Operations

The function performs the following operations at runtime:

1. The function runs when Amazon Lambda passes the `event` object to the `handler` function. In this example, the function accepts the optional `callback` parameter, which it uses to

return information to the caller. Amazon Lambda also passes a `context` object, which contains information and methods that the function can use while it runs. Note that in newer versions of Lambda, context is no longer used.

2. The function checks whether the `messageType` for the event is a configuration item or an oversized configuration item, and then returns the configuration item.
3. The handler calls the `isApplicable` function to determine whether the resource was deleted.

   > **Note**
   >
   > Rules reporting on deleted resources should return the evaluation result of `NOT_APPLICABLE` in order to avoid unnecessary rule evaluations.

4. The handler calls the `evaluateChangeNotificationCompliance` function and passes the `configurationItem` and `ruleParameters` objects that Amazon Config published in the event.

   The function first evaluates whether the resource is an EC2 instance. If the resource is not an EC2 instance, the function returns a compliance value of `NOT_APPLICABLE`.

   The function then evaluates whether the `instanceType` attribute in the configuration item is equal to the `desiredInstanceType` parameter value. If the values are equal, the function returns `COMPLIANT`. If the values are not equal, the function returns `NON_COMPLIANT`.
5. The handler prepares to send the evaluation results to Amazon Config by initializing the `putEvaluationsRequest` object. This object includes the `Evaluations` parameter, which identifies the compliance result, the resource type, and the ID of the resource that was evaluated. The `putEvaluationsRequest` object also includes the result token from the event, which identifies the rule and the event for Amazon Config.
6. The handler sends the evaluation results to Amazon Config by passing the object to the `putEvaluations` method of the `config` client.

Example Function for Periodic Evaluations

Amazon Config will invoke a function like the following example for periodic evaluations. Periodic evaluations occur at the frequency that you specify when you define the rule in Amazon Config.

If you use the Amazon Config console to create a rule that is associated with a function like this example, choose **Periodic** as the trigger type. If you use the Amazon Config API or Amazon CLI to create the rule, set the `MessageType` attribute to `ScheduledNotification`.

This example checks whether the total number of a specified resource exceeds a specified maximum.

```
'use strict';
import { ConfigServiceClient, ListDiscoveredResourcesCommand,
 PutEvaluationsCommand } from "@aws-sdk/client-config-service";

const configClient = new ConfigServiceClient({});

// Receives the event and context from AWS Lambda.
export const handler = async (event, context, callback) => {
    // Parses the invokingEvent and ruleParameters values, which contain JSON
 objects passed as strings.
    var invokingEvent = JSON.parse(event.invokingEvent),
        ruleParameters = JSON.parse(event.ruleParameters),
        numberOfResources = 0;

    if (isScheduledNotification(invokingEvent) &&
 hasValidRuleParameters(ruleParameters, callback)) {
        await countResourceTypes(ruleParameters.applicableResourceType, "",
 numberOfResources, async function (err, count) {
            if (err === null) {
                var putEvaluationsRequest;
                const compliance = evaluateCompliance(ruleParameters.maxCount,
 count);
                var annotation = '';
                if (compliance === "NON_COMPLIANT") {
                    annotation = "Description of why the resource is not
 compliant.";
                }
                // Initializes the request that contains the evaluation results.
                if (annotation) {
                    putEvaluationsRequest = {
                        Evaluations: [{
                            // Applies the evaluation result to the AWS account
 published in the event.
                            ComplianceResourceType: 'AWS::::Account',
                            ComplianceResourceId: event.accountId,
                            ComplianceType: compliance,
```

```
                            OrderingTimestamp: new Date(),
                            Annotation: annotation
                        }],
                        ResultToken: event.resultToken
                    };
                } else {
                    putEvaluationsRequest = {
                        Evaluations: [{
                            // Applies the evaluation result to the AWS account
 published in the event.
                            ComplianceResourceType: 'AWS::::Account',
                            ComplianceResourceId: event.accountId,
                            ComplianceType: compliance,
                            OrderingTimestamp: new Date()
                        }],
                        ResultToken: event.resultToken
                    };
                }

                // Sends the evaluation results to AWS Config.
                try {
                    await configClient.send(new
 PutEvaluationsCommand(putEvaluationsRequest));
                }
                catch (e) {
                    callback(e, null);
                }
            } else {
                callback(err, null);
            }
        });
    } else {
        console.log("Invoked for a notification other than Scheduled Notification...
 Ignoring.");
    }
};

// Checks whether the invoking event is ScheduledNotification.
function isScheduledNotification(invokingEvent) {
    return (invokingEvent.messageType === 'ScheduledNotification');
}

// Checks the rule parameters to see if they are valid
function hasValidRuleParameters(ruleParameters, callback) {
```

```
    // Regular express to verify that applicable resource given is a resource type
    const awsResourcePattern = /^AWS::(\w*)::(\w*)$/;
    const isApplicableResourceType =
 awsResourcePattern.test(ruleParameters.applicableResourceType);
    // Check to make sure the maxCount in the parameters is an integer
    const maxCountIsInt = !isNaN(ruleParameters.maxCount) &&
 parseInt(Number(ruleParameters.maxCount)) == ruleParameters.maxCount && !
isNaN(parseInt(ruleParameters.maxCount, 10));
    if (!isApplicableResourceType) {
        callback("The applicableResourceType parameter is not a valid resource
 type.", null);
    }
    if (!maxCountIsInt) {
        callback("The maxCount parameter is not a valid integer.", null);
    }
    return isApplicableResourceType && maxCountIsInt;
}

// Checks whether the compliance conditions for the rule are violated.
function evaluateCompliance(maxCount, actualCount) {
    if (actualCount > maxCount) {
        return "NON_COMPLIANT";
    } else {
        return "COMPLIANT";
    }
}

// Counts the applicable resources that belong to the AWS account.
async function countResourceTypes(applicableResourceType, nextToken, count,
 callback) {
    const input = { resourceType: applicableResourceType, nextToken: nextToken };
    const command = new ListDiscoveredResourcesCommand(input);
    try {
        const response = await configClient.send(command);
        count = count + response.resourceIdentifiers.length;
        if (response.nextToken !== undefined && response.nextToken != null) {
            countResourceTypes(applicableResourceType, response.nextToken, count,
 callback);
        }
        callback(null, count);
    } catch (e) {
        callback(e, null);
    }
    return count;
```

```
}
```

Function Operations

The function performs the following operations at runtime:

1. The function runs when Amazon Lambda passes the `event` object to the `handler` function. In this example, the function accepts the optional `callback` parameter, which it uses to return information to the caller. Amazon Lambda also passes a `context` object, which contains information and methods that the function can use while it runs. Note that in newer versions of Lambda, context is no longer used.
2. To count the resources of the specified type, the handler calls the `countResourceTypes` function, and it passes the `applicableResourceType` parameter that it received from the event. The `countResourceTypes` function calls the `listDiscoveredResources` method of the `config` client, which returns a list of identifiers for the applicable resources. The function uses the length of this list to determine the number of applicable resources, and it returns this count to the handler.
3. The handler prepares to send the evaluation results to Amazon Config by initializing the `putEvaluationsRequest` object. This object includes the `Evaluations` parameter, which identifies the compliance result and the Amazon Web Services account that was published in the event. You can use the `Evaluations` parameter to apply the result to any resource type that is supported by Amazon Config. The `putEvaluationsRequest` object also includes the result token from the event, which identifies the rule and the event for Amazon Config.
4. Within the `putEvaluationsRequest` object, the handler calls the `evaluateCompliance` function. This function tests whether the number of applicable resources exceeds the maximum assigned to the `maxCount` parameter, which was provided by the event. If the number of resources exceeds the maximum, the function returns `NON_COMPLIANT`. If the number of resources does not exceed the maximum, the function returns `COMPLIANT`.
5. The handler sends the evaluation results to Amazon Config by passing the object to the `putEvaluations` method of the `config` client.

Example Amazon Lambda Functions for Amazon Config Rules (Python)

Amazon Lambda executes functions in response to events that are published by Amazon services. The function for an Amazon Config Custom Lambda rule receives an event that is published by Amazon Config, and the function then uses data that it receives from the event and that it retrieves from the Amazon Config API to evaluate the compliance of the rule. The operations in a

function for a Config rule differ depending on whether it performs an evaluation that is triggered by configuration changes or triggered periodically.

For information about common patterns within Amazon Lambda functions, see Programming Model in the *Amazon Lambda Developer Guide*.

Example Function for Evaluations Triggered by Configuration Changes

Amazon Config will invoke a function like the following example when it detects a configuration change for a resource that is within a custom rule's scope.

If you use the Amazon Config console to create a rule that is associated with a function like this example, choose **Configuration changes** as the trigger type. If you use the Amazon Config API or Amazon CLI to create the rule, set the `MessageType` attribute to `ConfigurationItemChangeNotification` and `OversizedConfigurationItemChangeNotification`. These settings enable your rule to be triggered whenever Amazon Config generates a configuration item or an oversized configuration item as a result of a resource change.

```
import botocore
import boto3
import json
import datetime

# Set to True to get the lambda to assume the Role attached on the Config Service
 (useful for cross-account).
ASSUME_ROLE_MODE = False

# This gets the client after assuming the Config service role
# either in the same AWS account or cross-account.
def get_client(service, event):
    """Return the service boto client. It should be used instead of directly calling
 the client.
    Keyword arguments:
    service -- the service name used for calling the boto.client()
    event -- the event variable given in the lambda handler
    """
    if not ASSUME_ROLE_MODE:
        return boto3.client(service)
    credentials = get_assume_role_credentials(event["executionRoleArn"])
    return boto3.client(service, aws_access_key_id=credentials['AccessKeyId'],
                        aws_secret_access_key=credentials['SecretAccessKey'],
```

```
                        aws_session_token=credentials['SessionToken']
                       )

# Helper function used to validate input
def check_defined(reference, reference_name):
    if not reference:
        raise Exception('Error: ', reference_name, 'is not defined')
    return reference

# Check whether the message is OversizedConfigurationItemChangeNotification or not
def is_oversized_changed_notification(message_type):
    check_defined(message_type, 'messageType')
    return message_type == 'OversizedConfigurationItemChangeNotification'

# Get configurationItem using getResourceConfigHistory API
# in case of OversizedConfigurationItemChangeNotification
def get_configuration(resource_type, resource_id, configuration_capture_time):
    result = AWS_CONFIG_CLIENT.get_resource_config_history(
        resourceType=resource_type,
        resourceId=resource_id,
        laterTime=configuration_capture_time,
        limit=1)
    configurationItem = result['configurationItems'][0]
    return convert_api_configuration(configurationItem)

# Convert from the API model to the original invocation model
def convert_api_configuration(configurationItem):
    for k, v in configurationItem.items():
        if isinstance(v, datetime.datetime):
            configurationItem[k] = str(v)
    configurationItem['awsAccountId'] = configurationItem['accountId']
    configurationItem['ARN'] = configurationItem['arn']
    configurationItem['configurationStateMd5Hash'] =
 configurationItem['configurationItemMD5Hash']
    configurationItem['configurationItemVersion'] = configurationItem['version']
    configurationItem['configuration'] =
 json.loads(configurationItem['configuration'])
    if 'relationships' in configurationItem:
        for i in range(len(configurationItem['relationships'])):
            configurationItem['relationships'][i]['name'] =
 configurationItem['relationships'][i]['relationshipName']
    return configurationItem

# Based on the type of message get the configuration item
```

```
# either from configurationItem in the invoking event
# or using the getResourceConfigHistory API in getConfiguration function.
def get_configuration_item(invokingEvent):
    check_defined(invokingEvent, 'invokingEvent')
    if is_oversized_changed_notification(invokingEvent['messageType']):
        configurationItemSummary =
 check_defined(invokingEvent['configurationItemSummary'],
 'configurationItemSummary')
        return get_configuration(configurationItemSummary['resourceType'],
 configurationItemSummary['resourceId'],
 configurationItemSummary['configurationItemCaptureTime'])
    return check_defined(invokingEvent['configurationItem'], 'configurationItem')

# Check whether the resource has been deleted. If it has, then the evaluation is
 unnecessary.
def is_applicable(configurationItem, event):
    try:
        check_defined(configurationItem, 'configurationItem')
        check_defined(event, 'event')
    except:
        return True
    status = configurationItem['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']
    if status == 'ResourceDeleted':
        print("Resource Deleted, setting Compliance Status to NOT_APPLICABLE.")
    return (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope

def get_assume_role_credentials(role_arn):
    sts_client = boto3.client('sts')
    try:
        assume_role_response = sts_client.assume_role(RoleArn=role_arn,
 RoleSessionName="configLambdaExecution")
        return assume_role_response['Credentials']
    except botocore.exceptions.ClientError as ex:
        # Scrub error message for any internal account info leaks
        if 'AccessDenied' in ex.response['Error']['Code']:
            ex.response['Error']['Message'] = "AWS Config does not have permission
 to assume the IAM role."
        else:
            ex.response['Error']['Message'] = "InternalError"
            ex.response['Error']['Code'] = "InternalError"
        raise ex

def evaluate_change_notification_compliance(configuration_item, rule_parameters):
```

```
    check_defined(configuration_item, 'configuration_item')
    check_defined(configuration_item['configuration'],
 'configuration_item[\'configuration\']')
    if rule_parameters:
        check_defined(rule_parameters, 'rule_parameters')

    if (configuration_item['resourceType'] != 'AWS::EC2::Instance'):
        return 'NOT_APPLICABLE'

    elif rule_parameters.get('desiredInstanceType'):
        if (configuration_item['configuration']['instanceType'] in
 rule_parameters['desiredInstanceType']):
            return 'COMPLIANT'
    return 'NON_COMPLIANT'

def lambda_handler(event, context):

    global AWS_CONFIG_CLIENT

    check_defined(event, 'event')
    invoking_event = json.loads(event['invokingEvent'])
    rule_parameters = {}
    if 'ruleParameters' in event:
        rule_parameters = json.loads(event['ruleParameters'])

    compliance_value = 'NOT_APPLICABLE'

    AWS_CONFIG_CLIENT = get_client('config', event)
    configuration_item = get_configuration_item(invoking_event)
    if is_applicable(configuration_item, event):
        compliance_value = evaluate_change_notification_compliance(
                configuration_item, rule_parameters)

    response = AWS_CONFIG_CLIENT.put_evaluations(
       Evaluations=[
           {
               'ComplianceResourceType': invoking_event['configurationItem']
['resourceType'],
               'ComplianceResourceId': invoking_event['configurationItem']
['resourceId'],
               'ComplianceType': compliance_value,
               'OrderingTimestamp': invoking_event['configurationItem']
['configurationItemCaptureTime']
           },
```

```
        ],
        ResultToken=event['resultToken'])
```

Function Operations

The function performs the following operations at runtime:

1. The function runs when Amazon Lambda passes the `event` object to the `handler` function. In this example, the function accepts the optional `callback` parameter, which it uses to return information to the caller. Amazon Lambda also passes a `context` object, which contains information and methods that the function can use while it runs. Note that in newer versions of Lambda, context is no longer used.
2. The function checks whether the `messageType` for the event is a configuration item or an oversized configuration item, and then returns the configuration item.
3. The handler calls the `isApplicable` function to determine whether the resource was deleted.

   > **Note**
   >
   > Rules reporting on deleted resources should return the evaluation result of `NOT_APPLICABLE` in order to avoid unnecessary rule evaluations.

4. The handler calls the `evaluateChangeNotificationCompliance` function and passes the `configurationItem` and `ruleParameters` objects that Amazon Config published in the event.

   The function first evaluates whether the resource is an EC2 instance. If the resource is not an EC2 instance, the function returns a compliance value of `NOT_APPLICABLE`.

   The function then evaluates whether the `instanceType` attribute in the configuration item is equal to the `desiredInstanceType` parameter value. If the values are equal, the function returns `COMPLIANT`. If the values are not equal, the function returns `NON_COMPLIANT`.
5. The handler prepares to send the evaluation results to Amazon Config by initializing the `putEvaluationsRequest` object. This object includes the `Evaluations` parameter, which identifies the compliance result, the resource type, and the ID of the resource that was evaluated. The `putEvaluationsRequest` object also includes the result token from the event, which identifies the rule and the event for Amazon Config.

6. The handler sends the evaluation results to Amazon Config by passing the object to the `putEvaluations` method of the `config` client.

Example Function for Periodic Evaluations

Amazon Config will invoke a function like the following example for periodic evaluations. Periodic evaluations occur at the frequency that you specify when you define the rule in Amazon Config.

If you use the Amazon Config console to create a rule that is associated with a function like this example, choose **Periodic** as the trigger type. If you use the Amazon Config API or Amazon CLI to create the rule, set the `MessageType` attribute to `ScheduledNotification`.

```
import botocore
import boto3
import json
import datetime

# Set to True to get the lambda to assume the Role attached on the Config Service
 (useful for cross-account).
ASSUME_ROLE_MODE = False
DEFAULT_RESOURCE_TYPE = 'AWS::::Account'

# This gets the client after assuming the Config service role
# either in the same AWS account or cross-account.
def get_client(service, event):
    """Return the service boto client. It should be used instead of directly calling
 the client.
    Keyword arguments:
    service -- the service name used for calling the boto.client()
    event -- the event variable given in the lambda handler
    """
    if not ASSUME_ROLE_MODE:
        return boto3.client(service)
    credentials = get_assume_role_credentials(event["executionRoleArn"])
    return boto3.client(service, aws_access_key_id=credentials['AccessKeyId'],
                        aws_secret_access_key=credentials['SecretAccessKey'],
                        aws_session_token=credentials['SessionToken']
                       )

def get_assume_role_credentials(role_arn):
    sts_client = boto3.client('sts')
```

```
    try:
        assume_role_response = sts_client.assume_role(RoleArn=role_arn,
 RoleSessionName="configLambdaExecution")
        return assume_role_response['Credentials']
    except botocore.exceptions.ClientError as ex:
        # Scrub error message for any internal account info leaks
        if 'AccessDenied' in ex.response['Error']['Code']:
            ex.response['Error']['Message'] = "AWS Config does not have permission
 to assume the IAM role."
        else:
            ex.response['Error']['Message'] = "InternalError"
            ex.response['Error']['Code'] = "InternalError"
        raise ex

# Check whether the message is a ScheduledNotification or not.
def is_scheduled_notification(message_type):
    return message_type == 'ScheduledNotification'

def count_resource_types(applicable_resource_type, next_token, count):
    resource_identifier =
 AWS_CONFIG_CLIENT.list_discovered_resources(resourceType=applicable_resource_type,
 nextToken=next_token)
    updated = count + len(resource_identifier['resourceIdentifiers']);
    return updated

# Evaluates the configuration items in the snapshot and returns the compliance value
 to the handler.
def evaluate_compliance(max_count, actual_count):
    return 'NON_COMPLIANT' if int(actual_count) > int(max_count) else 'COMPLIANT'

def evaluate_parameters(rule_parameters):
    if 'applicableResourceType' not in rule_parameters:
        raise ValueError('The parameter with "applicableResourceType" as key must be
 defined.')
    if not rule_parameters['applicableResourceType']:
        raise ValueError('The parameter "applicableResourceType" must have a defined
 value.')
    return rule_parameters

# This generate an evaluation for config
def build_evaluation(resource_id, compliance_type, event,
 resource_type=DEFAULT_RESOURCE_TYPE, annotation=None):
    """Form an evaluation as a dictionary. Usually suited to report on scheduled
 rules.
```

```
    Keyword arguments:
    resource_id -- the unique id of the resource to report
    compliance_type -- either COMPLIANT, NON_COMPLIANT or NOT_APPLICABLE
    event -- the event variable given in the lambda handler
    resource_type -- the CloudFormation resource type (or AWS::::Account) to report
 on the rule (default DEFAULT_RESOURCE_TYPE)
    annotation -- an annotation to be added to the evaluation (default None)
    """
    eval_cc = {}
    if annotation:
        eval_cc['Annotation'] = annotation
    eval_cc['ComplianceResourceType'] = resource_type
    eval_cc['ComplianceResourceId'] = resource_id
    eval_cc['ComplianceType'] = compliance_type
    eval_cc['OrderingTimestamp'] = str(json.loads(event['invokingEvent'])
['notificationCreationTime'])
    return eval_cc

def lambda_handler(event, context):

    global AWS_CONFIG_CLIENT

    evaluations = []
    rule_parameters = {}
    resource_count = 0
    max_count = 0

    invoking_event = json.loads(event['invokingEvent'])
    if 'ruleParameters' in event:
        rule_parameters = json.loads(event['ruleParameters'])
        valid_rule_parameters = evaluate_parameters(rule_parameters)

    compliance_value = 'NOT_APPLICABLE'

    AWS_CONFIG_CLIENT = get_client('config', event)
    if is_scheduled_notification(invoking_event['messageType']):
        result_resource_count =
 count_resource_types(valid_rule_parameters['applicableResourceType'], '',
 resource_count)

    if valid_rule_parameters.get('maxCount'):
        max_count = valid_rule_parameters['maxCount']

    compliance_value = evaluate_compliance(max_count, result_resource_count)
```

```
    evaluations.append(build_evaluation(event['accountId'], compliance_value, event,
resource_type=DEFAULT_RESOURCE_TYPE))
    response = AWS_CONFIG_CLIENT.put_evaluations(Evaluations=evaluations,
ResultToken=event['resultToken'])
```

Function Operations

The function performs the following operations at runtime:

1. The function runs when Amazon Lambda passes the `event` object to the `handler` function. In this example, the function accepts the optional `callback` parameter, which it uses to return information to the caller. Amazon Lambda also passes a `context` object, which contains information and methods that the function can use while it runs. Note that in newer versions of Lambda, context is no longer used.
2. To count the resources of the specified type, the handler calls the `countResourceTypes` function, and it passes the `applicableResourceType` parameter that it received from the event. The `countResourceTypes` function calls the `listDiscoveredResources` method of the `config` client, which returns a list of identifiers for the applicable resources. The function uses the length of this list to determine the number of applicable resources, and it returns this count to the handler.
3. The handler prepares to send the evaluation results to Amazon Config by initializing the `putEvaluationsRequest` object. This object includes the `Evaluations` parameter, which identifies the compliance result and the Amazon Web Services account that was published in the event. You can use the `Evaluations` parameter to apply the result to any resource type that is supported by Amazon Config. The `putEvaluationsRequest` object also includes the result token from the event, which identifies the rule and the event for Amazon Config.
4. Within the `putEvaluationsRequest` object, the handler calls the `evaluateCompliance` function. This function tests whether the number of applicable resources exceeds the maximum assigned to the `maxCount` parameter, which was provided by the event. If the number of resources exceeds the maximum, the function returns `NON_COMPLIANT`. If the number of resources does not exceed the maximum, the function returns `COMPLIANT`.
5. The handler sends the evaluation results to Amazon Config by passing the object to the `putEvaluations` method of the `config` client.

Example Events for Amazon Config Rules

When the trigger for a rule occurs, Amazon Config invokes the rule's Amazon Lambda function by publishing an event. Then Amazon Lambda executes the function by passing the event to the function's handler.

Example Event for Evaluations Triggered by Configuration Changes

Amazon Config publishes an event when it detects a configuration change for a resource that is within a rule's scope. The following example event shows that the rule was triggered by a configuration change for an EC2 instance.

```
{
    "invokingEvent": "{\"configurationItem\":{\"configurationItemCaptureTime
\":\"2016-02-17T01:36:34.043Z\",\"awsAccountId\":\"123456789012\",
\"configurationItemStatus\":\"OK\",\"resourceId\":\"i-00000000\",\"ARN
\":\"arn:aws:ec2:us-east-2:123456789012:instance/i-00000000\",\"awsRegion
\":\"us-east-2\",\"availabilityZone\":\"us-east-2a\",\"resourceType\":
\"AWS::EC2::Instance\",\"tags\":{\"Foo\":\"Bar\"},\"relationships\":[{\"resourceId
\":\"eipalloc-00000000\",\"resourceType\":\"AWS::EC2::EIP\",\"name\":\"Is
 attached to ElasticIp\"}],\"configuration\":{\"foo\":\"bar\"}},\"messageType\":
\"ConfigurationItemChangeNotification\"}",
    "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
    "resultToken": "myResultToken",
    "eventLeftScope": false,
    "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
    "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-0123456",
    "configRuleName": "change-triggered-config-rule",
    "configRuleId": "config-rule-0123456",
    "accountId": "123456789012",
    "version": "1.0"
}
```

Example Event for Evaluations Triggered by Oversized Configuration Changes

Some resource changes generate oversized configuration items. The following example event shows that the rule was triggered by an oversized configuration change for an EC2 instance.

```
{
        "invokingEvent": "{\"configurationItemSummary\": {\"changeType\":
 \"UPDATE\",\"configurationItemVersion\": \"1.2\",\"configurationItemCaptureTime
```

```
\":\"2016-10-06T16:46:16.261Z\",\"configurationStateId\": 0,\"awsAccountId
\":\"123456789012\",\"configurationItemStatus\": \"OK\",\"resourceType
\": \"AWS::EC2::Instance\",\"resourceId\":\"i-00000000\",\"resourceName
\":null,\"ARN\":\"arn:aws:ec2:us-west-2:123456789012:instance/i-00000000\",
\"awsRegion\": \"us-west-2\",\"availabilityZone\":\"us-west-2a\",
\"configurationStateMd5Hash\":\"8f1ee69b287895a0f8bc5753eca68e96\",
\"resourceCreationTime\":\"2016-10-06T16:46:10.489Z\"},\"messageType\":
\"OversizedConfigurationItemChangeNotification\"}",
        "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
        "resultToken": "myResultToken",
        "eventLeftScope": false,
        "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
        "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-ec2-managed-instance-inventory",
        "configRuleName": "change-triggered-config-rule",
        "configRuleId": "config-rule-0123456",
        "accountId": "123456789012",
        "version": "1.0"
    }
```

Example Event for Evaluations Triggered by Periodic Frequency

Amazon Config publishes an event when it evaluates your resources at a frequency that you specify (such as every 24 hours). The following example event shows that the rule was triggered by a periodic frequency.

```
{
    "invokingEvent": "{\"awsAccountId\":\"123456789012\",\"notificationCreationTime
\":\"2016-07-13T21:50:00.373Z\",\"messageType\":\"ScheduledNotification\",
\"recordVersion\":\"1.0\"}",
    "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
    "resultToken": "myResultToken",
    "eventLeftScope": false,
    "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
    "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-0123456",
    "configRuleName": "periodic-config-rule",
    "configRuleId": "config-rule-6543210",
    "accountId": "123456789012",
    "version": "1.0"
}
```

Event Attributes

The JSON object for an Amazon Config event contains the following attributes:

`invokingEvent`

The event that triggers the evaluation for a rule. If the event is published in response to a resource configuration change, the value for this attribute is a string that contains a JSON `configurationItem` or a `configurationItemSummary` (for oversized configuration items). The configuration item represents the state of the resource at the moment that Amazon Config detected the change. For an example of a configuration item, see the output produced by the `get-resource-config-history` Amazon CLI command in Viewing Configuration History.

If the event is published for a periodic evaluation, the value is a string that contains a JSON object. The object includes information about the evaluation that was triggered.

For each type of event, a function must parse the string with a JSON parser to be able to evaluate its contents, as shown in the following Node.js example:

```
var invokingEvent = JSON.parse(event.invokingEvent);
```

`ruleParameters`

Key/value pairs that the function processes as part of its evaluation logic. You define parameters when you use the Amazon Config console to create a Custom Lambda rule. You can also define parameters with the `InputParameters` attribute in the `PutConfigRule` Amazon Config API request or the `put-config-rule` Amazon CLI command.

The JSON code for the parameters is contained within a string, so a function must parse the string with a JSON parser to be able to evaluate its contents, as shown in the following Node.js example:

```
var ruleParameters = JSON.parse(event.ruleParameters);
```

`resultToken`

A token that the function must pass to Amazon Config with the `PutEvaluations` call.

`eventLeftScope`

A Boolean value that indicates whether the Amazon resource to be evaluated has been removed from the rule's scope. If the value is `true`, the function indicates that the evaluation can be

ignored by passing `NOT_APPLICABLE` as the value for the `ComplianceType` attribute in the `PutEvaluations` call.

`executionRoleArn`

The ARN of the IAM role that is assigned to Amazon Config.

`configRuleArn`

The ARN that Amazon Config assigned to the rule.

`configRuleName`

The name that you assigned to the rule that caused Amazon Config to publish the event and invoke the function.

`configRuleId`

The ID that Amazon Config assigned to the rule.

`accountId`

The ID of the Amazon Web Services account that owns the rule.

`version`

A version number assigned by Amazon. The version will increment if Amazon adds attributes to Amazon Config events. If a function requires an attribute that is only in events that match or exceed a specific version, then that function can check the value of this attribute.

The current version for Amazon Config events is 1.0.

Managing Deleted Resources for Amazon Config Custom Lambda Rules

Rules reporting on deleted resources should return the evaluation result of `NOT_APPLICABLE` in order to avoid unnecessary rule evaluations.

When you delete a resource, Amazon Config creates a `configurationItem` with `ResourceDeleted` for the `configurationItemStatus`. You can use this metadata to check if a rule reports on a deleted resource. For more information on configuration items, see Concepts | Configuration Items.

Include the following code snippets to check for deleted resources and set the evaluation result of an Amazon Config custom lambda rule to `NOT_APPLICABLE` if it reports on a deleted resource:

Custom Lambda Rules (Node.js)

```
// Check whether the resource has been deleted. If the resource was deleted, then
 the evaluation returns not applicable.
function isApplicable(configurationItem, event) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(event, 'event');
    const status = configurationItem.configurationItemStatus;
    const eventLeftScope = event.eventLeftScope;
    return (status === 'OK' || status === 'ResourceDiscovered') && eventLeftScope
 === false;
}
```

Custom Lambda Rules (Python)

```
# Check whether the resource has been deleted. If the resource was deleted, then the
 evaluation returns not applicable.
def is_applicable(configurationItem, event):
    try:
        check_defined(configurationItem, 'configurationItem')
        check_defined(event, 'event')
    except:
        return True
    status = configurationItem['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']
    if status == 'ResourceDeleted':
        print("Resource Deleted, setting Compliance Status to NOT_APPLICABLE.")
    return (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope
```

Note

Amazon Config managed rules and Amazon Config custom policy rules handle this behavior by default.

If you create an Amazon Config custom lambd rule with Python using the Amazon Config Development Kit (RDK) and Amazon Config Development Kit Library (RDKlib), the imported Evaluator class will check this behavior. For information on how to write rules with the RDK and RDKlib, see Writing rules with the RDK and RDKlib.

Service-Linked Amazon Config Rules

A service-linked Amazon Config rule is a unique type of Amazon Config managed rules that supports other Amazon services to create Amazon Config rules in your account. Service-linked rules are predefined to include all the permissions required to call other Amazon services on your behalf. These rules are similar to standards that an Amazon service recommends in your Amazon Web Services account for compliance verification.

These service-linked Amazon Config rules are owned by Amazon service teams. The Amazon service team creates these rules in your Amazon Web Services account. You have read-only access to these rules. You cannot edit or delete these rules if you are subscribed to Amazon service that these rules are linked to.

Service-linked rules and the Amazon Command Line Interface

With the Amazon CLI, the PutConfigRule, DeleteConfigRule, and DeleteEvaluationResults APIs return access denied with the following error message:

```
INSUFFICIENT_SLCR_PERMISSIONS = "An AWS service owns
ServiceLinkedConfigRule. You do not have permissions to take action on this
rule."
```

Service-linked rules and the Amazon Config console

In the Amazon Config console, the service-linked Amazon Config rules are visible in the **Rules** page. The **Edit** and **Delete results** buttons are greyed in the console to restrict you from editing the rule. You can view details of the rule by choosing the rule.

Service-linked rules, remediation actions, and conformance packs

To add remediation actions to a service-linked rules in a conformance pack, you need to add the remediation action to the conformance pack template itself, and then update the conformance pack with your updated template. For information on updating conformance packs, see Deploying a Conformance Pack (Console), Deploying a Conformance Pack (Amazon CLI) and Managing Organizational Conformance Packs.

Editing and deleting service-linked rules

To edit or delete a service-linked rule, contact the Amazon service that created the rule. For example, for service-linked rules created by Amazon Security Hub, you can remove a service-linked rule by following these steps in the *Amazon Security Hub User Guide*: Disabling a security standard.

Adding Amazon Config Rules

You can use the Amazon Config console or the Amazon SDKs to add rules.

Topics

- Adding Rules (Console)
- Adding Rules (Amazon SDKs)

Adding Rules (Console)

The **Rules** page shows your rules and their current compliance results in a table. The result for each rule is **Evaluating...** until Amazon Config finishes evaluating your resources against the rule. You can update the results with the refresh button. When Amazon Config finishes evaluations, you can see the rules and resource types that are compliant or noncompliant. For more information, see Viewing Compliance Information and Evaluation Results for your Amazon Resources with Amazon Config.

> **Note**
>
> When you add a new rule, Amazon Config evaluates the applicable resources in your resource inventory, including previously recorded resources. For example, if you recorded `AWS::IoT::Policy` resources but later excluded them from recording, Amazon Config retains the initial configuration items (CIs) in your inventory. Although Amazon Config no longer updates these CIs when their associated resource types are excluded from recording, it retains their last recorded state and evaluates them when you add applicable rules. Amazon Config does not evaluate resources that are not in the resource inventory.
> For example, if you add the ??? rule but don't record and have never recorded `AWS::Amplify::Branch` resources, Amazon Config can't evaluate whether the Amazon Amplify branches in your account are compliant or noncompliant.
> For more information, see Recording Amazon Resources with Amazon Config.

Adding rules

To add a rule

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. In the Amazon Web Services Management Console menu, verify that the region selector is set to a region that supports Amazon Config rules. For the list of supported regions, see Amazon Config Regions and Endpoints in the *Amazon Web Services General Reference*.
3. In the left navigation, choose **Rules**.
4. On the **Rules** page, choose **Add rule**.
5. On the **Specify rule type** page, specify the rule type by completing the following steps:
   a. Type in the search field to filter the list of managed rules by rule name, description, and label. For example, type **EC2** to return rules that evaluate EC2 resource types or type **periodic** to return rules that are triggered periodically.
   b. You can also create your own custom rule. Choose **Create custom rule using Lambda** or **Create custom rule using Guard**, and follow the procedure in Creating Amazon Config Custom Lambda Rules or Creating Amazon Config Custom Policy Rules.
6. On the **Configure rule** page, configure your rule by completing the following steps:
   a. For **Name**, type a unique name for the rule.
   b. For **Description**, type a description for the rule.
   c. For **Evaluation mode**, choose when in the resource creation and management process you want Amazon Config to evaluate your resources. Depending on the rule, Amazon Config can evaluate your resource configurations before a resource has been deployed, after a resource has been deployed, or both.
      i. Choose **Turn on proactive evaluation** to allow you to run evaluations on the configuration settings of your resources before they are deployed.

         After you have turned on proactive evaluation, you can use the StartResourceEvaluation API and GetResourceEvaluationSummary API to check if the resources you specify in these commands would be flagged as NON_COMPLIANT by the proactive rules in your account in your Region.

For more information on using this commands, see Evaluating Your Resources with Amazon Config Rules. For a list of managed rules that support proactive evaluation, see List of Amazon Config Managed Rules by Evaluation Mode.

ii. Choose **Turn on detective evaluation** to evaluate the configuration settings of your existing resources.

For detective evaluation, there are two types of triggers: **When configuration changes** and **Periodic**.

A. If the trigger types for your rule include **Configuration changes**, specify one of the following options for **Scope of changes** with which Amazon Config invokes your Lambda function:

- **Resources** – When a resource that matches the specified resource type, or the type plus identifier, is created, changed, or deleted.
- **Tags** – When a resource with the specified tag is created, changed, or deleted.
- **All changes** – When a resource recorded by Amazon Config is created, changed, or deleted.

Amazon Config runs the evaluation when it detects a change to a resource that matches the rule's scope. You can use the scope to define which resources initiate evaluations.

B. If the trigger types for your rule include **Periodic**, specify the **Frequency** with which Amazon Config invokes your Lambda function.

d. For **Parameters**, you can customize the values for the provided keys if your rule includes parameters. A parameter is an attribute that your resources must adhere to before they are considered compliant with the rule.

7. On the **Review and create** page, review all your selections before adding the rule to your Amazon Web Services account. If your rule is not working as expected, you might see one of the following for **Compliance**:

- **No results reported** - Amazon Config evaluated your resources against the rule. The rule did not apply to the Amazon resources in its scope, the specified resources were deleted, or the evaluation results were deleted. To get evaluation results, update the rule, change its scope, or choose **Re-evaluate**.

This message may also appear if the rule didn't report evaluation results.

- **No resources in scope** - Amazon Config cannot evaluate your recorded Amazon resources against this rule because none of your resources are within the rule's scope. To get evaluation results, edit the rule and change its scope, or add resources for Amazon Config to record by using the **Settings** page.
- **Evaluations failed** - For information that can help you determine the problem, choose the rule name to open its details page and see the error message.

Adding Rules (Amazon SDKs)

Adding rules

The following code examples show how to use `PutConfigRule`.

CLI

Amazon CLI

To add an Amazon managed Config rule

The following command provides JSON code to add an Amazon managed Config rule:

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

`RequiredTagsForEC2Instances.json` is a JSON file that contains the rule configuration:

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
```

```
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

For the `ComplianceResourceTypes` attribute, this JSON code limits the scope to resources of the `AWS::EC2::Instance` type, so Amazon Config will evaluate only EC2 instances against the rule. Because the rule is a managed rule, the `Owner` attribute is set to `AWS`, and the `SourceIdentifier` attribute is set to the rule identifier, `REQUIRED_TAGS`. For the `InputParameters` attribute, the tag keys that the rule requires, `CostCenter` and `Owner`, are specified.

If the command succeeds, Amazon Config returns no output. To verify the rule configuration, run the describe-config-rules command, and specify the rule name.

To add a customer managed Config rule

The following command provides JSON code to add a customer managed Config rule:

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

`InstanceTypesAreT2micro.json` is a JSON file that contains the rule configuration:

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
    "SourceDetails": [
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
```

```
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

For the `ComplianceResourceTypes` attribute, this JSON code limits the scope to resources of the `AWS::EC2::Instance` type, so Amazon Config will evaluate only EC2 instances against the rule. Because this rule is a customer managed rule, the `Owner` attribute is set to `CUSTOM_LAMBDA`, and the `SourceIdentifier` attribute is set to the ARN of the Amazon Lambda function. The `SourceDetails` object is required. The parameters that are specified for the `InputParameters` attribute are passed to the Amazon Lambda function when Amazon Config invokes it to evaluate resources against the rule.

If the command succeeds, Amazon Config returns no output. To verify the rule configuration, run the describe-config-rules command, and specify the rule name.

- For API details, see PutConfigRule in *Amazon CLI Command Reference*.

Python

SDK for Python (Boto3)

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
```

```
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
publicly
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- For API details, see PutConfigRule in *Amazon SDK for Python (Boto3) API Reference*.

Updating Amazon Config Rules

You can use the Amazon Config console or the Amazon SDKs to update your rules.

Topics

- Updating Rules (Console)
- Updating Rules (Amazon SDKs)

Updating Rules (Console)

The **Rules** page shows your rules and their current compliance results in a table. The result for each rule is **Evaluating...** until Amazon Config finishes evaluating your resources against the rule. You can update the results with the refresh button. When Amazon Config finishes evaluations, you can see the rules and resource types that are compliant or noncompliant. For more information, see Viewing Compliance Information and Evaluation Results for your Amazon Resources with Amazon Config.

Updating rules

To update a rule

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. In the Amazon Web Services Management Console menu, verify that the region selector is set to a region that supports Amazon Config rules. For the list of supported regions, see Amazon Config Regions and Endpoints in the *Amazon Web Services General Reference*.
3. In the left navigation, choose **Rules**.
4. Choose a rule and **Edit rule** for the rule that you want to update.
5. Modify the settings on the **Edit rule** page to change your rule as needed.
6. Choose **Save**.

Updating Rules (Amazon SDKs)

Updating rules

If you are updating a rule that you added previously, you can specify the rule by `ConfigRuleName`, `ConfigRuleId`, or `ConfigRuleArn` in the `ConfigRule` data type that you use in this request. You use the same `PutConfigRule` command that you use when adding a rule.

The following code examples show how to use `PutConfigRule`.

CLI

Amazon CLI

To add an Amazon managed Config rule

The following command provides JSON code to add an Amazon managed Config rule:

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

RequiredTagsForEC2Instances.json is a JSON file that contains the rule configuration:

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

For the ComplianceResourceTypes attribute, this JSON code limits the scope to resources of the AWS::EC2::Instance type, so Amazon Config will evaluate only EC2 instances against the rule. Because the rule is a managed rule, the Owner attribute is set to AWS, and the SourceIdentifier attribute is set to the rule identifier, REQUIRED_TAGS. For the InputParameters attribute, the tag keys that the rule requires, CostCenter and Owner, are specified.

If the command succeeds, Amazon Config returns no output. To verify the rule configuration, run the describe-config-rules command, and specify the rule name.

To add a customer managed Config rule

The following command provides JSON code to add a customer managed Config rule:

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

InstanceTypesAreT2micro.json is a JSON file that contains the rule configuration:

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
    "SourceDetails": [
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

For the `ComplianceResourceTypes` attribute, this JSON code limits the scope to resources of the `AWS::EC2::Instance` type, so Amazon Config will evaluate only EC2 instances against the rule. Because this rule is a customer managed rule, the `Owner` attribute is set to `CUSTOM_LAMBDA`, and the `SourceIdentifier` attribute is set to the ARN of the Amazon Lambda function. The `SourceDetails` object is required. The parameters that are specified for the `InputParameters` attribute are passed to the Amazon Lambda function when Amazon Config invokes it to evaluate resources against the rule.

If the command succeeds, Amazon Config returns no output. To verify the rule configuration, run the describe-config-rules command, and specify the rule name.

- For API details, see PutConfigRule in *Amazon CLI Command Reference*.

Python

SDK for Python (Boto3)

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
 publicly
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
```

```
                    "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                },
                "InputParameters": "{}",
                "ConfigRuleState": "ACTIVE",
            }
        )
        logger.info("Created configuration rule %s.", rule_name)
    except ClientError:
        logger.exception("Couldn't create configuration rule %s.", rule_name)
        raise
```

- For API details, see PutConfigRule in *Amazon SDK for Python (Boto3) API Reference*.

Deleting Amazon Config Rules

You can use the Amazon Config console or the Amazon SDKs to delete your rules.

Topics

- Considerations
- Deleting Rules (Console)
- Deleting Rules (Amazon SDKs)

Considerations

Recommendation: Consider excluding the `AWS::Config::ResourceCompliance` resource type from recording before deleting rules

Deleting rules creates configuration items (CIs) for `AWS::Config::ResourceCompliance` that can affect your costs for the configuration recorder. If you are deleting rules which evaluate a large number of resource types, this can lead to a spike in the number of CIs recorded.

To avoid the associated costs, you can opt to disable recording for the `AWS::Config::ResourceCompliance` resource type before deleting rules, and re-enable recording after the rules have been deleted.

However, since deleting rules is an asynchronous process, it might take an hour or more to complete. During the time when recording is disabled for `AWS::Config::ResourceCompliance`, rule evaluations will not be recorded in the associated resource's history.

Deleting Rules (Console)

The **Rules** page shows your rules and their current compliance results in a table. The result for each rule is **Evaluating...** until Amazon Config finishes evaluating your resources against the rule. You can update the results with the refresh button. When Amazon Config finishes evaluations, you can see the rules and resource types that are compliant or noncompliant. For more information, see Viewing Compliance Information and Evaluation Results for your Amazon Resources with Amazon Config.

> **Note**
>
> Amazon Config evaluates only the resource types that it is recording. For example, if you add the **cloudtrail-enabled** rule but don't record the CloudTrail trail resource type, Amazon Config can't evaluate whether the trails in your account are compliant or noncompliant. For more information, see Recording Amazon Resources with Amazon Config.

Deleting rules

To delete a rule

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. In the Amazon Web Services Management Console menu, verify that the region selector is set to a region that supports Amazon Config rules. For the list of supported regions, see Amazon Config Regions and Endpoints in the *Amazon Web Services General Reference*.
3. In the left navigation, choose **Rules**.
4. Choose a rule from the table that you want to delete.
5. From the **Actions** dropdown list, choose **Delete rule**.
6. When prompted, type "Delete" (case-sensitive) and then choose **Delete**.

Deleting Rules (Amazon SDKs)

Deleting rules

The following code examples show how to use `DeleteConfigRule`.

CLI

Amazon CLI

To delete an Amazon Config rule

The following command deletes an Amazon Config rule named `MyConfigRule`:

```
aws configservice delete-config-rule --config-rule-name MyConfigRule
```

- For API details, see DeleteConfigRule in *Amazon CLI Command Reference*.

Python

SDK for Python (Boto3)

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client
```

```
    def delete_config_rule(self, rule_name):
        """
        Delete the specified rule.

        :param rule_name: The name of the rule to delete.
        """
        try:
            self.config_client.delete_config_rule(ConfigRuleName=rule_name)
            logger.info("Deleted rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't delete rule %s.", rule_name)
            raise
```

- For API details, see DeleteConfigRule in *Amazon SDK for Python (Boto3) API Reference*.

Viewing Details and Compliance Information for your Amazon Config Rules

> **Important**
>
> For accurate reporting on the compliance status, you must record the `AWS::Config::ResourceCompliance` resource type. For more information, see Recording Amazon Resources.

You can use the Amazon Config console or the Amazon SDKs to view your rules.

Topics

- Viewing Rules (Console)
- Viewing Rules (Amazon SDKs)

Viewing Rules (Console)

The **Rules** page shows your rules and their current compliance results in a table. The result for each rule is **Evaluating...** until Amazon Config finishes evaluating your resources against the rule. You

can update the results with the refresh button. When Amazon Config finishes evaluations, you can see the rules and resource types that are compliant or noncompliant. For more information, see Viewing Compliance Information and Evaluation Results for your Amazon Resources with Amazon Config.

> **Note**
>
> Amazon Config evaluates only the resource types that it is recording. For example, if you add the **cloudtrail-enabled** rule but don't record the CloudTrail trail resource type, Amazon Config can't evaluate whether the trails in your account are compliant or noncompliant. For more information, see Recording Amazon Resources with Amazon Config.

Viewing rules

To view your rules

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. In the Amazon Web Services Management Console menu, verify that the region selector is set to a region that supports Amazon Config rules. For the list of supported regions, see Amazon Config Regions and Endpoints in the *Amazon Web Services General Reference*.
3. In the left navigation, choose **Rules**.
4. The **Rules** page shows all the rule that are currently in your Amazon Web Services account. It lists the name, associated remediation action, and compliance status of each rule.

   - Choose **Add rule** to get started with creating a rule.
   - Choose a rule to see its settings, or choose a rule and **View details**.
   - See the compliance status of the rule when it evaluates your resources.
   - Choose a rule and **Edit rule** to change the configuration settings of the rule and set a remediation action for a noncompliant rule.

Viewing Rules (Amazon SDKs)

Viewing details for your rules

The following code examples show how to use `DescribeConfigRules`.

CLI

Amazon CLI

To get details for an Amazon Config rule

The following command returns details for an Amazon Config rule named `InstanceTypesAreT2micro`:

```
aws configservice describe-config-rules --config-rule-
names InstanceTypesAreT2micro
```

Output:

```
{
    "ConfigRules": [
        {
            "ConfigRuleState": "ACTIVE",
            "Description": "Evaluates whether EC2 instances are the t2.micro
 type.",
            "ConfigRuleName": "InstanceTypesAreT2micro",
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "Source": {
                "Owner": "CUSTOM_LAMBDA",
                "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
                "SourceDetails": [
                    {
                        "EventSource": "aws.config",
                        "MessageType": "ConfigurationItemChangeNotification"
                    }
                ]
            },
            "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}",
            "Scope": {
                "ComplianceResourceTypes": [
                    "AWS::EC2::Instance"
                ]
            },
            "ConfigRuleId": "config-rule-abcdef"
        }
    ]
```

```
}
```

- For API details, see DescribeConfigRules in *Amazon CLI Command Reference*.

PowerShell

Tools for PowerShell V4

Example 1: This sample lists config rules for the account, with selected properties.

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

Output:

```
ConfigRuleName                                  ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                  ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                           config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                             config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required      config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- For API details, see DescribeConfigRules in *Amazon Tools for PowerShell Cmdlet Reference (V4)*.

Tools for PowerShell V5

Example 1: This sample lists config rules for the account, with selected properties.

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

Output:

```
ConfigRuleName                                  ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                  ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                           config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                             config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required      config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- For API details, see DescribeConfigRules in *Amazon Tools for PowerShell Cmdlet Reference (V5)*.

Python

SDK for Python (Boto3)

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client
```

```
    def describe_config_rule(self, rule_name):
        """
        Gets data for the specified rule.

        :param rule_name: The name of the rule to retrieve.
        :return: The rule data.
        """
        try:
            response = self.config_client.describe_config_rules(
                ConfigRuleNames=[rule_name]
            )
            rule = response["ConfigRules"]
            logger.info("Got data for rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't get data for rule %s.", rule_name)
            raise
        else:
            return rule
```

- For API details, see DescribeConfigRules in *Amazon SDK for Python (Boto3) API Reference*.

Viewing compliance information for your rules

The following code examples show how to use `DescribeComplianceByConfigRule`.

CLI

Amazon CLI

To get compliance information for your Amazon Config rules

The following command returns compliance information for each Amazon Config rule that is violated by one or more Amazon resources:

```
aws configservice describe-compliance-by-config-rule --compliance-
types NON_COMPLIANT
```

In the output, the value for each `CappedCount` attribute indicates how many resources do not comply with the related rule. For example, the following output indicates that 3 resources do not comply with the rule named `InstanceTypesAreT2micro`.

Output:

```
{
    "ComplianceByConfigRules": [
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "InstanceTypesAreT2micro"
        },
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "RequiredTagsForVolumes"
        }
    ]
}
```

- For API details, see [DescribeComplianceByConfigRule](#) in *Amazon CLI Command Reference*.

PowerShell

Tools for PowerShell V4

Example 1: This example retrieves compliances details for the rule ebs-optimized-instance, for which there is no current evaluation results for the rule, hence it returns INSUFFICIENT_DATA

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

Output:

```
ComplianceContributorCount ComplianceType
```

```
-------------------------- --------------
                           INSUFFICIENT_DATA
```

Example 2: This example returns the number of non-compliant resources for the rule ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK.

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

Output:

```
CapExceeded CappedCount
----------- -----------
False       2
```

- For API details, see DescribeComplianceByConfigRule in *Amazon Tools for PowerShell Cmdlet Reference (V4)*.

Tools for PowerShell V5

Example 1: This example retrieves compliances details for the rule ebs-optimized-instance, for which there is no current evaluation results for the rule, hence it returns INSUFFICIENT_DATA

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

Output:

```
ComplianceContributorCount ComplianceType
-------------------------- --------------
                           INSUFFICIENT_DATA
```

Example 2: This example returns the number of non-compliant resources for the rule ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK.

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

Output:

```
CapExceeded CappedCount
----------- -----------
False       2
```

- For API details, see DescribeComplianceByConfigRule in *Amazon Tools for PowerShell Cmdlet Reference (V5)*.

Viewing the compliance summary for your rules

The following code examples show how to use `GetComplianceSummaryByConfigRule`.

CLI

Amazon CLI

To get the compliance summary for your Amazon Config rules

The following command returns the number of rules that are compliant and the number that are noncompliant:

```
aws configservice get-compliance-summary-by-config-rule
```

In the output, the value for each `CappedCount` attribute indicates how many rules are compliant or noncompliant.

Output:

```
{
    "ComplianceSummary": {
        "NonCompliantResourceCount": {
            "CappedCount": 3,
            "CapExceeded": false
        },
        "ComplianceSummaryTimestamp": 1452204131.493,
        "CompliantResourceCount": {
            "CappedCount": 2,
            "CapExceeded": false
        }
```

```
    }
}
```

- For API details, see GetComplianceSummaryByConfigRule in *Amazon CLI Command Reference*.

PowerShell

Tools for PowerShell V4

Example 1: This sample returns the number of Config rules that are non-compliant.

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

Output:

```
CapExceeded CappedCount
----------- -----------
False       9
```

- For API details, see GetComplianceSummaryByConfigRule in *Amazon Tools for PowerShell Cmdlet Reference (V4)*.

Tools for PowerShell V5

Example 1: This sample returns the number of Config rules that are non-compliant.

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

Output:

```
CapExceeded CappedCount
----------- -----------
False       9
```

- For API details, see GetComplianceSummaryByConfigRule in *Amazon Tools for PowerShell Cmdlet Reference (V5)*.

Viewing the evaluation results for your rules

The following code examples show how to use `GetComplianceDetailsByConfigRule`.

CLI

Amazon CLI

To get the evaluation results for an Amazon Config rule

The following command returns the evaluation results for all of the resources that don't comply with an Amazon Config rule named `InstanceTypesAreT2micro`:

```
aws configservice get-compliance-details-by-config-rule --config-rule-
name InstanceTypesAreT2micro --compliance-types NON_COMPLIANT
```

Output:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-2a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.18,
```

```
            "ConfigRuleInvokedTime": 1450314642.902,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-3a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.346,
            "ConfigRuleInvokedTime": 1450314643.124,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- For API details, see [GetComplianceDetailsByConfigRule](#) in *Amazon CLI Command Reference*.

PowerShell

Tools for PowerShell V4

Example 1: This example obtains the evaluation results for the rule access-keys-rotated and returns the output grouped by compliance-type

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

Output:

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

Example 2: This example queries compliance details for the rule access-keys-rotated for COMPLIANT resources.

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

Output:

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- For API details, see GetComplianceDetailsByConfigRule in *Amazon Tools for PowerShell Cmdlet Reference (V4)*.

Tools for PowerShell V5

Example 1: This example obtains the evaluation results for the rule access-keys-rotated and returns the output grouped by compliance-type

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

Output:

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

Example 2: This example queries compliance details for the rule access-keys-rotated for COMPLIANT resources.

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

Output:

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- For API details, see GetComplianceDetailsByConfigRule in *Amazon Tools for PowerShell Cmdlet Reference (V5)*.

Turning on Proactive Evaluation for Amazon Config Rules

You can use the Amazon Config console or the Amazon SDKs to turn on proactive evaluation rules. For a list of resource types and managed rules that support proactive evaluation, see Components of a Rule | Evaluation Modes.

Topics

- Turning on Proactive Evaluation (Console)
- Turning on Proactive Evaluation (Amazon SDKs)

Turning on Proactive Evaluation (Console)

The **Rules** page shows your rules and their current compliance results in a table. The result for each rule is **Evaluating...** until Amazon Config finishes evaluating your resources against the rule. You can update the results with the refresh button.

When Amazon Config finishes evaluations, you can see the rules and resource types that are compliant or noncompliant. For more information, see Viewing Compliance Information and Evaluation Results for your Amazon Resources with Amazon Config.

> **Note**
>
> Amazon Config evaluates only the resource types that it is recording. For example, if you add the **cloudtrail-enabled** rule but don't record the CloudTrail trail resource type, Amazon Config can't evaluate whether the trails in your account are compliant or noncompliant. For more information, see Recording Amazon Resources with Amazon Config.

Turning on proactive evaluation

You can use *proactive evaluation* to evaluate resources before they have been deployed. This allows you to evaluate whether a set of resource properties, if used to define an Amazon resource, would be COMPLIANT or NON_COMPLIANT given the set of proactive rules that you have in your account in your Region.

The Resource type schema states the properties of a resource. You can find the resource type schema in "*Amazon public extensions*" within the Amazon CloudFormation registry or with the following CLI commmand:

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

For more information, see Managing extensions through the Amazon CloudFormation registry and Amazon resource and property types reference in the Amazon CloudFormation User Guide.

> **Note**
>
> Proactive rules do not remediate resources that are flagged as NON_COMPLIANT or prevent them from being deployed.

To turn on proactive evalution

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. In the Amazon Web Services Management Console menu, verify that the Region selector is set to a Region that supports Amazon Config rules. For the list of supported Amazon Regions, see Amazon Config Regions and Endpoints in the *Amazon Web Services General Reference*.
3. In the left navigation, choose **Rules**. For a list of managed rules that support proactive evaluation, see List of Amazon Config Managed Rules by Evaluation Mode.
4. Choose a rule, and then choose **Edit rule** for the rule that you want to update.
5. For **Evaluation mode**, choose **Turn on proactive evaluation** to allow you to run evaluations on the configuration settings of your resources before they are deployed.
6. Choose **Save**.

After you have turned on proactive evaluation, you can use the StartResourceEvaluation API and GetResourceEvaluationSummary API to check if the resources you specify in these commands would be flagged as NON_COMPLIANT by the proactive rules in your account in your Region.

For example, start with the StartResourceEvaluation API:

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
               --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                   "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

You should receive the `ResourceEvaluationId` in the output:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

Then, use the `ResourceEvaluationId` with the GetResourceEvaluationSummary API to check the evaluation result:

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

You should receive output similiar to the following:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
```

```
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

To see additional information about the evaluation result, such as which rule flagged a resource as NON_COMPLIANT, use the GetComplianceDetailsByResource API.

Turning on Proactive Evaluation (Amazon SDKs)

Turning on proactive evaluation (Amazon CLI)

You can use *proactive evaluation* to evaluate resources before they have been deployed. This allows you to evaluate whether a set of resource properties, if used to define an Amazon resource, would be COMPLIANT or NON_COMPLIANT given the set of proactive rules that you have in your account in your Region.

The Resource type schema states the properties of a resource. You can find the resource type schema in "*Amazon public extensions*" within the Amazon CloudFormation registry or with the following CLI commmand:

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

For more information, see Managing extensions through the Amazon CloudFormation registry and Amazon resource and property types reference in the Amazon CloudFormation User Guide.

> **Note**
>
> Proactive rules do not remediate resources that are flagged as NON_COMPLIANT or prevent them from being deployed.

To turn on proactive evaluation

Use the `put-config-rule` command and enable `PROACTIVE` for `EvaluationModes`.

After you have turned on proactive evaluation, you can use the start-resource-evaluation CLI command and get-resource-evaluation-summary CLI command to check if the resources you specify in these commands would be flagged as NON_COMPLIANT by the proactive rules in your account in your Region.

For example, start with the **start-resource-evaluation** command:

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
               --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                   "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

You should receive the `ResourceEvaluationId` in the output:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

Then, use the `ResourceEvaluationId` with the **get-resource-evaluation-summary** to check the evaluation result:

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

You should receive output similiar to the following:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

To see additional information about the evaluation result, such as which rule flagged a resource as NON_COMPLIANT, use the get-compliance-details-by-resource CLI command.

> **Note**
>
> For a list of managed rules that support proactive evaluation, see List of Amazon Config Managed Rules by Evaluation Mode.

Turning on proactive evaluation (API)

You can use *proactive evaluation* to evaluate resources before they have been deployed. This allows you to evaluate whether a set of resource properties, if used to define an Amazon resource, would be COMPLIANT or NON_COMPLIANT given the set of proactive rules that you have in your account in your Region.

The Resource type schema states the properties of a resource. You can find the resource type schema in "*Amazon public extensions*" within the Amazon CloudFormation registry or with the following CLI commmand:

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

For more information, see Managing extensions through the Amazon CloudFormation registry and Amazon resource and property types reference in the Amazon CloudFormation User Guide.

> **Note**
>
> Proactive rules do not remediate resources that are flagged as NON_COMPLIANT or prevent them from being deployed.

To turn on proactive evaluation for a rule

Use the PutConfigRule action and enable `PROACTIVE` for `EvaluationModes`.

After you have turned on proactive evaluation, you can use the StartResourceEvaluation API and GetResourceEvaluationSummary API to check if the resources you specify in these commands would be flagged as NON_COMPLIANT by the proactive rules in your account in your Region. For example, start with the StartResourceEvaluation API:

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
               --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                   "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

You should receive the `ResourceEvaluationId` in the output:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

Then, use the `ResourceEvaluationId` with the GetResourceEvaluationSummary API to check the evaluation result:

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

You should receive output similiar to the following:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

To see additional information about the evaluation result, such as which rule flagged a resource as NON_COMPLIANT, use the GetComplianceDetailsByResource API.

> **Note**
>
> For a list of managed rules that support proactive evaluation, see List of Amazon Config Managed Rules by Evaluation Mode.

Sending Rule Evaluations to Security Hub

After adding an Amazon Config rule, you can also send rule evaluations to Amazon Security Hub. The integration between Amazon Config and Security Hub allows you to triage and remediate rule evaluations alongside other misconfigurations and security issues.

Send Rule Evaluations to Security Hub

To send rule evaluations to Security Hub, you must first set up Amazon Security Hub and Amazon Config, and then add at least one Amazon Config managed or custom rule. After this, Amazon Config immediately starts sending rule evaluations to Security Hub. Security Hub enriches the rule evaluations and transforms them into Security Hub findings.

For more information about this integration, see Available Amazon Service Integrations in the Amazon Security Hub User Guide.

Evaluating Your Resources with Amazon Config Rules

When you create custom rules or use managed rules, Amazon Config evaluates your resources against those rules. You can run on-demand evaluations for resources against your rules. For example, this is helpful when you create a custom rule and want to check that Amazon Config is correctly evaluating your resources or to identify if there is an issue with the evaluation logic of your Amazon Lambda function.

Example

1. You create a custom rule that evaluates whether your IAM users have active access keys.
2. Amazon Config evaluates your resources against your custom rule.
3. An IAM user who doesn't have an active access key exists in your account. Your rule doesn't correctly flag this resource as NON_COMPLIANT.
4. You fix the rule and start the evaluation again.

5. Because you fixed your rule, the rule correctly evaluates your resources, and flags the IAM user resource as NON_COMPLIANT.

When you add a rule to your account, you can specify when in the resource creation and management process that you want Amazon Config to evaluate your resources. The resource creation and management process is known as resource provisioning. You choose the *evaluation mode* to specify when in this process you want Amazon Config to evaluate your resources.

Depending on the rule, Amazon Config can evaluate your resource configurations before a resource has been deployed, after a resource has been deployed, or both. Evaluating a resource before it has been deployed is **proactive evaluation**. Evaluating a resource after it has been deployed is **detective evaluation**.

Proactive mode

Use proactive evaluation to evaluate resources before they have been deployed. This allows you to evaluate whether a set of resource properties, if used to define an Amazon resource, would be COMPLIANT or NON_COMPLIANT given the set of proactive rules that you have in your account in your Region.

The Resource type schema states the properties of a resource. You can find the resource type schema in "*Amazon public extensions*" within the Amazon CloudFormation registry or with the following CLI commmand:

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

For more information, see Managing extensions through the Amazon CloudFormation registry and Amazon resource and property types reference in the Amazon CloudFormation User Guide.

> **Note**
>
> Proactive rules do not remediate resources that are flagged as NON_COMPLIANT or prevent them from being deployed.

Evaluating your Resources

To turn on proactive evalution

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. In the Amazon Web Services Management Console menu, verify that the Region selector is set to a Region that supports Amazon Config rules. For the list of supported Amazon Regions, see Amazon Config Regions and Endpoints in the *Amazon Web Services General Reference*.
3. In the left navigation, choose **Rules**. For a list of managed rules that support proactive evaluation, see List of Amazon Config Managed Rules by Evaluation Mode.
4. Choose a rule, and then choose **Edit rule** for the rule that you want to update.
5. For **Evaluation mode**, choose **Turn on proactive evaluation** to allow you to run evaluations on the configuration settings of your resources before they are deployed.
6. Choose **Save**.

> **Note**
>
> You can also turn on proactive evaluation using the `put-config-rule` command and enabling `PROACTIVE` for `EvaluationModes` or using the PutConfigRule action and enabling `PROACTIVE` for `EvaluationModes`.

After you have turned on proactive evaluation, you can use the StartResourceEvaluation API and GetResourceEvaluationSummary API to check if the resources you specify in these commands would be flagged as NON_COMPLIANT by the proactive rules in your account in your Region.

For example, start with the StartResourceEvaluation API:

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
               --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                   "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

You should receive the `ResourceEvaluationId` in the output:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

Then, use the `ResourceEvaluationId` with the GetResourceEvaluationSummary API to check the evaluation result:

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

You should receive output similiar to the following:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

To see additional information about the evaluation result, such as which rule flagged a resource as NON_COMPLIANT, use the GetComplianceDetailsByResource API.

Detective mode

Use detective evaluation to evaluate resources that have already been deployed. This allows you to evaluate the configuration settings of your existing resources.

Evaluating your Resources (Console)

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.

2. In the Amazon Web Services Management Console menu, check that the region selector is set to a Region that supports Amazon Config rules. For the list of supported regions, see Amazon Config Regions and Endpoints in the *Amazon Web Services General Reference*.
3. In the navigation pane, choose **Rules**. The **Rules** page shows the name, associated remediation action, and compliance status of each rule.
4. Choose a rule from the table.
5. From the **Actions** dropdown list, choose **Re-evaluate**.
6. Amazon Config starts evaluating the resources against your rule.

> **Note**
>
> You can re-evaluate a rule one time each minute. You must wait for Amazon Config to complete the evaluation for your rule before you start another evaluation. You can't run an evaluation if at the same time the rule is being updated or if the rule is being deleted.

Evaluating your Resources (CLI)

- Use the **start-config-rules-evaluation** command:

```
$ aws configservice start-config-rules-evaluation --config-rule-
names ConfigRuleName
```

Amazon Config starts evaluating the recorded resource configurations against your rule. You can also specify multiple rules in your request:

```
$ aws configservice start-config-rules-evaluation --config-rule-
names ConfigRuleName1 ConfigRuleName2 ConfigRuleName3
```

Evaluating your Resources (API)

Use the StartConfigRulesEvaluation action.

Deleting Evaluation Results from Amazon Config Rules

After Amazon Config evaluates your rule, you can see the evaluation results on the **Rules** page or the **Rules details** page for the rule. If the evaluation results are incorrect or if you want to evaluate again, you can delete the current evaluation results for the rule. For example, if your rule was incorrectly evaluating your resources or you recently deleted resources from your account, you can delete the evaluation results and then run a new evaluation.

Deleting Evaluation Results (Console)

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. In the Amazon Web Services Management Console menu, verify that the Region selector is set to an Amazon Region that supports Amazon Config rules. For the list of supported Regions, see Amazon Config Regions and Endpoints in the *Amazon Web Services General Reference*.
3. In the navigation pane, choose **Rules**. The **Rules** page shows the name, associated remediation action, and compliance status of each rule.
4. Choose a rule from the table.
5. From the **Actions** dropdown list, choose **Delete results**.
6. When prompted, type **Delete** (this entry is case sensitive), and then choose **Delete**. After you delete an evaluation, you cannot retrieve it.
7. After the evaluation results are deleted, you can manually start a new evaluation.

Deleting Evaluation Results (CLI)

- Use the **delete-evaluation-results** command.

  ```
  $ aws configservice delete-evaluation-results --config-rule-name ConfigRuleName
  ```

  Amazon Config deletes the evaluation results for the rule.

Deleting Evaluation Results (API)

Use the DeleteEvaluationResults action.

Troubleshooting for Amazon Config rules

Check the following issues to troubleshoot if you cannot delete an Amazon Config rule or receive an error similair to the following: "An error has occurred with Amazon Config."

The Amazon Identity and Access Management (IAM) entity has permissions for the DeleteConfigRule API

1. Open the IAM console at https://console.amazonaws.cn/iam/.
2. In the navigation pane choose **Users** or **Roles**.
3. Choose the user or role that you used to delete the Amazon Config rule, and expand **Permissions policies**.
4. In the **Permissions** tab, choose **JSON**.
5. In the JSON preview pane, confirm that the IAM policy allows permissions for the DeleteConfigRule API.

The IAM entity permission boundary allows the DeleteConfigRule API

If the IAM entity has a permissions boundary, be sure that it allows permissions for the the DeleteConfigRule API.

1. Open the IAM console at https://console.amazonaws.cn/iam/.
2. In the navigation pane choose **Users** or **Roles**.
3. Choose the user or role that you used to delete the Amazon Config rule, expand **Permissions boundary**, and then choose **JSON**.
4. In the JSON preview pane, confirm that the IAM policy allows permissions for the DeleteConfigRule API.

> **Warning**
>
> IAM users have long-term credentials, which presents a security risk. To help mitigate this risk, we recommend that you provide these users with only the permissions they require to perform the task and that you remove these users when they are no longer needed.

The service control policy (SCP) allows the DeleteConfigRule API

1. Open the Amazon Organizations console at https://console.amazonaws.cn/organizations/ using the management account for the organization.
2. In Account name, choose the Amazon Web Services account.
3. In **Policies**, expand **Service control policies** and note the SCP policies that are attached.
4. At the top of the page, choose **Policies**.
5. Select the policy, and then choose **View details**.
6. In the JSON preview pane, confirm that the policy allows the DeleteConfigRule API.

The rule is not a service-linked rule

When you enable a security standard, Amazon Security Hub creates service-linked rules for you. You can't delete these service-linked rules using Amazon Config, and the delete button is grayed out. To remove a service-linked rule, see Disabling a security standard in the *Security Hub User Guide*.

No remediation actions are in progress

You cannot delete Amazon Config rules that have remediation actions in progress. Follow the steps to delete the remediation action that is associated with that rule. Then, try deleting the rule again.

> **Important**
>
> Only delete remediation actions that are in **failed** or **successful** states.

Remediating Noncompliant Resources with Amazon Config

Amazon Config allows you to remediate noncompliant resources that are evaluated by Amazon Config Rules. Amazon Config applies remediation using Amazon Systems Manager Automation documents. These documents define the actions to be performed on noncompliant Amazon resources evaluated by Amazon Config Rules. You can associate SSM documents by using Amazon Web Services Management Console or by using APIs.

Amazon Config provides a set of managed automation documents with remediation actions. You can also create and associate custom automation documents with Amazon Config rules.

Topics

- Region Support
- Setting Up Manual Remediation for Amazon Config
- Setting Up Auto Remediation for Amazon Config
- Deleting Remediation Actions for Amazon Config

Region Support

Currently, remediation actions for Amazon Config Rules is supported in the following regions:

Region Name	Region	Endpoint	Protocol	
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS	
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS	
US West (N.	us-west-1	config.us-west-1.amazonaws.com	HTTPS	

Region Name	Region	Endpoint	Protocol	
California)				
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS	
Africa (Cape Town)	af-south-1	config.af-south-1.amazonaws.com	HTTPS	
Asia Pacific (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS	
Asia Pacific (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS	
Asia Pacific (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS	
Asia Pacific (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS	
Asia Pacific (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS	
Asia Pacific (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS	

Region Name	Region	Endpoint	Protocol	
Asia Pacific (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS	
Asia Pacific (Singapore)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS	
Asia Pacific (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS	
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS	
Canada (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS	
Canada West (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS	
China (Beijing)	cn-north-1	config.cn-north-1.amazonaws.com.cn	HTTPS	
China (Ningxia)	cn-northwest-1	config.cn-northwest-1.amazonaws.com.cn	HTTPS	
Europe (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS	

Region Name	Region	Endpoint	Protocol	
Europe (Ireland)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS	
Europe (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS	
Europe (Milan)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS	
Europe (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS	
Europe (Spain)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS	
Europe (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS	
Europe (Zurich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS	
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS	
Middle East (Bahrain)	me-south-1	config.me-south-1.amazonaws.com	HTTPS	
Middle East (UAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS	

Region Name	Region	Endpoint	Protocol	
South America (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS	

Setting Up Manual Remediation for Amazon Config

To apply remediation on noncompliant resources, you can either choose the remediation action you want to associate from a prepopulated list or create your own custom remediation actions using SSM documents. Amazon Config provides a recommended list of remediation action in the Amazon Web Services Management Console.

Setting Up Manual Remediation (Console)

In the Amazon Web Services Management Console, you can either choose to manually remediate noncompliant resources by associating remediation actions with Amazon Config rules. With all remediation actions, you can either choose manual or automatic remediation.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. Choose **Rules** on the left and then on the **Rules** page, choose **Add Rule** to add new rules to the rule list

   For existing rules, select the noncompliant rule from the rule list and choose the **Actions** dropdown list.
3. From the **Actions** dropdown list, choose **Manage remediation**. Select "Manual remediation" and then choose the appropriate remediation action from the recommended list.

> **Note**
>
> You can only manage remediations for non-service linked Amazon Config rules. For more information, see Service-Linked Amazon Rules.

Depending on the selected remediation action, you see specific parameters or no parameters.

4. (Optional): If you want to pass the resource ID of noncompliant resources to the remediation action, choose **Resource ID parameter**. If selected, at runtime that parameter is substituted with the ID of the resource to be remediated.

   Each parameter has either a static value or a dynamic value. If you do not choose a specific resource ID parameter from the dropdown list, you can enter values for each key. If you choose a resource ID parameter from the dropdown list, you can enter values for all the other keys except the selected resource ID parameter.

5. Choose **Save**. The **Rules** page is displayed.

For troubleshooting failed remediation actions, you can run the Amazon Command Line Interface command `describe-remediation-execution-status` to get detailed view of a Remediation Execution for a set of resources. The details include state, timestamps for remediation execution steps, and any error messages for the failed steps.

Setting Up Manual Remediation (API)

Use the following Amazon Config API operation to set up manual remediation:

- PutRemediationConfigurations, adds or updates the remediation configuration with a specific Amazon Config rule with the selected target or action.
- StartRemediationExecution, runs an on-demand remediation for the specified Amazon Config rules against the last known remediation configuration.
- DescribeRemediationExecutionStatus, provides a detailed view of a Remediation Execution for a set of resources including state, timestamps for when steps for the remediation execution occur, and any error messages for steps that have failed.
- DescribeRemediationConfigurations, returns the details of one or more remediation configurations.

Setting Up Auto Remediation for Amazon Config

To apply remediation on noncompliant resources, you can either choose the remediation action you want to associate from a prepopulated list or create your own custom remediation actions using

SSM documents. Amazon Config provides a list of remediation action in the Amazon Web Services Management Console.

Setting Up Auto Remediation (Console)

In the Amazon Web Services Management Console, you can either choose to automatically remediate noncompliant resources by associating remediation actions with Amazon Config rules. With all remediation actions, you can either choose manual or automatic remediation.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. Choose **Rules** on the left and then on the **Rules** page, choose **Add Rule** to add new rules to the rule list.

   For existing rules, select the noncompliant rule from the rule list and choose the **Actions** dropdown list.
3. From the **Actions** dropdown list, choose **Manage remediation**. Select "Automatic remediation" and then choose the appropriate remediation action from the list.

   > **Note**
   >
   > You can only manage remediations for non-service linked Amazon Config rules. For more information, see Service-Linked Amazon Rules.

   Depending on the selected remediation action, you see specific parameters or no parameters.
4. Choose **Auto remediation** to automatically remediate noncompliant resources.

   If a resource is still noncompliant after auto remediation, you can set the rule to try auto remediation again. Enter the desired retries and seconds.

   > **Note**
   >
   > There are costs associated with running a remediation script multiple times. Retries only occur if remediation fails and work within the specified time period; for example, 5 retries in 300 seconds. For more information, see Systems Manager Automation Pricing .

5. (Optional): If you want to pass the resource ID of noncompliant resources to the remediation action, choose **Resource ID parameter**. If selected, at runtime that parameter is substituted with the ID of the resource to be remediated.

   Each parameter has either a static value or a dynamic value. If you do not choose a specific resource ID parameter from the dropdown list, you can enter values for each key. If you choose a resource ID parameter from the dropdown list, you can enter values for all the other keys except the selected resource ID parameter.
6. Choose **Save**. The **Rules** page is displayed.

For troubleshooting failed remediation actions

For troubleshooting failed remediation actions, you can run the Amazon Command Line Interface command `describe-remediation-execution-status` to get detailed view of a Remediation Execution for a set of resources. The details include state, timestamps for remediation execution steps, and any error messages for the failed steps.

Auto remediation can be initiated even for compliant resources

If you enable auto remediation for a specific Amazon Config rule using the PutRemediationConfigurations API or the Amazon Config console, it initiates the remediation process for all noncompliant resources for that specific rule. The auto remediation process relies on the compliance data snapshot which is captured on a periodic basis. Any noncompliant resource that is updated between the snapshot schedule will continue to be remediated based on the last known compliance data snapshot.

This means that in some cases auto remediation can be initiated even for compliant resources, since the bootstrap processor uses a database that can have stale evaluation results based on the last known compliance data snapshot.

Setting Up Auto Remediation (API)

Use the following Amazon Config API operation to set up auto remediation:

- PutRemediationExceptions, adds a new exception or updates an existing exception for a specific resource with a specific Amazon Config rule.
- DescribeRemediationExceptions, returns the details of one or more remediation exceptions.

Deleting Remediation Actions for Amazon Config

You can use the Amazon Config console or the Amazon CLI to delete remediation actions.

Deleting remediation actions (Console)

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. Choose **Rules** on the left and then on the **Rules** page, select the rule from the rule list and choose **View details**.
3. On the *name of the rule* page, go to the **Remediation action** section. Expand the section to view additional details.
4. In the **Remediation action** section, choose **Delete** and confirm your delete action.

   > **Note**
   >
   > If remediation is in progress, a remediation action won't be deleted. Once you choose delete a remediation action, you cannot retrieve the remediation action. Deleting a remediation action does not delete the associated rule.

   If a remediation action is deleted, the **Resource ID parameter** will be empty and display N/A. On the **Rules** page, the remediation action column displays **Not set** for the associated rule.

Deleting remediation actions (API)

Use the following Amazon Config API operation to set up auto remediation:

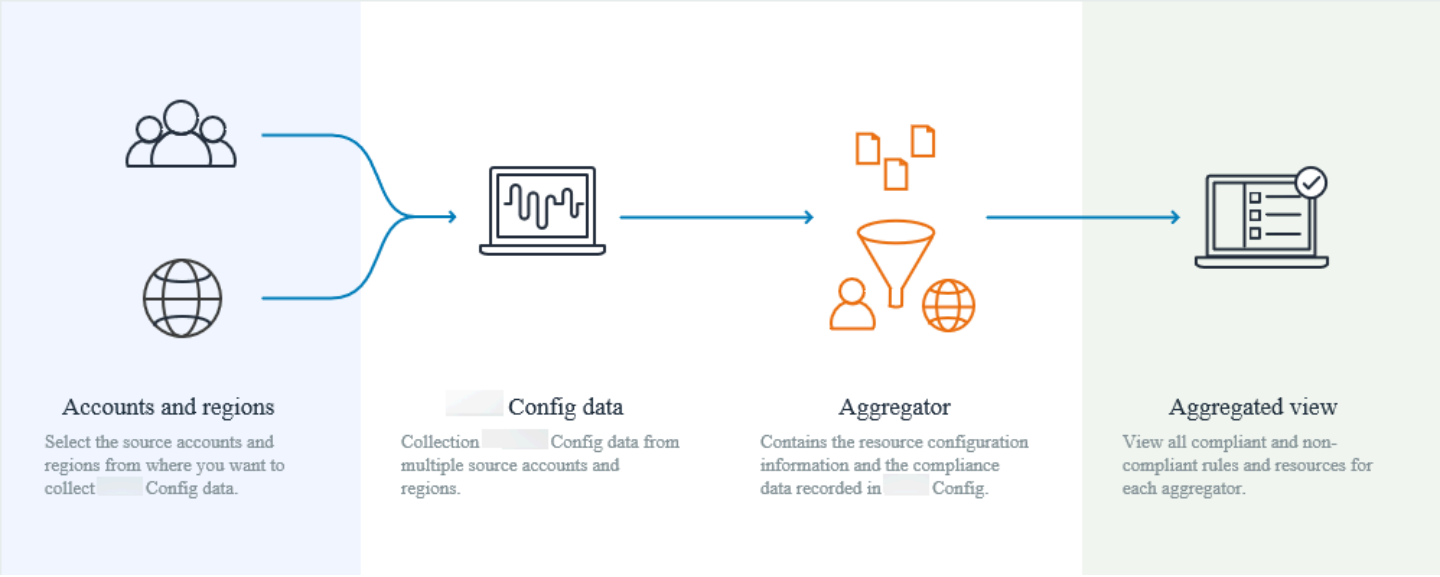
- DeleteRemediationConfiguration, deletes the remediation configuration.
- DeleteRemediationExceptions, deletes one or more remediation exceptions mentioned in the resource keys.

Multi-Account Multi-Region Data Aggregation for Amazon Config

An aggregator is an Amazon Config resource type that collects Amazon Config configuration and compliance data from the following:

- Multiple accounts and multiple Amazon Regions.
- Single account and multiple Amazon Regions.
- An organization in Amazon Organizations and all the accounts in that organization which have Amazon Config enabled.

Use an aggregator to view the resource configuration and compliance data recorded in Amazon Config. The following image displays how an aggregator collects Amazon Config data from multiple accounts and Regions.



Use Cases

- **Compliance Monitoring**: You can aggregate compliance data to assess the overall compliance postures of your organization, or across accounts and Regions.
- **Change Tracking**: You can track changes to resources over time across your organization, or across accounts and Regions.

- **Resource Relationships**: You can analyze resource dependencies and relationships across your organization, or across accounts and Regions.

> **Note**
>
> Aggregators provide a *read-only view* into the source accounts and Regions that the aggregator is authorized to view by replicating data from the source accounts into the aggregator account. Aggregators do not provide mutating access into a source account or region. For example, this means that you cannot deploy rules through an aggregator or push snapshot files to a source account or region through an aggregator.
> Using aggregators does not incur any additional costs.

Terminology

A *source account* is the Amazon Web Services account from which you want to aggregate Amazon Config resource configuration and compliance data. A source account can be an individual account or an organization in Amazon Organizations. You can provide source accounts individually or you can retrieve them through Amazon Organizations.

A *source region* is the Amazon Region from which you want to aggregate Amazon Config configuration and compliance data.

An *aggregator account* is an account where you create an aggregator.

Authorization refers to the permissions you grant to an aggregator account and region to collect your Amazon Config configuration and compliance data. Authorization is not required if you are aggregating source accounts that are part of Amazon Organizations.

A *service-linked aggregator* is linked to a specific Amazon Web Services service. The configuration and compliance data in scope are set by the linked service.

Region Support

Currently, multi-account multi-region data aggregation is supported in the following Regions:

Region Name	Region	Endpoint	Protocol	
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS	
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS	
US West (N. California)	us-west-1	config.us-west-1.amazonaws.com	HTTPS	
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS	
Africa (Cape Town)	af-south-1	config.af-south-1.amazonaws.com	HTTPS	
Asia Pacific (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS	
Asia Pacific (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS	
Asia Pacific (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS	
Asia Pacific	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS	

Region Name	Region	Endpoint	Protocol	
(Malaysia)				
Asia Pacific (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS	
Asia Pacific (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS	
Asia Pacific (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS	
Asia Pacific (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS	
Asia Pacific (Singapore)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS	
Asia Pacific (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS	
Asia Pacific (Taipei)	ap-east-2	config.ap-east-2.amazonaws.com	HTTPS	

Region Name	Region	Endpoint	Protocol	
Asia Pacific (Thailand)	ap-southeast-7	config.ap-southeast-7.amazonaws.com	HTTPS	
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS	
Canada (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS	
Canada West (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS	
China (Beijing)	cn-north-1	config.cn-north-1.amazonaws.com.cn	HTTPS	
China (Ningxia)	cn-northwest-1	config.cn-northwest-1.amazonaws.com.cn	HTTPS	
Europe (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS	
Europe (Ireland)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS	
Europe (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS	
Europe (Milan)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS	

Region Name	Region	Endpoint	Protocol	
Europe (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS	
Europe (Spain)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS	
Europe (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS	
Europe (Zurich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS	
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS	
Mexico (Central)	mx-central-1	config.mx-central-1.amazonaws.com	HTTPS	
Middle East (Bahrain)	me-south-1	config.me-south-1.amazonaws.com	HTTPS	
Middle East (UAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS	
South America (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS	

Viewing Compliance and Inventory Data in the Aggregator Dashboard for Amazon Config

The dashboard on the **Aggregators** page displays the configuration data of your aggregated Amazon resources. It provides an overview of your rules, conformance packs, and their compliance states.

The dashboard provides the total resource count of Amazon resources. The resource types and source accounts are ranked by the highest number of resources. It also provides a count of compliant and noncompliant rules and conformance packs. The noncompliant rules are ranked by highest number of noncompliant resources. The noncompliant conformance packs and source accounts are ranked by the highest number of noncompliant rules.

After setting up Amazon Config, it starts aggregating data from the specified source accounts into an aggregator. It might take a few minutes for the compliance status of rules to display.

Using the Aggregator Dashboard

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. Navigate to the **Aggregators** page. You can view:
   - Your rules and their compliance states.
   - Your conformance packs and their compliance states.
   - Your Amazon resources and their configuration data.
3. Choose an aggregator from the dashboard. Filter through your aggregators by aggregator name. You can view the following widgets:
   - **Resource inventory**

     View the top 10 resource types from the selected aggregator, in descending order by the resource count. Choose the total number of resources for the selected aggregator, displayed in parentheses after **Resource inventory**, to go to the aggregated **Resources** page, where you can view all the resources for an aggregator. Alternatively, choose a resource type in the widget to go to the aggregated **Resources** page, filtered using the specified resource type.
   - **Accounts by resource count**

View the top five accounts from the selected aggeregator in the descending order by the resource count. Choose an account in the widget to go to the **Resources** page, filtered using the specified account.

- **Noncompliant rules**

  View the top five noncompliant rules from the selected Aggregator, in descending order by the number of noncompliant resources. Choose a rule in the widget to go to the details page for the specified rule. Choose **View all noncompliant rules** to go to the aggregated **Rules** page, where you can view all the rules for an aggregator.

- **Accounts by noncompliant rules**

  View the top five accounts from the selected aggregator, in descending order by the number of noncompliant rules. Choose an account in the widget to go to the aggregated **Rules** page, where you can view all the rules for an aggregator filtered using the specified account.

- **Accounts by noncompliant conformance packs**

  View the top five accounts from the selected aggregagtor, in descending order by the number of noncompliant conformance packs. Choose an account in the widget to go to the aggregated **Conformance Pack** page, where you can view all conformance packs for an aggregagtor filtered using the specified account.

4. In the left navigation pane, choose one of the following options from the dropdown menu:

   - **Compliance dashboard**

     View automated compliance dashboards by using the widgets that summarize insights about resource compliance within your aggregator. You can see data such as the top 10 resource types by noncompliant resources, and top 10 account level conformance packs by noncompliant rules. For information about these graphs and charts, see Compliance dashboards.

   - **Conformance packs**

     View all conformance packs that are created and linked to the different Amazon Web Services accounts within your aggregator. The **Conformance Pack** page displays a table that lists the name, Region, account ID, and compliance status of each conformance pack. From this page, you can choose a conformance pack and **View details** for more information about its rules and resources and their compliance status.

   - **Rules**

View all rules that are created and linked to the different Amazon accounts within your aggregator. The **Rules** page displays a table that lists the name, compliance status, Region, and account of each rule. From this page, you can choose a rule and **View details** for information, such as its aggregator, Region, account ID, and resources in scope.

- **Inventory dashboard**

  View automated inventory dashboards by using the widgets that summarize insights about resource configuration data within your aggregator. You can see data such as the top 10 resource types by resource count, and the top 10 accounts by resource count. For information about these graphs and charts, see Inventory dashboards.

- **Resources**

  View all resources that are recorded and linked to the different Amazon accounts within your aggregator. From the **Resource** page, choose a resource and **View details** to view its details, the rules associated with it, and the current resource configuration. You can also see information about the resource, such as its aggregator, Region, account ID, resource name, resource type, and resource ID.

- **Authorizations**

  View and manage all accounts currently authorized or pending authorization. From the **Authorizations** page, choose **Add authorization** to provide access to another account. Choose **Delete authorization** to revoke access from an account ID.

Note

Troubleshooting
You might see the **Data collection from all source accounts and regions is incomplete** message displayed in the aggregated view for the following reasons:

- The transfer of noncompliant Amazon Config rules and configuration data of Amazon resources is in progress.
- Amazon Config can't find rules to match the filter that you applied. Select the appropriate account or Region, and try again.

You might see this message display in the aggregated view: **Data collection from your organization is incomplete. You can view the below data only for 24 hours.** It displays for the following reasons:

- Amazon Config can't access your organization details because of an IAM role that is not valid. If the IAM role remains not valid for more than 24 hours, Amazon Config deletes the data for the entire organization.
- Amazon Config service access is disabled in your organization.

Compliance Dashboard

View automated compliance dashboards by using widgets that summarize insights about resource compliance within your aggregator This dashboard displays only rules with compliance results.

Note

Limitations
The insights in the compliance dashboard are provided by the Advanced Queries feature of Amazon Config, and this feature does not support nested structures or unpacking nested arrays. This means that the compliance dashboard displays the overall compliance of a resource and not the compliance status for each specific rule which reports on a resource. For example, if you check the configuration item (CI) for the resource type `AWS::Config::ResourceCompliance`, the dashboard will display the compliance results for all the rules that report on that resource. If there are 10 rules that report on the resource, 9 of them are COMPLIANT, and only 1 is NON_COMPLIANT, the overall compliance of that resource will be NON_COMPLIANT.

Compliance Summary By Resources

Displays a pie chart comparing the number of compliant resources to noncompliant resources from the selected aggregator. Hover over the chart to see the exact number and percentage of compliant and noncompliant resources.

The data displayed depends on the settings of the configuration recorder for each account in the selected aggregator, and the Regions where the selected aggregator is configured to collect data.

Top 10 resource types by noncompliant resources

Displays a horizontal bar graph comparing up to 10 resource types from the selected aggregator in descending order by the number of noncompliant resources. Hover over the graph to see the exact number of noncompliant resources for each resource type.

The data displayed is dependent on the settings of the configuration recorder for each account in the selected aggregator and the Regions where the selected aggregator is configured to collect data.

Top 10 accounts by noncompliant resources

Top 10 accounts by noncompliant resources displays a horizontal bar graph comparing up to 10 accounts from the selected aggregator in descending order by the number of noncompliant resources. Hover over the graph to see the exact number of noncompliant resources for each account.

The data displayed depends on the settings of the configuration recorder for each account in the selected aggregator, and the Regions where the selected aggregator is configured to collect data.

Top 10 regions by noncompliant resources

Displays a horizontal bar graph comparing up to 10 Regions where the selected aggregator collects data in descending order by the number of noncompliant resources. Hover over the graph to see the exact number of noncompliant resources for each Region.

The data displayed depends on the settings of the configuration recorder for each account in the selected aggregator.

Top 10 account level conformance packs by noncompliant rules

Displays a horizontal bar graph comparing up to 10 account level conformance packs from the selected aggregator in descending order by the number of noncompliant rules. Hover over the graph to see the percentage of compliant and noncompliant rules for each account level conformance pack.

The data displayed depends on the settings of the configuration recorder for each account in the selected aggregator, and the Regions where the selected aggregator is configured to collect data.

Top 10 organization level conformance packs by noncompliant rules

Displays a horizontal bar graph comparing up to 10 organizational level conformance packs from the selected aggregator in descending order by the number of noncompliant rules. Hover over the graph to see the percentage of compliant and noncompliant rules in each organizational level conformance pack.

The data displayed is dependent on the settings of the configuration recorder for each account in the selected aggregator and the Regions where the selected aggregator is configured to collect data.

Top 10 accounts by noncompliant rules across conformance packs

Top 10 accounts by noncompliant rules across conformance packs displays a horizontal bar graph comparing up to 10 accounts from the selected aggregator in descending order by the number of noncompliant rules across all your conformance packs. Hover over the graph to see the exact number of noncompliant rules in each account.

The data displayed is dependent on the settings of the configuration recorder for each account in the selected aggregator and the Regions where the selected aggregator is configured to collect data.

Inventory Dashboard

View automated inventory dashboards by using widgets that summarize insights about resource configuration data within your aggregator.

Top 10 resource types by resource count

Displays a horizontal bar graph comparing up to 10 resource types from the selected aggregator in descending order by resource count. Hover over the graph to see the exact number of resources for each resource type.

The data displayed depends on the settings of the configuration recorder for each account in the selected aggregator, and the Regions where the selected aggregator is configured to collect data.

Resource count by region

Displays a horizontal bar graph comparing up to 10 Regions where the selected aggregator collects data in descending order by resource count. Hover over the graph to see the exact number of resources for each Region.

The data displayed depends on the settings of the configuration recorder for each account in the selected aggregator.

Top 10 accounts by resource count

Displays a horizontal bar graph comparing up to 10 accounts from the selected aggregator in descending order by resource count. Hover over the graph to see the exact number resources for each resource type.

The data displayed is dependent on the settings of the configuration recorder for each account in the selected aggregator and the Regions where the selected aggregator is configured to collect data.

Resource count by Amazon EC2 service resource types

Displays a horizontal bar graph comparing Amazon EC2 resource types from the selected aggregator in descending order by resource count. Hover over the graph to see the exact number of resources for each Amazon EC2 resource type.

The data displayed depends on the settings of the configuration recorder for each account in the selected aggregator, and the Regions where the selected aggregator is configured to collect data. To use this chart, you must configure the recorder to record Amazon EC2 resource types. For more information, see Selecting Which Resources Amazon Config Records.

Top 10 EC2 instance types used

Displays a horizontal bar graph comparing up to 10 Amazon EC2 instance types from the selected aggregator in descending order by usage. Hover over the graph to see usage for each EC2 instance type.

The data displayed depends on the settings of the configuration recorder for each account in the selected aggregator and the Regions where the selected aggregator is configured to collect data. To use this chart, you must configure the recorder to record the EC2 instance resource type. For more information, see Recoding Amazon Resources.

EBS Volume counts by volume type and size

Displays a vertical bar graph comparing EBS volumes from the selected aggregator by resource count. Hover over the graph to see the count and size breakdown for each type of EBS volume.

The data displayed depends on the settings of the configuration recorder for each account in the selected aggregator and the Regions where the selected aggregator is configured to collect data. To use this chart, you must configure the recorder to record the EC2 volume resource type. For more information, see Selecting Which Resources Amazon Config Records.

Number of EC2 instances that are running vs. stopped by type

Displays a horizontal bar graph comparing EC2 instance types from the selected aggregator that are running to EC2 instances that are stopped by instance type. Hover over the graph to see the exact number of stopped and running EC2 instances for each type.

The data displayed depends on the settings of the configuration recorder for each account in the selected aggregator and the Regions where the selected aggregator is configured to collect data. To use this chart, you must configure the recorder to record the EC2 instance resource type. For more information, see Recoding Amazon Resources.

Creating Aggregators for Amazon Config

You can use the Amazon Config console or the Amazon CLI to create your aggregators. From the Amazon Config you can choose **Add individual account IDs** or **Add my organization** from where you want to aggregate data. For the Amazon CLI there are two different procedures.

Creating Aggregators (Console)

On the **Aggregator** page, you can create an aggregator by specifying the source account IDs or organization and regions from where you want to aggregate data.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. Navigate to the **Aggregators** page and choose **Create aggregator**.
3. **Allow data replication**, gives permission to Amazon Config to replicate data from the source accounts into an aggregator account.

   Choose **Allow Amazon Config to replicate data from source account(s) into an aggregator account. You must select this checkbox to continue to add an aggregator**.

4. For **Aggregator name**, type the name for your aggregator.

   The aggregator name must be a unique name with a maximum of 64 alphanumeric characters. The name can contain hyphens and underscores.

5. For **Select source accounts**, either choose **Add individual account IDs** or **Add my organization** from where you want to aggregate data.

   > **Note**
   >
   > Authorization is required when using **Add individual account IDs** to select source accounts.

   - If you choose **Add individual account IDs**, you can add individual account IDs for an aggregator account.
     1. Choose **Add source accounts** to add account IDs.
     2. Choose **Add Amazon Web Services account IDs** to manually add comma-separated Amazon Web Services account IDs. If you want to aggregate data from the current account, type the account ID of the account.

        OR

        Choose **Upload a file** to upload a file (.txt or .csv) of comma-separated Amazon Web Services account IDs.
     3. Choose **Add source accounts** to confirm your selection.
   - If you choose **Add my organization**, you can add all accounts in your organization to an aggregator account.

     > **Note**
     >
     > You must be signed in to the management account or a registered delegated administrator and all the features must be enabled in your organization. If the caller is a management account, Amazon Config calls `EnableAwsServiceAccess` API to enable integration between Amazon Config and Amazon Organizations. If the caller is a registered delegated administrator, Amazon Config calls `ListDelegatedAdministrators` API to verify whether the caller is a valid delegated administrator.

Ensure that the management account registers delegated administrator for Amazon Config service principal name (config.amazonaws.com) before the delegated administrator creates an aggregator. To register a delegated administrator, see Registering a Delegated Administrator for Amazon Config.

You must assign an IAM role to allow Amazon Config to call read-only APIs for your organization.

1. Choose **Choose a role from your account** to select an existing IAM role.

> **Note**
>
> In the IAM console, attach the `AWSConfigRoleForOrganizations` managed policy to your IAM role. Attaching this policy allows Amazon Config to call Amazon Organizations `DescribeOrganization`, `ListAWSServiceAccessForOrganization`, and `ListAccounts` APIs. By default `config.amazonaws.com` is automatically specified as a trusted entity.

2. Or, choose **Create a role** and type a name for your IAM role name to create IAM role.

6. For **Regions**, choose the regions for which you want to aggregate data.
   - Select one region or multiple regions or all the Amazon Web Services Regions.
   - Select **Include future Amazon Web Services Regions** to aggregate data from all future Amazon Web Services Regions where multi-account multi-region data aggregation is enabled.
7. Choose **Save**. Amazon Config displays the aggregator.

Creating Aggregators using Individual Accounts (Amazon CLI)

1. Open a command prompt or a terminal window.
2. Enter the following command to create an aggregator named **`MyAggregator`**.

```
aws configservice put-configuration-aggregator --configuration-aggregator-name
 MyAggregator --account-aggregation-sources "[{\"AccountIds\": [\"AccountID1\",
\"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"
```

For `account-aggregation-sources`, enter one of the following.

- A comma-separated list of Amazon Web Services account IDs for which you want to aggregate data. Wrap the account IDs in square brackets, and be sure to escape quotation marks (for example, `"[{\"AccountIds\": [\"AccountID1\", \"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"`).
- You can also upload a JSON file of comma-separated Amazon Web Services account IDs. Upload the file using the following syntax: `--account-aggregation-sources MyFilePath/MyFile.json`

  The JSON file must be in the following format:

```
[
    {
        "AccountIds": [
            "AccountID1",
            "AccountID2",
            "AccountID3"
        ],
        "AllAwsRegions": true
    }
]
```

3. Press Enter to execute the command.

You should see output similar to the following:

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "AccountAggregationSources": [
            {
                "AllAwsRegions": true,
                "AccountIds": [
                    "AccountID1",
                    "AccountID2",
                    "AccountID3"
```

```
                ]
            }
        ],
        "LastUpdatedTime": 1517942461.442
    }
}
```

Creating Aggregators using Amazon Organizations (Amazon CLI)

Before you begin this procedure, you must be signed in to the management account or a registered delegated administrator and all the features must be enabled in your organization.

> **Note**
>
> Ensure that the management account registers a delegated administrator with both of the following Amazon Config service principal names (`config.amazonaws.com` and`config-multiaccountsetup.amazonaws.com`) before the delegated administrator creates an aggregator. To register a delegated administrator, see Registering a Delegated Administrator for Amazon Config.

1. Open a command prompt or a terminal window.
2. If have not created an IAM role for your Amazon Config aggregator, enter the following command:

```
aws iam create-role --role-name OrgConfigRole --assume-role-policy-document
 "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":\"\",\"Effect\":\"Allow\",
\"Principal\":{\"Service\":\"config.amazonaws.com\"},\"Action\":\"sts:AssumeRole
\"}]}" --description "Role for organizational AWS Config aggregator"
```

> **Note**
>
> Copy the Amazon Resource Name (ARN) from this IAM role for use when you create your Amazon Config aggregator. You can find the ARN on the response object.

3. If have not attached a policy to your IAM role, attach the AWSConfigRoleForOrganizations managed policy or enter the following command:

```
aws iam create-policy --policy-name OrgConfigPolicy --policy-document
 '{"Version":"2012-10-17","Statement":[{"Effect":"Allow","Action":
["organizations:ListAccounts","organizations:DescribeOrganization","organizations:ListAW
```

4. Enter the following command to create an aggregator named **MyAggregator**.

```
aws configservice put-configuration-aggregator --configuration-aggregator-name
 MyAggregator --organization-aggregation-source "{\"RoleArn\": \"Complete-Arn\",
\"AllAwsRegions\": true}"
```

5. Press Enter to execute the command.

   You should see output similar to the following:

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws-cn:iam::account-of-role-to-assume:role/name-
of-role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

Registering a Delegated Administrator for Amazon Config

Delegated administrators are accounts within a given Amazon Organization that are granted additional administrative privileges for a specified Amazon service. For more information, see Delegated administrator in the *Amazon Organizations User Guide*. You must use the Amazon CLI to register a delegated administrator.

Registering a Delegated Administrator

1. Log in with management account credentials.

2. Open a command prompt or a terminal window.
3. Enter the following command to enable service access as a delegated administrator for your organization to deploy and manage Amazon Config rules and conformance packs across your organization:

```
aws organizations enable-aws-service-access --service-principal=config-
multiaccountsetup.amazonaws.com
```

4. Enter the following command to enable service access as a delegated administrator for your organization to aggregate Amazon Config data across your organization:

```
aws organizations enable-aws-service-access --service-
principal=config.amazonaws.com
```

5. To check if the enable service access is complete, enter the following command and press Enter to execute the command.

```
aws organizations list-aws-service-access-for-organization
```

   You should see output similar to the following:

```
{
    "EnabledServicePrincipals": [
        {
            "ServicePrincipal": [
                "config.amazonaws.com",
                "config-multiaccountsetup.amazonaws.com"
        ],
            "DateEnabled": 1607020860.881
        }
    ]
}
```

6. Next, enter the following command to register a member account as a delegated administrator for Amazon Config.

```
aws organizations register-delegated-administrator --service-principal=config-
multiaccountsetup.amazonaws.com --account-id MemberAccountID
```

   and

```
aws organizations register-delegated-administrator --service-
principal=config.amazonaws.com --account-id MemberAccountID
```

7. To check if the registration of delegated administrator is complete, enter the following command from the management account and press Enter to execute the command.

```
aws organizations list-delegated-administrators --service-principal=config-
multiaccountsetup.amazonaws.com
```

and

```
aws organizations list-delegated-administrators --service-
principal=config.amazonaws.com
```

You should see output similar to the following:

```
{
    "DelegatedAdministrators": [
        {
            "Id": "MemberAccountID",
            "Arn": "arn:aws:organizations::ManagementAccountID:account/o-
c7esubdi38/MemberAccountID",
            "Email": "name@amazon.com",
            "Name": "name",
            "Status": "ACTIVE",
            "JoinedMethod": "INVITED",
            "JoinedTimestamp": 1604867734.48,
            "DelegationEnabledDate": 1607020986.801
        }
    ]
}
```

Editing Aggregators for Amazon Config

You can use the Amazon Config console or the Amazon CLI to edit your aggregators.

Editing Aggregators (Console)

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. Navigate to the **Aggregator** page, and choose the aggregator name.
3. Choose **Actions** and then choose **Edit**.
4. Use the sections on the **Edit aggregator** page to change the source accounts, IAM roles, or regions for the aggregator.

   > **Note**
   >
   > You cannot change source type from individual account(s) to organization and vice versa.

5. Choose **Save**.

Editing Aggregators (Amazon CLI)

1. You can use the `put-configuration-aggregator` command to update or edit a configuration aggregator.

   Enter the following command to add a new account ID to **`MyAggregator`**:

   ```
   aws configservice put-configuration-aggregator --configuration-aggregator-name
    MyAggregator --account-aggregation-sources "[{\"AccountIds\": [\"AccountID1\",
   \"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"
   ```

2. Depending on your source account you should see output similar to the following:

   For individuals accounts

   ```
   {
       "ConfigurationAggregator": {
           "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
   aggregator/config-aggregator-xz2upuu6",
           "CreationTime": 1517952090.769,
           "ConfigurationAggregatorName": "MyAggregator",
           "AccountAggregationSources": [
               {
                   "AllAwsRegions": true,
   ```

```
                "AccountIds": [
                    "AccountID1",
                    "AccountID2",
                    "AccountID3",
                    "AccountID4"
                ]
            }
        ],
        "LastUpdatedTime": 1517952566.445
    }
}
```

OR

For an organization

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws-cn:iam::account-of-role-to-assume:role/name-
of-role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

Deleting Aggregators for Amazon Config

You can use the Amazon Config console or the Amazon CLI to delete your aggregators.

Deleting Aggregators (Console)

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. Navigate to the **Aggregator** page, and choose the aggregator name.

3. Choose **Actions** and then choose **Delete**.

   A warning message is displayed. Deleting an aggregator results in the loss of all aggregated data. You cannot recover this data but data in the source account(s) is not impacted.

4. Choose **Delete** to confirm your selection.

Deleting Aggregators (Amazon CLI)

Enter the following command:

```
aws configservice delete-configuration-aggregator --configuration-aggregator-name
 MyAggregator
```

If successful, the command executes with no additional output.

Authorizing Aggregator Accounts to Collect Amazon Config Configuration and Compliance Data

Authorization refers to the permissions you grant to an aggregator account and region to collect your Amazon Config configuration and compliance data. Authorization is not required if you are aggregating source accounts that are part of Amazon Organizations. You can use the Amazon Config console or the Amazon CLI to authorize aggregator accounts.

Topics

- Considerations
- Adding Authorization

Considerations

There are two types of aggregators: Individual account aggregator and Organization aggregator

For an individual account aggregator, authorization is required for all source accounts and Regions that you want to include, including both external accounts and Regions and Organization member accounts and Regions.

For an organization aggregator, authorization is not required for Organization member account regions since authorization is integrated with the Amazon Organizations service.

Aggregators do not automatically enable Amazon Config on your behalf

Amazon Config needs to be enabled in the source account and Region for either type of aggregator, in order for Amazon Config data to be generated in the source account and Region.

Adding Authorization

Adding Authorization (Console)

You can add authorization to grant permission to aggregator accounts and Regions to collect Amazon Config configuration and compliance data.

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. Navigate to the **Authorizations** page and choose **Add authorization**.
3. For **Aggregator account**, type the 12-digit account ID of an aggregator account.
4. For **Aggregator region**, choose the Amazon Web Services Regions where the aggregator account is allowed to collect Amazon Config configuration and compliance data.
5. Choose **Add authorization** to confirm your selection.

   Amazon Config displays an aggregator account, Region, and authorization status.

> **Note**
>
> You can also add authorizations to aggregator accounts and Regions programatically using Amazon CloudFormation sample templates. For more information, see AWS::Config::AggregationAuthorization in the *Amazon CloudFormation User Guide*.

Authorizing a Pending Request (Console)

If you have a pending authorization request from an existing aggregator account you will see the request status on the **Authorizations** page. You can authorize a pending request from this page.

1. Choose the aggregator account that you want to authorize, and then choose **Authorize**.

   A confirmation message is displayed to confirm that you want to grant the aggregator account permission to collect Amazon Config data from this account.

2. Choose **Authorize** again to confirm that you want to grant permission to the aggregator account.

   The authorization status changes from **Requesting for authorization** to **Authorized**.

Authorization approval period

Authorization approval is required to add source accounts to an individual account aggregator. A pending authorization approval request will be available for 7 days after an individual account aggregator adds a source account.

Adding Authorization (Amazon CLI)

1. Open a command prompt or a terminal window.
2. Enter the following command:

```
aws configservice put-aggregation-authorization --authorized-account-id
  AccountID --authorized-aws-region Region
```

3. You should see output similar to the following:

```
{
    "AggregationAuthorization": {
        "AuthorizedAccountId": "AccountID",
        "AggregationAuthorizationArn":
 "arn:aws:config:Region:AccountID:aggregation-authorization/AccountID/Region",
        "CreationTime": 1518116709.993,
        "AuthorizedAwsRegion": "Region"
    }
}
```

Deleting Authorization for Aggregator Accounts to Collect Amazon Config Configuration and Compliance Data

Authorization refers to the permissions you grant to an aggregator account and region to collect your Amazon Config configuration and compliance data. Authorization is not required if you are aggregating source accounts that are part of Amazon Organizations. You can use the Amazon Config console or the Amazon CLI to delete authorizations.

Topics

- Considerations
- Deleting Authorization

Considerations

There are two types of aggregators: Individual account aggregator and Organization aggregator

For an individual account aggregator, authorization is required for all source accounts and Regions that you want to include, including both external accounts and Regions and Organization member accounts and Regions.

For an organization aggregator, authorization is not required for Organization member account regions since authorization is integrated with the Amazon Organizations service.

Aggregators do not automatically enable Amazon Config on your behalf

Amazon Config needs to be enabled in the source account and Region for either type of aggregator, in order for Amazon Config data to be generated in the source account and Region.

Deleting Authorization

Deleting Authorization (Console)

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. Choose the aggregator account that you want to delete authorization, and then choose **Delete**.

A warning message is displayed. When you delete this authorization, Amazon Config data will no longer be shared with the aggregator account.

3. Choose **Delete** again to confirm your selection.

   The aggregator account is now deleted.

Deleting Authorization (Amazon CLI)

Enter the following command:

```
aws configservice delete-aggregation-authorization --authorized-account-id
  AccountID --authorized-aws-region Region
```

If successful, the command executes with no additional output.

Viewing Aggregators for Amazon Config

You can use the Amazon Config console or the Amazon CLI to view your aggregators.

Viewing Aggregators (Console)

To view your conformance packs in the Amazon Web Services Management Console, see Aggregator Dashboard.

Viewing Aggregators (Amazon CLI)

1. Enter the following command:

   ```
   aws configservice describe-configuration-aggregators
   ```

2. Depending on your source account you should see output similar to the following:

   For individuals accounts

   ```
   {
       "ConfigurationAggregators": [
           {
               "ConfigurationAggregatorArn":
    "arn:aws:config:Region:AccountID:config-aggregator/config-aggregator-floqpus3",
   ```

```
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "MyAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        }
    ]
}
```

OR

For an organization

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws-cn:iam::account-of-role-to-assume:role/name-
of-role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

Troubleshooting for Multi-Account Multi-Region Data Aggregation for Amazon Config

Amazon Config might not aggregate data from source accounts for one of the following reasons:

If this happens	Do this
Amazon Config is not enabled in the source account for accounts within an Organization.	Enable Amazon Config in the source account and authorize the aggregator account to collect data.
Authorization is not granted to an aggregator account.	Sign in to the source account and grant authorization to the aggregator account to collect Amazon Config data.
There might be a temporary issue that is preventing data aggregation.	Data aggregation is subject to delays. Wait for a few minutes.

Amazon Config might not aggregate data from an organization for one of the following reasons:

If this happens	Do this
Amazon Config is unable to access your organization details due to invalid IAM role.	Create an IAM role or select a valid IAM role from the IAM role list. **Note** If the IAM role is invalid for more than 7 days, Amazon Config deletes data for entire organization.
Amazon Config service access is disabled in your organization.	You can enable integration between Amazon Config and Amazon Organizations through the `EnableAWSServiceAccess` API. If you choose **Add my organization** in console, Amazon Config automatically enables the integration between Amazon Config and Amazon Organizations.
Amazon Config is unable to access your organization details because	Enable all features in Amazon Organizations console.

If this happens	Do this
all features is not enabled in your organization.	
Organizational changes such as adding an account, removing an account, enabling service access, and disabling service access are not updated in Middle East (Bahrain) and Asia Pacific (Hong Kong) regions immediately.	Organizational changes are subject to 2 hour delay. Wait for 2 hours to see all organization changes.

Querying the Current Configuration State of Amazon Resources with Amazon Config

Introducing a preview feature for advanced queries that allows you to use generative artificial intelligence (generative AI) capabilities to enter prompts in plain English and convert them into a ready-to-use query format. For more information, see Natural language query processor for advanced queries.

You can use Amazon Config to query the current configuration state of Amazon resources based on configuration properties for a single account and Region or across multiple accounts and Regions. You can perform property-based queries against current Amazon resource state metadata across a list of resources that Amazon Config supports. For more information on the list of supported resource types, see Supported Resource Types for Advanced Queries.

Advanced queries provides a single query endpoint and a query language to get current resource state metadata without performing service-specific describe API calls. You can use configuration aggregators to run the same queries from a central account across multiple accounts and Amazon Regions.

Topics

- Features
- Query Components for Amazon Config
- Query Using the SQL Query Editor for Amazon Config (Console)
- Query Using the SQL Query Editor for Amazon Config (Amazon CLI)
- Natural language query processor for Amazon Config advanced queries
- Example Queries for Amazon Config
- Example Relationship Queries for Amazon Config
- Limitations
- CIDR notation/IP range behavior for advanced queries
- Multiple properties within an array behavior for advanced queries
- Region Support

Features

Amazon Config uses a subset of structured query language (SQL) SELECT syntax to perform property-based queries and aggregations on the current configuration item (CI) data. The queries range in complexity from matches against tag and/or resource identifiers, to more complex queries, such as viewing all Amazon S3 buckets that have versioning disabled. This allows you to query exactly the current resource state you need without performing Amazon service-specific API calls.

It supports aggregation functions such as AVG, COUNT, MAX, MIN, and SUM.

You can use advanced query for:

- Inventory management; for example, to retrieve a list of Amazon EC2 instances of a particular size.
- Security and operational intelligence; for example, to retrieve a list of resources that have a specific configuration property enabled or disabled.
- Cost optimization; for example, to identify a list of Amazon EBS volumes that are not attached to any EC2 instance.
- Compliance data; for example, to retrieve a list of all your conformance packs and their compliance status.

For information about how to use the Amazon SQL Query Language, see What Is SQL (Structured Query Language)?.

Query Components for Amazon Config

The SQL SELECT query components for Amazon Config advanced queries are as follows.

Synopsis

```
SELECT property [, ...]
[ WHERE condition ]
[ GROUP BY property ]
[ ORDER BY property [ ASC | DESC ] [, property [ ASC | DESC ] ...] ]
```

Parameters

[WHERE condition]

Filters results according to the `condition` you specify.

Comparison operators

- = (equals)
- `IN` (list membership)
- `BETWEEN` (range check)

Logic operators

- `AND`
- `OR`
- `NOT`

[GROUP BY property]

Aggregates the result set into groups of rows with matching values for the given property.

The GROUP BY clause is applicable to aggregations.

[ORDER BY property [ASC | DESC] [, property [ASC | DESC] ...]]

Sorts a result set by one or more output `properties`.

When the clause contains multiple properties, the result set is sorted according to the first `property`, then according to the second `property` for rows that have matching values for the first property, and so on.

Examples

```
SELECT resourceId WHERE resourceType='AWS::EC2::Instance'
```

```
SELECT configuration.complianceType, COUNT(*) WHERE resourceType =
 'AWS::Config::ResourceCompliance' GROUP BY configuration.complianceType
```

Query Using the SQL Query Editor for Amazon Config (Console)

Introducing a preview feature for advanced queries that allows you to use generative artificial intelligence (generative AI) capabilities to enter prompts in plain English and convert them into a ready-to-use query format. For more information, see Natural language query processor for advanced queries.

You can either use Amazon sample queries or you can create your own query called as custom queries.

Considerations

Prerequisites

If you are using the one of the following Amazon managed policies, you will have the necessary permissions to run and save a query: AWSServiceRoleForConfig (service-linked role) or AWS_ConfigRole.

Otherwise, you must have the permissions included in the AWSConfigUserAccess Amazon managed policy.

List of properties that you can query

An updated list of properties and their data types is available in GitHub.

Advanced queries and aggregators

To run a query on an aggregator, create an aggregator. For more information, see Creating Aggregators for Amazon Config.

If you already have an aggregator set up, in the query scope, choose the aggregator to run an advanced query on that aggregator. When you select an aggregator, consider adding the Amazon Web Services account ID and Amazon Region in the query statement to view that information in the results.

Use an Amazon Sample Query

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.

2. Choose **Advanced queries** from the left navigation to query your resource configurations for a single account and Region or for multiple accounts and Regions.
3. On the **Advanced queries** page, choose an appropriate query from the list of queries. You can filter through the list of queries either by the name, description, creator, or tags. To filter for Amazon queries, choose **Creator**, and enter **Amazon**. The query that you select is displayed in the SQL query editor. You can edit the selected query to fit your needs.
4. To save this query to a new query, choose **Save As**.
   - In the **Query Name** field, update the name of the query.
   - In the **Description** field, update the description of the query.
   - Enter up to 50 unique tags for this query.
   - Choose **Save**.
5. Choose **Run**. The query results are displayed in the table below the query editor.
6. Choose **Export as** to export the query results in CSV or JSON format.

Create your custom query

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. Choose **Advanced queries** from the left navigation to query your resource configurations for a single account and Region or for multiple accounts and Regions.
3. To create your custom query, choose **New query**.

   To view or edit a custom query, filter a query either by the name, description, creator or tags. To filter custom queries, choose **Creater** and enter **Custom**.
4. On the **Query editor** page, create your own query for this account and Region. You can also select an appropriate aggregator to create a query for multiple accounts and Regions.
5. Edit if you wish you make changes to this query. Choose **Save Query** to save this query.
   - In the **Query Name** field, update the name of the query.
   - In the **Description** field, update the description of the query.
   - Enter up to 50 unique tags for this query.
   - Choose **Save**.
6. Choose **Run**. The query results are displayed in the table below the query editor.

7. Choose **Export as** to export the query results in CSV or JSON format.

Query Using the SQL Query Editor for Amazon Config (Amazon CLI)

The Amazon CLI is a unified tool to manage your Amazon services. With just one tool to download and configure, you can control multiple Amazon services from the command line and use scripts to automate them. For more information about the Amazon CLI and for instructions on installing the Amazon CLI tools, see the following in the *Amazon Command Line Interface User Guide*.

- Amazon Command Line Interface User Guide
- Getting Set Up with the Amazon Command Line Interface

If necessary, enter `aws configure` to configure the Amazon CLI to use an Amazon Region where advanced queries are available.

Considerations

Prerequisites

If you are using the one of the following Amazon managed policies, you will have the necessary permissions to run and save a query: AWSServiceRoleForConfig (service-linked role) or AWS_ConfigRole.

Otherwise, you must have the permissions included in the AWSConfigUserAccess Amazon managed policy.

List of properties that you can query

An updated list of properties and their data types is available in GitHub.

Advanced queries and aggregators

To run a query on an aggregator, create an aggregator. For more information, see Creating Aggregators for Amazon Config.

If you already have an aggregator set up, in the query scope, choose the aggregator to run an advanced query on that aggregator. When you select an aggregator, consider adding the Amazon

Web Services account ID and Amazon Region in the query statement to view that information in the results.

Query Resource Configuration Data

To query your resource configuration data using the query editor (Amazon CLI) for a single account and Region

1. Open a command prompt or a terminal window.
2. Enter the following command to query your resource configuration data.

```
aws configservice select-resource-config --expression "SELECT resourceId WHERE
 resourceType='AWS::EC2::Instance'"
```

Depending on your query, the output looks like the following.

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}"
    ]
}
```

To query your resource configuration data using the query editor (Amazon CLI) for multiple accounts and Regions

1. Open a command prompt or a terminal window.
2. Enter the following command to query your resource configuration data.

```
aws configservice select-aggregate-resource-config --expression "SELECT resourceId
 WHERE resourceType='AWS::EC2::Instance'" --configuration-aggregator-name my-
aggregator
```

Depending on your query, the output looks like the following.

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}"
    ]
}
```

Note

While using the `AWS::IAM::User`, `AWS::IAM::Group`, `AWS::IAM::Role`, and `AWS::IAM::Policy` resource types in an advanced query, use `awsRegion = 'global'`.

Save a Query

1. Open a command prompt or a terminal window.
2. Enter the following command to save a query.

```
aws configservice put-stored-query --stored-query "{\"QueryName\": \"cli-test\",
 \"Expression\": \"SELECT *\", \"Description\": \"cli test query\" }"
```

```
        --tags "[{ \"Key\": \"first-tag\", \"Value\": \"\" }, { \"Key\": \"second-
tag\", \"Value\": \"non-empty-tag-value\" }]"
```

3. Depending on your query, the output looks like the following.

```
{
    "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-test/
query-e65mijt4rmam5pab"
}
```

> **Note**
>
> `--tags` is optional. When you pass the tags, the saved tags will not be returned by either `list-stored-queries` or `get-stored-query`. You must use `list-tag-for-resources` to retrieve the associated tags for a saved query.
> `--description` is optional while creating or updating a query.

View all the Saved Queries

1. Enter the following command to view the list of all saved queries.

```
aws configservice list-stored-queries
```

2. Depending on your query, the output looks like the following.

```
{
    "StoredQueryMetadata": [
        {
            "QueryId": "query-e65mijt4rmam5pab",
            "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-
test/query-e65mijt4rmam5pab",
            "QueryName": "cli-test"
        },
        {
            "QueryId": "query-rltwlewlqfivadxq",
            "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-
test-2/query-rltwlewlqfivadxq",
            "QueryName": "cli-test-2",
            "Description": "cli test query"
        }
```

```
    ]
}
}
```

Get Details of a Saved Query

1. Enter the following command to get details of a specific saved query.

```
aws configservice get-stored-query --query-name cli-test
```

2. Depending on your query, the output looks like the following.

```
{
    "StoredQuery": {
        "QueryId": "query-e65mijt4rmam5pab",
        "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-test/
query-e65mijt4rmam5pab",
        "QueryName": "cli-test",
        "Description": "cli test query",
        "Expression": "SELECT *"
    }
}
```

Delete a Saved Query

- Enter the following command to delete your saved query.

```
aws configservice delete-stored-query --query-name cli-test
```

If successful, the command runs with no additional output.

Natural language query processor for Amazon Config advanced queries

The natural language query processor for advanced queries is in preview release for Amazon Config and is subject to change.

The natural language query processor for advanced queries uses Amazon Bedrock, a generative artificial intelligence (generative AI) technology which allows you to enter prompts in plain English and convert them into a ready-to-use query format. With the natural language query processor, you can query your Amazon Web Services account or across an Amazon organization.

A prompt can be a question or a statement. For example, you can enter prompts such as "Which load balancers are created after January 1, 2024?" and “List all my lambda function that is running node js 16.”

Considerations

The natural language query processor cannot do the following actions:

- Generate queries from languages other than English.
- Generate queries from prompts that do not relate to advanced queries.
- Generate queries from prompts with more than 1000 characters.
- Generate queries from follow-up corrections or from previous sessions.
- Explain code that has been generated.

Query using the natural language query processor

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. Choose **Advanced queries** from the left navigation to query your resource configurations for a single account and Region or for multiple accounts and Regions.
3. On the **Advanced queries** page, choose **New query** to go to the Query editor.
    - (Optional) To run a query on an aggregator, create an aggregator. For more information, see Creating Aggregators for Amazon Config.
    - If you've already set up an aggregator, in the query scope, choose the aggregator to run an advanced query on that aggregator. When you select an aggregator, consider adding the Amazon Web Services account ID and Amazon Region in the query statement to view that information in the results.
4. In the Query editor, go to the **Natural language query processor** section. Enter a prompt in plain English, and then choose **Generate**. For examples, see Example prompts.

5. After you generate a query, you can choose **Copy** (functionally equivalent to Ctrl+C) to copy the query to your clipboard, or choose **Populate to editor**. If populated to the editor, you can edit the generated query to fit your needs.
6. To save this query to a new query, choose **Save As**.
   - In the **Query Name** field, update the name of the query.
   - In the **Description** field, update the description of the query.
   - Enter up to 50 unique tags for this query.
   - Choose **Save**.
7. Choose **Run**. The query results display in the table below the query editor.
8. Choose **Export as** to export the query results in CSV or JSON format.

> **Note**
>
> The query results are paginated. When you export, up to 500 results are exported. You can also use the APIs to retrieve all the results. The results are paginated and you can retrieve 100 results at a time.

Example prompts

The following are prompts and the generate queries which you can use as examples.

Example: What load balancers were created after January 1, 2024?

Prompt: What load balancers were created after January 1, 2024?

Generated query:

```
SELECT
    resourceId,
    resourceType,
    resourceCreationTime
WHERE
    resourceType IN ('AWS::ElasticLoadBalancing::LoadBalancer',
 'AWS::ElasticLoadBalancingV2::LoadBalancer')
AND
    resourceCreationTime > '2024-01-01T00:00:00.0Z'
ORDER BY
```

```
    resourceCreationTime
DESC
```

Example: Which of my RDS database instances are publicly accessible?

Prompt: Which of my RDS database instances are publicly accessible?

Generated query:

```
SELECT
    resourceId,
    resourceType,
    configuration.publiclyAccessible
WHERE
    resourceType = 'AWS::RDS::DBInstance'
AND
    configuration.publiclyAccessible = true
```

Example: How many EC2 instances were created in last one year?

Prompt: How many EC2 instances were created in last one year?

Generated query:

```
SELECT
    COUNT(*)
WHERE
    resourceType = 'AWS::EC2::Instance'
AND
    resourceCreationTime
BETWEEN
    '2023-05-10T16:56:25.000Z'
AND
    '2024-05-10T16:56:25.000Z'
```

Example: How many EC2 instances do I have in each of my Amazon Web Services accounts?

Prompt: How many EC2 instances do I have in each of my Amazon Web Services accounts?

Generated query:

```
SELECT
    accountId,
```

```
    COUNT(*)
WHERE
    resourceType = 'AWS::EC2::Instance'
GROUP BY
    accountId'
```

Example: Which IAM roles have the managed policy AdministratorAccess attached?

Prompt: Which IAM roles have the managed policy AdministratorAccess attached?

Generated query:

```
SELECT
    resourceId,
    resourceName,
    resourceType
WHERE
    resourceType = 'AWS::IAM::Role'
AND
    configuration.attachedManagedPolicies.policyName = 'AdministratorAccess'
```

Example: EBS volumes without encryption

Prompt: EBS volumes without encryption

Generated query:

```
SELECT
    accountId
WHERE
    resourceType = 'AWS::EC2::Volume'
AND
    configuration.encrypted = false
```

Example: Get noncompliant resources

Prompt: Get noncompliant resources

Generated query:

```
SELECT
    resourceId,
    resourceType
```

```
WHERE
    resourceType = 'AWS::Config::ResourceCompliance'
AND
    configuration.complianceType = 'NON_COMPLIANT'
```

Example: List all my lambda function that is running node js 16

Prompt: List all my lambda function that is running node js 16

Generated query:

```
SELECT
    accountId,
    resourceName
WHERE
    resourceType = 'AWS::Lambda::Function'
AND
    configuration.runtime = 'nodejs16.x'
```

Example: What ACM certificates expire the next 30 days?

Prompt: What ACM certificates expire the next 30 days?

Generated query:

```
SELECT
    resourceId,
    configuration.domainName,
    configuration.notAfter
WHERE
    resourceType = 'AWS::ACM::Certificate'
AND
    configuration.notAfter
BETWEEN
    '2024-05-10 16:59:53'
AND
    '2024-06-10 16:59:53'
```

Note

The times in the generated query depend on the time when you enter the prompt.

Providing feedback

You can provide overall feedback about the natural language query processor or feedback about a specific generated query.

Providing feedback on the natural language query processor

Choose the **Provide feedback** button that appears above natural language query processor to the right. You can enter your satisfaction or dissatisfaction and provide feedback on how Amazon Config can make the natural language query more helpful.

> **Note**
>
> Do not disclose any personal, commercially sensitive, or confidential information.

Providing feedback on a specific generated query

You can provide your feedback on a generated query by choose the thumbs up or thumbs down button that appears below the generated query.

Region Support

The natural language query processor is supported in the following Regions.

Region Name	Region	Endpoint	Protocol
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS

Example Queries for Amazon Config

View the following example queries.

Query to list all EC2 instances with AMI ID ami-12345

Query:

```
SELECT
    resourceId,
    resourceType,
    configuration.instanceType,
    configuration.placement.tenancy,
    configuration.imageId,
    availabilityZone
WHERE
    resourceType = 'AWS::EC2::Instance'
AND
    configuration.imageId = 'ami-12345'
```

Results:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.instanceType"
            },
            {
                "Name": "configuration.placement.tenancy"
            },
            {
                "Name": "configuration.imageId"
            },
            {
                "Name": "availabilityZone"
            }
        ]
    },
    "Results": [
```

```
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2a\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t1.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2a\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}"
    ]
}
```

Query for count of resources grouped by their Amazon Config rules compliance status

Query:

```
SELECT
    configuration.complianceType,
    COUNT(*)
WHERE
    resourceType = 'AWS::Config::ResourceCompliance'
GROUP BY
    configuration.complianceType
```

Results:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "configuration.complianceType"
```

```
            },
            {
                "Name": "COUNT(*)"
            }
        ]
    },
    "Results": [
        "{\"COUNT(*)\":163,\"configuration\":{\"complianceType\":\"NON_COMPLIANT
\"}}",
        "{\"COUNT(*)\":2,\"configuration\":{\"complianceType\":\"COMPLIANT\"}}"
    ]
}
```

Query for the compliance status of Amazon Conformance packs

Query:

```
SELECT
    resourceId,
    resourceName,
    resourceType,
    configuration.complianceType
WHERE
    resourceType = 'AWS::Config::ConformancePackCompliance'
```

Results:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "resourceName"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.complianceType"
            }
        ]
```

```
    },
    "Results": [
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"COMPLIANT\"},\"resourceName\":\"MyConformancePack1\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}",
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"NON_COMPLIANT\"},\"resourceName\":\"MyConformancePack2\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}",
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"NON_COMPLIANT\"},\"resourceName\":\"MyConformancePack3\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}"
    ]
}
```

Query to get counts of Amazon resources grouped by account ID

Query:

```
aws configservice select-aggregate-resource-config --expression "SELECT COUNT(*),
 accountId group by accountId" --configuration-aggregator-name my-aggregator
```

Results:

```
{
    "Results": [
        "{\"COUNT(*)\":2407,\"accountId\":\"accountId\"}",
        "{\"COUNT(*)\":726,\"accountId\":\"accountId\"}"
    ],
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "COUNT(*)"
            },
            {
                "Name": "accountId"
            }
        ]
    }
}
```

Query to list all EC2 volumes that are not in use

Query:

```
SELECT
    resourceId,
    accountId,
    awsRegion,
    resourceType,
    configuration.volumeType,
    configuration.size,
    resourceCreationTime,
    tags,
    configuration.encrypted,
    configuration.availabilityZone,
    configuration.state.value
WHERE
    resourceType = 'AWS::EC2::Volume'
AND
    configuration.state.value = 'available'
```

Results:


```
{
    "Results": [
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0174de9c962f6581c\",
\"awsRegion\":\"us-west-2\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"us-west-2a\"},\"resourceCreationTime\":\"2020-02-21T07:39:43.771Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}",
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0cbeb652a74af2f8f\",
\"awsRegion\":\"us-east-1\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"us-east-1a\"},\"resourceCreationTime\":\"2020-02-21T07:28:40.639Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}"
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0a49952d528ec8ba2\",
\"awsRegion\":\"ap-south-1\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"ap-south-1a\"},\"resourceCreationTime\":\"2020-02-21T07:39:31.800Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}",
    ],
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
```

```
            {
                "Name": "accountId"
            },
            {
                "Name": "awsRegion"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.volumeType"
            },
            {
                "Name": "configuration.size"
            },
            {
                "Name": "resourceCreationTime"
            },
            {
                "Name": "tags"
            },
            {
                "Name": "configuration.encrypted"
            },
            {
                "Name": "configuration.availabilityZone"
            },
            {
                "Name": "configuration.state.value"
            }
        ]
    }
}
```

Example Relationship Queries for Amazon Config

View the following example relationship queries.

Find EIPs related to an EC2 instance

```
SELECT
    resourceId
```

```
WHERE
    resourceType = 'AWS::EC2::EIP'
    AND relationships.resourceId = 'i-abcd1234'
```

Find EIPs related to an EC2 network interface

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::EIP'
    AND relationships.resourceId = 'eni-abcd1234'
```

Find EC2 instances and network interfaces related to a security group

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::NetworkInterface')
    AND relationships.resourceId = 'sg-abcd1234'
```

OR

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::Instance'
    AND relationships.resourceId = 'sg-abcd1234'

SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::NetworkInterface'
    AND relationships.resourceId = 'sg-abcd1234'
```

Find EC2 instances, network ACLs, network interfaces and route tables related to a subnet

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::NetworkACL',
 'AWS::EC2::NetworkInterface', 'AWS::EC2::RouteTable')
```

```
    AND relationships.resourceId = 'subnet-abcd1234'
```

Find EC2 instances, internet gateways, network ACLs, network interfaces, route tables, subnets and security groups related to a VPC

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::InternetGateway',
 'AWS::EC2::NetworkACL', 'AWS::EC2::NetworkInterface', 'AWS::EC2::RouteTable',
 'AWS::EC2::Subnet', 'AWS::EC2::SecurityGroup')
    AND relationships.resourceId = 'vpc-abcd1234'
```

Find EC2 route tables related to a VPN gateway

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::RouteTable'
    AND relationships.resourceId = 'vgw-abcd1234'
```

Limitations

Note

Advanced query does not support querying resources which have not been configured to be recorded by the configuration recorder. Amazon Config creates Configuration Items (CIs) with `ResourceNotRecorded` in the `configurationItemStatus` when a resource has been discovered but is not configured to be recorded by the configuration recorder. While an aggregator will aggregate these CIs, advanced query does not support querying CIs with `ResourceNotRecorded`. Update your recorder settings to enable recording of the resource types that you want to query.

As a subset of SQL `SELECT`, the query syntax has following limitations:

- No support for `ALL`, `AS`, `DISTINCT`, `FROM`, `HAVING`, `JOIN`, and `UNION` keywords in a query. `NULL` value queries are not supported.

- No support for complex CASE statements for creating a priority field directly in the query.
- No support for querying on third-party resources. Third-party resources retrieved using advanced queries will have the configuration field set as NULL.
- No support for nested structures (such as tags) to be unpacked with SQL queries.
- No support for querying deleted resources. To discover deleted resources, see Looking Up Resources That Are Discovered by Amazon Config.
- The SELECT all columns shorthand (that is SELECT *) selects only the top-level, scalar properties of a CI. The scalar properties returned are `accountId`, `awsRegion`, `arn`, `availabilityZone`, `configurationItemCaptureTime`, `resourceCreationTime`, `resourceId`, `resourceName`, `resourceType`, and `version`.
- Wildcard limitations:
  - Wildcards are supported only for property values and not for property keys (for example, `...WHERE someKey LIKE 'someValue%'` is supported but `...WHERE 'someKey%' LIKE 'someValue%'` is not supported).
  - Support for only suffix wildcards (for example, `...LIKE 'AWS::EC2::%'` and `...LIKE 'AWS::EC2::_'` is supported but `...LIKE '%::EC2::Instance'` and `...LIKE '_::EC2::Instance'`is not supported).
  - Wildcard matches must be at least three characters long (for example, `...LIKE 'ab%'` and `...LIKE 'ab_'` is not allowed but `...LIKE 'abc%'` and `...LIKE 'abc_'` is allowed).

  Note

  The "_" (single underscore) is also treated as a wildcard.

- Aggregation limitations:
  - Aggregate functions can accept only a single argument or property.
  - Aggregate functions cannot take other functions as arguments.
  - GROUP BY with an ORDER BY clause referencing aggregate functions may contain only a single property.
  - For all other aggregations GROUP BY clauses may contain up to three properties.
  - Pagination is supported for all aggregate queries except when ORDER BY clause has an aggregate function. For example, GROUP BY X, ORDER BY Y does not work if Y is an aggregate function.
  - No support for HAVING clauses in aggregations.

- Mismatched identifier limitations:

  Mismatched identifiers are properties that have the same spelling but different cases (upper and lower case). Advanced query does not support processing queries that contain mismatched identifiers. For example:

  - Two properties that have the exact same spelling but with different casing (`configuration.dbclusterIdentifier` and `configuration.dBClusterIdentifier`).
  - Two properties where one property is a subset of the other, and they have different casing (`configuration.ipAddress` and `configuration.ipaddressPermissions`).

CIDR notation/IP range behavior for advanced queries

CIDR notation is converted to IP ranges for search.

This means that "=" and "BETWEEN" search for any range that includes the provided IP, instead of for an exact one.

To search for an exact IP range, you need to add in additional conditions to exclude IPs outside of the range.

Example Searching for exact CIDR block 10.0.0.0/24

```
SELECT * WHERE resourceType = 'AWS::EC2::SecurityGroup'
  AND configuration.ipPermissions.ipRanges BETWEEN '10.0.0.0'
  AND '10.0.0.255'
  AND NOT configuration.ipPermissions.ipRanges < '10.0.0.0'
  AND NOT configuration.ipPermissions.ipRanges > '10.0.0.255'
```

Example Searching for exact IP address 192.168.0.2/32

```
SELECT * WHERE resourceType = 'AWS::EC2::SecurityGroup'
  AND configuration.ipPermissions.ipRanges = '192.168.0.2'
  AND NOT configuration.ipPermissions.ipRanges > '192.168.0.2'
  AND NOT configuration.ipPermissions.ipRanges < '192.168.0.2'
```

Multiple properties within an array behavior for advanced queries

When querying against multiple properties within an array of objects, matches are computed against *all the array elements*.

For example, for a resource R with rules A and B, the resource is compliant to rule A but noncompliant to rule B. The resource R is stored as:

```
{
    configRuleList: [
        {
            configRuleName: 'A', complianceType: 'compliant'
        },
        {
            configRuleName: 'B', complianceType: 'non_compliant'
        }
    ]
}
```

R will be returned by this query:

```
SELECT configuration WHERE configuration.configRuleList.complianceType =
 'non_compliant'
AND configuration.configRuleList.configRuleName = 'A'
```

The first condition `configuration.configRuleList.complianceType = 'non_compliant'` is applied to ALL elements in R.configRuleList, because R has a rule (rule B) with complianceType = 'non_compliant', the condition is evaluated as true.

The second condition `configuration.configRuleList.configRuleName` is applied to ALL elements in R.configRuleList, because R has a rule (rule A) with configRuleName = 'A', the condition is evaluated as true. As both conditions are true, R will be returned.

Region Support

Advanced queries is supported in the following Regions:

Region Name	Region	Endpoint	Protocol	
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS	
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS	
US West (N. California)	us-west-1	config.us-west-1.amazonaws.com	HTTPS	
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS	
Africa (Cape Town)	af-south-1	config.af-south-1.amazonaws.com	HTTPS	
Asia Pacific (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS	
Asia Pacific (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS	
Asia Pacific (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS	
Asia Pacific	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS	

Region Name	Region	Endpoint	Protocol	
(Malaysia)				
Asia Pacific (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS	
Asia Pacific (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS	
Asia Pacific (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS	
Asia Pacific (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS	
Asia Pacific (Singapore)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS	
Asia Pacific (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS	
Asia Pacific (Taipei)	ap-east-2	config.ap-east-2.amazonaws.com	HTTPS	

Region Name	Region	Endpoint	Protocol	
Asia Pacific (Thailand)	ap-southeast-7	config.ap-southeast-7.amazonaws.com	HTTPS	
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS	
Canada (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS	
Canada West (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS	
China (Beijing)	cn-north-1	config.cn-north-1.amazonaws.com.cn	HTTPS	
China (Ningxia)	cn-northwest-1	config.cn-northwest-1.amazonaws.com.cn	HTTPS	
Europe (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS	
Europe (Ireland)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS	
Europe (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS	
Europe (Milan)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS	

Region Name	Region	Endpoint	Protocol	
Europe (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS	
Europe (Spain)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS	
Europe (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS	
Europe (Zurich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS	
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS	
Mexico (Central)	mx-central-1	config.mx-central-1.amazonaws.com	HTTPS	
Middle East (Bahrain)	me-south-1	config.me-south-1.amazonaws.com	HTTPS	
Middle East (UAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS	
South America (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS	

Deleting Amazon Config Data

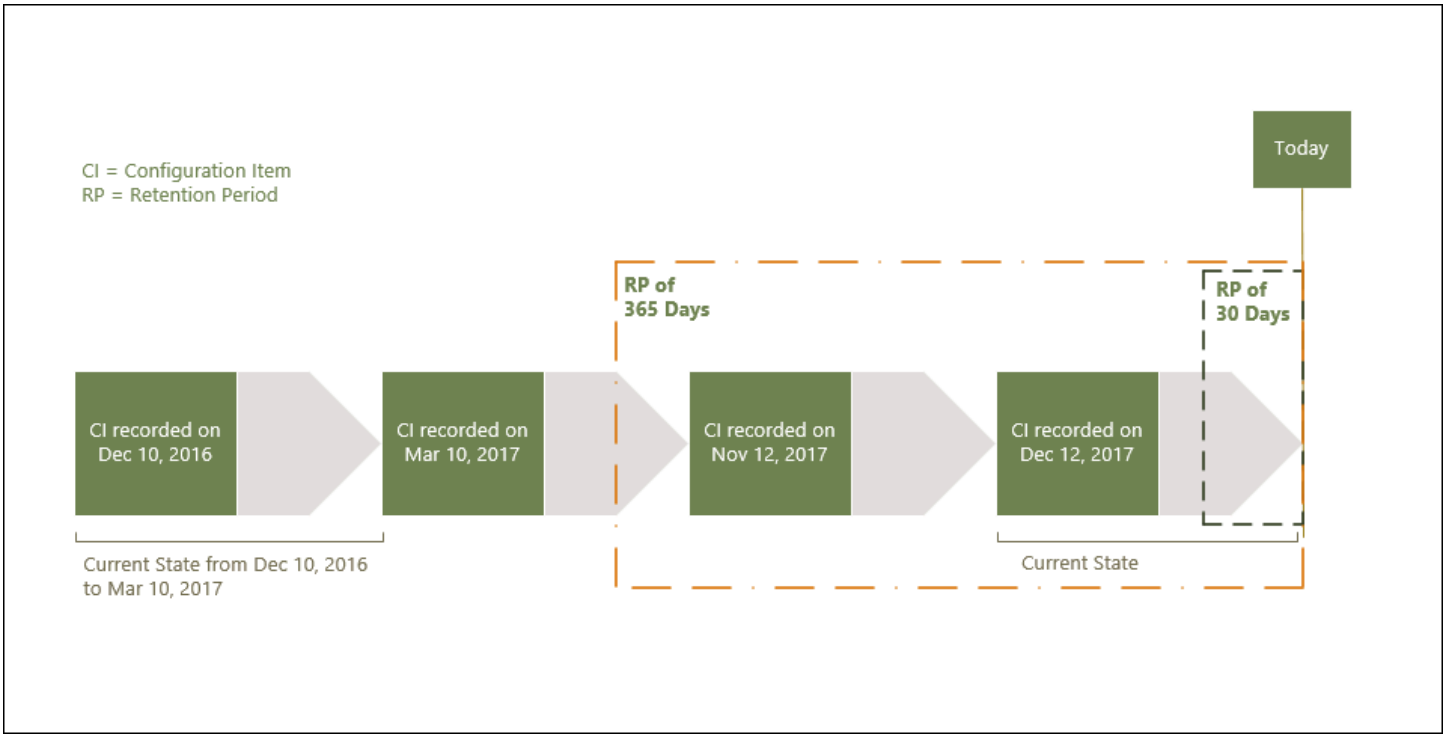
> **Note**
>
> While Amazon Config uses Amazon Simple Storage Service (Amazon S3) and Amazon Simple Notification Service (Amazon SNS) for sending configuration snapshots and configuration history files, Amazon Config has its own data store and retention policies. The information on this page is specific for Amazon Config. Amazon S3 and Amazon SNS have their own separate data store and retention policies.

Amazon Config allows you to delete your data by specifying a retention period for your `ConfigurationItems`. When you specify a retention period, Amazon Config retains your `ConfigurationItems` for that specified period. You can choose a period between a minimum of 30 days and a maximum of 7 years (2557 days). Amazon Config deletes data older than your specified retention period. If you do not specify a retention period, Amazon Config continues to store `ConfigurationItems` for the default period of 7 years (2557 days). When recording is switched on, the current state of the resource is when a `ConfigurationItem` is recorded and until the next change (a new `ConfigurationItem`) is recorded.

To understand the behavior of retention period, let's take a look at the timeline.

- When recording is switched on, the current state of a resource always exists and can't be deleted irrespective of the date the `ConfigurationItem` is recorded.
- When Amazon Config records new `ConfigurationItems`, the previous `ConfigurationItems` are deleted depending on the specified retention period.

In the following timeline, Amazon Config records `ConfigurationItems` at the following dates. For the purpose of this timeline, today is represented as May 24, 2018.



The following table explains which `ConfigurationItems` are displayed on the Amazon Config timeline based on selected retention period.

Retention Period	Configuration Items displayed on timeline	Explanation
30 days	December 12, 2017	The current state of the resource started from December 12, 2017 when the `ConfigurationItem` was recorded and is valid until today (May 24, 2018). When recording is turned on, the current state always exists.
365 days	December 12, 2017; November 12, 2017, and March 10, 2017	The retention period shows the current state December 12, 2017 and previous `ConfigurationItems` November 12, 2017 and March 10, 2017.

Retention Period	Configuration Items displayed on timeline	Explanation
		The `ConfigurationItem` for March 10, 2017 is displayed on the timeline because that configuration state represented the current state 365 days ago.

After you specify a retention period, Amazon Config APIs no longer return `ConfigurationItems` that represent a state older than the specified retention period.

Note

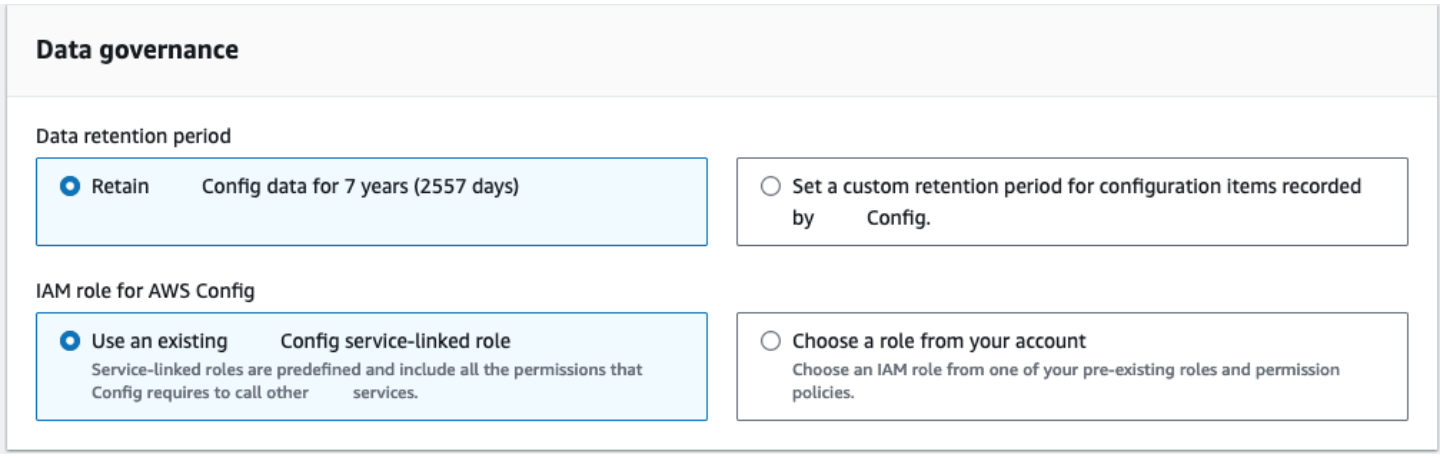
- Amazon Config cannot record your `ConfigurationItems` if recording is switched off.
- Amazon Config cannot record your `ConfigurationItems` if your IAM role has insufficient permissions. For more information, see Permissions for the IAM Role Assigned to Amazon Config.

Setting Data Retention Period in Amazon Web Services Management Console

In the Amazon Web Services Management Console, if you do not select a data retention period, the default period is 7 years or 2557 days.

To set a custom data retention period for configuration items select the checkbox. You can select 1 year, 3 years, 5 years, or a custom period. For a custom period, enter the number of days between 30 and 2557 days.

The following image displays where you can set the data retention period in **Data Governance**. You can access **Data Governance** on the **Edit Settings** page from the Amazon Config console by choosing **Settings** in the left navigation bar, and then choosing **Edit**.


Data governance
Data retention period
Retain Config data for 7 years (2557 days)
Set a custom retention period for configuration items recorded by Config.
IAM role for AWS Config
Use an existing Config service-linked role
Service-linked roles are predefined and include all the permissions that Config requires to call other services.
Choose a role from your account
Choose an IAM role from one of your pre-existing roles and permission policies.

Security in Amazon Config

Cloud security at Amazon is the highest priority. As an Amazon customer, you benefit from data centers and network architectures that are built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between Amazon and you. The shared responsibility model describes this as security *of* the cloud and security *in* the cloud:

- **Security of the cloud** – Amazon is responsible for protecting the infrastructure that runs Amazon services in the Amazon Cloud. Amazon also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the Amazon Compliance Programs. To learn about the compliance programs that apply to Amazon Config, see Amazon services in Scope by Compliance Program.
- **Security in the cloud** – Your responsibility is determined by the Amazon service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations.

This documentation helps you understand how to apply the shared responsibility model when using Amazon Config. The following topics show you how to configure Amazon Config to meet your security and compliance objectives.

Topics

- Data Protection in Amazon Config
- Identity and Access Management for Amazon Config
- Incident Response in Amazon Config
- Compliance Validation for Amazon Config
- Resilience in Amazon Config
- Infrastructure Security in Amazon Config
- Cross-service confused deputy prevention
- Security Best Practices for Amazon Config

Data Protection in Amazon Config

The Amazon shared responsibility model applies to data protection in Amazon Config. As described in this model, Amazon is responsible for protecting the global infrastructure that runs all of the Amazon Web Services Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. You are also responsible for the security configuration and management tasks for the Amazon Web Services services that you use. For more information about data privacy, see the Data Privacy FAQ.

For data protection purposes, we recommend that you protect Amazon Web Services account credentials and set up individual users with Amazon IAM Identity Center or Amazon Identity and Access Management (IAM). That way, each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with Amazon resources. We require TLS 1.2 and recommend TLS 1.3.
- Set up API and user activity logging with Amazon CloudTrail. For information about using CloudTrail trails to capture Amazon activities, see Working with CloudTrail trails in the *Amazon CloudTrail User Guide*.
- Use Amazon encryption solutions, along with all default security controls within Amazon Web Services services.
- Use advanced managed security services such as Amazon Macie, which assists in discovering and securing sensitive data that is stored in Amazon S3.
- If you require FIPS 140-3 validated cryptographic modules when accessing Amazon through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see Federal Information Processing Standard (FIPS) 140-3.

We strongly recommend that you never put confidential or sensitive information, such as your customers' email addresses, into tags or free-form text fields such as a **Name** field. This includes when you work with Amazon Config or other Amazon Web Services services using the console, API, Amazon CLI, or Amazon SDKs. Any data that you enter into tags or free-form text fields used for names may be used for billing or diagnostic logs. If you provide a URL to an external server, we strongly recommend that you do not include credentials information in the URL to validate your request to that server.

Encryption of Data at Rest

Data is encrypted at rest using transparent server-side encryption. This helps reduce the operational burden and complexity involved in protecting sensitive data. With encryption at rest, you can build security-sensitive applications that meet encryption compliance and regulatory requirements.

Encryption of Data in Transit

Data gathered and accessed by Amazon Config is exclusively over a Transport Layer Security (TLS) protected channel.

Identity and Access Management for Amazon Config

Amazon Identity and Access Management (IAM) is an Amazon Web Services service that helps an administrator securely control access to Amazon resources. IAM administrators control who can be *authenticated* (signed in) and *authorized* (have permissions) to use Amazon Config resources. IAM is an Amazon Web Services service that you can use with no additional charge.

Topics

- Audience
- Authenticating with identities
- Managing access using policies
- How Amazon Config works with IAM
- Identity-based policy examples for Amazon Config
- Amazon managed policies for Amazon Config
- Permissions for the IAM Role Assigned to Amazon Config
- Updating the IAM Role for the customer managed configuration recorder
- Permissions for the Amazon S3 Bucket for the Amazon Config Delivery Channel
- Permissions for the KMS Key for the Amazon Config Delivery Channel
- Permissions for the Amazon SNS Topic
- Troubleshooting Amazon Config identity and access
- Using Service-Linked Roles for Amazon Config

Audience

How you use Amazon Identity and Access Management (IAM) differs, depending on the work that you do in Amazon Config.

Service user – If you use the Amazon Config service to do your job, then your administrator provides you with the credentials and permissions that you need. As you use more Amazon Config features to do your work, you might need additional permissions. Understanding how access is managed can help you request the right permissions from your administrator. If you cannot access a feature in Amazon Config, see Troubleshooting Amazon Config identity and access.

Service administrator – If you're in charge of Amazon Config resources at your company, you probably have full access to Amazon Config. It's your job to determine which Amazon Config features and resources your service users should access. You must then submit requests to your IAM administrator to change the permissions of your service users. Review the information on this page to understand the basic concepts of IAM. To learn more about how your company can use IAM with Amazon Config, see How Amazon Config works with IAM.

IAM administrator – If you're an IAM administrator, you might want to learn details about how you can write policies to manage access to Amazon Config. To view example Amazon Config identity-based policies that you can use in IAM, see Identity-based policy examples for Amazon Config.

Authenticating with identities

Authentication is how you sign in to Amazon using your identity credentials. You must be *authenticated* (signed in to Amazon) as the Amazon Web Services account root user, as an IAM user, or by assuming an IAM role.

If you access Amazon programmatically, Amazon provides a software development kit (SDK) and a command line interface (CLI) to cryptographically sign your requests by using your credentials. If you don't use Amazon tools, you must sign requests yourself. For more information about using the recommended method to sign requests yourself, see Amazon Signature Version 4 for API requests in the *IAM User Guide*.

Regardless of the authentication method that you use, you might be required to provide additional security information. For example, Amazon recommends that you use multi-factor authentication (MFA) to increase the security of your account. To learn more, see Amazon Multi-factor authentication in IAM in the *IAM User Guide*.

Amazon Web Services account root user

When you create an Amazon Web Services account, you begin with one sign-in identity that has complete access to all Amazon Web Services services and resources in the account. This identity is called the Amazon Web Services account *root user* and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you don't use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform. For the complete list of tasks that require you to sign in as the root user, see Tasks that require root user credentials in the *IAM User Guide*.

Federated identity

As a best practice, require human users, including users that require administrator access, to use federation with an identity provider to access Amazon Web Services services by using temporary credentials.

A *federated identity* is a user from your enterprise user directory, a web identity provider, the Amazon Directory Service, or any user that accesses Amazon Web Services services by using credentials provided through an identity source. When federated identities access Amazon Web Services accounts, they assume roles, and the roles provide temporary credentials.

IAM users and groups

An *IAM user* is an identity within your Amazon Web Services account that has specific permissions for a single person or application. Where possible, we recommend relying on temporary credentials instead of creating IAM users who have long-term credentials such as passwords and access keys. However, if you have specific use cases that require long-term credentials with IAM users, we recommend that you rotate access keys. For more information, see Rotate access keys regularly for use cases that require long-term credentials in the *IAM User Guide*.

An *IAM group* is an identity that specifies a collection of IAM users. You can't sign in as a group. You can use groups to specify permissions for multiple users at a time. Groups make permissions easier to manage for large sets of users. For example, you could have a group named *IAMAdmins* and give that group permissions to administer IAM resources.

Users are different from roles. A user is uniquely associated with one person or application, but a role is intended to be assumable by anyone who needs it. Users have permanent long-term credentials, but roles provide temporary credentials. To learn more, see Use cases for IAM users in the *IAM User Guide*.

IAM roles

An *IAM role* is an identity within your Amazon Web Services account that has specific permissions. It is similar to an IAM user, but is not associated with a specific person. To temporarily assume an IAM role in the Amazon Web Services Management Console, you can switch from a user to an IAM role (console). You can assume a role by calling an Amazon CLI or Amazon API operation or by using a custom URL. For more information about methods for using roles, see Methods to assume a role in the *IAM User Guide*.

IAM roles with temporary credentials are useful in the following situations:

- **Federated user access** – To assign permissions to a federated identity, you create a role and define permissions for the role. When a federated identity authenticates, the identity is associated with the role and is granted the permissions that are defined by the role. For information about roles for federation, see Create a role for a third-party identity provider (federation) in the *IAM User Guide*.
- **Temporary IAM user permissions** – An IAM user or role can assume an IAM role to temporarily take on different permissions for a specific task.
- **Cross-account access** – You can use an IAM role to allow someone (a trusted principal) in a different account to access resources in your account. Roles are the primary way to grant cross-account access. However, with some Amazon Web Services services, you can attach a policy directly to a resource (instead of using a role as a proxy). To learn the difference between roles and resource-based policies for cross-account access, see Cross account resource access in IAM in the *IAM User Guide*.
- **Cross-service access** – Some Amazon Web Services services use features in other Amazon Web Services services. For example, when you make a call in a service, it's common for that service to run applications in Amazon EC2 or store objects in Amazon S3. A service might do this using the calling principal's permissions, using a service role, or using a service-linked role.
  - **Forward access sessions (FAS)** – When you use an IAM user or role to perform actions in Amazon, you are considered a principal. When you use some services, you might perform an action that then initiates another action in a different service. FAS uses the permissions of the principal calling an Amazon Web Services service, combined with the requesting Amazon Web Services service to make requests to downstream services. FAS requests are only made when a service receives a request that requires interactions with other Amazon Web Services services or resources to complete. In this case, you must have permissions to perform both actions. For policy details when making FAS requests, see Forward access sessions.

- **Service role** – A service role is an IAM role that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see Create a role to delegate permissions to an Amazon Web Services service in the *IAM User Guide*.
- **Service-linked role** – A service-linked role is a type of service role that is linked to an Amazon Web Services service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your Amazon Web Services account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.

- **Applications running on Amazon EC2** – You can use an IAM role to manage temporary credentials for applications that are running on an EC2 instance and making Amazon CLI or Amazon API requests. This is preferable to storing access keys within the EC2 instance. To assign an Amazon role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. An instance profile contains the role and enables programs that are running on the EC2 instance to get temporary credentials. For more information, see Use an IAM role to grant permissions to applications running on Amazon EC2 instances in the *IAM User Guide*.

Managing access using policies

You control access in Amazon by creating policies and attaching them to Amazon identities or resources. A policy is an object in Amazon that, when associated with an identity or resource, defines their permissions. Amazon evaluates these policies when a principal (user, root user, or role session) makes a request. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in Amazon as JSON documents. For more information about the structure and contents of JSON policy documents, see Overview of JSON policies in the *IAM User Guide*.

Administrators can use Amazon JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

By default, users and roles have no permissions. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies. The administrator can then add the IAM policies to roles, and users can assume the roles.

IAM policies define permissions for an action regardless of the method that you use to perform the operation. For example, suppose that you have a policy that allows the `iam:GetRole` action.

A user with that policy can get role information from the Amazon Web Services Management Console, the Amazon CLI, or the Amazon API.

Identity-based policies

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Define custom IAM permissions with customer managed policies in the *IAM User Guide*.

Identity-based policies can be further categorized as *inline policies* or *managed policies*. Inline policies are embedded directly into a single user, group, or role. Managed policies are standalone policies that you can attach to multiple users, groups, and roles in your Amazon Web Services account. Managed policies include Amazon managed policies and customer managed policies. To learn how to choose between a managed policy or an inline policy, see Choose between managed policies and inline policies in the *IAM User Guide*.

Resource-based policies

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are IAM *role trust policies* and Amazon S3 *bucket policies*. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must specify a principal in a resource-based policy. Principals can include accounts, users, roles, federated users, or Amazon Web Services services.

Resource-based policies are inline policies that are located in that service. You can't use Amazon managed policies from IAM in a resource-based policy.

Access control lists (ACLs)

Access control lists (ACLs) control which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format.

Amazon S3, Amazon WAF, and Amazon VPC are examples of services that support ACLs. To learn more about ACLs, see Access control list (ACL) overview in the *Amazon Simple Storage Service Developer Guide*.

Other policy types

Amazon supports additional, less-common policy types. These policy types can set the maximum permissions granted to you by the more common policy types.

- **Permissions boundaries** – A permissions boundary is an advanced feature in which you set the maximum permissions that an identity-based policy can grant to an IAM entity (IAM user or role). You can set a permissions boundary for an entity. The resulting permissions are the intersection of an entity's identity-based policies and its permissions boundaries. Resource-based policies that specify the user or role in the `Principal` field are not limited by the permissions boundary. An explicit deny in any of these policies overrides the allow. For more information about permissions boundaries, see Permissions boundaries for IAM entities in the *IAM User Guide*.
- **Service control policies (SCPs)** – SCPs are JSON policies that specify the maximum permissions for an organization or organizational unit (OU) in Amazon Organizations. Amazon Organizations is a service for grouping and centrally managing multiple Amazon Web Services accounts that your business owns. If you enable all features in an organization, then you can apply service control policies (SCPs) to any or all of your accounts. The SCP limits permissions for entities in member accounts, including each Amazon Web Services account root user. For more information about Organizations and SCPs, see Service control policies in the *Amazon Organizations User Guide*.
- **Resource control policies (RCPs)** – RCPs are JSON policies that you can use to set the maximum available permissions for resources in your accounts without updating the IAM policies attached to each resource that you own. The RCP limits permissions for resources in member accounts and can impact the effective permissions for identities, including the Amazon Web Services account root user, regardless of whether they belong to your organization. For more information about Organizations and RCPs, including a list of Amazon Web Services services that support RCPs, see Resource control policies (RCPs) in the *Amazon Organizations User Guide*.
- **Session policies** – Session policies are advanced policies that you pass as a parameter when you programmatically create a temporary session for a role or federated user. The resulting session's permissions are the intersection of the user or role's identity-based policies and the session policies. Permissions can also come from a resource-based policy. An explicit deny in any of these policies overrides the allow. For more information, see Session policies in the *IAM User Guide*.

Multiple policy types

When multiple types of policies apply to a request, the resulting permissions are more complicated to understand. To learn how Amazon determines whether to allow a request when multiple policy types are involved, see Policy evaluation logic in the *IAM User Guide*.

How Amazon Config works with IAM

Before you use IAM to manage access to Amazon Config, learn what IAM features are available to use with Amazon Config.

IAM features you can use with Amazon Config

IAM feature	Amazon Config support
Identity-based policies	Yes
Resource-based policies	No
Policy actions	Yes
Policy resources	Yes
Policy condition keys (service-specific)	Yes
ACLs	No
ABAC (tags in policies)	Yes
Temporary credentials	Yes
Forward access sessions (FAS)	Yes
Service roles	Yes
Service-linked roles	Yes

To get a high-level view of how Amazon Config and other Amazon services work with most IAM features, see Amazon services that work with IAM in the *IAM User Guide*.

Identity-based policies for Amazon Config

Supports identity-based policies: Yes

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Define custom IAM permissions with customer managed policies in the *IAM User Guide*.

With IAM identity-based policies, you can specify allowed or denied actions and resources as well as the conditions under which actions are allowed or denied. You can't specify the principal in an identity-based policy because it applies to the user or role to which it is attached. To learn about all of the elements that you can use in a JSON policy, see IAM JSON policy elements reference in the *IAM User Guide*.

Identity-based policy examples for Amazon Config

To view examples of Amazon Config identity-based policies, see Identity-based policy examples for Amazon Config.

Resource-based policies within Amazon Config

Supports resource-based policies: No

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are IAM *role trust policies* and Amazon S3 *bucket policies*. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must specify a principal in a resource-based policy. Principals can include accounts, users, roles, federated users, or Amazon Web Services services.

To enable cross-account access, you can specify an entire account or IAM entities in another account as the principal in a resource-based policy. Adding a cross-account principal to a resource-based policy is only half of establishing the trust relationship. When the principal and the resource are in different Amazon Web Services accounts, an IAM administrator in the trusted account must also grant the principal entity (user or role) permission to access the resource. They grant permission by attaching an identity-based policy to the entity. However, if a resource-based policy grants access to a principal in the same account, no additional identity-based policy is required. For more information, see Cross account resource access in IAM in the *IAM User Guide*.

Policy actions for Amazon Config

Supports policy actions: Yes

Administrators can use Amazon JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Action` element of a JSON policy describes the actions that you can use to allow or deny access in a policy. Policy actions usually have the same name as the associated Amazon API operation. There are some exceptions, such as *permission-only actions* that don't have a matching API operation. There are also some operations that require multiple actions in a policy. These additional actions are called *dependent actions*.

Include actions in a policy to grant permissions to perform the associated operation.

To see a list of Amazon Config actions, see Actions defined by Amazon Config in the *Service Authorization Reference*.

Policy actions in Amazon Config use the following prefix before the action:

```
config
```

To specify multiple actions in a single statement, separate them with commas.

```
"Action": [
      "config:action1",
      "config:action2"
         ]
```

You can specify multiple actions using wildcards (*). For example, to specify all actions that begin with the word `Describe`, include the following action:

```
"Action": "config:Describe*"
```

To view examples of Amazon Config identity-based policies, see Identity-based policy examples for Amazon Config.

Policy resources for Amazon Config

Supports policy resources: Yes

Administrators can use Amazon JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Resource` JSON policy element specifies the object or objects to which the action applies. Statements must include either a `Resource` or a `NotResource` element. As a best practice, specify a resource using its Amazon Resource Name (ARN). You can do this for actions that support a specific resource type, known as *resource-level permissions*.

For actions that don't support resource-level permissions, such as listing operations, use a wildcard (*) to indicate that the statement applies to all resources.

```
"Resource": "*"
```

To see a list of Amazon Config resource types and their ARNs, see Resources defined by Amazon Config in the *Service Authorization Reference*. To learn with which actions you can specify the ARN of each resource, see Actions defined by Amazon Config.

To view examples of Amazon Config identity-based policies, see Identity-based policy examples for Amazon Config.

Policy condition keys for Amazon Config

Supports service-specific policy condition keys: Yes

Administrators can use Amazon JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Condition` element (or `Condition` *block*) lets you specify conditions in which a statement is in effect. The `Condition` element is optional. You can create conditional expressions that use condition operators, such as equals or less than, to match the condition in the policy with values in the request.

If you specify multiple `Condition` elements in a statement, or multiple keys in a single `Condition` element, Amazon evaluates them using a logical `AND` operation. If you specify multiple values for a single condition key, Amazon evaluates the condition using a logical `OR` operation. All of the conditions must be met before the statement's permissions are granted.

You can also use placeholder variables when you specify conditions. For example, you can grant an IAM user permission to access a resource only if it is tagged with their IAM user name. For more information, see IAM policy elements: variables and tags in the *IAM User Guide*.

Amazon supports global condition keys and service-specific condition keys. To see all Amazon global condition keys, see Amazon global condition context keys in the *IAM User Guide*.

To see a list of Amazon Config condition keys, see Condition keys for Amazon Config in the *Service Authorization Reference*. To learn with which actions and resources you can use a condition key, see Actions defined by Amazon Config.

To view examples of Amazon Config identity-based policies, see Identity-based policy examples for Amazon Config.

ACLs in Amazon Config

Supports ACLs: No

Access control lists (ACLs) control which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format.

ABAC with Amazon Config

Supports ABAC (tags in policies): Yes

Attribute-based access control (ABAC) is an authorization strategy that defines permissions based on attributes. In Amazon, these attributes are called *tags*. You can attach tags to IAM entities (users or roles) and to many Amazon resources. Tagging entities and resources is the first step of ABAC. Then you design ABAC policies to allow operations when the principal's tag matches the tag on the resource that they are trying to access.

ABAC is helpful in environments that are growing rapidly and helps with situations where policy management becomes cumbersome.

To control access based on tags, you provide tag information in the condition element of a policy using the `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, or `aws:TagKeys` condition keys.

If a service supports all three condition keys for every resource type, then the value is **Yes** for the service. If a service supports all three condition keys for only some resource types, then the value is **Partial**.

For more information about ABAC, see Define permissions with ABAC authorization in the *IAM User Guide*. To view a tutorial with steps for setting up ABAC, see Use attribute-based access control (ABAC) in the *IAM User Guide*.

For more information about tagging Amazon Config resources, see Tagging Your Amazon Config Resources.

Using temporary credentials with Amazon Config

Supports temporary credentials: Yes

Some Amazon Web Services services don't work when you sign in using temporary credentials. For additional information, including which Amazon Web Services services work with temporary credentials, see Amazon Web Services services that work with IAM in the *IAM User Guide*.

You are using temporary credentials if you sign in to the Amazon Web Services Management Console using any method except a user name and password. For example, when you access Amazon using your company's single sign-on (SSO) link, that process automatically creates temporary credentials. You also automatically create temporary credentials when you sign in to the console as a user and then switch roles. For more information about switching roles, see Switch from a user to an IAM role (console) in the *IAM User Guide*.

You can manually create temporary credentials using the Amazon CLI or Amazon API. You can then use those temporary credentials to access Amazon. Amazon recommends that you dynamically generate temporary credentials instead of using long-term access keys. For more information, see Temporary security credentials in IAM.

Forward access sessions for Amazon Config

Supports forward access sessions (FAS): Yes

When you use an IAM user or role to perform actions in Amazon, you are considered a principal. When you use some services, you might perform an action that then initiates another action in a different service. FAS uses the permissions of the principal calling an Amazon Web Services service, combined with the requesting Amazon Web Services service to make requests to downstream services. FAS requests are only made when a service receives a request that requires interactions with other Amazon Web Services services or resources to complete. In this case, you must have permissions to perform both actions. For policy details when making FAS requests, see Forward access sessions.

Service roles for Amazon Config

Supports service roles: Yes

A service role is an IAM role that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see Create a role to delegate permissions to an Amazon Web Services service in the *IAM User Guide*.

> **Warning**
>
> Changing the permissions for a service role might break Amazon Config functionality. Edit service roles only when Amazon Config provides guidance to do so.

Service-linked roles for Amazon Config

Supports service-linked roles: Yes

A service-linked role is a type of service role that is linked to an Amazon Web Services service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your Amazon Web Services account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.

For details about creating or managing Amazon Config service-linked roles, see Using Service-Linked Roles for Amazon Config.

For details about creating or managing service-linked roles, see Amazon services that work with IAM. Find a service in the table that includes a `Yes` in the **Service-linked role** column. Choose the **Yes** link to view the service-linked role documentation for that service.

Identity-based policy examples for Amazon Config

By default, users and roles don't have permission to create or modify Amazon Config resources. They also can't perform tasks by using the Amazon Web Services Management Console, Amazon Command Line Interface (Amazon CLI), or Amazon API. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies. The administrator can then add the IAM policies to roles, and users can assume the roles.

To learn how to create an IAM identity-based policy by using these example JSON policy documents, see Create IAM policies (console) in the *IAM User Guide*.

For details about actions and resource types defined by Amazon Config, including the format of the ARNs for each of the resource types, see Actions, resources, and condition keys for Amazon Config in the *Service Authorization Reference*.

Topics

- Policy best practices
- Sign up for an Amazon Web Services account
- Secure IAM users
- Using the Amazon Config console
- Allow users to view their own permissions
- Read-only access to Amazon Config
- Full access to Amazon Config
- Supported Resource-Level Permissions for Amazon Config Rule API Actions
- Supported Resource-Level Permissions for Multi-Account Multi-Region Data Aggregation

Policy best practices

Identity-based policies determine whether someone can create, access, or delete Amazon Config resources in your account. These actions can incur costs for your Amazon Web Services account. When you create or edit identity-based policies, follow these guidelines and recommendations:

- **Get started with Amazon managed policies and move toward least-privilege permissions** – To get started granting permissions to your users and workloads, use the *Amazon managed policies* that grant permissions for many common use cases. They are available in your Amazon Web Services account. We recommend that you reduce permissions further by defining Amazon customer managed policies that are specific to your use cases. For more information, see Amazon managed policies or Amazon managed policies for job functions in the *IAM User Guide*.
- **Apply least-privilege permissions** – When you set permissions with IAM policies, grant only the permissions required to perform a task. You do this by defining the actions that can be taken on specific resources under specific conditions, also known as *least-privilege permissions*. For more information about using IAM to apply permissions, see Policies and permissions in IAM in the *IAM User Guide*.
- **Use conditions in IAM policies to further restrict access** – You can add a condition to your policies to limit access to actions and resources. For example, you can write a policy condition to specify that all requests must be sent using SSL. You can also use conditions to grant access to service actions if they are used through a specific Amazon Web Services service, such as Amazon CloudFormation. For more information, see IAM JSON policy elements: Condition in the *IAM User Guide*.

- **Use IAM Access Analyzer to validate your IAM policies to ensure secure and functional permissions** – IAM Access Analyzer validates new and existing policies so that the policies adhere to the IAM policy language (JSON) and IAM best practices. IAM Access Analyzer provides more than 100 policy checks and actionable recommendations to help you author secure and functional policies. For more information, see Validate policies with IAM Access Analyzer in the *IAM User Guide*.
- **Require multi-factor authentication (MFA)** – If you have a scenario that requires IAM users or a root user in your Amazon Web Services account, turn on MFA for additional security. To require MFA when API operations are called, add MFA conditions to your policies. For more information, see Secure API access with MFA in the *IAM User Guide*.

For more information about best practices in IAM, see Security best practices in IAM in the *IAM User Guide*.

Sign up for an Amazon Web Services account

If you do not have an Amazon Web Services account, use the following procedure to create one.

To sign up for Amazon Web Services

1. Open http://www.amazonaws.cn/ and choose **Sign Up**.
2. Follow the on-screen instructions.

Amazon sends you a confirmation email after the sign-up process is complete. At any time, you can view your current account activity and manage your account by going to http://www.amazonaws.cn/ and choosing **My Account**.

Secure IAM users

After you sign up for an Amazon Web Services account, safeguard your administrative user by turning on multi-factor authentication (MFA). For instructions, see Enable a virtual MFA device for an IAM user (console) in the *IAM User Guide*.

To give other users access to your Amazon Web Services account resources, create IAM users. To secure your IAM users, turn on MFA and only give the IAM users the permissions needed to perform their tasks.

For more information about creating and securing IAM users, see the following topics in the *IAM User Guide*:

- Creating an IAM user in your Amazon Web Services account
- Access management for Amazon resources
- Example IAM identity-based policies

Using the Amazon Config console

To access the Amazon Config console, you must have a minimum set of permissions. These permissions must allow you to list and view details about the Amazon Config resources in your Amazon Web Services account. If you create an identity-based policy that is more restrictive than the minimum required permissions, the console won't function as intended for entities (users or roles) with that policy.

You don't need to allow minimum console permissions for users that are making calls only to the Amazon CLI or the Amazon API. Instead, allow access to only the actions that match the API operation that they're trying to perform.

To ensure that users and roles can still use the Amazon Config console, also attach the Amazon Config `AWSConfigUserAccess` Amazon managed policy to the entities. For more information, see Adding permissions to a user in the *IAM User Guide*.

You must give users permissions to interact with Amazon Config. For users who need full access to Amazon Config, use the Full access to Amazon Config managed policy.

To provide access, add permissions to your users, groups, or roles:

- Users managed in IAM through an identity provider:

  Create a role for identity federation. Follow the instructions in Create a role for a third-party identity provider (federation) in the *IAM User Guide*.
- IAM users:
  - Create a role that your user can assume. Follow the instructions in Create a role for an IAM user in the *IAM User Guide*.
  - (Not recommended) Attach a policy directly to a user or add a user to a user group. Follow the instructions in Adding permissions to a user (console) in the *IAM User Guide*.

Allow users to view their own permissions

This example shows how you might create a policy that allows IAM users to view the inline and managed policies that are attached to their user identity. This policy includes permissions to complete this action on the console or programmatically using the Amazon CLI or Amazon API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws-cn:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Read-only access to Amazon Config

The following example shows an Amazon managed policy, `AWSConfigUserAccess` that grants read-only access to Amazon Config.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "config:Get*",
        "config:Describe*",
        "config:Deliver*",
        "config:List*",
        "config:Select*",
        "tag:GetResources",
        "tag:GetTagKeys",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

In the policy statements, the `Effect` element specifies whether the actions are allowed or denied. The `Action` element lists the specific actions that the user is allowed to perform. The `Resource` element lists the Amazon resources the user is allowed to perform those actions on. For policies that control access to Amazon Config actions, the `Resource` element is always set to `*`, a wildcard that means "all resources."

The values in the `Action` element correspond to the APIs that the services support. The actions are preceded by `config:` to indicate that they refer to Amazon Config actions. You can use the `*` wildcard character in the `Action` element, such as in the following examples:

- `"Action": ["config:*ConfigurationRecorder"]`

  This allows all Amazon Config actions that end with "ConfigurationRecorder" (`StartConfigurationRecorder`, `StopConfigurationRecorder`).

- `"Action": ["config:*"]`

  This allows all Amazon Config actions, but not actions for other Amazon services.

- `"Action": ["*"]`

  This allows all Amazon actions. This permission is suitable for a user who acts as an Amazon administrator for your account.

The read-only policy doesn't grant user permission for the actions such as `StartConfigurationRecorder`, `StopConfigurationRecorder`, and `DeleteConfigurationRecorder`. Users with this policy are not allowed to start configuration recorder, stop configuration recorder, or delete configuration recorder. For the list of Amazon Config actions, see the Amazon Config API Reference.

Full access to Amazon Config

The following example shows a policy that grants full access to Amazon Config. It grants users the permission to perform all Amazon Config actions. It also lets users manage files in Amazon S3 buckets and manage Amazon SNS topics in the account that the user is associated with.

> **Important**
>
> This policy grants broad permissions. Before granting full access, consider starting with a minimum set of permissions and granting additional permissions as necessary. Doing so is better practice than starting with permissions that are too lenient and then trying to tighten them later.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sns:AddPermission",
                "sns:CreateTopic",
                "sns:DeleteTopic",
                "sns:GetTopicAttributes",
                "sns:ListPlatformApplications",
```

```
                "sns:ListTopics",
                "sns:SetTopicAttributes"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:GetBucketAcl",
                "s3:GetBucketLocation",
                "s3:GetBucketNotification",
                "s3:GetBucketPolicy",
                "s3:GetBucketRequestPayment",
                "s3:GetBucketVersioning",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
                "s3:ListBucketVersions",
                "s3:PutBucketPolicy"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:ListRolePolicies",
                "iam:ListRoles",
                "iam:PutRolePolicy",
                "iam:AttachRolePolicy",
                "iam:CreatePolicy",
                "iam:CreatePolicyVersion",
                "iam:DeletePolicyVersion",
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
```

```
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "config.amazonaws.com",
                        "ssm.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:LookupEvents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "config:*",
                "tag:Get*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeDocument",
                "ssm:GetDocument",
                "ssm:DescribeAutomationExecutions",
                "ssm:GetAutomationExecution",
                "ssm:ListDocuments",
                "ssm:StartAutomationExecution"
            ],
            "Resource": "*"
        }

    ]
}
```

Supported Resource-Level Permissions for Amazon Config Rule API Actions

Resource-level permissions refers to the ability to specify which resources users are allowed to perform actions on. Amazon Config supports resource-level permissions for certain Amazon Config rule API actions. This means that for certain Amazon Config rule actions, you can control the conditions under which when users are allowed to use those actions. These conditions can be actions that must be fulfilled, or specific resources that users are allowed to use.

The following table describes the Amazon Config rule API actions that currently support resource-level permissions. It also describes the supported resources and their ARNs for each action. When specifying an ARN, you can use the * wildcard in your paths; for example, when you cannot or do not want to specify exact resource IDs.

> **Important**
>
> If an Amazon Config rule API action is not listed in this table, then it does not support resource-level permissions. If an Amazon Config rule action does not support resource-level permissions, you can grant users permissions to use the action, but you have to specify a * for the resource element of your policy statement.

API Action	Resources
DeleteConfigRule	Config Rule arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
DeleteEvaluationResults	Config Rule arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
DescribeCompliance ByConfigRule	Config Rule arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*

API Action	Resources
DescribeConfigRuleEvaluationStatus	Config Rule arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
GetComplianceDetailsByConfigRule	Config Rule arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
PutConfigRule	Config Rule arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
StartConfigRulesEvaluation	Config Rule arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
PutRemediationConfigurations	Remediation Configuration arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*
DescribeRemediationConfigurations	Remediation Configuration arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*
DeleteRemediationConfiguration	Remediation Configuration arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*

API Action	Resources
PutRemediationExceptions	Remediation Configuration arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*
DescribeRemediationExceptions	Remediation Configuration arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*
DeleteRemediationExceptions	Remediation Configuration arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*

For example, you want to allow read access and deny write access to specific rules to specific users.

In the first policy, you allow the Amazon Config rule read actions such as `DescribeConfigRuleEvaluationStatus` on the specified rules.

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "VisualEditor0",
                "Effect": "Allow",
                "Action": [
                    "config:StartConfigRulesEvaluation",
                    "config:DescribeComplianceByConfigRule",
                    "config:DescribeConfigRuleEvaluationStatus",
                    "config:GetComplianceDetailsByConfigRule"
                ],
                "Resource": [
                    "arn:aws:config:region:accountID:config-rule/config-rule-ID",
                    "arn:aws:config:region:accountID:config-rule/config-rule-ID"
```

```
                ]
            }
        ]
    }
```

In the second policy, you deny the Amazon Config rule write actions on the specific rule.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": [
                "config:PutConfigRule",
                "config:DeleteConfigRule",
                "config:DeleteEvaluationResults"
               ],
            "Resource": "arn:aws:config:region:accountID:config-rule/config-rule-ID"
           }
      ]
   }
```

With resource-level permissions, you can allow read access and deny write access to perform specific actions on Amazon Config rule API actions.

Supported Resource-Level Permissions for Multi-Account Multi-Region Data Aggregation

You can use resource-level permissions to control a user's ability to perform specific actions on multi-account multi-region data aggregation. The following Amazon Config `Aggregator` APIs support resource level permissions:

- BatchGetAggregateResourceConfig
- DeleteConfigurationAggregator
- DescribeAggregateComplianceByConfigRules
- DescribeAggregateComplianceByConformancePacks
- DescribeConfigurationAggregatorSourcesStatus
- GetAggregateComplianceDetailsByConfigRule

- GetAggregateConfigRuleComplianceSummary
- GetAggregateConformancePackComplianceSummary
- GetAggregateDiscoveredResourceCounts
- GetAggregateResourceConfig
- ListAggregateDiscoveredResources
- PutConfigurationAggregator
- SelectAggregateResourceConfig

For example, you can restrict access to resource data from specific users by creating two aggregators `AccessibleAggregator` and `InAccessibleAggregator` and attaching an IAM policy that allows access to `AccessibleAggregator` but denies access to `InAccessibleAggregator`.

IAM Policy for AccessibleAggregator

In this policy, you allow access to the supported aggregator actions for the Amazon Config Amazon Resource Name (ARN) that you specify. In this example, the Amazon Config ARN is `arn:aws:config:ap-northeast-1:`*`AccountID`*`:config-aggregator/config-aggregator-mocpsqhs`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigAllow",
            "Effect": "Allow",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
```

```
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-aggregator/
config-aggregator-mocpsqhs"
        }
    ]
}
```

IAM Policy for InAccessibleAggregator

In this policy, you deny access to the supported aggregator actions for the Amazon Config ARN that you specify. In this example, the Amazon Config ARN is `arn:aws:config:ap-northeast-1:`*`AccountID`*`:config-aggregator/config-aggregator-pokxzldx`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigDeny",
            "Effect": "Deny",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-aggregator/
config-aggregator-pokxzldx"
        }
    ]
}
```

If a user of the developer group tries to perform any of these actions on the Amazon Config ARN that you specified, that user will get an access denied exception.

Checking User Access Permissions

To show the aggregators that you have created, run the following Amazon CLI command:

```
aws configservice describe-configuration-aggregators
```

When command has successfully completed, you will be able to see the details for all the aggregators associated with your account. In this example, those are `AccessibleAggregator` and `InAccessibleAggregator`:

```
{
    "ConfigurationAggregators": [
        {
            "ConfigurationAggregatorArn": "arn:aws:config:ap-
northeast-1:AccountID:config-aggregator/config-aggregator-mocpsqhs",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "AccessibleAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        },
        {
            "ConfigurationAggregatorArn": "arn:aws:config:ap-
northeast-1:AccountID:config-aggregator/config-aggregator-pokxzldx",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "InAccessibleAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
```

```
            ],
            "LastUpdatedTime": 1517942461.455
        }
    ]
}
```

> **Note**
>
> For `account-aggregation-sources` enter a comma-separated list of Amazon account IDs for which you want to aggregate data. Wrap the account IDs in square brackets, and be sure to escape quotation marks (for example, `"[{\"AccountIds\": [\"AccountID1\",\"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"`).

Attach the following IAM policy to deny access to `InAccessibleAggregator`, or the aggregator to which you want to deny access.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigDeny",
            "Effect": "Deny",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-aggregator/
config-aggregator-pokxzldx"
```

```
        }
    ]
}
```

Next, you can confirm that the IAM policy works for restricting access to rules for a specific aggregator:

```
aws configservice get-aggregate-compliance-details-by-config-rule --configuration-
aggregator-name InAccessibleAggregator --config-rule-name rule name --account-
id AccountID --aws-region AwsRegion
```

The command should return an access denied exception:

```
An error occurred (AccessDeniedException) when calling the
 GetAggregateComplianceDetailsByConfigRule operation: User:
 arn:aws:iam::AccountID:user/ is not
authorized to perform: config:GetAggregateComplianceDetailsByConfigRule on resource:
 arn:aws:config:AwsRegion-1:AccountID:config-aggregator/config-aggregator-pokxzldx
```

Amazon managed policies for Amazon Config

An Amazon managed policy is a standalone policy that is created and administered by Amazon. Amazon managed policies are designed to provide permissions for many common use cases so that you can start assigning permissions to users, groups, and roles.

Keep in mind that Amazon managed policies might not grant least-privilege permissions for your specific use cases because they're available for all Amazon customers to use. We recommend that you reduce permissions further by defining customer managed policies that are specific to your use cases.

You cannot change the permissions defined in Amazon managed policies. If Amazon updates the permissions defined in an Amazon managed policy, the update affects all principal identities (users, groups, and roles) that the policy is attached to. Amazon is most likely to update an Amazon managed policy when a new Amazon Web Services service is launched or new API operations become available for existing services.

For more information, see Amazon managed policies in the *IAM User Guide*.

Amazon managed policy: AWSConfigServiceRolePolicy

Amazon Config uses the service-linked role named **AWSServiceRoleForConfig** to call other Amazon services on your behalf. When you use the Amazon Web Services Management Console to set up Amazon Config, this SLR is automatically created by Amazon Config if you select the option to use the Amazon Config SLR instead of your own Amazon Identity and Access Management (IAM) service role.

The **AWSServiceRoleForConfig** SLR contains the managed policy `AWSConfigServiceRolePolicy`. This managed policy contains read-only and write-only permissions for Amazon Config resources and read-only permissions for resources in other services that Amazon Config supports. For more information, see Supported Resource Types for Amazon Config and Using Service-Linked Roles for Amazon Config.

View the policy: AWSConfigServiceRolePolicy.

> **Recommended: Use the Service-linked role**
>
> It is recommended that you use the service-linked role unless you have a particular use case. A service-linked role adds all the necessary permissions for Amazon Config to run as expected. Some features such as service-linked configuration recorders require you to use the service-linked role.

Amazon managed policy: AWS_ConfigRole

To record your Amazon resource configurations, Amazon Config requires IAM permissions to get the configuration details about your resources. If you want to create an IAM role for Amazon Config, you can use the managed policy `AWS_ConfigRole` and attach it to your IAM role.

This IAM policy is updated each time Amazon Config adds support for an Amazon resource type. This means that Amazon Config will continue to have the required permissions to record configuration data of supported resource types as long as the **AWS_ConfigRole** role has this managed policy attached. For more information, see Supported Resource Types for Amazon Config and Permissions for the IAM Role Assigned to Amazon Config.

View the policy: AWS_ConfigRole.

Amazon managed policy: AWSConfigUserAccess

This IAM policy provides access to use Amazon Config, including searching by tags on resources and reading all tags. This does not provide permission to configure Amazon Config, which requires administrative privileges.

View the policy: AWSConfigUserAccess.

Amazon managed policy: ConfigConformsServiceRolePolicy

To deploy and manage conformance packs, Amazon Config requires IAM permissions and certain permissions from other Amazon services. These allow you to deploy and manage conformance packs with full functionality and are updated each time Amazon Config adds new functionality for conformance packs. For more information on conformance packs, see Conformance packs.

View the policy: ConfigConformsServiceRolePolicy.

Amazon managed policy: AWSConfigRulesExecutionRole

To deploy Amazon Custom Lambda Rules, Amazon Config requires IAM permissions and certain permissions from other Amazon services. These allow Amazon Lambda functions to access the Amazon Config API and the configuration snapshots that Amazon Config delivers periodically to Amazon S3. This access is required by functions that evaluate configuration changes for Amazon Custom Lambda rules and is updated each time Amazon Config adds new functionality. For more information on Amazon Custom Lambda Rules, see Creating Amazon Config Custom Lambda Rules. For more information on configuration snapshots, see Concepts | Configuration Snapshot. For more information on the delivery of configuration snapshots, see Managing the Delivery Channel.

View the policy: AWSConfigRulesExecutionRole.

Amazon managed policy: AWSConfigMultiAccountSetupPolicy

To centrally deploy, update, and delete Amazon Config rules and conformance packs across member accounts in an organization in Amazon Organizations, Amazon Config requires IAM permissions and certain permissions from other Amazon services. This managed policy is updated each time Amazon Config adds new functionality for multi-account setup. For more information, see Managing Amazon Config Rules Across All Accounts in Your Organization and Managing Conformance Packs Across All Accounts in Your Organization.

View the policy: AWSConfigMultiAccountSetupPolicy.

Amazon managed policy: AWSConfigRoleForOrganizations

To allow Amazon Config to call read-only Amazon Organizations APIs, Amazon Config requires IAM permissions and certain permissions from other Amazon services. This managed policy is updated each time Amazon Config adds new functionality for multi-account setup. For more information, see Managing Amazon Config Rules Across All Accounts in Your Organization and Managing Conformance Packs Across All Accounts in Your Organization.

View the policy: AWSConfigRoleForOrganizations.

Amazon managed policy: AWSConfigRemediationServiceRolePolicy

To allow Amazon Config to remediate `NON_COMPLIANT` resources on your behalf, Amazon Config requires IAM permissions and certain permissions from other Amazon services. This managed policy is updated each time Amazon Config adds new functionality for remediation. For more information on remediation, see Remediating Noncompliant Resources with Amazon Config Rules. For more information on the conditions that initiate the possible Amazon Config evaluation results, see Concepts | Amazon Config Rules.

View the policy: AWSConfigRemediationServiceRolePolicy.

Amazon Config updates to Amazon managed policies

View details about updates to Amazon managed policies for Amazon Config since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the Amazon Config Document history page.

Change	Description	Date
AWSConfigServiceRolePolicy – Add "backup-gateway:GetHypervisor", "backup-gateway:ListHypervisors", "bcm-data-exports:GetExport", "bcm-data-exports:ListExports", "bcm-data-exports:ListTagsForResource", "bedrock:GetAgent", "bedrock:GetAgent	This policy now supports additional permissions for Amazon Backup gateway, Amazon Billing and Cost Management, Amazon Bedrock, Amazon CloudFormation, Amazon CloudFront, Amazon Entity Resolution, Amazon IoT Core Device Advisor, Amazon Lambda,	June 18, 2025

Change	Description	Date
ActionGroup", "bedrock: GetAgentKnowledgeBase", "bedrock:GetDataSource ", "bedrock:GetFlowAlias", "bedrock:GetFlowVersio n", "bedrock:ListAgent ActionGroups", "bedrock:List AgentKnowledgeBases", "bedrock:ListDataSources", "bedrock:ListFlowAliases", "bedrock:ListFlowVersions", "cloudformation:BatchDescri beTypeConfigurations", "cloudformation:Describ eStackInstance", "cloudforma tion:DescribeStackSet", "cloudformation:ListSt ackInstances", "cloudfor mation:ListStackSets", "cloudfront:GetPublicKey", "cloudfront:GetRealtimeLogC onfig", "cloudfront:ListPubl icKeys", "cloudfront:ListRe altimeLogConfigs", "entityre solution:GetIdMappingWorkfl ow", "entityresolution:GetSc hemaMapping", "enti tyresolution:ListIdMappingW orkflows", "entityresolution :ListSchemaMappings", "entit yresolution:ListTagsForReso urce", "iotdeviceadvisor:Get SuiteDefinition", "iotdevice advisor:ListSuiteDefinitions", "lambda:GetEventSourceMa	Amazon Network Manager, Amazon Private Certificate Authority, Amazon Relationa l Database Service, Amazon Redshift, Amazon S3 Tables, Amazon Systems Manager Quick Setup.	

Change	Description	Date
pping", "lambda:ListEventSourceMappings", "mediapackagev2:GetChannel", "mediapackagev2:ListChannels", "networkmanager:GetTransitGatewayPeering", "networkmanager:ListPeerings", "pca-connector-ad:GetDirectoryRegistration", "pca-connector-ad:ListDirectoryRegistrations", "pca-connector-ad:ListTagsForResource", "rds:DescribeDBShardGroups", "rds:DescribeIntegrations", "redshift:DescribeIntegrations", "s3tables:GetTableBucket", "s3tables:GetTableBucketEncryption", "s3tables:GetTableBucketMaintenanceConfiguration", "s3tables:ListTableBuckets", "ssm-quicksetup:GetConfigurationManager", "ssm-quicksetup:ListConfigurationManagers"		

Change	Description	Date
AWS_ConfigRole – Add "backup-gateway:GetHypervisor", "backup-gateway:ListHypervisors", "bcm-data-exports:GetExport", "bcm-data-exports:ListExports", "bcm-data-exports:ListTagsForResource", "bedrock:GetAgent", "bedrock:GetAgentActionGroup", "bedrock:GetAgentKnowledgeBase", "bedrock:GetDataSource", "bedrock:GetFlowAlias", "bedrock:GetFlowVersion", "bedrock:ListAgentActionGroups", "bedrock:ListAgentKnowledgeBases", "bedrock:ListDataSources", "bedrock:ListFlowAliases", "bedrock:ListFlowVersions", "cloudformation:BatchDescribeTypeConfigurations", "cloudformation:DescribeStackInstance", "cloudformation:DescribeStackSet", "cloudformation:ListStackInstances", "cloudformation:ListStackSets", "cloudfront:GetPublicKey", "cloudfront:GetRealtimeLogConfig", "cloudfront:ListPublicKeys", "cloudfront:ListRealtimeLogConfigs", "entityresolution:GetIdMapp	This policy now supports additional permissions for Amazon Backup gateway, Amazon Billing and Cost Management, Amazon Bedrock, Amazon CloudFormation, Amazon CloudFront, Amazon Entity Resolution, Amazon IoT Core Device Advisor, Amazon Lambda, Amazon Network Manager, Amazon Private Certificate Authority, Amazon Relational Database Service, Amazon Redshift, Amazon S3 Tables, Amazon Systems Manager Quick Setup.	June 18, 2025

Change	Description	Date
ingWorkflow", "entityre solution:GetSchemaMapping", "entityresolution:ListIdMap pingWorkflows", "entityre solution:ListSchemaMappings ", "entityresolution:ListTagsF orResource", "iotdevic eadvisor:GetSuiteDefinition ", "iotdeviceadvisor:ListSuite Definitions", "lambda:G etEventSourceMappi ng", "lambda:ListEventS ourceMappings", "networkm anager:GetTransitGatewayPee ring", "networkmanager:Li stPeerings", "pca-connector-ad:GetDirectoryRegistration", "pca-connector-ad:ListDirec toryRegistrations", "pca-conn ector-ad:ListTagsForResourc e", "rds:DescribeDBSha rdGroups", "rds:DescribeInteg rations", "redshift:Describe Integrations", "s3tables :GetTableBucket", "s3tables :GetTableBucketEncryption", "s3tables:GetTableBucketMai ntenanceConfiguration", "s3tables:ListTableBuckets", "ssm-quicksetup:GetConfigur ationManager", "ssm-quic ksetup:ListConfigurationMan agers"		

Change	Description	Date
AWS_ConfigRole – Add "bedrock:GetGuardrail", "bedrock:GetInferenceProfile", "bedrock:GetKnowledgeBase", "bedrock:ListGuardrails", "bedrock:ListInferenceProfiles", "bedrock:ListKnowledgeBases", "bedrock:ListTagsForResource"	This policy now supports additional permissions for Amazon Bedrock.	May 27, 2025
AWSConfigServiceRolePolicy – Add "bedrock:GetGuardrail", "bedrock:GetInferenceProfile", "bedrock:GetKnowledgeBase", "bedrock:ListGuardrails", "bedrock:ListInferenceProfiles", "bedrock:ListKnowledgeBases", "bedrock:ListTagsForResource"	This policy now supports additional permissions for Amazon Bedrock.	May 27, 2025

Change	Description	Date
AWS_ConfigRole – Add "b2bi:GetPartnership", "b2bi:GetProfile", "b2bi:ListPartnerships", "b2bi:ListProfiles", "bedrock:ListAgents", "cleanrooms:GetConfiguredTable", "cleanrooms:GetConfiguredTableAnalysisRule", "cleanrooms:GetMembership", "cleanrooms:GetPrivacyBudgetTemplate", "cleanrooms:ListConfiguredTables", "cleanrooms:ListMemberships", "cleanrooms:ListPrivacyBudgetTemplates", "codeconnections:GetConnection", "codeconnections:ListConnections", "codeconnections:ListTagsForResource", "directconnect:DescribeConnections", "dms:DescribeReplicationConfigs", "logs:DescribeAccountPolicies", "logs:DescribeResourcePolicies", "macie2:ListAutomatedDiscoveryAccounts", "managedblockchain:GetAccessor", "managedblockchain:ListAccessors", "qbusiness:GetApplication", "qbusiness:ListApplications", "qbusiness:ListTagsForResource", "route53profiles:GetProfile", "route53profiles:GetProfileAssociation",	This policy now supports additional permissions for Amazon B2B Data Interchange, Amazon Bedrock, Amazon Clean Rooms, Amazon CodeConnections, Amazon Direct Connect, Amazon Database Migration Service (Amazon DMS), Amazon CloudWatch Logs, Amazon Macie, Amazon Managed Blockchain, Amazon Q Business, Route 53 Profiles, Amazon Simple Storage Service (Amazon S3), Amazon SageMaker AI, Amazon Security Hub, and Amazon Systems Manager Incident Manager, Amazon Systems Manager Incident Manager Contacts, and Amazon Systems Manager.	April 08, 2025

Change	Description	Date
"route53profiles:ListProfileAssociations", "route53profiles:ListProfiles", "route53profiles:ListTagsForResource", "s3:GetAccessGrantsInstance", "s3:GetAccessGrantsLocation", "s3:ListAccessGrantsInstances", "s3:ListAccessGrantsLocations", "sagemaker:DescribeCluster", "sagemaker:DescribeMlflowTrackingServer", "sagemaker:DescribeStudioLifecycleConfig", "sagemaker:ListClusters", "sagemaker:ListMlflowTrackingServers", "sagemaker:ListStudioLifecycleConfigs", "securityhub:DescribeStandardsControls", "securityhub:GetEnabledStandards", "ssm-contacts:GetContact", "ssm-contacts:GetContactChannel", "ssm-contacts:ListContactChannels", "ssm-contacts:ListContacts", "ssm-incidents:GetResponsePlan", "ssm-incidents:ListResponsePlans", "ssm-incidents:ListTagsForResource", "ssm:DescribeInstanceInformation"		

Change	Description	Date
AWSConfigServiceRolePolicy – Add "b2bi:GetPartnership", "b2bi:GetProfile", "b2bi:ListPartnerships", "b2bi:ListProfiles", "bedrock:ListAgents", "cleanrooms:GetConfiguredTable", "cleanrooms:GetConfiguredTableAnalysisRule", "cleanrooms:GetMembership", "cleanrooms:GetPrivacyBudgetTemplate", "cleanrooms:ListConfiguredTables", "cleanrooms:ListMemberships", "cleanrooms:ListPrivacyBudgetTemplates", "codeconnections:GetConnection", "codeconnections:ListConnections", "codeconnections:ListTagsForResource", "directconnect:DescribeConnections", "dms:DescribeReplicationConfigs", "logs:DescribeAccountPolicies", "logs:DescribeResourcePolicies", "macie2:ListAutomatedDiscoveryAccounts", "managedblockchain:GetAccessor", "managedblockchain:ListAccessors", "qbusiness:GetApplication", "qbusiness:ListApplications", "qbusiness:ListTagsForResource", "route53profiles:GetProfile", "route53profiles:GetProfileAssociation",	This policy now supports additional permissions for Amazon B2B Data Interchange, Amazon Bedrock, Amazon Clean Rooms, Amazon CodeConnections, Amazon Direct Connect, Amazon Database Migration Service (Amazon DMS), Amazon CloudWatch Logs, Amazon Macie, Amazon Managed Blockchain, Amazon Q Business, Route 53 Profiles, Amazon Simple Storage Service (Amazon S3), Amazon SageMaker AI, Amazon Security Hub, and Amazon Systems Manager Incident Manager, Amazon Systems Manager Incident Manager Contacts, and Amazon Systems Manager. This policy also now supports permission to access all Amazon API Gateway domain names by including the resource pattern "`arn:aws:apigateway:::/domainnames/`".	April 08, 2025

Change	Description	Date
"route53profiles:ListProfileAssociations", "route53profiles:ListProfiles", "route53profiles:ListTagsForResource", "s3:GetAccessGrantsInstance", "s3:GetAccessGrantsLocation", "s3:ListAccessGrantsInstances", "s3:ListAccessGrantsLocations", "sagemaker:DescribeCluster", "sagemaker:DescribeMlflowTrackingServer", "sagemaker:DescribeStudioLifecycleConfig", "sagemaker:ListClusters", "sagemaker:ListMlflowTrackingServers", "sagemaker:ListStudioLifecycleConfigs", "securityhub:DescribeStandardsControls", "securityhub:GetEnabledStandards", "ssm-contacts:GetContact", "ssm-contacts:GetContactChannel", "ssm-contacts:ListContactChannels", "ssm-contacts:ListContacts", "ssm-incidents:GetResponsePlan", "ssm-incidents:ListResponsePlans", "ssm-incidents:ListTagsForResource", "ssm:DescribeInstanceInformation"		
AWS_ConfigRole – Add "ec2:GetAllowedImagesSettings"	This policy now supports additional permissions for Amazon Elastic Compute Cloud (Amazon EC2).	March 4, 2025

Change	Description	Date
AWSConfigServiceRolePolicy – Add "ec2:GetAllowedImagesSettings"	This policy now supports additional permissions for Amazon Elastic Compute Cloud (Amazon EC2).	March 4, 2025
AWS_ConfigRole – Add "cleanrooms-ml:GetTrainingDataset", "cleanrooms-ml:ListTrainingDatasets", "comprehend:DescribeFlywheel", "comprehend:ListFlywheels", "comprehend:ListTagsForResource", "ec2:GetSnapshotBlockPublicAccessState", "omics:GetAnnotationStore", "omics:GetRunGroup", "omics:GetSequenceStore", "omics:GetVariantStore", "omics:ListAnnotationStores", "omics:ListRunGroups", "omics:ListSequenceStores", "omics:ListTagsForResource", "omics:ListVariantStores", "s3express:GetEncryptionConfiguration", "s3express:GetLifecycleConfiguration", "ses:GetDedicatedIpPool", "ses:GetDedicatedIps", and "ses:ListDedicatedIpPools"	This policy now supports additional permissions for Amazon Clean Rooms, Amazon Comprehend, Amazon Elastic Compute Cloud (Amazon EC2), Amazon HealthOmics, Amazon Simple Storage Service (Amazon S3), and Amazon Simple Email Service (Amazon SES).	January 16, 2025

Change	Description	Date
AWSConfigServiceRolePolicy – Add "cleanrooms-ml:GetTrainingDataset", "cleanrooms-ml:ListTrainingDatasets", "comprehend:DescribeFlywheel", "comprehend:ListFlywheels", "comprehend:ListTagsForResource", "ec2:GetSnapshotBlockPublicAccessState", "omics:GetAnnotationStore", "omics:GetRunGroup", "omics:GetSequenceStore", "omics:GetVariantStore", "omics:ListAnnotationStores", "omics:ListRunGroups", "omics:ListSequenceStores", "omics:ListTagsForResource", "omics:ListVariantStores", "s3express:GetEncryptionConfiguration", "s3express:GetLifecycleConfiguration", "ses:GetDedicatedIpPool", "ses:GetDedicatedIps", and "ses:ListDedicatedIpPools"	This policy now supports additional permissions for Amazon Clean Rooms, Amazon Comprehend, Amazon Elastic Compute Cloud (Amazon EC2), Amazon HealthOmics, Amazon Simple Storage Service (Amazon S3), and Amazon Simple Email Service (Amazon SES).	January 16, 2025
AWSConfigServiceRolePolicy – Add "organizations:ListAWSServiceAccessForOrganization"	This policy now supports additional permissions for Amazon Organizations.	December 18, 2024

Change	Description	Date
AWS_ConfigRole – Add "app-integrations:GetApplication", "app-integrations:ListApplications", "app-integrations:ListTagsForResource", "appconfig:GetExtension", "appconfig:ListExtensions", "cloudtrail:GetInsightSelectors", "connect:DescribeQueue", "connect:DescribeRoutingProfile", "connect:DescribeSecurityProfile", "connect:ListQueueQuickConnects", "connect:ListQueues", "connect:ListRoutingProfileQueues", "connect:ListRoutingProfiles", "connect:ListSecurityProfileApplications", "connect:ListSecurityProfilePermissions", "connect:ListSecurityProfiles", "datazone:GetDomain", "datazone:ListDomains", "devops-guru:ListNotificationChannels", "glue:GetRegistry", "glue:ListRegistries", "identitystore:DescribeGroup", "identitystore:DescribeGroupMembership" "identitystore:ListGroupMemberships", "identitystore:ListGroups", "iot:DescribeThingGroup", "iot:DescribeThingType", "iot:ListThingGroups", "iot	This policy now supports additional permissions for Amazon AppConfig, Amazon CloudTrail, Amazon Connect, Amazon DataZone, Amazon DevOps Guru, Amazon Glue, Identity Store, Amazon IoT, Amazon IoT FleetWise, Amazon IoT Wireless, Amazon Interactive Video Service (Amazon IVS), Amazon CloudWatch Logs, Amazon CloudWatch Observability Access Manager, Amazon Payment Cryptography, Amazon Relational Database Service (Amazon RDS), Amazon Rekognition, Amazon Simple Storage Service (Amazon S3), Amazon EventBridge Scheduler, Amazon Systems Manager, and Amazon VPC Lattice.	November 7, 2024

Change	Description	Date
:ListThingTypes", "iotfleetwise:GetDecoderManifest", "iotfleetwise:GetFleet", "iotfleetwise:GetModelManifest", "iotfleetwise:GetSignalCatalog", "iotfleetwise:GetVehicle", "iotfleetwise:ListDecoderManifestNetworkInterfaces", "iotfleetwise:ListDecoderManifests", "iotfleetwise:ListDecoderManifestSignals", "iotfleetwise:ListFleets", "iotfleetwise:ListModelManifestNodes", "iotfleetwise:ListModelManifests", "iotfleetwise:ListSignalCatalogNodes", "iotfleetwise:ListSignalCatalogs", "iotfleetwise:ListTagsForResource", "iotfleetwise:ListVehicles", "iotwireless:GetDestination", "iotwireless:GetDeviceProfile", "iotwireless:GetWirelessGateway", "iotwireless:ListDestinations", "iotwireless:ListDeviceProfiles", "iotwireless:ListWirelessGateways", "ivschat:GetLoggingConfiguration", "ivschat:GetRoom" "ivschat:ListLoggingConfigurations", "ivschat:ListRooms", "ivschat:ListTagsForResource", "logs:GetLogAnomalyDetector", "logs:ListLogAnomalyDete		

Change	Description	Date
ctors", "oam:GetSink" "oam :GetSinkPolicy", "oam:List Sinks", "payment-cryptograp hy:GetAlias", "payment- cryptography:GetKey", "payment-cryptography:L istAliases", "payment-crypt ography:ListKeys", "payment -cryptography:ListTagsForRe source", "rds:DescribeDBPro xyTargetGroups", "rds:Desc ribeDBProxyTargets", "rekog nition:DescribeProjects", "s3:GetStorageLensGroup", "s3:ListStorageLensGroups", "s3:ListTagsForResource", " scheduler:GetScheduleGroup" , "scheduler:ListScheduleGrou ps", "scheduler:ListTagsFor Resource", "ssm:GetServiceSet ting", "vpc-lattice:GetAcce ssLogSubscription", "vpc-la ttice:GetService", "vpc-latt ice:GetServiceNetwork", "vp c-lattice:GetTargetGroup", "vpc-lattice:ListAccessLogS ubscriptions", "vpc-lattice :ListServiceNetworks", "vpc- lattice:ListServices", "vpc-lat tice:ListTagsForResource", "vpc-lattice:ListTargetGrou ps", and "vpc-lattice:ListT argets"		

Change	Description	Date
AWSConfigServiceRolePolicy – Add "app-integrations:GetApplication", "app-integrations:ListApplications", "app-integrations:ListTagsForResource", "appconfig:GetExtension", "appconfig:ListExtensions", "cloudtrail:GetInsightSelectors", "connect:DescribeQueue", "connect:DescribeRoutingProfile", "connect:DescribeSecurityProfile", "connect:ListQueueQuickConnects", "connect:ListQueues", "connect:ListRoutingProfileQueues", "connect:ListRoutingProfiles", "connect:ListSecurityProfileApplications", "connect:ListSecurityProfilePermissions", "connect:ListSecurityProfiles", "datazone:GetDomain", "datazone:ListDomains", "devops-guru:ListNotificationChannels", "glue:GetRegistry", "glue:ListRegistries", "identitystore:DescribeGroup", "identitystore:DescribeGroupMembership" "identitystore:ListGroupMemberships", "identitystore:ListGroups", "iot:DescribeThingGroup", "iot:DescribeThingType",	This policy now supports additional permissions for Amazon AppConfig, Amazon CloudTrail, Amazon Connect, Amazon DataZone, Amazon DevOps Guru, Amazon Glue, Identity Store, Amazon IoT, Amazon IoT FleetWise, Amazon IoT Wireless, Amazon Interactive Video Service (Amazon IVS), Amazon CloudWatch Logs, Amazon CloudWatch Observability Access Manager, Amazon Payment Cryptography, Amazon Relational Database Service (Amazon RDS), Amazon Rekognition, Amazon Simple Storage Service (Amazon S3), Amazon EventBridge Scheduler, Amazon Systems Manager, and Amazon VPC Lattice.	November 7, 2024

Change	Description	Date
"iot:ListThingGroups", "iot :ListThingTypes", "iotfleet wise:GetDecoderManifest", "iotfleetwise:GetFleet", "iotfleetwise:GetModelManif est", "iotfleetwise:GetSign alCatalog", "iotfleetwise:GetV ehicle", "iotfleetwise:List DecoderManifestNetworkInter faces", "iotfleetwise:ListD ecoderManifests", "iotfleet wise:ListDecoderManifestSig nals", "iotfleetwise:ListFl eets", "iotfleetwise:ListMo delManifestNodes", "iotflee twise:ListModelManifests", "iotfleetwise:ListSignalCat alogNodes", "iotfleetwise:L istSignalCatalogs", "iotfle etwise:ListTagsForResource" , "iotfleetwise:ListVehicles", "iotwireless:GetDestination", "iotwireless:GetDeviceProfi le", "iotwireless:GetWirele ssGateway", "iotwireless:Li stDestinations", "iotwirele ss:ListDeviceProfiles", "io twireless:ListWirelessGatew ays", "ivschat:GetLoggingCo nfiguration", "ivschat: GetRoom" "ivschat:ListLoggi ngConfigurations", "ivschat: ListRooms", "ivschat:ListTa gsForResource", "logs:Get LogAnomalyDetector",		

Change	Description	Date
"logs:ListLogAnomalyDetectors", "oam:GetSink" "oam:GetSinkPolicy", "oam:ListSinks", "payment-cryptography:GetAlias", "payment-cryptography:GetKey", "payment-cryptography:ListAliases", "payment-cryptography:ListKeys", "payment-cryptography:ListTagsForResource", "rds:DescribeDBProxyTargetGroups", "rds:DescribeDBProxyTargets", "rekognition:DescribeProjects", "s3:GetStorageLensGroup", "s3:ListStorageLensGroups", "s3:ListTagsForResource", "scheduler:GetScheduleGroup", "scheduler:ListScheduleGroups", "scheduler:ListTagsForResource", "ssm:GetServiceSetting", "vpc-lattice:GetAccessLogSubscription", "vpc-lattice:GetService", "vpc-lattice:GetServiceNetwork", "vpc-lattice:GetTargetGroup", "vpc-lattice:ListAccessLogSubscriptions", "vpc-lattice:ListServiceNetworks", "vpc-lattice:ListServices", "vpc-lattice:ListTagsForResource", "vpc-lattice:ListTargetGroups", and "vpc-lattice:ListTargets"		

Change	Description	Date
AWS_ConfigRole – Add "aoss:BatchGetCollection," "aoss:BatchGetLifecyclePolicy," "aoss:BatchGetVpcEndpoint," "aoss:GetAccessPolicy," "aoss:GetSecurityConfig," "aoss:GetSecurityPolicy," "aoss:ListAccessPolicies," "aoss:ListCollections," "aoss:ListLifecyclePolicies," "aoss:ListSecurityConfigs," "aoss:ListSecurityPolicies," "aoss:ListVpcEndpoints," "appstream:DescribeAppBlockBuilders," "backup:GetRestoreTestingPlan," "backup:GetRestoreTestingSelection", "backup:ListRestoreTestingPlans," "backup:ListRestoreTestingSelections," "cloudTrail:GetChannel, "cloudTrail:ListChannels," "glue:GetTrigger," "glue:ListTriggers, "imagebuilder:GetLifecyclePolicy," "imagebuilder:ListLifecyclePolicies," "iot:DescribeBillingGroup," "iot:ListBillingGroups," "ivs:GetEncoderConfiguration," "ivs:GetPlaybackRestrictionPolicy," "ivs:GetStage," "ivs:GetStorageConfiguration," "ivs:ListEncoderConfigurations," "ivs:ListPlaybackRest	This policy now supports additional permissions for Amazon OpenSearch Service Severless, Amazon AppStream, Amazon Backup, Amazon CloudTrail, Amazon Glue, EC2 Image Builder, Amazon IoT, Amazon Interactive Video Service (Amazon IVS), AWS Elemental MediaConnect, AWS Elemental MediaTailor, Amazon HealthOmics, and Amazon EventBridge Scheduler.	September 16, 2024

Change	Description	Date
rictionPolicies," "ivs:List Stages," "ivs:ListStorageCo nfigurations," "mediacon nect:DescribeBridge", "medi aconnect:DescribeGatewa," "mediaconnect:ListBridges," "mediaconnect:ListGateways", "mediatailor:DescribeChanne l," "mediatailor:DescribeLi veSource," "mediatailor:Des cribeSourceLocation," "medi atailor:DescribeVodSource", "mediatailor:ListChannels," "mediatailor:ListLiveSourc es", "mediatailor:ListSourc eLocations," "mediatai lor:ListVodSources," "omics :GetWorkflow," "omics:Li stWorkflows," "scheduler:Ge tSchedule," and "schedule r:ListSchedules"		

Change	Description	Date
AWSConfigServiceRolePolicy – Add "aoss:BatchGetCollection," "aoss:BatchGetLifecyclePolicy," "aoss:BatchGetVpcEndpoint," "aoss:GetAccessPolicy," "aoss:GetSecurityConfig," "aoss:GetSecurityPolicy," "aoss:ListAccessPolicies," "aoss:ListCollections," "aoss:ListLifecyclePolicies," "aoss:ListSecurityConfigs," "aoss:ListSecurityPolicies," "aoss:ListVpcEndpoints," "appstream:DescribeAppBlockBuilders," "backup:GetRestoreTestingPlan," "backup:GetRestoreTestingSelection", "backup:ListRestoreTestingPlans," "backup:ListRestoreTestingSelections," "cloudTrail:GetChannel, "cloudTrail:ListChannels," "glue:GetTrigger," "glue:ListTriggers, "imagebuilder:GetLifecyclePolicy," "imagebuilder:ListLifecyclePolicies," "iot:DescribeBillingGroup," "iot:ListBillingGroups," "ivs:GetEncoderConfiguration," "ivs:GetPlaybackRestrictionPolicy," "ivs:GetStage," "ivs:GetStorageConfiguration," "ivs:ListEncoderConfigurations," "ivs:ListPla	This policy now supports additional permissions for Amazon OpenSearch Service Severless, Amazon AppStream, Amazon Backup, Amazon CloudTrail, Amazon Glue, EC2 Image Builder, Amazon IoT, Amazon Interactive Video Service (Amazon IVS), AWS Elemental MediaConnect, AWS Elemental MediaTailor, Amazon HealthOmics, and Amazon EventBridge Scheduler.	September 16, 2024

Change	Description	Date
ybackRestrictionPolicies," "ivs:ListStages," "ivs:List StorageConfigurations," "mediaconnect:DescribeBridge", "mediaconnect:DescribeGatewa," "mediaconnect:List Bridges," "mediaconnect:ListGateways", "mediatailor:DescribeChannel," "mediatailor:DescribeLiveSource," "mediatailor:DescribeSourceLocation," "mediatailor:DescribeVodSource", "mediatailor:ListChannels," "mediatailor:ListLiveSources", "mediatailor:ListSourceLocations," "mediatailor:ListVodSources," "omics:GetWorkflow," "omics:ListWorkflows," "scheduler:GetSchedule," and "scheduler:ListSchedules"		
AWS_ConfigRole – Add "elasticfilesystem:DescribeTags," "redshift:DescribeTags," and "ssm-sap:ListTagsForResource"	This policy now supports additional permissions for Amazon Elastic File System (Amazon EFS), Amazon Redshift and Amazon Systems Manager for SAP.	June 17, 2024
AWSConfigServiceRolePolicy – Add "elasticfilesystem:DescribeTags," "redshift:DescribeTags," and "ssm-sap:ListTagsForResource"	This policy now supports additional permissions for Amazon Elastic File System (Amazon EFS), Amazon Redshift and Amazon Systems Manager for SAP.	June 17, 2024

Change	Description	Date
AWS_ConfigRole – Add "aps:DescribeAlertManagerDefinition," "cloudwatch:DescribeAlarmsForMetric," "cognito-identity:DescribeIdentityPool," "cognito-identity:GetPrincipalTagAttributeMap," "elasticache:DescribeCacheSecurityGroups," "elasticache:DescribeUserGroups," "elasticache:DescribeUsers," "elasticache:DescribeGlobalReplicationGroups," "fsx:DescribeDataRepositoryAssociations," "glue:GetDatabase," "glue:GetDatabases," "iam:ListUsers," "lambda:GetLayerVersion," "lambda:ListLayers," "lambda:ListLayerVersions," "ram:GetPermission," "ram:ListPermissionAssociations," "ram:ListPermissions," "ram:ListPermissionVersions," "redshift-serverless:GetNamespace," "redshift-serverless:GetWorkgroup," "redshift-serverless:ListNamespaces," "redshift-serverless:ListTagsForResource," "redshift-serverless:ListWorkgroups," "sagemaker:DescribeInferenceExperiment," "sagemaker:ListInferenceExperiments," and "sns:GetSMSSandboxAccountStatus"	This policy now supports additional permissions for Amazon Managed Service for Prometheus, Amazon CloudWatch, Amazon Cognito, Amazon ElastiCache, Amazon FSx, Amazon Glue, Amazon Identity and Access Management (IAM), Amazon Lambda, Amazon RAM, Amazon Redshift Serverless, Amazon SageMaker AI, and Amazon Simple Notification Service (Amazon SNS).	February 22, 2024

Change	Description	Date
AWSConfigServiceRolePolicy – Add "aps:DescribeAlertManagerDefinition," "cloudwatch:DescribeAlarmsForMetric," "cognito-identity:DescribeIdentityPool, "cognito-identity:GetPrincipalTagAttributeMap," "elasticache:DescribeCacheSecurityGroups," "elasticache:DescribeUserGroups," "elasticache:DescribeUsers," "elasticache:DescribeGlobalReplicationGroups," "fsx:DescribeDataRepositoryAssociations," "glue:GetDatabase," "glue:GetDatabases," "iam:ListUsers," "lambda:GetLayerVersion," "lambda:ListLayers," "lambda:ListLayerVersions," "ram:GetPermission," "ram:ListPermissionAssociations," "ram:ListPermissions," "ram:ListPermissionVersions," "redshift-serverless:GetNamespace," "redshift-serverless:GetWorkgroup," "redshift-serverless:ListNamespaces," "redshift-serverless:ListTagsForResource," "redshift-serverless:ListWorkgroups," "sagemaker:DescribeInferenceExperiment," "sagemaker:ListInference	This policy now supports additional permissions for Amazon Managed Service for Prometheus, Amazon CloudWatch, Amazon Cognito, Amazon ElastiCache, Amazon FSx, Amazon Glue, Amazon Identity and Access Management (IAM), Amazon Lambda, Amazon RAM, Amazon Redshift Serverless, Amazon SageMaker AI, and Amazon Simple Notification Service (Amazon SNS).	February 22, 2024

Change	Description	Date
Experiments," and "sns:GetSMSSandboxAccountStatus"		
AWSConfigUserAccess – Amazon Config starts tracking changes for this Amazon managed policy	This policy provides access to use Amazon Config, including searching by tags on resources and reading all tags. This does not provide permission to configure Amazon Config, which requires administrative privileges.	February 22, 2024
AWS_ConfigRole – Add "appconfig:GetExtensionAssociation," "appconfig:ListExtensionAssociations," "aps:DescribeLoggingConfiguration," "dms:DescribeReplicationTaskAssessmentRuns," "iam:GetOpenIDConnectProvider," "iam:ListOpenIDConnectProviders," "kafka:DescribeVpcConnection," "kafka:GetClusterPolicy," "kafka:ListVpcConnections," "logs:DescribeMetricFilters," "organizations:ListDelegatedAdministrators," "s3:GetBucketPolicyStatus," "s3express:GetBucketPolicy," and "s3express:ListAllMyDirectoryBuckets"	This policy now supports additional permissions for Amazon AppConfig, Amazon Managed Service for Prometheus, Amazon Database Migration Service (Amazon DMS), (Amazon Identity and Access Management) IAM, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon CloudWatch Logs, Amazon Organizations, and Amazon Simple Storage Service (Amazon S3).	Decemeber 5, 2023

Change	Description	Date
AWSConfigServiceRolePolicy – Add "appconfig:GetExtensionAssociation," "appconfig:ListExtensionAssociations," "aps:DescribeLoggingConfiguration," "dms:DescribeReplicationTaskAssessmentRuns," "iam:GetOpenIDConnectProvider," "iam:ListOpenIDConnectProviders," "kafka:DescribeVpcConnection," "kafka:GetClusterPolicy," "kafka:ListVpcConnections," "logs:DescribeMetricFilters," "organizations:ListDelegatedAdministrators," "s3:GetBucketPolicyStatus," "s3express:GetBucketPolicy," and "s3express:ListAllMyDirectoryBuckets"	This policy now supports additional permissions for Amazon AppConfig, Amazon Managed Service for Prometheus, Amazon Database Migration Service (Amazon DMS), (Amazon Identity and Access Management) IAM, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon CloudWatch Logs, Amazon Organizations, and Amazon Simple Storage Service (Amazon S3).	December 5, 2023

Change	Description	Date
AWS_ConfigRole – Add "backup:DescribeProtectedResource," "cognito-identity:GetIdentityPoolRoles," "cognito-identity:ListIdentityPools," "cognito-identity:ListTagsForResource," "cognito-idp:DescribeIdentityProvider," "cognito-idp:DescribeResourceServer," "cognito-idp:DescribeUserPool," "cognito-idp:DescribeUserPoolClient," "cognito-idp:DescribeUserPoolDomain," "cognito-idp:GetGroup," "cognito-idp:GetUserPoolMfaConfig," "cognito-idp:ListGroups," "cognito-idp:ListIdentityProviders," "cognito-idp:ListResourceServers," "cognito-idp:ListUserPoolClients," "cognito-idp:ListUserPools," "cognito-idp:ListTagsForResource," "connect:DescribeEvaluationForm," "connect:DescribeInstanceStorageConfig," "connect:DescribePrompt," "connect:DescribeRule," "connect:DescribeUser," "connect:GetTaskTemplate," "connect:ListApprovedOrigins," "connect:ListEvaluationForms," "connect:ListInstanceStorageConfigs," "connect:ListIntegrationAssociation	This policy now supports additional permissions for Amazon Cognito, Amazon Connect, Amazon EMR, Amazon Ground Station, Amazon Mainframe Modernization, Amazon MemoryDB, Amazon Organizations, Amazon QuickSight, Amazon Relational Database Service (Amazon RDS), Amazon Redshift, Amazon Route 53, Amazon Service Catalog, and Amazon Transfer Family.	November 17, 2023

Change	Description	Date
s," "connect:ListPrompts," "connect:ListRules," "connect:ListSecurityKeys," "connect:ListTagsForResource," "connect:ListTaskTemplates," "connect:ListUsers," "emr-containers:DescribeVirtualCluster," "emr-containers:ListVirtualClusters," "emr-serverless:GetApplication," "emr-serverless:ListApplications," "groundstation:GetDataflowEndpointGroup," "groundstation:ListDataflowEndpointGroups," "m2:GetEnvironment," "m2:ListEnvironments," "m2:ListTagsForResource," "memorydb:DescribeAcls," "memorydb:DescribeClusters," "memorydb:DescribeParameterGroups," "memorydb:DescribeParameters," "memorydb:DescribeSubnetGroups," "organizations:ListRoots," "quicksight:DescribeAccountSubscription," "quicksight:DescribeDataSetRefreshProperties," "rds:DescribeEngineDefaultClusterParameters," "redshift:DescribeEndpointAccess," "redshift:DescribeEndpointAuthorization," "route53:GetChange," "route53:ListCidrBlocks," "route53:ListCidrL		

Change	Description	Date
ocations," "serviceCatalog:DescribePortfolioShares," "transfer:DescribeProfile," and "transfer:ListProfiles"		
AWS_ConfigRole – Add "Sid": "AWSConfigServiceRolePolicyStatementID," "Sid": "AWSConfigSLRLogStatementID," "Sid": "AWSConfigSLRLogEventStatementID," and "Sid": "AWSConfigSLRApiGatewayStatementID"	This policy now adds security identifiers (SID) for `AWSConfigServiceRolePolicyStatementID` , `AWSConfigSLRLogStatementID` , `AWSConfigSLRLogEventStatementID` ,and `AWSConfigSLRApiGatewayStatementID` .	November 17, 2023

Change	Description	Date
AWSConfigServiceRolePolicy – Add "backup:DescribeProtectedResource," "cognito-identity:GetIdentityPoolRoles," "cognito-identity:ListIdentityPools," "cognito-identity:ListTagsForResource," "cognito-idp:DescribeIdentityProvider," "cognito-idp:DescribeResourceServer," "cognito-idp:DescribeUserPool," "cognito-idp:DescribeUserPoolClient," "cognito-idp:DescribeUserPoolDomain," "cognito-idp:GetGroup," "cognito-idp:GetUserPoolMfaConfig," "cognito-idp:ListGroups," "cognito-idp:ListIdentityProviders," "cognito-idp:ListResourceServers," "cognito-idp:ListUserPoolClients," "cognito-idp:ListUserPools," "cognito-idp:ListTagsForResource," "connect:DescribeEvaluationForm," "connect:DescribeInstanceStorageConfig," "connect:DescribePrompt," "connect:DescribeRule," "connect:DescribeUser," "connect:GetTaskTemplate," "connect:ListApprovedOrigins," "connect:ListEvaluationForms," "connect:ListInstanceStorageConfigs," "connect	This policy now supports additional permissions for Amazon Cognito, Amazon Connect, Amazon EMR, Amazon Ground Station, Amazon Mainframe Modernization, Amazon MemoryDB, Amazon Organizations, Amazon QuickSight, Amazon Relational Database Service (Amazon RDS), Amazon Redshift, Amazon Route 53, Amazon Service Catalog, and Amazon Transfer Family.	November 17, 2023

Change	Description	Date
:ListIntegrationAssociations," "connect:ListPrompts," "connect:ListRules," "connect:ListSecurityKeys," "connect:ListTagsForResource," "connect:ListTaskTemplates," "connect:ListUsers," "emr-containers:DescribeVirtualCluster," "emr-containers:ListVirtualClusters," "emr-serverless:GetApplication," "emr-serverless:ListApplications," "groundstation:GetDataflowEndpointGroup," "groundstation:ListDataflowEndpointGroups," "m2:GetEnvironment," "m2:ListEnvironments," "m2:ListTagsForResource," "memorydb:DescribeAcls," "memorydb:DescribeClusters," "memorydb:DescribeParameterGroups," "memorydb:DescribeParameters," "memorydb:DescribeSubnetGroups," "organizations:ListRoots," "quicksight:DescribeAccountSubscription," "quicksight:DescribeDataSetRefreshProperties," "rds:DescribeEngineDefaultClusterParameters," "redshift:DescribeEndpointAccess," "redshift:DescribeEndpointAuthorization," "route53:GetChange," "route53:ListCid		

Change	Description	Date
rBlocks," "route53:ListCidrLocations," "serviceCatalog:DescribePortfolioShares," "transfer:DescribeProfile," and "transfer:ListProfiles"		
AWSConfigServiceRolePolicy – Add "Sid": "AWSConfigServiceRolePolicyStatementID," "Sid": "AWSConfigSLRLogStatementID," "Sid": "AWSConfigSLRLogEventStatementID," and "Sid": "AWSConfigSLRApiGatewayStatementID"	This policy now adds security identifiers (SID) for `AWSConfigServiceRolePolicyStatementID` , `AWSConfigSLRLogStatementID` , `AWSConfigSLRLogEventStatementID` , and `AWSConfigSLRApiGatewayStatementID` .	November 17, 2023

Change	Description	Date
AWS_ConfigRole – Add "acm-pca:GetCertificateAuthorityCertificate," "appmesh:DescribeMesh," "appmesh:ListGatewayRoutes," "connect:DescribeInstance," "connect:DescribeQuickConnect," "connect:ListQuickConnects," "ecs:DescribeCapacityProviders," "evidently:GetSegment," "evidently:ListSegments," "grafana:DescribeWorkspace," "grafana:DescribeWorkspaceAuthentication," "grafana:DescribeWorkspaceConfiguration," "grafana:DescribeWorkspaceConfiguration," "guardduty:GetMemberDetectors," "inspector2:BatchGetAccountStatus," "inspector2:GetDelegatedAdminAccount," "inspector2:ListMembers," "iot:DescribeCACertificate," "iot:ListCACertificates," "iot:ListTagsForResource," "iottwinmaker:GetSyncJob," "iottwinmaker:ListSyncJobs," "kafka:ListTagsForResource," "kafkaconnect:DescribeConnector," "kafkaconnect:ListConnectors," "lambda:GetCodeSigningConfig," "lambda:ListCodeSigningConfigs," "lambda:ListT	This policy now supports additional permissions for Amazon Private CA, Amazon App Mesh, Amazon Connect, Amazon Elastic Container Service (Amazon ECS), Amazon CloudWatch Evidently, Amazon Managed Grafana, Amazon GuardDuty, Amazon Inspector, Amazon IoT, Amazon IoT TwinMaker, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Lambda, Amazon Network Manager, Amazon Organizations, and Amazon SageMaker AI.	October 4, 2023

Change	Description	Date
ags," "networkmanager:GetConnectPeer," "organizations:DescribeOrganization," "organizations:ListTargetsForPolicy," "sagemaker:DescribeDataQualityJob," "sagemaker:DescribeModelExplainabilityJob," "sagemaker:ListDataQualityJob," and "sagemaker:ExplainabilityJob"		

Change	Description	Date
AWSConfigServiceRolePolicy – Add "acm-pca:GetCertificateAuthorityCertificate," "appmesh:DescribeMesh," "appmesh:ListGatewayRoutes," "connect:DescribeInstance," "connect:DescribeQuickConnect," "connect:ListQuickConnects," "ecs:DescribeCapacityProviders," "evidently:GetSegment," "evidently:ListSegments," "grafana:DescribeWorkspace," "grafana:DescribeWorkspaceAuthentication," "grafana:DescribeWorkspaceConfiguration," "grafana:DescribeWorkspaceConfiguration," "guardduty:GetMemberDetectors," "inspector2:BatchGetAccountStatus," "inspector2:GetDelegatedAdminAccount," "inspector2:ListMembers," "iot:DescribeCACertificate," "iot:ListCACertificates," "iot:ListTagsForResource," "iottwinmaker:GetSyncJob," "iottwinmaker:ListSyncJobs," "kafka:ListTagsForResource," "kafkaconnect:DescribeConnector," "kafkaconnect:ListConnectors," "lambda:GetCodeSigningConfig," "lambda:ListCodeSi	This policy now supports additional permissions for Amazon Private CA, Amazon App Mesh, Amazon Connect, Amazon Elastic Container Service (Amazon ECS), Amazon CloudWatch Evidently, Amazon Managed Grafana, Amazon GuardDuty, Amazon Inspector, Amazon IoT, Amazon IoT TwinMaker, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Lambda, Amazon Network Manager, Amazon Organizations, and Amazon SageMaker AI.	October 4, 2023

Change	Description	Date
gningConfigs," "lambda:ListTags," "networkmanager:GetConnectPeer," "organizations:DescribeOrganization," "organizations:ListTargetsForPolicy," "sagemaker:DescribeDataQualityJob," "sagemaker:DescribeModelExplainabilityJob," "sagemaker:ListDataQualityJob," and "sagemaker:ExplainabilityJob"		
AWSConfigServiceRolePolicy – Remove "ssm:GetParameter"	This policy now removes permissions for Amazon Systems Manager (Systems Manager).	September 6, 2023

Change	Description	Date
AWS_ConfigRole – Add "appmesh:DescribeGatewayRoute","appstream:DescribeStacks", "aps:ListTagsForResource", "cloudfront:GetFunction", "cloudfront:GetOriginAccessControl", "cloudfront:ListFunctions", "cloudfront:ListOriginAccessControls", "codeartifact:ListPackages", "codeartifact:ListPackageVersions", "codebuild:BatchGetReportGroups", "codebuild:ListReportGroups", "connect:ListInstanceAttributes", "connect:ListInstances", "glue:GetPartition", "glue:GetPartitions", "guardduty:GetAdministratorAccount", "iam:ListInstanceProfileTags", "inspector2:ListFilters", "iot:DescribeJobTemplate", "iot:DescribeProvisioningTemplate", "iot:ListJobTemplates", "iot:ListProvisioningTemplates", "iottwinmaker:GetComponentType", "iottwinmaker:ListComponentTypes", "iotwireless:GetFuotaTask", "iotwireless:GetMulticastGroup", "iotwireless:ListFuotaTasks", "iotwireless:ListMulticastGroups", "kafka:ListScramSe	This policy now supports additional permissions for Amazon App Mesh, Amazon CloudFormation, Amazon CloudFront Amazon CodeArtifact, Amazon CodeBuild, Amazon Connect, Amazon Glue, Amazon GuardDuty, Amazon Identity and Access Management (IAM), Amazon Inspector, Amazon IoT, Amazon IoT TwinMaker, Amazon IoT Wireless, Amazon Managed Streaming for Apache Kafka, Amazon Macie, AWS Elemental MediaConnect, Amazon Network Manager, Amazon Organizations, Amazon Resource Explorer, Amazon Route 53, Amazon Simple Storage Service (Amazon S3), and Amazon Simple Notification Service (Amazon SNS).	July 28, 2023

Change	Description	Date
crets", "macie2:ListTagsForResource", "mediaconnect:ListTagsForResource", "networkmanager:GetConnectPeer", "networkmanager:ListConnectPeers", "organizations:DescribeEffectivePolicy", "organizations:DescribeResourcePolicy", "resource-explorer-2:GetIndex", "resource-explorer-2:ListIndexes", "resource-explorer-2:ListTagsForResource", "route53:ListCidrCollections", "s3:GetMultiRegionAccessPointPolicy", "s3:GetMultiRegionAccessPointPolicyStatus", and "sns:GetDataProtectionPolicy"		

Change	Description	Date
AWSConfigServiceRolePolicy – Add "appmesh:DescribeGatewayRoute", "appstream:DescribeStacks", "aps:ListTagsForResource", "cloudfront:GetFunction", "cloudfront:GetOriginAccessControl", "cloudfront:ListFunctions", "cloudfront:ListOriginAccessControls", "codeartifact:ListPackages", "codeartifact:ListPackageVersions", "codebuild:BatchGetReportGroups", "codebuild:ListReportGroups", "connect:ListInstanceAttributes", "connect:ListInstances", "glue:GetPartition", "glue:GetPartitions", "guardduty:GetAdministratorAccount", "iam:ListInstanceProfileTags", "inspector2:ListFilters", "iot:DescribeJobTemplate", "iot:DescribeProvisioningTemplate", "iot:ListJobTemplates", "iot:ListProvisioningTemplates", "iottwinmaker:GetComponentType", "iottwinmaker:ListComponentTypes", "iotwireless:GetFuotaTask", "iotwireless:GetMulticastGroup", "iotwireless:ListFuotaTasks", "iotwireless:ListMulticastGroups", "kafka:ListScramSe	This policy now supports additional permissions for Amazon App Mesh, Amazon AppStream 2.0, Amazon CloudFormation, Amazon CloudFront, Amazon CodeArtifact, Amazon CodeBuild, Amazon Connect, Amazon Glue, Amazon GuardDuty, Amazon Identity and Access Management (IAM), Amazon Inspector, Amazon IoT, Amazon IoT TwinMaker, Amazon IoT Wireless, Amazon Managed Streaming for Apache Kafka, Amazon Macie, AWS Elemental MediaConnect, Amazon Network Manager, Amazon Organizations, Amazon Resource Explorer, Amazon Route 53, Amazon Simple Storage Service (Amazon S3), Amazon Simple Notification Service (Amazon SNS), and Amazon EC2 Systems Manager (SSM).	July 28, 2023

Change	Description	Date
crets", "macie2:ListTagsForResource", "mediaconnect:ListTagsForResource", "networkmanager:GetConnectPeer", "networkmanager:ListConnectPeers", "organizations:DescribeEffectivePolicy", "organizations:DescribeResourcePolicy", "resource-explorer-2:GetIndex", "resource-explorer-2:ListIndexes", "resource-explorer-2:ListTagsForResource", "route53:ListCidrCollections", "s3:GetMultiRegionAccessPointPolicy", "s3:GetMultiRegionAccessPointPolicyStatus", "sns:GetDataProtectionPolicy", "ssm:DescribeParameters", "ssm:GetParameter", and "ssm:ListTagsForResource"		

Change	Description	Date
AWS_ConfigRole – Add "amplify:GetBranch", "amplify:ListBranches", "app-integrations:GetEventIntegration", "app-integrations:ListEventIntegrationAssociations", "app-integrations:ListEventIntegrations", "appmesh:DescribeRoute", "appmesh:ListRoutes", "aps:ListRuleGroupsNamespaces", "athena:GetPreparedStatement", "athena:ListPreparedStatements", "batch:DescribeSchedulingPolicies", "batch:ListSchedulingPolicies", "cloudformation:ListTypes", "cloudtrail:ListTrails", "codeartifact:ListDomains", "codeguru-profiler:DescribeProfilingGroup", "codeguru-profiler:GetNotificationConfiguration", "codeguru-profiler:GetPolicy", "codeguru-profiler:ListProfilingGroups", "ds:DescribeDomainControllers", “dynamodb:DescribeTableReplicaAutoScaling" "dynamodb:DescribeTimeToLive", "ec2:DescribeTrafficMirrorFilters", "evidently:GetLaunch", "evidently:ListLaunches", "forecast:DescribeDa	This policy now supports additional permissions for Amazon Amplify, Amazon Connect, Amazon App Mesh, Amazon Managed Service for Prometheus, Amazon Athena, Amazon Batch, Amazon CloudFormation, Amazon CloudTrail, Amazon CodeArtifact, Amazon CodeGuru, Amazon Directory Service, Amazon DynamoDB, Amazon Elastic Compute Cloud (Amazon EC2), Amazon CloudWatch Evidently, Amazon Organizations, Amazon Forecast, Amazon IoT Greengrass, Amazon Ground Station, Amazon Identity and Access Management (IAM), Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Lightsail, Amazon CloudWatch Logs, AWS Elemental MediaConnect, AWS Elemental MediaTailor, Amazon Pinpoint, Amazon Virtual Private Cloud (Amazon VPC), Amazon Personalize, Amazon QuickSight, Amazon Migration Hub Refactor Spaces, Amazon Simple Storage Service (Amazon	June 13, 2023

Change	Description	Date
tasetGroup", "forecast :ListDatasetGroups", "greeng rass:DescribeComponent", "greengrass:GetComponent", "greengrass:ListComponents", "greengrass:ListComponentVe rsions", "groundstation:GetM issionProfile", "groundstati on:ListMissionProfiles", "iam:ListGroups", "iam:ListR oles", "kafka:DescribeCon figuration", "kafka:Describe ConfigurationRevision", "kafka:ListConfigurations", "lightsail:GetRelationalDat abases" "logs:ListTagsLogG roup", "mediaconnec t:DescribeFlow", "mediacon nect:ListFlows", "mediatailo r:GetPlaybackConfiguration" , "mediatailor:ListPlaybackC onfigurations", "mobiletarge ting:GetApplicationSettings ", "mobiletargeting:GetEmail Template", "mobiletargeting: GetEventStream", "mobileta rgeting:ListTemplates", "networkmanager:GetCus tomerGatewayAssociations", "networkmanager:Get LinkAssociations", "organiza tions:DescribeAccount", "organizations:Describ eOrganizationalUnit", "organizations:ListAccou	S3), Amazon SageMaker AI, Amazon Transfer Family.	

Change	Description	Date
nts", "organizations:ListAccountsForParent", "organizations:ListOrganizationalUnitsForParent", "organizations:ListTagsForResource", "personalize:DescribeDataset", "personalize:DescribeDatasetGroup", "personalize:DescribeSchema", "personalize:DescribeSolution", "personalize:ListDatasetGroups", "personalize:ListDatasetImportJobs", "personalize:ListDatasets", "personalize:ListSchemas", "personalize:ListSolutions", "personalize:ListTagsForResource", "quicksight:ListTemplates", "refactor-spaces:GetEnvironment", "refactor-spaces:GetService", "refactor-spaces:ListApplications", "refactor-spaces:ListEnvironments", "refactor-spaces:ListServices", "s3:GetAccessPointPolicyStatusForObjectLambda", "sagemaker:DescribeDeviceFleet", "sagemaker:DescribeFeatureGroup", "sagemaker:ListDeviceFleets", "sagemaker:ListFeatureGroups", "sagemaker:ListModels", and "transfer:ListTagsForResource"		

Change	Description	Date
AWSConfigServiceRolePolicy – Add "amplify:GetBranch", "amplify:ListBranches", "app-integrations:GetEventIntegration", "app-integrations:ListEventIntegrationAssociations", "app-integrations:ListEventIntegrations", "appmesh:DescribeRoute", "appmesh:ListRoutes", "aps:ListRuleGroupsNamespaces", "athena:GetPreparedStatement", "athena:ListPreparedStatements", "batch:DescribeSchedulingPolicies", "batch:ListSchedulingPolicies", "cloudformation:ListTypes", "cloudtrail:ListTrails", "codeartifact:ListDomains", "codeguru-profiler:DescribeProfilingGroup", "codeguru-profiler:GetNotificationConfiguration", "codeguru-profiler:GetPolicy", "codeguru-profiler:ListProfilingGroups", "ds:DescribeDomainControllers", "dynamodb:DescribeTableReplicaAutoScaling", "dynamodb:DescribeTimeToLive", "ec2:DescribeTrafficMirrorFilters", "evidently:GetLaunch", "evidently:ListLaunches", "forecast:DescribeDatasetGroup", "forecast	This policy now supports additional permissions for Amazon Amplify, Amazon Connect, Amazon App Mesh, Amazon Managed Service for Prometheus, Amazon Athena, Amazon Batch, Amazon CloudFormation, Amazon CloudTrail, Amazon CodeArtifact, Amazon CodeGuru, Amazon Directory Service, Amazon DynamoDB, Amazon Elastic Compute Cloud (Amazon EC2), Amazon CloudWatch Evidently, Amazon Organizations,Amazon Forecast, Amazon IoT Greengrass, Amazon Ground Station, Amazon Identity and Access Management (IAM), Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Lightsail, Amazon CloudWatch Logs, AWS Elemental MediaConnect, AWS Elemental MediaTailor, Amazon Pinpoint, Amazon Virtual Private Cloud (Amazon VPC), Amazon Personalize, Amazon QuickSight, Amazon Migration Hub Refactor Spaces, Amazon Simple Storage Service (Amazon	June 13, 2023

Change	Description	Date
:ListDatasetGroups", "greengrass:DescribeComponent", "greengrass:GetComponent", "greengrass:ListComponents", "greengrass:ListComponentVersions", "groundstation:GetMissionProfile", "groundstation:ListMissionProfiles", "iam:ListGroups", "iam:ListRoles", "kafka:DescribeConfiguration", "kafka:DescribeConfigurationRevision", "kafka:ListConfigurations", "lightsail:GetRelationalDatabases", "logs:ListTagsLogGroup", "mediaconnect:DescribeFlow", "mediaconnect:ListFlows", "mediatailor:GetPlaybackConfiguration", "mediatailor:ListPlaybackConfigurations", "mobiletargeting:GetApplicationSettings", "mobiletargeting:GetEmailTemplate", "mobiletargeting:GetEventStream", "mobiletargeting:ListTemplates", "networkmanager:GetCustomerGatewayAssociations", "networkmanager:GetLinkAssociations", "organizations:DescribeAccount", "organizations:DescribeOrganizationalUnit", "organizations:ListAccounts", "organizations:Lis	S3), Amazon SageMaker AI, Amazon Transfer Family.	

Change	Description	Date
tAccountsForParent", "organizations:ListOrganizationalUnitsForParent", "organizations:ListTagsForResource", "personalize:DescribeDataset", "personalize:DescribeDatasetGroup", "personalize:DescribeSchema", "personalize:DescribeSolution", "personalize:ListDatasetGroups", "personalize:ListDatasetImportJobs", "personalize:ListDatasets", "personalize:ListSchemas", "personalize:ListSolutions", "personalize:ListTagsForResource", "quicksight:ListTemplates", "refactor-spaces:GetEnvironment", "refactor-spaces:GetService", "refactor-spaces:ListApplications", "refactor-spaces:ListEnvironments", "refactor-spaces:ListServices", "s3:GetAccessPointPolicyStatusForObjectLambda", "sagemaker:DescribeDeviceFleet", "sagemaker:DescribeFeatureGroup", "sagemaker:ListDeviceFleets", "sagemaker:ListFeatureGroups", "sagemaker:ListModels", and "transfer:ListTagsForResource"		

Change	Description	Date
AWSConfigServiceRolePolicy – Add amplify:GetApp, amplify:ListApps, appmesh:DescribeVirtualGateway, appmesh:DescribeVirtualNode, appmesh:DescribeVirtualRouter, appmesh:DescribeVirtualService, appmesh:ListMeshes, appmesh:ListTagsForResource, appmesh:ListVirtualGateways, appmesh:ListVirtualNodes, appmesh:ListVirtualRouters, appmesh:ListVirtualServices, apprunner:DescribeVpcConnector, apprunner:ListVpcConnectors, cloudformation:ListTypes, cloudfront:ListResponseHeadersPolicies, codeartifact:ListRepositories, ds:DescribeEventTopics, ds:ListLogSubscriptions, GetInstanceTypesFromInstanceRequirement ec2:GetManagedPrefixListEntries, kendra:DescribeIndex, kendra:ListIndices, kendra:ListTagsForResource, logs:DescribeDestinations, logs:GetDataProtectionPolicy, macie2:DescribeOrganizationConfiguration, macie2:GetAutomatedD	This policy now supports additional permissions for Amazon Managed Workflows for Amazon Amplify, Amazon App Mesh, Amazon App Runner, Amazon CloudFront, Amazon CodeArtifact, Amazon Elastic Compute Cloud, Amazon Kendra, Amazon Macie, Amazon Route 53, Amazon SageMaker AI, Amazon Transfer Family, Amazon Pinpoint, Amazon Migration Hub, Amazon Resilience Hub, Amazon CloudWatch, Amazon Directory Service, and Amazon WAF.	April 13, 2023

Change	Description	Date
iscoveryConfiguration, macie2:GetClassificationExportConfiguration, macie2:GetCustomDataIdentifier, macie2:GetFindingsPublicationConfiguration, macie2:ListCustomDataIdentifiers, mobiletargeting:GetEmailChannel, refactor-spaces:GetEnvironment, refactor-spaces:ListEnvironments, resiliencehub:ListTagsForResource, route53:GetDNSSEC, sagemaker:DescribeDomain, sagemaker:DescribeModelBiasJobDefinition, sagemaker:DescribeModelQualityJobDefinition, sagemaker:DescribePipeline, sagemaker:DescribeProject, sagemaker:ListDomains, sagemaker:ListModelBiasJobDefinitions, sagemaker:ListModelQualityJobDefinitions, sagemaker:ListPipelines, sagemaker:ListProjects, transfer:DescribeAgreement, transfer:DescribeCertificate, transfer:ListAgreements, transfer:ListCertificates, and waf-regional:ListLoggingConfigurations		

Change	Description	Date
AWS_ConfigRole – Add amplify:GetApp, amplify:ListApps, appmesh:DescribeVirtualGateway, appmesh:DescribeVirtualNode, appmesh:DescribeVirtualRouter, appmesh:DescribeVirtualService, appmesh:ListMeshes, appmesh:ListTagsForResource, appmesh:ListVirtualGateways, appmesh:ListVirtualNodes, appmesh:ListVirtualRouters, appmesh:ListVirtualServices, apprunner:DescribeVpcConnector, apprunner:ListVpcConnectors, cloudformation:ListTypes, cloudfront:ListResponseHeadersPolicies, codeartifact:ListRepositories, ds:DescribeEventTopics, ds:ListLogSubscriptions, ec2:GetInstanceTypesFromInstanceRequirement, ec2:GetManagedPrefixListEntries, kendra:DescribeIndex, kendra:ListIndices, kendra:ListTagsForResource, logs:DescribeDestinations, logs:GetDataProtectionPolicy, macie2:DescribeOrganizationConfiguration, macie2:GetAutomatedDiscoveryConfiguration, macie	This policy now supports additional permissions for Amazon Managed Workflows for Amazon Amplify, Amazon App Mesh, Amazon App Runner, Amazon CloudFront, Amazon CodeArtifact, Amazon Elastic Compute Cloud, Amazon Kendra, Amazon Macie, Amazon Route 53, Amazon SageMaker AI, Amazon Transfer Family, Amazon Pinpoint, Amazon Migration Hub, Amazon Resilience Hub, Amazon CloudWatch, Amazon Directory Service, and Amazon WAF.	April 13, 2023

Change	Description	Date
2:GetClassificationExportConfiguration, macie2:GetCustomDataIdentifier, macie2:GetFindingsPublicationConfiguration, macie2:ListCustomDataIdentifiers, mobiletargeting:GetEmailChannel, refactor-spaces:GetEnvironment, refactor-spaces:ListEnvironments, resiliencehub:ListTagsForResource, route53:GetDNSSEC, sagemaker:DescribeDomain, sagemaker:DescribeModelBiasJobDefinition, sagemaker:DescribeModelQualityJobDefinition, sagemaker:DescribePipeline, sagemaker:DescribeProject, sagemaker:ListDomains, sagemaker:ListModelBiasJobDefinitions, sagemaker:ListModelQualityJobDefinitions, sagemaker:ListPipelines, sagemaker:ListProjects, transfer:DescribeAgreement, transfer:DescribeCertificate, transfer:ListAgreements, transfer:ListCertificates, and waf-regional:ListLoggingConfigurations		

Change	Description	Date
AWSConfigServiceRolePolicy – Add appflow:DescribeFlow, appflow:ListFlows, appflow:ListTagsForResource, apprunner:DescribeService, apprunner:ListServices, apprunner:ListTagsForResource, appstream:DescribeApplications, appstream:DescribeFleets, cloudfront:GetResponseHeadersPolicy, cloudwatch:ListTagsForResource, codeartifact:DescribeRepository, codeartifact:GetRepositoryPermissionsPolicy, codeartifact:ListTagsForResource, codecommit:GetRepository, codecommit:GetRepositoryTriggers, codecommit:ListRepositories, codecommit:ListTagsForResource, devicefarm:GetInstanceProfile, devicefarm:ListInstanceProfiles, devicefarm:ListProjects, evidently:GetProject, evidently:ListProjects, evidently:ListTagsForResource, forecast:DescribeDataset, forecast:ListDatasets, forecast:ListTagsForResource, groundstation:GetConfig, groundstation:ListConfigs, groundstation:ListTagsForResource, iam:GetInstanceProfile, iam:	This policy now supports additional permissions for Amazon Managed Workflows for Amazon AppFlow, Amazon App Runner, Amazon AppStream 2.0, Amazon CloudFront, Amazon CloudWatch, Amazon CodeArtifact, Amazon CodeCommit, Amazon Device Farm, Amazon CloudWatch Evidently, Amazon Forecast, Amazon Ground Station, Amazon Identity and Access Management (IAM), Amazon IoT, Amazon MemoryDB, Amazon Pinpoint, Amazon Network Manager, Amazon Panorama, Amazon Relational Database Service (Amazon RDS), Amazon Redshift, and Amazon SageMaker AI.	March 30, 2023

Change	Description	Date
GetSAMLProvider, iam:GetServerCertificate, iam:ListAccessKeys, iam:ListGroups, iam:ListInstanceProfiles, iam:ListMFADevices, iam:ListMFADeviceTags, iam:ListRoles, iam:ListSAMLProviders, iot:DescribeFleetMetric, iot:ListFleetMetrics, memorydb:DescribeUsers, memorydb:ListTags, mobiletargeting:GetApp, mobiletargeting:GetCampaigns, networkmanager:GetDevices, networkmanager:GetLinks, networkmanager:GetSites, panorama:ListNodes, rds:DescribeDBProxyEndpoints, redshift:DescribeScheduledActions, sagemaker:DescribeAppImageConfig, sagemaker:DescribeImage, sagemaker:DescribeImageVersion, sagemaker:ListAppImageConfigs, sagemaker:ListImages, and sagemaker:ListImageVersions		

Change	Description	Date
AWS_ConfigRole – Add appflow:DescribeFlow, appflow:ListFlows, appflow:ListTagsForResource, apprunner:DescribeService, apprunner:ListServices, apprunner:ListTagsForResource, appstream:DescribeApplications, appstream:DescribeFleets, cloudformation:ListTypes, cloudfront:GetResponseHeadersPolicy, cloudfront:ListDistributions, cloudwatch:ListTagsForResource, codeartifact:DescribeRepository, codeartifact:GetRepositoryPermissionsPolicy, codeartifact:ListTagsForResource, codecommit:GetRepository, codecommit:GetRepositoryTriggers, codecommit:ListRepositories, codecommit:ListTagsForResource, devicefarm:GetInstanceProfile, devicefarm:ListInstanceProfiles, devicefarm:ListProjects, ec2:DescribeTrafficMirrorFilters, evidently:GetProject, evidently:ListProjects, evidently:ListTagsForResource, forecast:DescribeDataset, forecast:ListDatasets, forecast:ListTagsForResource, groundstation:GetConfig,	This policy now supports additional permissions for Amazon Managed Workflows for Amazon AppFlow, Amazon App Runner, Amazon AppStream 2.0, Amazon CloudFormation, Amazon CloudFront, Amazon CloudWatch, Amazon CodeArtifact, Amazon CodeCommit, Amazon Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon CloudWatch Evidently, Amazon Forecast, Amazon Ground Station, Amazon Identity and Access Management (IAM), Amazon IoT, Amazon MemoryDB, Amazon Pinpoint, Amazon Network Manager, Amazon Panorama, Amazon Relational Database Service (Amazon RDS), Amazon Redshift, and Amazon SageMaker AI.	March 30, 2023

Change	Description	Date
groundstation:ListConfigs, groundstation:ListTagsForResource, iam:GetInstanceProfile, iam:GetSAMLProvider, iam:GetServerCertificate, iam:ListAccessKeys, iam:ListGroups, iam:ListInstanceProfiles, iam:ListMFADevices, iam:ListMFADeviceTags, iam:ListRoles, iam:ListSAMLProviders, iot:DescribeFleetMetric, iot:ListFleetMetrics, memorydb:DescribeUsers, memorydb:ListTags, mobiletargeting:GetApp, mobiletargeting:GetCampaigns, network manager:GetDevices, networkmanager:GetLinks, networkmanager:GetSites, panorama:ListNodes, rds:DescribeDBProxyEndpoints, redshift:DescribeScheduledActions, sagemaker:DescribeAppImageConfig, sagemaker:DescribeImage, sagemaker:DescribeImageVersion, sagemaker:ListAppImageConfigs, sagemaker:ListImages, and sagemaker:ListImageVersions		

Change	Description	Date
AWSConfigRulesExecutionRole – Amazon Config starts tracking changes for this Amazon managed policy	This policy allow Amazon Lambda functions to access the Amazon Config API and the configuration snapshots that Amazon Config delivers periodically to Amazon S3. This access is required by functions that evaluate configuration changes for Amazon Custom Lambda rules.	March 7, 2023
AWSConfigRoleForOrganizations – Amazon Config starts tracking changes for this Amazon managed policy	This policy allows Amazon Config to call read-only Amazon Organizations APIs.	March 7, 2023
AWSConfigRemediationServiceRolePolicy – Amazon Config starts tracking changes for this Amazon managed policy	This policy allows Amazon Config to remediate `NON_COMPLIANT` resources on your behalf.	March 7, 2023
AWSConfigServiceRolePolicy – Add auditmanager:GetAccountStatus	This policy now grants permission to return the registration status of an account in Amazon Audit Manager.	March 3, 2023
AWS_ConfigRole – Add auditmanager:GetAccountStatus	This policy now grants permission to return the registration status of an account in Amazon Audit Manager.	March 3, 2023

Change	Description	Date
AWSConfigMultiAccountSetupPolicy – Amazon Config starts tracking changes for this Amazon managed policy	This policy allows Amazon Config to call Amazon services and deploy Amazon Config resources across an organization with Amazon Organizations.	February 27, 2023

Change	Description	Date
AWSConfigServiceRolePolicy – Add airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar	This policy now supports additional permissions for Amazon Managed Workflows for Apache Airflow, Amazon IoT, Amazon AppStream 2.0, Amazon CodeGuru Reviewer, Amazon HealthLake, Amazon Kinesis Video Streams, Amazon Application Recovery Controller (ARC), Amazon Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Pinpoint, Amazon Identity and Access Management (IAM), Amazon GuardDuty, and Amazon CloudWatch Logs.	February 1, 2023

Change	Description	Date
m:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		

Change	Description	Date
AWS_ConfigRole – Add airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar	This policy now supports additional permissions for Amazon Managed Workflows for Apache Airflow, Amazon IoT, Amazon AppStream 2.0, Amazon CodeGuru Reviewer, Amazon HealthLake, Amazon Kinesis Video Streams, Amazon Application Recovery Controller (ARC), Amazon Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Pinpoint, Amazon Identity and Access Management (IAM), Amazon GuardDuty, and Amazon CloudWatch Logs.	February 1, 2023

Change	Description	Date
m:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		
ConfigConformsServiceRolePolicy – Update config:DescribeConfigRules	As a security best practice, this policy now removes broad resource-level permission for `config:DescribeConfigRules` .	January 12, 2023

Change	Description	Date
AWSConfigServiceRolePolicy – Add APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, Amazon Transfer Family devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, networkmanager:ListTa	This policy now supports additional permissions for Amazon Managed Service for Prometheus, Amazon Audit Manager, Amazon Device Farm, Amazon Database Migration Service (Amazon DMS), Amazon Directory Service, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Glue, Amazon IoT, Amazon Lightsail, AWS Elemental MediaPackage, Amazon Network Manager, Amazon QuickSight, Amazon Resource Access Manager, Amazon Application Recovery Controller (ARC), Amazon Simple Storage Service (Amazon S3), and Amazon Timestream.	Decemeber 15, 2022

Change	Description	Date
gsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

Change	Description	Date
AWS_ConfigRole – Add APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, networkmanager:ListTagsForResource, quicksight:D	This policy now supports additional permissions for Amazon Managed Service for Prometheus, Amazon Audit Manager, Amazon Device Farm, Amazon Database Migration Service (Amazon DMS), Amazon Directory Service, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Glue, Amazon IoT, Amazon Lightsail, AWS Elemental MediaPackage, Amazon Network Manager, Amazon QuickSight, Amazon Resource Access Manager, Amazon Application Recovery Controller (ARC), Amazon Simple Storage Service (Amazon S3), and Amazon Timestream.	Decemeber 15, 2022

Change	Description	Date
escribeDashboard, quicksigh t:DescribeDashboardPermissi ons, quicksight:DescribeTem plate, quicksight:DescribeT emplatePermissions, quicksi ght:ListDashboards, quicksigh t:ListTemplates, ram:ListRe sources, route53-recovery-c ontrol-config:DescribeContr olPanel, route53-recovery- control-config:ListControlPa nels, route53-recovery- control-config:ListTag sForResource, route53resolv er:GetResolverQueryLogConfi gAssociation, route53resolv er:ListResolverQueryLogConf igAssociations, s3:GetAcces sPointForObjectLambda, s3:G etAccessPointPolicyForObjec tLambda, s3:GetAccessPointP olicyStatusForObjectLambda, s3:GetMultiRegionAccessPoi nt, s3:ListAccessPointsForO bjectLambda, s3:ListMultiRe gionAccessPoints, timestrea m:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

Change	Description	Date
AWSConfigServiceRolePolicy – Add cloudformation:ListStackResources and cloudformation:ListStacks	This policy now grants permission to return descriptions of all resources of a specified Amazon CloudFormation stack and return the summary information for stacks whose status matches the specified StackStatusFilter.	November 7, 2022
AWS_ConfigRole – Add cloudformation:ListStackResources and cloudformation:ListStacks	This policy now grants permission to return descriptions of all resources of a specified Amazon CloudFormation stack and return the summary information for stacks whose status matches the specified StackStatusFilter.	November 7, 2022

Change	Description	Date
AWSConfigServiceRolePolicy – Add acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers	This policy now supports additional permissions for Amazon Certificate Manager, Amazon Managed Workflows for Apache Airflow, Amazon Amplify, Amazon AppConfig, Amazon Keyspaces, Amazon CloudWatch, Amazon Connect, Amazon Glue DataBrew, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service (Amazon EKS), Amazon EventBridge, Amazon Fault Injection Service, Amazon Fraud Detector, Amazon FSx, Amazon GameLift Servers, Amazon Location Service, Amazon IoT, Amazon Lex, Amazon Lightsail, Amazon Pinpoint, Amazon OpsWorks, Amazon Panorama, Amazon Resource Access Manager, Amazon QuickSight, Amazon Relational Database Service (Amazon RDS), Amazon Rekognition, Amazon RoboMaker, Amazon Resource Groups, Amazon Route 53, Amazon Simple Storage Service (Amazon S3), Amazon Cloud Map,	October 19, 2022

Change	Description	Date
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewise:DescribeProject,	and Amazon Security Token Service.	

Change	Description	Date
iotsitewise:ListAssetModels, iotsitewise:ListDashboards, iotsitewise:ListGateways, iotsitewise:ListPortals, iotsitewise:ListProjectAssets, iotsitewise:ListProjects, iotsitewise:ListTagsForResource, iotwireless:GetServiceProfile, iotwireless:GetWirelessDevice, iotwireless:GetWirelessGatewayTaskDefinition, iotwireless:ListServiceProfiles, iotwireless:ListTagsForResource, iotwireless:ListWirelessDevices, iotwireless:ListWirelessGatewayTaskDefinitions, lex:DescribeBotVersion, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDatabase, lightsail:GetRelationalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign, mobiletargeting:GetSegment, mobiletargeting:GetSegments, opsworks:DescribeInstances, opsworks:DescribeTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplicationInstance, panorama:DescribeApplicationInstanc		

Change	Description	Date
eDetails, panorama:Describe Package, panorama:DescribeP ackageVersion, panorama:Lis tApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermis sions, rds:DescribeDBProxie s, rds:DescribeGlobalClusters, rekognition:ListStreamProc essors, resource-groups:Ge tGroup, resource-groups:Get GroupConfiguration, resourc e-groups:GetGroupQuery, resource-groups:GetTags, re source-groups:ListGroupReso urces, resource-groups:Li stGroups, robomaker:ListRob otApplications, robomaker:L istSimulationApplications, route53resolver:GetResolver DnssecConfig, route53resolv er:ListResolverDnssecConfig s, s3:ListStorageLensConfig urations, schemas:GetResourc ePolicy, servicediscovery:L istInstances, sts:GetCa llerIdentity, synthetics:Ge tGroup, synthetics:ListAss ociatedGroups, synthetics:L istGroupResources, and synthetics:ListGroups		

Change	Description	Date
AWS_ConfigRole – Add acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers	This policy now supports additional permissions for Amazon Certificate Manager, Amazon Managed Workflows for Apache Airflow, Amazon Amplify, Amazon AppConfig, Amazon Keyspaces, Amazon CloudWatch, Amazon Connect, Amazon Glue DataBrew, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service (Amazon EKS), Amazon EventBridge, Amazon Fault Injection Service, Amazon Fraud Detector, Amazon FSx, Amazon GameLift Servers, Amazon Location Service, Amazon IoT, Amazon Lex, Amazon Lightsail, Amazon Pinpoint, Amazon OpsWorks, Amazon Panorama, Amazon Resource Access Manager, Amazon QuickSight, Amazon Relational Database Service (Amazon RDS), Amazon Rekognition, Amazon RoboMaker, Amazon Resource Groups, Amazon Route 53, Amazon Simple Storage Service (Amazon S3), Amazon Cloud Map,	October 19, 2022

Change	Description	Date
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewise:DescribeProject,	and Amazon Security Token Service.	

Change	Description	Date
iotsitewise:ListAssetModels, iotsitewise:ListDashboards, iotsitewise:ListGateways, iotsitewise:ListPortals, iotsitewise:ListProjectAssets, iotsitewise:ListProjects, iotsitewise:ListTagsForResource, iotwireless:GetServiceProfile, iotwireless:GetWirelessDevice, iotwireless:GetWirelessGatewayTaskDefinition, iotwireless:ListServiceProfiles, iotwireless:ListTagsForResource, iotwireless:ListWirelessDevices, iotwireless:ListWirelessGatewayTaskDefinitions, lex:DescribeBotVersion, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDatabase, lightsail:GetRelationalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign, mobiletargeting:GetSegment, mobiletargeting:GetSegments, opsworks:DescribeInstances, opsworks:DescribeTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplicationInstance, panorama:DescribeApplicationInstanc		

Change	Description	Date
eDetails, panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

Change	Description	Date
AWSConfigServiceRolePolicy – Add Glue::GetTable	This policy now grants permission to retrieve the Amazon Glue Table definition in a Data Catalog for a specified table.	September 14, 2022
AWS_ConfigRole – Add Glue::GetTable	This policy now grants permission to retrieve the Amazon Glue Table definition in a Data Catalog for a specified table.	September 14, 2022

Change	Description	Date
AWSConfigServiceRolePolicy – Add appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorFilte	This policy now supports additional permissions for Amazon AppFlow, Amazon CloudWatch, Amazon CloudWatch RUM, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon DevOps Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon EventBridge, Amazon EventBridge Schemas, Amazon FinSpace, Amazon Fraud Detector, Amazon GameLift Servers, Amazon Interactive Video Service (Amazon IVS), Amazon Managed Service for Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon QuickSight, Amazon Application Recovery Controller (ARC), Amazon Route 53 Resolver, Amazon Simple Storage	September 7, 2022

Change	Description	Date
rs, ec2:DescribeTrafficMirrorTargets, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:Descr	Service (Amazon S3), Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream, Amazon AppConfig, Amazon AppSync, Amazon Auto Scaling, Amazon Backup, Amazon Budgets, Amazon Cost Explorer, Amazon Cloud9, Amazon Directory Service, Amazon DataSync, AWS Elemental MediaPackage, Amazon Glue, Amazon IoT, Amazon IoT Analytics, Amazon IoT Events, Amazon IoT SiteWise, Amazon IoT TwinMaker, Amazon Lake Formation, Amazon License Manager, Amazon Resilience Hub, Amazon Signer, and Amazon Transfer Family.	

Change	Description	Date
ibeFleetCapacity, gamelift: DescribeFleetLocationAttrib utes, gamelift:DescribeFlee tLocationCapacity, gamelift :DescribeFleetPortSettings, gamelift:DescribeGameServe rGroup, gamelift:DescribeGa meSessionQueues, g amelift:DescribeMatchmaking Configurations, gamelift:De scribeMatchmakingRuleSets, gamelift:DescribeRuntimeCon figuration, gamelift:DescribeS cript, gamelift:DescribeVpc PeeringAuthorizations, gamelift:ListAliases, gamel ift:ListBuilds, gamelift: ListFleets, gamelift:ListGa meServerGroups, gamelift: ListScripts, gamelift:ListT agsForResource, geo:ListM aps, glue:GetClassifier, glue:GetClassifiers, imagebuil der:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeli ne, imagebuilder:GetImageRe cipe, imagebuilder:ListC ontainerRecipes, imagebuild er:ListImageBuildVersions, imagebuilder:ListImagePipel ines, imagebuilder:ListI mageRecipes, imagebuilder:L istImages, iot:DescribeCertif icate, iot:DescribeDimensio		

Change	Description	Date
n, iot:DescribeRoleAlias, iot:DescribeSecurityProfile, iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:Descri		

Change	Description	Date
beAsset, iotsitewise:ListAccessPolicies, iotsitewise:ListAssets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorkspace, iottwinmaker:ListEntities, iottwinmaker:ListScenes, iottwinmaker:ListTagsForResource, iottwinmaker:ListWorkspaces, ivs:GetPlaybackKeyPair, ivs:GetRecordingConfiguration, ivs:GetStreamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, ivs:ListRecordingConfigurations, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplications, lakeformation:DescribeResource, lakeformation:GetDataLakeSettings, lakeformation:ListPermissions, lakeformation:ListResources, lex:DescribeBot, lex:DescribeBotAlias, lex:DescribeResourcePolicy, lex:ListBotAliases, lex:ListBotLocales, lex:ListBots, lex:ListTagsForResource, license-manager:GetGrant, license-manager:GetLicense, license-manager:ListDistributedGrants, license-manager:ListLicenses, license-manager:ListReceivedGrants, lightsail:GetAlarm		

Change	Description	Date
s, lightsail:GetBuckets, lightsail:GetCertificates, lightsail:GetDisk, lightsail :GetDisks, lightsail:GetInsta nce, lightsail:GetInstances , lightsail:GetKeyPair, light sail:GetLoadBalancer, lightsail :GetLoadBalancers, lightsai l:GetLoadBalancerTlsCertifi cates, lightsail:GetStati cIp, lightsail:GetStaticIps, lookoutequipment:Describe InferenceScheduler, lookout equipment:ListTagsForResour ce, lookoutmetrics:Describe Alert, lookoutmetrics:Descr ibeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyD etectors, lookoutmetrics:Li stMetricSets, lookoutmetric s:ListTagsForResource, lookoutvision:Describe Project, lookoutvision:List Projects, managedblockchain :GetMember, managedbl ockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvit ations, managedblockchain:L istMembers, managedbl ockchain:ListNodes, mediapa ckage-vod:DescribePackaging Group, mediapackage-vod:ListPackagingGroups,		

Change	Description	Date
mediapackage-vod:ListTagsForResource, mobiletargeting:GetInAppTemplate, mobiletargeting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:De		

Change	Description	Date
scribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings, resiliencehub:ListResiliencyPolicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor,		

Change	Description	Date
rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint, s3-outposts:GetAccessPointPolicy, s3-outposts:GetBucket, s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging, s3-outposts:GetLifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:Describ		

Change	Description	Date
eTable, timestream:ListDatabases, timestream:ListTables, timestream:ListTagsForResource, transfer:DescribeServer, transfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		

Change	Description	Date
AWS_ConfigRole – Add appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorTargets, ec2:G	This policy now supports additional permissions for Amazon AppFlow, Amazon CloudWatch, Amazon CloudWatch RUM, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon DevOps Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon EventBridge, Amazon EventBridge Schemas, Amazon FinSpace, Amazon Fraud Detector, Amazon GameLift Servers, Amazon Interactive Video Service (Amazon IVS), Amazon Managed Service for Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon QuickSight, Amazon Application Recovery Controller (ARC), Amazon Route 53 Resolver, Amazon Simple Storage	September 7, 2022

Change	Description	Date
etNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity, gamelift:DescribeFleetLocationAttrib	Service (Amazon S3), Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream, Amazon AppConfig, Amazon AppSync, Amazon Auto Scaling, Amazon Backup, Amazon Budgets, Amazon Cost Explorer, Amazon Cloud9, Amazon Directory Service, Amazon DataSync, AWS Elemental MediaPackage, Amazon Glue, Amazon IoT, Amazon IoT Analytics, Amazon IoT Events, Amazon IoT SiteWise, Amazon IoT TwinMaker, Amazon Lake Formation, Amazon License Manager, Amazon Resilience Hub, Amazon Signer, and Amazon Transfer Family	

Change	Description	Date
utes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias, iot:DescribeSecurityProfile,		

Change	Description	Date
iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolicies, iotsitewise:ListAs		

Change	Description	Date
sets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorkspace, iottwinmaker:ListEntities, iottwinmaker:ListScenes, iottwinmaker:ListTagsForResource, iottwinmaker:ListWorkspaces, ivs:GetPlaybackKeyPair, ivs:GetRecordingConfiguration, ivs:GetStreamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, ivs:ListRecordingConfigurations, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplications, lakeformation:DescribeResource, lakeformation:GetDataLakeSettings, lakeformation:ListPermissions, lakeformation:ListResources, lex:DescribeBot, lex:DescribeBotAlias, lex:DescribeResourcePolicy, lex:ListBotAliases, lex:ListBotLocales, lex:ListBots, lex:ListTagsForResource, license-manager:GetGrant, license-manager:GetLicense, license-manager:ListDistributedGrants, license-manager:ListLicenses, license-manager:ListReceivedGrants, lightsail:GetAlarms, lightsail:GetBuckets, lightsail:GetCertificates,		

Change	Description	Date
lightsail:GetDisk, lightsail :GetDisks, lightsail:GetInsta nce, lightsail:GetInstances , lightsail:GetKeyPair, light sail:GetLoadBalancer, lightsail :GetLoadBalancers, lightsai l:GetLoadBalancerTlsCertifi cates, lightsail:GetStati cIp, lightsail:GetStaticIps, lookoutequipment:Describe InferenceScheduler, lookout equipment:ListTagsForResour ce, lookoutmetrics:Describe Alert, lookoutmetrics:Descr ibeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyD etectors, lookoutmetrics:Li stMetricSets, lookoutmetric s:ListTagsForResource, lookoutvision:Describe Project, lookoutvision:List Projects, managedblockchain :GetMember, managedbl ockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvit ations, managedblockchain:L istMembers, managedbl ockchain:ListNodes, mediapa ckage-vod:DescribePackaging Group, mediapackage- vod:ListPackagingGroups, mediapackage-vod:L istTagsForResource, mobilet		

Change	Description	Date
argeting:GetInAppTemplate, mobiletargeting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, res		

Change	Description	Date
iliencehub:ListAppVersionResourceMappings, resiliencehub:ListResiliencyPolicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:Li		

Change	Description	Date
stTagsForResource, s3-outposts:GetAccessPoint, s3-outposts:GetAccessPointPolicy, s3-outposts:GetBucket, s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging, s3-outposts:GetLifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTab		

Change	Description	Date
les, timestream:ListTagsFor Resource, transfer:DescribeS erver, transfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer: ListUsers, transfer:ListWor kflows, voiceid:DescribeDo main, and voiceid:ListTa gsForResource		

Change	Description	Date
AWSConfigServiceRolePolicy – Add airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar	This policy now supports additional permissions for Amazon Managed Workflows for Apache Airflow, Amazon IoT, Amazon AppStream 2.0, Amazon CodeGuru Reviewer, Amazon HealthLake, Amazon Kinesis Video Streams, Amazon Application Recovery Controller (ARC), Amazon Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Pinpoint, Amazon Identity and Access Management (IAM), Amazon GuardDuty, and Amazon CloudWatch Logs.	February 1, 2023

Change	Description	Date
m:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		

Change	Description	Date
AWS_ConfigRole – Add airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar	This policy now supports additional permissions for Amazon Managed Workflows for Apache Airflow, Amazon IoT, Amazon AppStream 2.0, Amazon CodeGuru Reviewer, Amazon HealthLake, Amazon Kinesis Video Streams, Amazon Application Recovery Controller (ARC), Amazon Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Pinpoint, Amazon Identity and Access Management (IAM), Amazon GuardDuty, and Amazon CloudWatch Logs.	February 1, 2023

Change	Description	Date
m:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		
ConfigConformsServiceRolePolicy – Update config:DescribeConfigRules	As a security best practice, this policy now removes broad resource-level permission for `config:DescribeConfigRules` .	January 12, 2023

Change	Description	Date
AWSConfigServiceRolePolicy – Add APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, Amazon Transfer Family devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, networkmanager:ListTa	This policy now supports additional permissions for Amazon Managed Service for Prometheus, Amazon Audit Manager, Amazon Device Farm, Amazon Database Migration Service (Amazon DMS), Amazon Directory Service, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Glue, Amazon IoT, Amazon Lightsail, AWS Elemental MediaPackage, Amazon Network Manager, Amazon QuickSight, Amazon Resource Access Manager, Amazon Application Recovery Controller (ARC), Amazon Simple Storage Service (Amazon S3), and Amazon Timestream.	Decemeber 15, 2022

Change	Description	Date
gsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

Change	Description	Date
AWS_ConfigRole – Add APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, networkmanager:ListTagsForResource, quicksight:D	This policy now supports additional permissions for Amazon Managed Service for Prometheus, Amazon Audit Manager, Amazon Device Farm, Amazon Database Migration Service (Amazon DMS), Amazon Directory Service, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Glue, Amazon IoT, Amazon Lightsail, AWS Elemental MediaPackage, Amazon Network Manager, Amazon QuickSight, Amazon Resource Access Manager, Amazon Application Recovery Controller (ARC), Amazon Simple Storage Service (Amazon S3), and Amazon Timestream.	December 15, 2022

Change	Description	Date
escribeDashboard, quicksigh t:DescribeDashboardPermissi ons, quicksight:DescribeTem plate, quicksight:DescribeT emplatePermissions, quicksi ght:ListDashboards, quicksigh t:ListTemplates, ram:ListRe sources, route53-recovery-c ontrol-config:DescribeContr olPanel, route53-recovery- control-config:ListControlPa nels, route53-recovery- control-config:ListTag sForResource, route53resolv er:GetResolverQueryLogConfi gAssociation, route53resolv er:ListResolverQueryLogConf igAssociations, s3:GetAcces sPointForObjectLambda, s3:G etAccessPointPolicyForObjec tLambda, s3:GetAccessPointP olicyStatusForObjectLambda, s3:GetMultiRegionAccessPoi nt, s3:ListAccessPointsForO bjectLambda, s3:ListMultiRe gionAccessPoints, timestrea m:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

Change	Description	Date
AWSConfigServiceRolePolicy – Add cloudformation:ListStackResources and cloudformation:ListStacks	This policy now grants permission to return descriptions of all resources of a specified Amazon CloudFormation stack and return the summary information for stacks whose status matches the specified StackStatusFilter.	November 7, 2022
AWS_ConfigRole – Add cloudformation:ListStackResources and cloudformation:ListStacks	This policy now grants permission to return descriptions of all resources of a specified Amazon CloudFormation stack and return the summary information for stacks whose status matches the specified StackStatusFilter.	November 7, 2022

Change	Description	Date
AWSConfigServiceRolePolicy – Add acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers	This policy now supports additional permissions for Amazon Certificate Manager, Amazon Managed Workflows for Apache Airflow, Amazon Amplify, Amazon AppConfig, Amazon Keyspaces, Amazon CloudWatch, Amazon Connect, Amazon Glue DataBrew, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service (Amazon EKS), Amazon EventBridge, Amazon Fault Injection Service, Amazon Fraud Detector, Amazon FSx, Amazon GameLift Servers, Amazon Location Service, Amazon IoT, Amazon Lex, Amazon Lightsail, Amazon Pinpoint, Amazon OpsWorks, Amazon Panorama, Amazon Resource Access Manager, Amazon QuickSight, Amazon Relational Database Service (Amazon RDS), Amazon Rekognition, Amazon RoboMaker, Amazon Resource Groups, Amazon Route 53, Amazon Simple Storage Service (Amazon S3), Amazon Cloud Map,	October 19, 2022

Change	Description	Date
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewise:DescribeProject,	and Amazon Security Token Service.	

Change	Description	Date
iotsitewise:ListAssetModels, iotsitewise:ListDashboards, iotsitewise:ListGateways, iotsitewise:ListPortals, iotsitewise:ListProjectAssets, iotsitewise:ListProjects, iotsitewise:ListTagsForResource, iotwireless:GetServiceProfile, iotwireless:GetWirelessDevice, iotwireless:GetWirelessGatewayTaskDefinition, iotwireless:ListServiceProfiles, iotwireless:ListTagsForResource, iotwireless:ListWirelessDevices, iotwireless:ListWirelessGatewayTaskDefinitions, lex:DescribeBotVersion, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDatabase, lightsail:GetRelationalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign, mobiletargeting:GetSegment, mobiletargeting:GetSegments, opsworks:DescribeInstances, opsworks:DescribeTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplicationInstance, panorama:DescribeApplicationInstanc		

Change	Description	Date
eDetails, panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

Change	Description	Date
AWS_ConfigRole – Add acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers	This policy now supports additional permissions for Amazon Certificate Manager, Amazon Managed Workflows for Apache Airflow, Amazon Amplify, Amazon AppConfig, Amazon Keyspaces, Amazon CloudWatch, Amazon Connect, Amazon Glue DataBrew, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service (Amazon EKS), Amazon EventBridge, Amazon Fault Injection Service, Amazon Fraud Detector, Amazon FSx, Amazon GameLift Servers, Amazon Location Service, Amazon IoT, Amazon Lex, Amazon Lightsail, Amazon Pinpoint, Amazon OpsWorks, Amazon Panorama, Amazon Resource Access Manager, Amazon QuickSight, Amazon Relational Database Service (Amazon RDS), Amazon Rekognition, Amazon RoboMaker, Amazon Resource Groups, Amazon Route 53, Amazon Simple Storage Service (Amazon S3), Amazon Cloud Map,	October 19, 2022

Change	Description	Date
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewise:DescribeProject,	and Amazon Security Token Service.	

Change	Description	Date
iotsitewise:ListAssetModels, iotsitewise:ListDashboards, iotsitewise:ListGateways, iotsitewise:ListPortals, iotsitewise:ListProjectAssets, iotsitewise:ListProjects, iotsitewise:ListTagsForResource, iotwireless:GetServiceProfile, iotwireless:GetWirelessDevice, iotwireless:GetWirelessGatewayTaskDefinition, iotwireless:ListServiceProfiles, iotwireless:ListTagsForResource, iotwireless:ListWirelessDevices, iotwireless:ListWirelessGatewayTaskDefinitions, lex:DescribeBotVersion, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDatabase, lightsail:GetRelationalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign, mobiletargeting:GetSegment, mobiletargeting:GetSegments, opsworks:DescribeInstances, opsworks:DescribeTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplicationInstance, panorama:DescribeApplicationInstanc		

Change	Description	Date
eDetails, panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

Change	Description	Date
AWSConfigServiceRolePolicy – Add Glue::GetTable	This policy now grants permission to retrieve the Amazon Glue Table definition in a Data Catalog for a specified table.	September 14, 2022
AWS_ConfigRole – Add Glue::GetTable	This policy now grants permission to retrieve the Amazon Glue Table definition in a Data Catalog for a specified table.	September 14, 2022

Change	Description	Date
AWSConfigServiceRolePolicy – Add appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorFilte	This policy now supports additional permissions for Amazon AppFlow, Amazon CloudWatch, Amazon CloudWatch RUM, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon DevOps Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon EventBridge, Amazon EventBridge Schemas, Amazon FinSpace, Amazon Fraud Detector, Amazon GameLift Servers, Amazon Interactive Video Service (Amazon IVS), Amazon Managed Service for Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon QuickSight, Amazon Application Recovery Controller (ARC), Amazon Route 53 Resolver, Amazon Simple Storage	September 7, 2022

Change	Description	Date
rs, ec2:DescribeTrafficMirrorTargets, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:Descr	Service (Amazon S3), Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream, Amazon AppConfig, Amazon AppSync, Amazon Auto Scaling, Amazon Backup, Amazon Budgets, Amazon Cost Explorer, Amazon Cloud9, Amazon Directory Service, Amazon DataSync, AWS Elemental MediaPackage, Amazon Glue, Amazon IoT, Amazon IoT Analytics, Amazon IoT Events, Amazon IoT SiteWise, Amazon IoT TwinMaker, Amazon Lake Formation, Amazon License Manager, Amazon Resilience Hub, Amazon Signer, and Amazon Transfer Family.	

Change	Description	Date
ibeFleetCapacity, gamelift: DescribeFleetLocationAttrib utes, gamelift:DescribeFlee tLocationCapacity, gamelift :DescribeFleetPortSettings, gamelift:DescribeGameServe rGroup, gamelift:DescribeGa meSessionQueues, g amelift:DescribeMatchmaking Configurations, gamelift:De scribeMatchmakingRuleSets, gamelift:DescribeRuntimeCon figuration, gamelift:DescribeS cript, gamelift:DescribeVpc PeeringAuthorizations, gamelift:ListAliases, gamel ift:ListBuilds, gamelift: ListFleets, gamelift:ListGa meServerGroups, gamelift: ListScripts, gamelift:ListT agsForResource, geo:ListM aps, glue:GetClassifier, glue:GetClassifiers, imagebuil der:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeli ne, imagebuilder:GetImageRe cipe, imagebuilder:ListC ontainerRecipes, imagebuild er:ListImageBuildVersions, imagebuilder:ListImagePipel ines, imagebuilder:ListI mageRecipes, imagebuilder:L istImages, iot:DescribeCertif icate, iot:DescribeDimensio		

Change	Description	Date
n, iot:DescribeRoleAlias, iot:DescribeSecurityProfile, iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:Descri		

Change	Description	Date
beAsset, iotsitewise:ListAccessPolicies, iotsitewise:ListAssets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorkspace, iottwinmaker:ListEntities, iottwinmaker:ListScenes, iottwinmaker:ListTagsForResource, iottwinmaker:ListWorkspaces, ivs:GetPlaybackKeyPair, ivs:GetRecordingConfiguration, ivs:GetStreamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, ivs:ListRecordingConfigurations, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplications, lakeformation:DescribeResource, lakeformation:GetDataLakeSettings, lakeformation:ListPermissions, lakeformation:ListResources, lex:DescribeBot, lex:DescribeBotAlias, lex:DescribeResourcePolicy, lex:ListBotAliases, lex:ListBotLocales, lex:ListBots, lex:ListTagsForResource, license-manager:GetGrant, license-manager:GetLicense, license-manager:ListDistributedGrants, license-manager:ListLicenses, license-manager:ListReceivedGrants, lightsail:GetAlarm		

Change	Description	Date
s, lightsail:GetBuckets, lightsail:GetCertificates, lightsail:GetDisk, lightsail :GetDisks, lightsail:GetInsta nce, lightsail:GetInstances , lightsail:GetKeyPair, light sail:GetLoadBalancer, lightsail :GetLoadBalancers, lightsai l:GetLoadBalancerTlsCertifi cates, lightsail:GetStati cIp, lightsail:GetStaticIps, lookoutequipment:Describe InferenceScheduler, lookout equipment:ListTagsForResour ce, lookoutmetrics:Describe Alert, lookoutmetrics:Descr ibeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyD etectors, lookoutmetrics:Li stMetricSets, lookoutmetric s:ListTagsForResource, lookoutvision:Describe Project, lookoutvision:List Projects, managedblockchain :GetMember, managedbl ockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvit ations, managedblockchain:L istMembers, managedbl ockchain:ListNodes, mediapa ckage-vod:DescribePackaging Group, mediapackage-vod:ListPackagingGroups,		

Change	Description	Date
mediapackage-vod:ListTagsForResource, mobiletargeting:GetInAppTemplate, mobiletargeting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:De		

Change	Description	Date
scribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings, resiliencehub:ListResiliencyPolicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor,		

Change	Description	Date
rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint, s3-outposts:GetAccessPointPolicy, s3-outposts:GetBucket, s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging, s3-outposts:GetLifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:Describ		

Change	Description	Date
eTable, timestream:ListDatabases, timestream:ListTables, timestream:ListTagsForResource, transfer:DescribeServer, transfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		

Change	Description	Date
AWS_ConfigRole – Add appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorTargets, ec2:G	This policy now supports additional permissions for Amazon AppFlow, Amazon CloudWatch, Amazon CloudWatch RUM, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon DevOps Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon EventBridge, Amazon EventBridge Schemas, Amazon FinSpace, Amazon Fraud Detector, Amazon GameLift Servers, Amazon Interactive Video Service (Amazon IVS), Amazon Managed Service for Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon QuickSight, Amazon Application Recovery Controller (ARC), Amazon Route 53 Resolver, Amazon Simple Storage	September 7, 2022

Change	Description	Date
etNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity, gamelift:DescribeFleetLocationAttrib	Service (Amazon S3), Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream, Amazon AppConfig, Amazon AppSync, Amazon Auto Scaling, Amazon Backup, Amazon Budgets, Amazon Cost Explorer, Amazon Cloud9, Amazon Directory Service, Amazon DataSync, AWS Elemental MediaPackage, Amazon Glue, Amazon IoT, Amazon IoT Analytics, Amazon IoT Events, Amazon IoT SiteWise, Amazon IoT TwinMaker, Amazon Lake Formation, Amazon License Manager, Amazon Resilience Hub, Amazon Signer, and Amazon Transfer Family	

Change	Description	Date
utes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias, iot:DescribeSecurityProfile,		

Change	Description	Date
iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolicies, iotsitewise:ListAs		

Change	Description	Date
sets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorkspace, iottwinmaker:ListEntities, iottwinmaker:ListScenes, iottwinmaker:ListTagsForResource, iottwinmaker:ListWorkspaces, ivs:GetPlaybackKeyPair, ivs:GetRecordingConfiguration, ivs:GetStreamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, ivs:ListRecordingConfigurations, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplications, lakeformation:DescribeResource, lakeformation:GetDataLakeSettings, lakeformation:ListPermissions, lakeformation:ListResources, lex:DescribeBot, lex:DescribeBotAlias, lex:DescribeResourcePolicy, lex:ListBotAliases, lex:ListBotLocales, lex:ListBots, lex:ListTagsForResource, license-manager:GetGrant, license-manager:GetLicense, license-manager:ListDistributedGrants, license-manager:ListLicenses, license-manager:ListReceivedGrants, lightsail:GetAlarms, lightsail:GetBuckets, lightsail:GetCertificates,		

Change	Description	Date
lightsail:GetDisk, lightsail :GetDisks, lightsail:GetInsta nce, lightsail:GetInstances , lightsail:GetKeyPair, light sail:GetLoadBalancer, lightsail :GetLoadBalancers, lightsai l:GetLoadBalancerTlsCertifi cates, lightsail:GetStati cIp, lightsail:GetStaticIps, lookoutequipment:Describe InferenceScheduler, lookout equipment:ListTagsForResour ce, lookoutmetrics:Describe Alert, lookoutmetrics:Descr ibeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyD etectors, lookoutmetrics:Li stMetricSets, lookoutmetric s:ListTagsForResource, lookoutvision:Describe Project, lookoutvision:List Projects, managedblockchain :GetMember, managedbl ockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvit ations, managedblockchain:L istMembers, managedbl ockchain:ListNodes, mediapa ckage-vod:DescribePackaging Group, mediapackage- vod:ListPackagingGroups, mediapackage-vod:L istTagsForResource, mobilet		

Change	Description	Date
argeting:GetInAppTemplate, mobiletargeting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, res		

Change	Description	Date
iliencehub:ListAppVersionResourceMappings, resiliencehub:ListResiliencyPolicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:Li		

Change	Description	Date
stTagsForResource, s3-outposts:GetAccessPoint, s3-outposts:GetAccessPointPolicy, s3-outposts:GetBucket, s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging, s3-outposts:GetLifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTab		

Change	Description	Date
les, timestream:ListTagsFor Resource, transfer:DescribeS erver, transfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer: ListUsers, transfer:ListWor kflows, voiceid:DescribeDo main, and voiceid:ListTa gsForResource		
AWSConfigServiceRolePolicy – Add datasync:ListAgent s, datasync:ListLocations, datasync:ListTasks, servicedi scovery:ListNamespaces, ser vicediscovery:ListServices, and ses:ListContactLists	This policy now grants permission to return a list of Amazon DataSync a gents, DataSync source and destination locations, and DataSync tasks in an Amazon Web Services account; list summary information about the Amazon Cloud Map namespaces and services that are associated with one or more specified namespaces in an Amazon Web Services account; and list all the Amazon Simple Email Service (Amazon SES) contact lists available in Amazon Web Services account.	August 22, 2022

Change	Description	Date
AWS_ConfigRole – Add datasync:ListAgents, datasync:ListLocations, datasync:ListTasks, servicediscovery:ListNamespaces, servicediscovery:ListServices, and ses:ListContactLists	This policy now grants permission to return a list of Amazon DataSync agents, DataSync source and destination locations, and DataSync tasks in an Amazon Web Services account; list summary information about the Amazon Cloud Map namespaces and services that are associated with one or more specified namespaces in an Amazon Web Services account; and list all the Amazon Simple Email Service (Amazon SES) contact lists available in Amazon Web Services account.	August 22, 2022
ConfigConformsServiceRolePolicy – Add cloudwatch:PutMetricData	This policy now grants permission to publish metric data points to Amazon CloudWatch.	July 25, 2022

Change	Description	Date
AWSConfigServiceRolePolicy – Add amplifyuibuilder:ExportThemes, amplifyuibuilder:GetTheme, appconfig:GetApplication, appconfig:GetApplication, appconfig:GetConfigurationProfile, appconfig:GetConfigurationProfile, appconfig:GetDeployment, appconfig:GetDeploymentStrategy, appconfig:GetEnvironment, appconfig:GetHostedConfigurationVersion, appconfig:ListTagsForResource, appsync:GetGraphqlApi, appsync:ListGraphqlApis, billingconductor:ListPricingRulesAssociatedToPricingPlan, billingconductor:ListAccountAssociations, billingconductor:ListBillingGroups, billingconductor:ListCustomLineItems, billingconductor:ListPricingPlans, billingconductor:ListPricingRules, billingconductor:ListTagsForResource, datasync:DescribeAgent, datasync:DescribeLocationEfs, datasync:DescribeLocationFsxLustre, datasync:DescribeLocationHdfs, datasync:DescribeLocationNfs, datasync:DescribeLocatio	This policy now supports additional permissions for Amazon Elastic Container Service (Amazon ECS), Amazon ElastiCache, Amazon EventBridge, Amazon FSx, Amazon Managed Service for Apache Flink, Amazon Location Service, Amazon Managed Streaming for Apache Kafka, Amazon QuickSight, Amazon Rekognition, Amazon RoboMaker, Amazon Simple Storage Service (Amazon S3), Amazon Simple Email Service (Amazon SES), Amazon Amplify, Amazon AppConfig, Amazon AppSync, Amazon Billing Conductor, Amazon DataSync, Amazon Firewall Manager, Amazon Glue, Amazon IAM Identity Center (IAM Identity Center), EC2 Image Builder, and Elastic Load Balancing.	July 15, 2022

Change	Description	Date
nObjectStorage, datasync:DescribeLocationS3, datasync:DescribeLocationSmb, datasync:DescribeTask, datasync:ListTagsForResource, ecr:DescribePullThroughCacheRules, ecr:DescribeRegistry, ecr:GetRegistryPolicy, elasticache:DescribeCacheParameters, elasticloadbalancing:DescribeListenerCertificates, elasticloadbalancing:DescribeTargetGroupAttributes, elasticloadbalancing:DescribeTargetGroups, elasticloadbalancing:DescribeTargetHealth, events:DescribeApiDestination, events:DescribeArchive, fms:GetNotificationChannel, fms:GetPolicy, fms:ListPolicies, fms:ListTagsForResource, fsx:DescribeVolumes, geo:DescribeGeofenceCollection, geo:DescribeMap, geo:DescribePlaceIndex, geo:DescribeRouteCalculator, geo:DescribeTracker, geo:ListTrackerConsumers, glue:BatchGetJobs, glue:BatchGetWorkflows, glue:GetCrawler, glue:GetCrawlers, glue:GetJob, glue:GetJobs, glue:GetWorkflow, imagebuilder: GetComponent, imagebuilder: List		

Change	Description	Date
ComponentBuildVersions, imagebuilder: ListCompo nents, imagebuilder:GetDist ributionConfiguration, imag ebuilder:GetInfrastructureC onfiguration, imagebuilder: ListDistributionConfigurati ons, imagebuilder:ListInfra structureConfigurations, kafka:DescribeClusterV2, kafka:ListClustersV2, kines isanalytics:DescribeApplica tion, kinesisanalytics:List TagsForResource, quicksight :DescribeDataSource, quicks ight:DescribeDataSourcePerm issions, quicksight:ListTag sForResource, rekognition:D escribeStreamProcessor, rekognition:ListTagsF orResource, robomaker:Descr ibeRobotApplication, roboma ker:DescribeSimulationAppli cation, s3:GetStorageLensCo nfiguration, s3:GetStorageL ensConfigurationTagging, se rvicediscovery:GetInstance, servicediscovery:GetNamespa ce, servicediscovery:GetSer vice, servicediscovery:List TagsForResource, ses:Descr ibeReceiptRule, ses:Describ eReceiptRuleSet, ses:GetCo ntactList, ses:GetEmailTemp late, ses:GetTemplate, and		

Change	Description	Date
sso:GetInlinePolicyForPermissionSet		

Change	Description	Date
AWS_ConfigRole – Add amplifyuibuilder:ExportThemes, amplifyuibuilder:GetTheme, appconfig:GetApplication, appconfig:GetApplication, appconfig:GetConfigurationProfile, appconfig:GetConfigurationProfile, appconfig:GetDeployment, appconfig:GetDeploymentStrategy, appconfig:GetEnvironment, appconfig:GetHostedConfigurationVersion, appconfig:ListTagsForResource, appsync:GetGraphqlApi, appsync:ListGraphqlApis, billingconductor:ListPricingRulesAssociatedToPricingPlan, billingconductor:ListAccountAssociations, billingconductor:ListBillingGroups, billingconductor:ListCustomLineItems, billingconductor:ListPricingPlans, billingconductor:ListPricingRules, billingconductor:ListTagsForResource, datasync:DescribeAgent, datasync:DescribeLocationEfs, datasync:DescribeLocationFsxLustre, datasync:DescribeLocationHdfs, datasync:DescribeLocationNfs, datasync:DescribeLocationObjectStorage, datasync:De	This policy now supports additional permissions for Amazon Elastic Container Service (Amazon ECS), Amazon ElastiCache, Amazon EventBridge, Amazon FSx, Amazon Managed Service for Apache Flink, Amazon Location Service, Amazon Managed Streaming for Apache Kafka, Amazon QuickSight, Amazon Rekognition, Amazon RoboMaker, Amazon Simple Storage Service (Amazon S3), Amazon Simple Email Service (Amazon SES), Amazon Amplify, Amazon AppConfig, Amazon AppSync, Amazon Billing Conductor, Amazon DataSync, Amazon Firewall Manager, Amazon Glue, Amazon IAM Identity Center (IAM Identity Center), EC2 Image Builder, and Elastic Load Balancing.	July 15, 2022

Change	Description	Date
scribeLocationS3, datasync: DescribeLocationSmb, datasync:DescribeTask, datasync: ListTagsForResource, ecr:DescribePullThroughCacheRules, ecr:DescribeRegistry, ecr:GetRegistryPolicy, elasticache:DescribeCacheParameters, elasticloadbalancing:DescribeListenerCertificates, elasticloadbalancing:DescribeTargetGroupAttributes, elasticloadbalancing:DescribeTargetGroups, elasticloadbalancing:DescribeTargetHealth, events:DescribeApiDestination, events:DescribeArchive, fms:GetNotificationChannel, fms:GetPolicy, fms:ListPolicies, fms:ListTagsForResource, fsx:DescribeVolumes, geo:DescribeGeofenceCollection, geo:DescribeMap, geo:DescribePlaceIndex, geo:DescribeRouteCalculator, geo:DescribeTracker, geo:ListTrackerConsumers, glue:BatchGetJobs, glue:BatchGetWorkflows, glue:GetCrawler, glue:GetCrawlers, glue:GetJob, glue:GetJobs, glue:GetWorkflow, imagebuilder: GetComponent, imagebuilder: ListComponentBuildVersions,		

Change	Description	Date
imagebuilder: ListComponents, imagebuilder:GetDistributionConfiguration, imagebuilder:GetInfrastructureConfiguration, imagebuilder:ListDistributionConfigurations, imagebuilder:ListInfrastructureConfigurations, kafka:DescribeClusterV2, kafka:ListClustersV2, kinesisanalytics:DescribeApplication, kinesisanalytics:ListTagsForResource, quicksight:DescribeDataSource, quicksight:DescribeDataSourcePermissions, quicksight:ListTagsForResource, rekognition:DescribeStreamProcessor, rekognition:ListTagsForResource, robomaker:DescribeRobotApplication, robomaker:DescribeSimulationApplication, s3:GetStorageLensConfiguration, s3:GetStorageLensConfigurationTagging, servicediscovery:GetInstance, servicediscovery:GetNamespace, servicediscovery:GetService, servicediscovery:ListTagsForResource, ses:DescribeReceiptRule, ses:DescribeReceiptRuleSet, ses:GetContactList, ses:GetEmailTemplate, ses:GetTemplate, and		

Change	Description	Date
sso:GetInlinePolicyForPermissionSet		

Change	Description	Date
AWSConfigServiceRolePolicy – Add athena:GetDataCatalog, athena:ListDataCatalogs, athena:ListTagsForResource, detective:ListGraphs, detective:ListTagsForResource, glue:BatchGetDevEndpoints, glue:GetDevEndpoint, glue:GetDevEndpoints, glue:GetSecurityConfiguration, glue:GetSecurityConfigurations, glue:GetTags glue:GetWorkGroup, glue:ListCrawlers, glue:ListDevEndpoints, glue:ListJobs, glue:ListMembers, glue:ListWorkflows, glue:ListWorkGroups, guardduty:GetFilter, guardduty:GetIPSet, guardduty:GetThreatIntelSet, guardduty:GetMembers, guardduty:ListFilters, guardduty:ListIPSets, guardduty:ListTagsForResource, guardduty:ListThreatIntelSets, macie:GetMacieSession, ram:GetResourceShareAssociations, ram:GetResourceShares, ses:GetConfigurationSet, ses:GetConfigurationSetEventDestinations, ses:ListConfigurationSets, sso:DescribeInstanceAccessControlAttributeConfiguration, sso:DescribePer	This policy now grants permission to get a specified Amazon Athena data catalog, list the Athena data catalogs in an Amazon Web Services account, and list tags associated with an Athena workgroup or data catalog resource; to get a list of Amazon Detective behavior graphs and list tags for a Detective behavior graph; get a list of resource metadata for a given list of Amazon Glue development endpoint names, get information about a specified Amazon Glue development endpoint, get all the Amazon Glue development endpoints in an Amazon Web Services account, retrieve a specified Amazon Glue security configuration, get all Amazon Glue security configurations, get a list of tags associated with an Amazon Glue resource, get information about an Amazon Glue workgroup with the specified name, retrieve the names of all Amazon Glue crawler resources in an Amazon account, get the	May 31, 2022

Change	Description	Date
missionSet, sso:ListManaged PoliciesInPermissionSet, sso:ListPermissionSets, and sso:ListTagsForResource	names of all Amazon Glue `DevEndpoint` resources in an Amazon Web Services account, list the names of all Amazon Glue job resources in an Amazon Web Services account, get details about Amazon Glue member acc ounts, list names of Amazon Glue workflows created in an account, and list available Amazon Glue workgroups for an account; to retrieve details about an Amazon GuardDuty filter, retrieve a GuardDuty IPSet, retrieve a GuardDuty ThreatInt elSet, retrieve GuardDuty member accounts, get a list of GuardDuty filters, get the IPSets of the GuardDuty service, retrieve tags for the GuardDuty Service, and get the ThreatIntelSets of the GuardDuty service; to get the current status and configura tion settings for an Amazon Macie account; to retrieve the resource and principal associations for Amazon Resource Access Manager (Amazon RAM) resource shares and retrieve details about Amazon RAM resour ce shares; to get informati	

Change	Description	Date
	on about an Amazon Simple Email Service (Amazon SES) existing configuration set, get a list of event destinations that are associated with an Amazon SES configuration set, and list all of the configuration sets associated with an Amazon SES account; and to get a list of Identity Center directory attributes, get the details of an Amazon IAM Identity Center permission set, get the IAM managed policy that is attached to a specified IAM Identity Center permission set, get the permissions set for an IAM Identity Center instance, and get tags for IAM Identity Center resources.	

Change	Description	Date
AWS_ConfigRole – Add athena:GetDataCatalog, athena:ListDataCatalogs, athena:ListTagsForResource, detective:ListGraphs, detective:ListTagsForResource, glue:BatchGetDevEndpoints, glue:GetDevEndpoint, glue:GetDevEndpoints, glue:GetSecurityConfiguration, glue:GetSecurityConfigurations, glue:GetTags glue:GetWorkGroup, glue:ListCrawlers, glue:ListDevEndpoints, glue:ListJobs, glue:ListMembers, glue:ListWorkflows, glue:ListWorkGroups, guardduty:GetFilter, guardduty:GetIPSet, guardduty:GetThreatIntelSet, guardduty:GetMembers, guardduty:ListFilters, guardduty:ListIPSets, guardduty:ListTagsForResource, guardduty:ListThreatIntelSets, macie:GetMacieSession, ram:GetResourceShareAssociations, ram:GetResourceShares, ses:GetConfigurationSet, ses:GetConfigurationSetEventDestinations, ses:ListConfigurationSets, sso:DescribeInstanceAccessControlAttributeConfiguration, sso:DescribePer	This policy now grants permission to get a specified Amazon Athena data catalog, list the Athena data catalogs in an Amazon Web Services account, and list tags associated with an Athena workgroup or data catalog resource; to get a list of Amazon Detective behavior graphs and list tags for a Detective behavior graph; get a list of resource metadata for a given list of Amazon Glue development endpoint names, get information about a specified Amazon Glue development endpoint, get all the Amazon Glue development endpoints in an Amazon Web Services account, retrieve a specified Amazon Glue security configuration, get all Amazon Glue security configurations, get a list of tags associated with an Amazon Glue resource, get information about an Amazon Glue workgroup with the specified name, retrieve the names of all Amazon Glue crawler resources in an Amazon account, get the	May 31, 2022

Change	Description	Date
missionSet, sso:ListManaged PoliciesInPermissionSet, sso:ListPermissionSets, and sso:ListTagsForResource	names of all Amazon Glue `DevEndpoint` resources in an Amazon Web Services account, list the names of all Amazon Glue job resources in an Amazon Web Services account, get details about Amazon Glue member acc ounts, list names of Amazon Glue workflows created in an account, and list available Amazon Glue workgroups for an account; to retrieve details about an Amazon GuardDuty filter, retrieve a GuardDuty IPSet, retrieve a GuardDuty ThreatInt elSet, retrieve GuardDuty member accounts, get a list of GuardDuty filters, get the IPSets of the GuardDuty service, retrieve tags for the GuardDuty Service, and get the ThreatIntelSets of the GuardDuty service; to get the current status and configura tion settings for an Amazon Macie account; to retrieve the resource and principal associations for Amazon Resource Access Manager (Amazon RAM) resource shares and retrieve details about Amazon RAM resour ce shares; to get informati	

Change	Description	Date
	on about an Amazon Simple Email Service (Amazon SES) existing configuration set, get a list of event destinations that are associated with an Amazon SES configuration set, and list all of the configuration sets associated with an Amazon SES account; and to get a list of Identity Center directory attributes, get the details of an Amazon IAM Identity Center permission set, get the IAM managed policy that is attached to a specified IAM Identity Center permission set, get the permissions set for an IAM Identity Center instance, and get tags for IAM Identity Center resources.	

Change	Description	Date
AWSConfigServiceRolePolicy – Add cloudformation:GetResource, cloudformation:ListResources, cloudtrail:GetEventDataStore, cloudtrail:ListEventDataStores, dax:DescribeParameterGroups, dax:DescribeParameters, dax:DescribeSubnetGroups, DMS:DescribeReplicationTasks, and organizations:ListPolicies	This policy now grants permission to get information about all or a specified Amazon CloudTrail event data store (EDS), get information about all or a specified Amazon CloudFormation resource, get a list of a DynamoDB Accelerator (DAX) parameter group or subnet group, get information about Amazon Database Migration Service (Amazon DMS) replication tasks for your account in the current region being accessed, and get a list all policies in an Amazon Organizations of a specified type.	April 7, 2022

Change	Description	Date
AWS_ConfigRole – Add cloudformation:GetResource, cloudformation:ListResources, cloudtrail:GetEventDataStore, cloudtrail:ListEventDataStores, dax:DescribeParameterGroups, dax:DescribeParameters, dax:DescribeSubnetGroups, DMS:DescribeReplicationTasks, and organizations:ListPolicies	This policy now grants permission to get information about all or a specified Amazon CloudTrail event data store (EDS), get information about all or a specified Amazon CloudFormation resource, get a list of a DynamoDB Accelerator (DAX) parameter group or subnet group, get information about Amazon Database Migration Service (Amazon DMS) replication tasks for your account in the current region being accessed, and get a list all policies in an Amazon Organizations of a specified type.	April 7, 2022

Change	Description	Date
AWSConfigServiceRolePolicy – Add backup-gateway:ListTagsForResource, backup-gateway:ListVirtualMachines, batch:DescribeComputeEnvironments, batch:DescribeJobQueues, batch:ListTagsForResource, dax:ListTags, dms:DescribeCertificates, dynamodb:DescribeGlobalTable, dynamodb:DescribeGlobalTableSettings, ec2:DescribeClientVpnAuthorizationRules, ec2:DescribeClientVpnEndpoints, ec2:DescribeDhcpOptions, ec2:DescribeFleets, ec2:DescribeNetworkAcls, ec2:DescribePlacementGroups, ec2:DescribeSpotFleetRequests, ec2:DescribeVolumeAttribute, ec2:DescribeVolumes, eks:DescribeFargateProfile, eks:ListFargateProfiles, eks:ListTagsForResource, fsx:ListTagsForResource, guardduty:ListOrganizationAdminAccounts, kms:ListAliases, opsworks:DescribeLayers, opsworks:DescribeStacks, opsworks:ListTags, rds:DescribeDBClusterParameterGroups, rds:DescribeDBClusterPara	This policy now supports additional permissions for Amazon Backup, Amazon Batch, DynamoDB Accelerator, Amazon Database Migration Service, Amazon DynamoDB, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service, Amazon FSx, Amazon GuardDuty, Amazon Key Management Service, Amazon OpsWorks, Amazon Relational Database Service, Amazon WAFV2, and Amazon WorkSpaces.	March 14, 2022

Change	Description	Date
meters, states:DescribeActivity, states:ListActivities, wafv2:GetRuleGroup, wafv2:ListRuleGroups, wafv2:ListTagsForResource, workspaces:DescribeConnectionAliases, workspaces:DescribeTags, and workspaces:DescribeWorkspaces		

Change	Description	Date
AWS_ConfigRole – Add backup-gateway:ListTagsForResource, backup-gateway:ListVirtualMachines, batch:DescribeComputeEnvironments, batch:DescribeJobQueues, batch:ListTagsForResource, dax:ListTags, dms:DescribeCertificates, dynamodb:DescribeGlobalTable, dynamodb:DescribeGlobalTableSettings, ec2:DescribeClientVpnAuthorizationRules, ec2:DescribeClientVpnEndpoints, ec2:DescribeDhcpOptions, ec2:DescribeFleets, ec2:DescribeNetworkAcls, ec2:DescribePlacementGroups, ec2:DescribeSpotFleetRequests, ec2:DescribeVolumeAttribute, ec2:DescribeVolumes, eks:DescribeFargateProfile, eks:ListFargateProfiles, eks:ListTagsForResource, fsx:ListTagsForResource, guardduty:ListOrganizationAdminAccounts, kms:ListAliases, opsworks:DescribeLayers, opsworks:DescribeStacks, opsworks:ListTags, rds:DescribeDBClusterParameterGroups, rds:DescribeDBClusterParameters, states:DescribeAct	This policy now supports additional permissions for Amazon Backup, Amazon Batch, DynamoDB Accelerator, Amazon Database Migration Service, Amazon DynamoDB, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service, Amazon FSx, Amazon GuardDuty, Amazon Key Management Service, Amazon OpsWorks, Amazon Relational Database Service, Amazon WAFV2, and Amazon WorkSpaces.	March 14, 2022

Change	Description	Date
ivity, states:ListActivities, wafv2:GetRuleGroup, wafv2:ListRuleGroups, wafv2:ListTagsForResource, workspaces:DescribeConnectionAliases, workspaces:DescribeTags, and workspaces:DescribeWorkspaces		

Change	Description	Date
AWSConfigServiceRolePolicy – Add elasticbeanstalk:DescribeEnvironments, elasticbeanstalk:DescribeConfigurationSettings, account:GetAlternateContact, organizations:DescribePolicy, organizations:ListParents, organizations:ListPoliciesForTarget, es:GetCompatibleElasticsearchVersions, rds:DescribeOptionGroups, rds:DescribeOptionGroups, es:GetCompatibleVersions, codedeploy:GetDeploymentConfig, ecr-public:GetRepositoryPolicy, access-analyzer:GetArchiveRule, and ecs:ListTaskDefinitionFamilies	This policy now grants permission to get details about Elastic Beanstalk environments and a description of the settings for the specified Elastic Beanstalk configuration set, get a map of OpenSearch or Elasticsearch versions, describe the available Amazon RDS option groups for a database, and get information about a CodeDeploy deployment configuration. This policy also now grants permission to retrieve the specified alternate contact attached to an Amazon Web Services account, retrieve information about an Amazon Organizations policy, retrieve an Amazon ECR repository policy, retrieve information about an archived Amazon Config rule, retrieve a list of Amazon ECS task definition families, list the root or parent organizational units (OUs) of the specified child OU or account, and list the policies that are attached to the specified target root, organizational unit, or account.	February 10, 2022

Change	Description	Date
AWS_ConfigRole – Add elasticbeanstalk:DescribeEnvironments, elasticbeanstalk:DescribeConfigurationSettings, account:GetAlternateContact, organizations:DescribePolicy, organizations:ListParents, organizations:ListPoliciesForTarget, es:GetCompatibleElasticsearchVersions, rds:DescribeOptionGroups, rds:DescribeOptionGroups, es:GetCompatibleVersions, codedeploy:GetDeploymentConfig, ecr-public:GetRepositoryPolicy, access-analyzer:GetArchiveRule, and ecs:ListTaskDefinitionFamilies	This policy now grants permission to get details about Elastic Beanstalk environments and a description of the settings for the specified Elastic Beanstalk configuration set, get a map of OpenSearch or Elasticsearch versions, describe the available Amazon RDS option groups for a database, and get information about a CodeDeploy deployment configuration. This policy also now grants permission to retrieve the specified alternate contact attached to an Amazon Web Services account, retrieve information about an Amazon Organizations policy, retrieve an Amazon ECR repository policy, retrieve information about an archived Amazon Config rule, retrieve a list of Amazon ECS task definition families, list the root or parent organizational units (OUs) of the specified child OU or account, and list the policies that are attached to the specified target root, organizational unit, or account.	February 10, 2022

Change	Description	Date
AWSConfigServiceRolePolicy – Add logs:CreateLogStream, logs:CreateLogGroup, and logs:PutLogEvent	This policy now grants permission to create Amazon CloudWatch log groups and streams and to write logs to created log streams.	December 15, 2021
AWS_ConfigRole – Add logs:CreateLogStream, logs:CreateLogGroup, and logs:PutLogEvent	This policy now grants permission to create Amazon CloudWatch log groups and streams and to write logs to created log streams.	Decemeber 15, 2021
AWSConfigServiceRolePolicy – Add es:DescribeDomain, es:DescribeDomains, rds:DescribeDBParameters, and, elasticache:DescribeSnapshots	This policy now grants permission to get details about an Amazon OpenSearch Service (OpenSearch Service) domain/domains and to get a detailed parameter list for a particular Amazon Relational Database Service (Amazon RDS) DB parameter group. This policy also grants permission to get detais about Amazon ElastiCache snapshots.	September 8, 2021

Change	Description	Date
AWS_ConfigRole – Add es:DescribeDomain, es:DescribeDomains, rds:DescribeDBParameters, and, elasticache:DescribeSnapshots	This policy now grants permission to get details about an Amazon OpenSearch Service (OpenSearch Service) domain/domains and to get a detailed parameter list for a particular Amazon Relational Database Service (Amazon RDS) DB parameter group. This policy also grants permission to get detais about Amazon ElastiCache snapshots.	September 8, 2021

Change	Description	Date
AWSConfigServiceRolePolicy – Add logs:ListTagsLogGroup, states:ListTagsForResource, states:ListStateMachines, states:DescribeStateMachine, and additional permissions for Amazon resource types	This policy now grants permission to list tags for a log group, list tags for a state machine, and list all state machines. This policy now grants permission to get details about a state machine. This policy also now supports additional permissions for Amazon EC2 Systems Manager (SSM), Amazon Elastic Container Registry, Amazon FSx, Amazon Data Firehose, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Relational Database Service (Amazon RDS), Amazon Route 53, Amazon SageMaker AI, Amazon Simple Notification Service, Amazon Database Migration Service, Amazon Global Accelerator, and Amazon Storage Gateway.	July 28, 2021

Change	Description	Date
AWS_ConfigRole – Add logs: ListTagsLogGroup, states:ListTagsForResource, states:ListStateMachines, states:DescribeStateMachine, and additional permissions for Amazon resource types	This policy now grants permission to list tags for a log group, list tags for a state machine, and list all state machines. This policy now grants permission to get details about a state machine. This policy also now supports additional permissions for Amazon EC2 Systems Manager (SSM), Amazon Elastic Container Registry, Amazon FSx, Amazon Data Firehose, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Relational Database Service (Amazon RDS), Amazon Route 53, Amazon SageMaker AI, Amazon Simple Notification Service, Amazon Database Migration Service, Amazon Global Accelerator, and Amazon Storage Gateway.	July 28, 2021

Change	Description	Date
AWSConfigServiceRolePolicy – Add ssm:DescribeDocumentPermission and additional permissions for Amazon resource types	This policy now grants permission to view the permissions of Amazon Systems Manager documents and information about IAM Access Analyzer. This policy now supports additional Amazon resource types for Amazon Kinesis, Amazon ElastiCache, Amazon EMR, Amazon Network Firewall, Amazon Route 53, and Amazon Relational Database Service (Amazon RDS). These permission changes allow Amazon Config to invoke the read-only APIs required to support these resource types. This policy also now support filtering Lambda@Edge functions for the lambda-inside-vpc Amazon Config managed rule.	June 8, 2021

Change	Description	Date
AWS_ConfigRole – Add ssm:DescribeDocumentPermission and additional permissions for Amazon resource types	This policy now grants permission to view the permissions of Amazon Systems Manager documents and information about IAM Access Analyzer. This policy now supports additional Amazon resource types for Amazon Kinesis, Amazon ElastiCache, Amazon EMR, Amazon Network Firewall, Amazon Route 53, and Amazon Relational Database Service (Amazon RDS). These permission changes allow Amazon Config to invoke the read-only APIs required to support these resource types. This policy also now support filtering Lambda@Edge functions for the lambda-inside-vpc Amazon Config managed rule.	June 8, 2021

Change	Description	Date
AWSConfigServiceRolePolicy – Add apigateway:GET permission to make read-only GET calls to API Gateway and s3:GetAccessPointPolicy permission and s3:GetAccessPointPolicyStatus permission to invoke Amazon S3 read-only APIs	This policy now grants permissions that allow Amazon Config to make read-only GET calls to API Gateway to support a Amazon Config Rule for API Gateway. The policy also adds permissions that allow Amazon Config to invoke Amazon Simple Storage Service (Amazon S3) read-only APIs, which are required to support the new `AWS::S3::AccessPoint` resource type.	May 10, 2021
AWS_ConfigRole – Add apigateway:GET permission to make read-only GET calls to API Gateway and s3:GetAccessPointPolicy permission and s3:GetAccessPointPolicyStatus permission to invoke Amazon S3 read-only APIs	This policy now grants permissions that allow Amazon Config to make read-only GET calls to API Gateway to support a Amazon Config for API Gateway. The policy also adds permissions that allow Amazon Config to invoke Amazon Simple Storage Service (Amazon S3) read-only APIs, which are required to support the new `AWS::S3::AccessPoint` resource type.	May 10, 2021

Change	Description	Date
AWSConfigServiceRolePolicy – Add ssm:ListDocuments permission and additiona l permissions for Amazon resource types	This policy now grants permission to view informati on about Amazon Systems Manager specified documents . This policy also now supports additional Amazon resource types for Amazon Backup, Amazon Elastic File System, Amazon ElastiCac he, Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Amazon Kinesis, Amazon SageMaker AI, Amazon Database Migration Service, and Amazon Route 53. These permission changes allow Amazon Config to invoke the read-only APIs required to support these resource types.	April 1, 2021

Change	Description	Date
AWS_ConfigRole – Add ssm:ListDocuments permission and additional permissions for Amazon resource types	This policy now grants permission to view information about Amazon Systems Manager specified documents. This policy also now supports additional Amazon resource types for Amazon Backup, Amazon Elastic File System, Amazon ElastiCache, Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Amazon Kinesis, Amazon SageMaker AI, Amazon Database Migration Service, and Amazon Route 53. These permission changes allow Amazon Config to invoke the read-only APIs required to support these resource types.	April 1, 2021
`AWSConfigRole` is deprecated	`AWSConfigRole` is deprecated. The replacement policy is `AWS_ConfigRole`.	April 1, 2021
Amazon Config started tracking changes	Amazon Config started tracking changes for its Amazon managed policies.	April 1, 2021

Permissions for the IAM Role Assigned to Amazon Config

An IAM role lets you define a set of permissions. Amazon Config assumes the role that you assign to it to write to your S3 bucket, publish to your SNS topic, and make `Describe` or `List` API

requests to get configuration details for your Amazon resources. For more information about IAM roles, see IAM Roles in the *IAM User Guide*.

When you use the Amazon Config console to create or update an IAM role, Amazon Config automatically attaches the required permissions for you. For more information, see Setting Up Amazon Config with the Console.

Policies and compliance results

IAM policies and other policies managed in Amazon Organizations can impact whether Amazon Config has permissions to record configuration changes for your resources. Additionally, rules directly evaluate the configuration of a resource and rules don't take into account these policies when running evaluations. Make sure that the policies in effect align with how you intend to use Amazon Config.

Contents

- Creating IAM Role Policies
  - Adding an IAM Trust Policy to your Role
  - IAM Role Policy for your S3 Bucket
  - IAM Role Policy for KMS Key
  - IAM Role Policy for Amazon SNS Topic
  - IAM Role Policy for Getting Configuration Details
  - Managing Permissions for S3 Bucket Recording

Creating IAM Role Policies

When you use the Amazon Config console to create an IAM role, Amazon Config automatically attaches the required permissions to the role for you.

If you are using the Amazon CLI to set up Amazon Config or you are updating an existing IAM role, you must manually update the policy to allow Amazon Config to access your S3 bucket, publish to your SNS topic, and get configuration details about your resources.

Adding an IAM Trust Policy to your Role

You can create an IAM trust policy that enables Amazon Config to assume a role and use it to track your resources. For more information about trust policies, see Roles terms and concepts in the *IAM User Guide*.

The following is an example trust policy for Amazon Config roles:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    }
  ]
}
```

You can use the `AWS:SourceAccount` condition in the IAM Role Trust relationship above to restrict the Config service principal to only interact with the Amazon IAM Role when performing operations on behalf of specific accounts.

Amazon Config also supports the `AWS:SourceArn` condition which restricts the Config service principal to only assume the IAM Role when performing operations on behalf of the owning account. When using the Amazon Config service principal, the `AWS:SourceArn` property will always be set to `arn:aws:config:sourceRegion:sourceAccountID:*` where `sourceRegion` is the region of the customer managed configuration recorder and `sourceAccountID` is the ID of the account containing the customer managed configuration recorder.

For example, add the following condition restrict the Config service principal to only assume the IAM Role only on behalf of a customer managed configuration recorder in the `us-east-1` region

in the account 123456789012: `"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`.

IAM Role Policy for your S3 Bucket

The following example policy grants Amazon Config permission to access your S3 bucket:

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource":[
        "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/myAccountID/*"
      ],
      "Condition":{
        "StringLike":{
          "s3:x-amz-acl":"bucket-owner-full-control"
        }
      }
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:GetBucketAcl"
      ],
      "Resource":"arn:aws:s3:::amzn-s3-demo-bucket"
    }
  ]
}
```

IAM Role Policy for KMS Key

The following example policy grants Amazon Config permission to use KMS-based encryption on new objects for S3 bucket delivery:

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "myKMSKeyARN"
        }
    ]
}
```

IAM Role Policy for Amazon SNS Topic

The following example policy grants Amazon Config permission to access your SNS topic:

```
{
  "Version": "2012-10-17",
  "Statement":
   [
     {
      "Effect":"Allow",
      "Action":"sns:Publish",
      "Resource":"mySNStopicARN"
     }
    ]
}
```

If your SNS topic is encrypted for additional setup instructions, see Configuring Amazon KMS Permissions in the *Amazon Simple Notification Service Developer Guide*.

IAM Role Policy for Getting Configuration Details

It is recommended to use the Amazon Config service-linked role: `AWSServiceRoleForConfig`. Service-linked roles are predefined and include all the permissions that Amazon Config requires to call other Amazon Web Services services. The Amazon Config service-linked role is required for service-linked configuration recorders. For more information, see Using Service-Linked Roles for Amazon Config.

If you create or update a role with the console, Amazon Config attaches the **AWSServiceRoleForConfig** for you.

If you use the Amazon CLI, use the `attach-role-policy` command and specify the Amazon Resource Name (ARN) for **AWSServiceRoleForConfig**:

```
$ aws iam attach-role-policy --role-name myConfigRole --policy-arn
 arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForConfig
```

Managing Permissions for S3 Bucket Recording

Amazon Config records and delivers notifications when an S3 bucket is created, updated, or deleted.

It is recommended to use the Amazon Config service-linked role: `AWSServiceRoleForConfig`. Service-linked roles are predefined and include all the permissions that Amazon Config requires to call other Amazon Web Services services. The Amazon Config service-linked role is required for service-linked configuration recorders. For more information, see Using Service-Linked Roles for Amazon Config.

Updating the IAM Role for the customer managed configuration recorder

You can update the IAM role used by the customer managed configuration recorder. Before you update the IAM role, ensure that you have created a new role to replace the old one. You must attach policies to the new role that grant permissions to Amazon Config to record configurations and deliver them to your delivery channel.

For information about creating an IAM role and attaching the required policies to the IAM role, see Step 3: Creating an IAM Role.

> **Note**
>
> To find the ARN of an existing IAM role, go to the IAM console at https://console.amazonaws.cn/iam/. Choose **Roles** in the navigation pane. Then choose the name of the desired role and find the ARN at the top of the **Summary** page.

Updating the IAM Role

You can update your IAM role using the Amazon Web Services Management Console or the Amazon CLI.

To update the IAM role (Console)

1. Sign in to the Amazon Web Services Management Console and open the Amazon Config console at https://console.amazonaws.cn/config/home.
2. Choose **Settings** in the navigation pane.
3. On the **Customer managed recorder** tab, choose **Edit** on the Settings page.
4. In the **Data governance**, section, choose the IAM role for Amazon Config:
   - **Use an existing Amazon Config service-linked role** – Amazon Config creates a role that has the required permissions.
   - **Choose a role from your account** – For **Existing roles**, choose an IAM role in your account.
5. Choose **Save**.

To update the IAM role (Amazon CLI)

Use the `put-configuration-recorder` command and specify the Amazon Resource Name (ARN) of the new role:

```
$ aws configservice put-configuration-recorder --configuration-recorder
 name=configRecorderName,roleARN=arn:aws:iam::012345678912:role/myConfigRole
```

Permissions for the Amazon S3 Bucket for the Amazon Config Delivery Channel

> **Important**
>
> This page is about setting up the Amazon S3 Bucket for the Amazon Config delivery channel. This page is not about the `AWS::S3::Bucket` resource type that the Amazon Config configuration recorder can record.

Amazon S3 buckets and objects are private by default. Only the Amazon Web Services account that created the bucket (the resource owner) has access permissions. Resource owners can grant access to other resources and users by creating access policies.

When Amazon Config automatically creates an S3 bucket for you, it adds the required permissions. However, if you specify an existing S3 bucket, you must add these permissions manually.

Topics

- Required Permissions for the Amazon S3 Bucket When Using IAM Roles
- Required Permissions for the Amazon S3 Bucket When Using Service-Linked Roles
- Granting Amazon Config access to the Amazon S3 Bucket
- Required Permissions for the Amazon S3 Bucket When Delivering Cross-Account

Required Permissions for the Amazon S3 Bucket When Using IAM Roles

Amazon Config uses the IAM role you assigned to the configuration recorder to deliver configuration history and snapshots to S3 buckets in your account. For cross-account delivery, Amazon Config first attempts to use the assigned IAM role. If the bucket policy doesn't grant `WRITE` access to the IAM role, Amazon Config uses the `config.amazonaws.com` service principal. The bucket policy must grant `WRITE` access to `config.amazonaws.com` to complete the delivery. After successful delivery, Amazon Config maintains ownership of all objects it delivers to the cross-account S3 bucket.

Amazon Config calls the Amazon S3 HeadBucket API with the IAM role you assigned to the configuration recorder to confirm if the S3 bucket exists and its location. If you do not have the necessary permissions for Amazon Config to confirm, you will see an `AccessDenied` error in your Amazon CloudTrail logs. However, Amazon Config can still deliver configuration history and snapshots even if Amazon Config does not have the necessary permissions to confirm if the S3 bucket exists and its location.

> **Minimum permissions**
>
> The Amazon S3 `HeadBucket` API requires the `s3:ListBucket` action.

Required Permissions for the Amazon S3 Bucket When Using Service-Linked Roles

The Amazon Config service-linked role does not have permission to put objects to Amazon S3 buckets. If you set up Amazon Config using a service-linked role, Amazon Config will use the `config.amazonaws.com` service principal to deliver configuration history and snapshots. The

S3 bucket policy in your account or cross-account destinations must include permissions for the Amazon Config service principal to write objects.

Granting Amazon Config access to the Amazon S3 Bucket

Complete the following steps enable Amazon Config to deliver configuration history and snapshots to an Amazon S3 bucket.

1. Sign in to the Amazon Web Services Management Console using the account that has the S3 bucket.
2. Open the Amazon S3 console at https://console.amazonaws.cn/s3/.
3. Select the bucket that you want Amazon Config to use to deliver configuration items, and then choose **Properties**.
4. Choose **Permissions**.
5. Choose **Edit Bucket Policy**.
6. Copy the following policy into the **Bucket Policy Editor** window:

> **Security best practices**
>
> We strongly recommend that you restrict access in the bucket policy with the `AWS:SourceAccount` condition. This makes sure that Amazon Config is granted access on behalf of expected users only.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
```

```
      }
    },
    {
      "Sid": "AWSConfigBucketExistenceCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    },
    {
      "Sid": "AWSConfigBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/[optional] prefix/
AWSLogs/sourceAccountID/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    }
  ]
}
```

7. Substitute the following values in the bucket policy:

   - *amzn-s3-demo-bucket* – Name of the Amazon S3 bucket where Amazon Config will deliver configuration history and snapshots.
   - *[optional] prefix* – An optional addition to the Amazon S3 object key that helps create a folder-like organization in the bucket.

- *sourceAccountID* – ID of the account where Amazon Config will deliver configuration history and snapshots.

8. Choose **Save** and then **Close**.

The AWS:SourceAccount condition restricts Amazon Config operations to specified Amazon Web Services accounts. For multi-account configurations within an organization delivering to a single S3 bucket, use IAM roles with Amazon Organizations conditions keys instead of service-linked roles. For example, AWS:PrincipalOrgID. For more information, see Managing access permissions for an organization in the *Amazon Organizations User guide*.

The AWS:SourceArn condition restricts Amazon Config operations to specified delivery channels. The AWS:SourceArn format is as follows: arn:aws:config:*sourceRegion*:*123456789012*.

For example, to restrict S3 bucket access to a delivery channel in the US East (N. Virginia) Region for account 123456789012, add the following condition:

```
"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:"}
```

Required Permissions for the Amazon S3 Bucket When Delivering Cross-Account

When Amazon Config is configured to deliver configuration history and snapshots to an Amazon S3 bucket in a different account (cross-account setup), where the configuration recorder and the S3 bucket specified for delivery channel are in different Amazon Web Services accounts, the following permissions are required:

- The IAM role you assign to the configuration recorder needs explicit permission to perform the s3:ListBucket operation. This is because Amazon Config calls the Amazon S3 HeadBucket API with this IAM role to determine the bucket location.
- The S3 bucket policy must include permissions for both the Amazon Config service principal and the IAM role assigned to the configuration recorder.

The following is an example bucket policy configuration:

```
{
      "Sid": "AWSConfigBucketExistenceCheck",
      "Effect": "Allow",
      "Principal": {
```

```
        "Service": "config.amazonaws.com",
        "AWS": "IAM Role-Arn assigned to the configuration recorder"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
}
```

Permissions for the KMS Key for the Amazon Config Delivery Channel

Use the information in this topic if you want to create a policy for an Amazon KMS key for your S3 bucket that allows you to use KMS-based encryption on objects delivered by Amazon Config for S3 bucket delivery.

Contents

- Required Permissions for the KMS Key When Using IAM Roles (S3 Bucket Delivery)
- Required Permissions for the Amazon KMS Key When Using Service-Linked Roles (S3 Bucket Delivery)
- Granting Amazon Config access to the Amazon KMS Key

Required Permissions for the KMS Key When Using IAM Roles (S3 Bucket Delivery)

If you set up Amazon Config using an IAM role, you can attach the follow permission policy to the KMS Key:

```
{
    "Id": "Policy_ID",
    "Statement": [
        {
            "Sid": "AWSConfigKMSPolicy",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Effect": "Allow",
```

```
            "Resource": "*myKMSKeyARN*",
            "Principal": {
                "AWS": [
                    "account-id1",
                    "account-id2",
                    "account-id3"
                ]
            }
        }
    ]
}
```

Note

If the IAM role, Amazon S3 bucket policy, or Amazon KMS key do not provide appropriate access to Amazon Config, then Amazon Config's attempt to send configuration information to the Amazon S3 bucket will fail. In this event, Amazon Config sends the information again, this time as the Amazon Config service principal. For this case, you must attach a permission policy, mentioned below, to the Amazon KMS key to grant Amazon Config access to use the key when delivering information to the Amazon S3 bucket.

Required Permissions for the Amazon KMS Key When Using Service-Linked Roles (S3 Bucket Delivery)

The Amazon Config service-linked role does not have permission to access the Amazon KMS key. So, if you set up Amazon Config using a service-linked role, Amazon Config will send information as the Amazon Config service principal instead. You will need to attach an access policy, mentioned below, to the Amazon KMS key to grant Amazon Config access to use the Amazon KMS key when delivering information to the Amazon S3 bucket.

Granting Amazon Config access to the Amazon KMS Key

This policy allows Amazon Config to use an Amazon KMS key when delivering information to an Amazon S3 bucket

```
{
    "Id": "Policy_ID",
    "Statement": [
```

```
        {
            "Sid": "AWSConfigKMSPolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "config.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "myKMSKeyARN",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceAccount": "sourceAccountID"
                }
            }
        }
    ]
}
```

Substitute the following values in the key policy:

- *myKMSKeyARN* – The ARN of the Amazon KMS key used to encrypt data in the Amazon S3 bucket that Amazon Config will deliver configuration items to.
- *sourceAccountID* – The ID of the account for which Amazon Config will deliver configuration items to.

You can use the `AWS:SourceAccount` condition in the Amazon KMS key policy above to restrict the Config service principal to only interact with the Amazon KMS key when performing operations on behalf of specific accounts.

Amazon Config also supports the `AWS:SourceArn` condition which restricts the Config service principal to only interact with the Amazon S3 bucket when performing operations on behalf of specific Amazon Config delivery channels. When using the Amazon Config service principal, the `AWS:SourceArn` property will always be set to `arn:aws:config:sourceRegion:sourceAccountID:*` where `sourceRegion` is the region of the delivery channel and `sourceAccountID` is the ID of the account containing the delivery channel. For more information on Amazon Config delivery channels, see Managing the Delivery Channel. For example, add the following condition to restrict the Config service principal to interact with your Amazon S3 bucket only on behalf of a delivery channel in the `us-east-1` region

in the account 123456789012: `"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`.

Permissions for the Amazon SNS Topic

This topic describes how to configure Amazon Config to deliver Amazon SNS topics owned by a different account. Amazon Config must have the required permissions to send notifications to an Amazon SNS topic.

When the Amazon Config console creates a new Amazon SNS topic for you, Amazon Config grants the necessary permissions. If you choose an existing Amazon SNS topic, makes sure that the Amazon SNS topic includes the required permissions and follows security best practices.

> **Cross-Region Amazon SNS topics are not supported**
>
> Amazon Config currently supports only access within the same Amazon Web Services Region and across accounts.

Contents

- Required Permissions for the Amazon SNS Topic When Using IAM Roles
- Required Permissions for the Amazon SNS Topic When Using Service-Linked Roles
- Granting Amazon Config access to the Amazon SNS topic
- Troubleshooting for the Amazon SNS Topic

Required Permissions for the Amazon SNS Topic When Using IAM Roles

You can attach a permissions policy to the Amazon SNS topic owned by a different account. If you want to use an Amazon SNS topic from another account, make sure to attach the following policy to the existing Amazon SNS topic.

```
{
  "Id": "Policy_ID",
  "Statement": [
    {
      "Sid": "AWSConfigSNSPolicy",
      "Action": [
        "sns:Publish"
```

```
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:sns:region:account-id:myTopic",
      "Principal": {
        "AWS": [
          "account-id1",
          "account-id2",
          "account-id3"
        ]
      }
    }
  ]
}
```

For the `Resource` key, *`account-id`* is the Amazon account number of the topic owner. For *`account-id1`*, *`account-id2`*, and *`account-id3`*, use the Amazon Web Services accounts that will send data to an Amazon SNS topic. You can substitute appropriate values for *`region`* and *`myTopic`*.

When Amazon Config sends a notification to an Amazon SNS topic, it first attempts to use the IAM role, but this attempt fails if the role or Amazon Web Services account does not have permission to publish to the topic. In this event, Amazon Config sends the notification again, this time as an Amazon Config service principal name (SPN). Before the publication can succeed, the access policy for the topic must grant `sns:Publish` access to the `config.amazonaws.com` principal name. You must attach an access policy, described in the next section, to the Amazon SNS topic to grant Amazon Config access to the Amazon SNS topic if the IAM role does not have permission to publish to the topic.

Required Permissions for the Amazon SNS Topic When Using Service-Linked Roles

The Amazon Config service-linked role does not have permission to access the Amazon SNS topic. So, if you set up Amazon Config using a service-linked role (SLR), Amazon Config will send information as the Amazon Config service principal instead. You will need to attach an access policy, mentioned below, to the Amazon SNS topic to grant Amazon Config access to send information to the Amazon SNS topic.

For same-account setup, when the Amazon SNS topic and SLR are in the same account and the Amazon SNS policy grants the SLR "`sns:Publish`" permission, you do not need to use the Amazon Config SPN. The permissions policy below and security best practice recommendations are for cross-account setup.

Granting Amazon Config access to the Amazon SNS topic

This policy allows Amazon Config to send a notification to an Amazon SNS topic. To grant Amazon Config access to the Amazon SNS topic from another account, you will need to attach the following permissions policy.

> **Note**
>
> As a security best practice, it is strongly recommended to make sure Amazon Config is accessing resources on behalf of expected users only by restricting access to the accounts listed in `AWS:SourceAccount` condition.

```
{
"Id": "Policy_ID",
"Statement": [
  {
    "Sid": "AWSConfigSNSPolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "config.amazonaws.com"
    },
    "Action": "sns:Publish",
      "Resource": "arn:aws:sns:region:account-id:myTopic",
        "Condition" : {
        "StringEquals": {
          "AWS:SourceAccount": [
            "account-id1",
            "account-id2",
            "account-id3"
          ]
        }
      }
    }
  ]
}
```

For the `Resource` key, *`account-id`* is the Amazon account number of the topic owner. For *`account-id1`*, *`account-id2`*, and *`account-id3`*, use the Amazon Web Services accounts that will send data to an Amazon SNS topic. You can substitute appropriate values for *`region`* and *`myTopic`*.

You can use the `AWS:SourceAccount` condition in the previous Amazon SNS topic policy to restrict the Amazon Config service principal name (SPN) to interact only with the Amazon SNS topic when performing operations on behalf of specific accounts.

Amazon Config also supports the `AWS:SourceArn` condition which restricts the Amazon Config service principal name (SPN) to only interact with the S3 bucket when performing operations on behalf of specific Amazon Config delivery channels. When using the Amazon Config service principal name (SPN), the `AWS:SourceArn` property will always be set to `arn:aws:config:sourceRegion:sourceAccountID:*` where `sourceRegion` is the Region of the delivery channel and `sourceAccountID` is the ID of the account containing the delivery channel. For more information about Amazon Config delivery channels, see Managing the Delivery Channel. For example, add the following condition to restrict the Amazon Config service principal name (SPN) to interact with your S3 bucket only on behalf of a delivery channel in the `us-east-1` Region in the account `123456789012`: `"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`.

Troubleshooting for the Amazon SNS Topic

Amazon Config must have permissions to send notifications to an Amazon SNS topic. If an Amazon SNS topic cannot receive notifications, verify that the IAM role that Amazon Config was assuming has the required `sns:Publish` permissions.

Troubleshooting Amazon Config identity and access

Use the following information to help you diagnose and fix common issues that you might encounter when working with Amazon Config and IAM.

Topics

- I am not authorized to perform an action in Amazon Config
- I am not authorized to perform iam:PassRole
- I want to allow people outside of my Amazon Web Services account to access my Amazon Config resources

I am not authorized to perform an action in Amazon Config

If you receive an error that you're not authorized to perform an action, your policies must be updated to allow you to perform the action.

The following example error occurs when the `mateojackson` IAM user tries to use the console to view details about a fictional *`my-example-widget`* resource but does not have the fictional `config:`*`GetWidget`* permissions.

```
User: arn:aws-cn:iam::123456789012:user/mateojackson is not authorized to perform:
 config:GetWidget on resource: my-example-widget
```

In this case, Mateo's policy must be updated to allow him to access the *`my-example-widget`* resource using the `config:`*`GetWidget`* action.

If you need help, contact your Amazon administrator. Your administrator is the person who provided you with your sign-in credentials.

I am not authorized to perform iam:PassRole

If you receive an error that you're not authorized to perform the `iam:PassRole` action, your policies must be updated to allow you to pass a role to Amazon Config.

Some Amazon Web Services services allow you to pass an existing role to that service instead of creating a new service role or service-linked role. To do this, you must have permissions to pass the role to the service.

The following example error occurs when an IAM user named `marymajor` tries to use the console to perform an action in Amazon Config. However, the action requires the service to have permissions that are granted by a service role. Mary does not have permissions to pass the role to the service.

```
User: arn:aws-cn:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In this case, Mary's policies must be updated to allow her to perform the `iam:PassRole` action.

If you need help, contact your Amazon administrator. Your administrator is the person who provided you with your sign-in credentials.

I want to allow people outside of my Amazon Web Services account to access my Amazon Config resources

You can create a role that users in other accounts or people outside of your organization can use to access your resources. You can specify who is trusted to assume the role. For services that support

resource-based policies or access control lists (ACLs), you can use those policies to grant people access to your resources.

To learn more, consult the following:

- To learn whether Amazon Config supports these features, see How Amazon Config works with IAM.
- To learn how to provide access to your resources across Amazon Web Services accounts that you own, see Providing access to an IAM user in another Amazon Web Services account that you own in the *IAM User Guide*.
- To learn how to provide access to your resources to third-party Amazon Web Services accounts, see Providing access to Amazon Web Services accounts owned by third parties in the *IAM User Guide*.
- To learn how to provide access through identity federation, see Providing access to externally authenticated users (identity federation) in the *IAM User Guide*.
- To learn the difference between using roles and resource-based policies for cross-account access, see Cross account resource access in IAM in the *IAM User Guide*.

Using Service-Linked Roles for Amazon Config

Amazon Config uses Amazon Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to Amazon Config. Service-linked roles are predefined by Amazon Config and include all the permissions that the service requires to call other Amazon services on your behalf.

A service-linked role makes setting up Amazon Config easier because you don't have to manually add the necessary permissions. Amazon Config defines the permissions of its service-linked roles, and unless defined otherwise, only Amazon Config can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

For information about other services that support service-linked roles, see Amazon Services That Work with IAM and look for the services that have **Yes** in the **Service-Linked Role** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

Service-Linked Role Permissions for Amazon Config

Amazon Config uses the service-linked role named **AwsServiceRoleForConfig** – Amazon Config uses this service-linked role to call other Amazon services on your behalf.

The **AwsServiceRoleForConfig** service-linked role trusts the `config.amazonaws.com` service to assume the role.

The permissions policy for the `AwsServiceRoleForConfig` role contains read-only and write-only permissions for Amazon Config resources and read-only permissions for resources in other services that Amazon Config supports. To view the managed policy for **AwsServiceRoleForConfig**, see Amazon managed policies for Amazon Config.

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-Linked Role Permissions in the *IAM User Guide*.

To use a service-linked role with Amazon Config, you must configure permissions on your Amazon S3 bucket and Amazon SNS topic. For more information, see Required Permissions for the Amazon S3 Bucket When Using Service-Linked Roles, Required Permissions for the Amazon KMS Key When Using Service-Linked Roles (S3 Bucket Delivery), and Required Permissions for the Amazon SNS Topic When Using Service-Linked Roles.

Creating a Service-Linked Role for Amazon Config

In the IAM CLI or the IAM API, create a service-linked role with the `config.amazonaws.com` service name. For more information, see Creating a Service-Linked Role in the *IAM User Guide*. If you delete this service-linked role, you can use this same process to create the role again.

Editing a Service-Linked Role for Amazon Config

Amazon Config does not allow you to edit the **AwsServiceRoleForConfig** service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a Service-Linked Role in the *IAM User Guide*.

Deleting a Service-Linked Role for Amazon Config

If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way you don't have an unused entity that is not actively monitored

or maintained. However, you must clean up the resources for your service-linked role before you can manually delete it.

> **Note**
>
> If the Amazon Config service is using the role when you try to delete the resources, then the deletion might fail. If that happens, wait for a few minutes and try the operation again.

To delete Amazon Config resources used by the AwsServiceRoleForConfig

Ensure that you do not have `ConfigurationRecorders` using the service-linked role. You can use the Amazon Config console to stop the configuration recorder. To stop recording, under **Recording is on**, choose **Turn off**.

You can delete the `ConfigurationRecorder` using Amazon Config API. To delete, use the `delete-configuration-recorder` command.

```
        $ aws configservice delete-configuration-recorder --configuration-recorder-
name default
```

To manually delete the service-linked role using IAM

Use the IAM console, the IAM CLI, or the IAM API to delete the AwsServiceRoleForConfig service-linked role. For more information, see Deleting a Service-Linked Role in the *IAM User Guide*.

Incident Response in Amazon Config

Security is the highest priority at Amazon. As part of the Amazon Cloud shared responsibility model, Amazon manages a data center, network, and software architecture that meets the requirements of the most security-sensitive organizations. Amazon is responsible for any incident response with respect to the Amazon Config service itself. Also, as an Amazon customer, you share a responsibility for maintaining security in the cloud. This means you control the security you choose to implement from the Amazon tools and features you have access to, and are responsible for incident response on your side of the shared responsibility model.

By establishing a security baseline that meets the objectives for your applications running in the cloud, you're able to detect deviations that you can respond to. Since security incident response

can be a complex topic, we encourage you to review the following resources so that you are better able to understand the impact that incident response (IR) and your choices have on your corporate goals: Amazon Security Incident Response Guide, Amazon Security Best Practices whitepaper, and the Security Perspective of the Amazon Cloud Adoption Framework (CAF) white paper.

Compliance Validation for Amazon Config

Third-party auditors assess the security and compliance of Amazon Config as part of multiple Amazon compliance programs. These include SOC, PCI, FedRAMP, HIPAA, and others.

To learn whether an Amazon Web Services service is within the scope of specific compliance programs, see Amazon Web Services services in Scope by Compliance Program and choose the compliance program that you are interested in. For general information, see Amazon Web Services Compliance Programs.

You can download third-party audit reports using Amazon Artifact. For more information, see Downloading Reports in Amazon Artifact.

Your compliance responsibility when using Amazon Web Services services is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. Amazon provides the following resources to help with compliance:

- Security & Compliance – These solution implementation guides discuss architectural considerations and provide steps for deploying security and compliance features.
- Amazon Compliance Resources – This collection of workbooks and guides might apply to your industry and location.
- Evaluating Resources with Rules in the *Amazon Config Developer Guide* – The Amazon Config service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- Amazon Security Hub – This Amazon Web Services service provides a comprehensive view of your security state within Amazon. Security Hub uses security controls to evaluate your Amazon resources and to check your compliance against security industry standards and best practices. For a list of supported services and controls, see Security Hub controls reference.
- Amazon GuardDuty – This Amazon Web Services service detects potential threats to your Amazon Web Services accounts, workloads, containers, and data by monitoring your environment for suspicious and malicious activities. GuardDuty can help you address various compliance requirements, like PCI DSS, by meeting intrusion detection requirements mandated by certain compliance frameworks.

Resilience in Amazon Config

The Amazon global infrastructure is built around Amazon Regions and Availability Zones. Amazon Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about Amazon Regions and Availability Zones, see Amazon Global Infrastructure.

Infrastructure Security in Amazon Config

As a managed service, Amazon Config is protected by Amazon global network security. For information about Amazon security services and how Amazon protects infrastructure, see Amazon Cloud Security. To design your Amazon environment using the best practices for infrastructure security, see Infrastructure Protection in *Security Pillar Amazon Well-Architected Framework*.

You use Amazon published API calls to access Amazon Config through the network. Clients must support the following:

- Transport Layer Security (TLS). We require TLS 1.2 and recommend TLS 1.3.
- Cipher suites with perfect forward secrecy (PFS) such as DHE (Ephemeral Diffie-Hellman) or ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Most modern systems such as Java 7 and later support these modes.

Additionally, requests must be signed by using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the Amazon Security Token Service (Amazon STS) to generate temporary security credentials to sign requests.

Configuration and Vulnerability Analysis

For Amazon Config, Amazon handles basic security tasks such as guest operating system (OS) and database patching, firewall configuration, and disaster recovery.

Cross-service confused deputy prevention

The confused deputy problem is a security issue where an entity that doesn't have permission to perform an action can coerce a more-privileged entity to perform the action. In Amazon, cross-service impersonation can result in the confused deputy problem. Cross-service impersonation can occur when one service (the *calling service*) calls another service (the *called service*). The calling service can be manipulated to use its permissions to act on another customer's resources in a way it should not otherwise have permission to access. To prevent this, Amazon provides tools that help you protect your data for all services with service principals that have been given access to resources in your account.

We recommend using the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in resource policies to limit the permissions that Amazon Config gives another service to the resource. Use `aws:SourceArn` if you want only one resource to be associated with the cross-service access. Use `aws:SourceAccount` if you want to allow any resource in that account to be associated with the cross-service use.

The most effective way to protect against the confused deputy problem is to use the `aws:SourceArn` global condition context key with the full ARN of the resource. If you don't know the full ARN of the resource or if you are specifying multiple resources, use the `aws:SourceArn` global context condition key with wildcard characters (*) for the unknown portions of the ARN. For example, `arn:aws-cn:`*`servicename`*`:*:`*`123456789012`*`:*`.

If the `aws:SourceArn` value does not contain the account ID, such as an Amazon S3 bucket ARN, you must use both global condition context keys to limit permissions.

The following example shows how you can use the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in Amazon Config to prevent the confused deputy problem: Granting Amazon Config access to the Amazon S3 Bucket.

Security Best Practices for Amazon Config

Amazon Config provides a number of security features to consider as you develop and implement your own security policies. The following best practices are general guidelines and don’t represent a complete security solution. Because these best practices might not be appropriate or sufficient for your environment, treat them as helpful considerations rather than prescriptions.

- Leverage tagging for Amazon Config, which makes is easier to manage, search for, and filter resources.

- Confirm your delivery channels have been properly set, and once confirmed, verify that Amazon Config is recording properly.

For more information, see Amazon Config best practices blog.

Logging and Monitoring in Amazon Config

Amazon Config is integrated with Amazon CloudTrail, a service that provides a record of actions taken by a user, role, or an Amazon service in Amazon Config. Monitoring is an important part of maintaining the reliability, availability, and performance of Amazon Config and your Amazon solutions.

Topics

- Logging Amazon Config API Calls with Amazon CloudTrail
- Monitoring

Logging Amazon Config API Calls with Amazon CloudTrail

CloudTrail captures all API calls for Amazon Config as events. The calls captured include calls from the Amazon Config console and code calls to the Amazon Config API operations. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Amazon Config. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**. Using the information collected by CloudTrail, you can determine the request that was made to Amazon Config, the IP address from which the request was made, who made the request, when it was made, and additional details.

To learn more about CloudTrail, see the Amazon CloudTrail User Guide.

Topics

- Amazon Config Information in CloudTrail
- Understanding Amazon Config Log File Entries
- Example Log Files

Amazon Config Information in CloudTrail

CloudTrail is enabled on your Amazon Web Services account when you create the account. When activity occurs in Amazon Config, that activity is recorded in a CloudTrail event along with other Amazon service events in **Event history**. You can view, search, and download recent events in your Amazon Web Services account. For more information, see Viewing Events with CloudTrail Event History.

For an ongoing record of events in your Amazon Web Services account, including events for Amazon Config, create a trail. A *trail* enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all Amazon Web Services Regions. The trail logs events from all Regions in the Amazon partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other Amazon services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following:

- Overview for Creating a Trail
- CloudTrail Supported Services and Integrations
- Configuring Amazon SNS Notifications for CloudTrail
- Receiving CloudTrail Log Files from Multiple Regions and Receiving CloudTrail Log Files from Multiple Accounts

All Amazon Config operations are logged by CloudTrail and are documented in the Amazon Config API Reference. For example, calls to the DeliverConfigSnapshot, DeleteDeliveryChannel, and DescribeDeliveryChannels operations generate entries in the CloudTrail log files.

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or Amazon Identity and Access Management (IAM) user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another Amazon service.

For more information, see the CloudTrail userIdentity Element.

Understanding Amazon Config Log File Entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

Example Log Files

For examples of the CloudTrail log entries, see the following topics.

DeleteDeliveryChannel

The following is an example CloudTrail log file for the DeleteDeliveryChannel operation.


```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:32:57Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DeleteDeliveryChannel",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-internal/3",
      "requestParameters": {
        "deliveryChannelName": "default"
      },
      "responseElements": null,
      "requestID": "207d695a-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "5dcff7a9-e414-411a-a43e-88d122a0ad4a",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```


DeliverConfigSnapshot

The following is an example CloudTrail log file for the DeliverConfigSnapshot operation.


```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAABCDEFGHIJKLNMOPQ:Config-API-Test",
```

```
        "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-12-11T00:58:42Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDAABCDEFGHIJKLNMOPQ",
            "arn": "arn:aws:iam::111111111111:role/JaneDoe",
            "accountId": "111111111111",
            "userName": "JaneDoe"
          }
        }
      },
      "eventTime": "2014-12-11T00:58:53Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DeliverConfigSnapshot",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "deliveryChannelName": "default"
      },
      "responseElements": {
        "configSnapshotId": "58d50f10-212d-4fa4-842e-97c614da67ce"
      },
      "requestID": "e0248561-80d0-11e4-9f1c-7739d36a3df2",
      "eventID": "3e88076c-eae1-4aa6-8990-86fe52aedbd8",
      "eventType": "AwsApiCall",
      recipientAccountId": "111111111111"
    }
```

DescribeConfigurationRecorderStatus

The following is an example CloudTrail log file for the DescribeConfigurationRecorderStatus operation.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
```

```
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:44Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeConfigurationRecorderStatus",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "8442f25d-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "a675b36b-455f-4e18-a4bc-d3e01749d3f1",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```


DescribeConfigurationRecorders

The following is an example CloudTrail log file for the DescribeConfigurationRecorders operation.


```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:34:52Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeConfigurationRecorders",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
```

```
      "responseElements": null,
      "requestID": "6566b55c-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "6259a9ad-889e-423b-beeb-6e1eec84a8b5",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

DescribeDeliveryChannels

Following is an example CloudTrail log file for the DescribeDeliveryChannels operation.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:02Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeDeliveryChannels",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "6b6aee3f-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "3e15ebc5-bf39-4d2a-8b64-9392807985f1",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

GetResourceConfigHistory

The following is an example CloudTrail log file for the GetResourceConfigHistory operation.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "AssumedRole",
```

```
        "principalId": "AIDAABCDEFGHIJKLNMOPQ:Config-API-Test",
        "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-12-11T00:58:42Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDAABCDEFGHIJKLNMOPQ",
            "arn": "arn:aws:iam::111111111111:role/JaneDoe",
            "accountId": "111111111111",
            "userName": "JaneDoe"
          }
        }
      },
      "eventTime": "2014-12-11T00:58:42Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "GetResourceConfigHistory",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "resourceId": "vpc-a12bc345",
        "resourceType": "AWS::EC2::VPC",
        "limit": 0,
        "laterTime": "Dec 11, 2014 12:58:42 AM",
        "earlierTime": "Dec 10, 2014 4:58:42 PM"
      },
      "responseElements": null,
      "requestID": "d9f3490d-80d0-11e4-9f1c-7739d36a3df2",
      "eventID": "ba9c1766-d28f-40e3-b4c6-3ffb87dd6166",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111111111111"
      }
```


PutConfigurationRecorder

The following is an example CloudTrail log file for the PutConfigurationRecorder operation.


```
{
      "eventVersion": "1.02",
```

```
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:23Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "PutConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorder": {
          "name": "default",
          "roleARN": "arn:aws:iam::222222222222:role/config-role-pdx"
        }
      },
      "responseElements": null,
      "requestID": "779f7917-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "c91f3daa-96e8-44ee-8ddd-146ac06565a7",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

PutDeliveryChannel

The following is an example CloudTrail log file for the PutDeliveryChannel operation.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:33:08Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "PutDeliveryChannel",
```

```
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "deliveryChannel": {
          "name": "default",
          "s3BucketName": "config-api-test-pdx",
          "snsTopicARN": "arn:aws:sns:us-west-2:222222222222:config-api-test-pdx"
        }
      },
      "responseElements": null,
      "requestID": "268b8d4d-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "b2db05f1-1c73-4e52-b238-db69c04e8dd4",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

StartConfigurationRecorder

The following is an example CloudTrail log file for the StartConfigurationRecorder operation.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:34Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "StartConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorderName": "default"
      },
      "responseElements": null,
      "requestID": "7e03fa6a-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "55a5507f-f306-4896-afe3-196dc078a88d",
      "eventType": "AwsApiCall",
```

```
      "recipientAccountId": "222222222222"
    }
```

StopConfigurationRecorder

The following is an example CloudTrail log file for the StopConfigurationRecorder operation.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:13Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "StopConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorderName": "default"
      },
      "responseElements": null,
      "requestID": "716deea3-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "6225a85d-1e49-41e9-bf43-3cfc5549e560",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

Monitoring

You can use other Amazon services to monitor Amazon Config resources.

- You can use Amazon Simple Notification Service (SNS) to send you notifications every time a supported Amazon resource is created, updated, or otherwise modified as a result of user API activity.

- You can use Amazon EventBridge to detect and react to changes in the status of Amazon Config events.

Topics

- Monitoring Amazon Resource Changes with Amazon SQS
- Monitoring Amazon Config with Amazon EventBridge

Monitoring Amazon Resource Changes with Amazon SQS

Amazon Config uses Amazon Simple Notification Service (SNS) to send you notifications every time a supported Amazon resource is created, updated, or otherwise modified as a result of user API activity. However, you might be interested in only certain resource configuration changes. For example, you might consider it critical to know when someone modifies the configuration of a security group, but not need to know every time there is a change to tags on your Amazon EC2 instances. Or, you might want to write a program that performs specific actions when specific resources are updated. For example, you might want to start a certain workflow when a security group configuration is changed. If you want to programmatically consume the data from Amazon Config in these or other ways, use an Amazon Simple Queue Service queue as the notification endpoint for Amazon SNS.

> **Note**
>
> Notifications can also come from Amazon SNS in the form of an email, a Short Message Service (SMS) message to SMS-enabled mobile phones and smartphones, a notification message to an application on a mobile device, or a notification message to one or more HTTP or HTTPS endpoints.

You can have a single SQS queue subscribe to multiple topics, whether you have one topic for each region or one topic for each account for each region. You must subscribe the queue to your desired SNS topic. (You can subscribe multiple queues to one SNS topic.) For more information, see Sending Amazon SNS Messages to Amazon SQS Queues.

Permissions for Amazon SQS

To use Amazon SQS with Amazon Config, you must configure a policy that grants permissions to your account to perform all actions that are allowed on an SQS queue. The following example

policy grants the account number 111122223333 and account number 444455556666 permission to send messages pertaining to each configuration change to the queue named arn:aws:sqs:us-east-2:444455556666:queue1.

```
{
  "Version": "2012-10-17",
  "Id": "Queue1_Policy_UUID",
  "Statement":
    {
       "Sid":"Queue1_SendMessage",
       "Effect": "Allow",
       "Principal": {
            "AWS": ["111122223333","444455556666"]
         },
        "Action": "sqs:SendMessage",
        "Resource": "arn:aws:sqs:us-east-2:444455556666:queue1"
     }
}
```

You must also create a policy that grants permissions for connections between an SNS topic and the SQS queue that subscribes to that topic. The following is an example policy that permits the SNS topic with the Amazon Resource Name (ARN) arn:aws:sns:us-east-2:111122223333:test-topic to perform any actions on the queue named arn:aws:sqs:us-east-2:111122223333:test-topic-queue.

Note

The account for the SNS topic and the SQS queue must be in the same region.

```
{
  "Version": "2012-10-17",
  "Id": "SNStoSQS",
  "Statement":
    {
      "Sid":"rule1",
      "Effect": "Allow",
      "Principal": {
        "Service": "sns.amazonaws.com"
      },
```

```
      "Action": "SQS:SendMessage",
      "Resource": "arn:aws:sqs:us-east-2:111122223333:test-topic-queue",
      "Condition" : {
        "StringEquals" : {
          "aws:SourceArn":"arn:aws:sns:us-east-2:111122223333:test-topic"
        }
      }
    }
}
```

Each policy can include statements that cover only a single queue, not multiple queues. For information about other restrictions on Amazon SQS policies, see Special Information for Amazon SQS Policies.

Monitoring Amazon Config with Amazon EventBridge

Amazon EventBridge delivers a near real-time stream of system events that describe changes in Amazon resources. Use Amazon EventBridge to detect and react to changes in the status of Amazon Config events.

You can create a rule that runs whenever there is a state transition, or when there is a transition to one or more states that are of interest. Then, based on rules you create, Amazon EventBridge invokes one or more target actions when an event matches the values you specify in a rule. Depending on the type of event, you might want to send notifications, capture event information, take corrective action, initiate events, or take other actions.

Before you create event rules for Amazon Config, however, you should do the following:

- Familiarize yourself with events, rules, and targets in EventBridge. For more information, see What Is Amazon EventBridge?
- For more information about how to get started with EventBridge and set up rules, see Getting started with Amazon EventBridge.
- Create the target or targets you will use in your event rules.

Topics

- Considerations
- Amazon EventBridge format for Amazon Config
- Creating Amazon EventBridge Rule for Amazon Config

Considerations

You will not receive alerts through EventBridge for the following resource types if you are not recording them with Amazon Config:

- `AWS::ACM::Certificate`
- `AWS::CloudTrail::Trail`
- `AWS::CloudWatch::Alarm`
- `AWS::EC2::CustomerGateway`
- `AWS::EC2::EIP`
- `AWS::EC2::Host`
- `AWS::EC2::Instance`
- `AWS::EC2::InternetGateway`
- `AWS::EC2::NetworkAcl`
- `AWS::EC2::NetworkInterface`
- `AWS::EC2::RouteTable`
- `AWS::EC2::SecurityGroup`
- `AWS::EC2::Subnet`
- `AWS::EC2::VPC`
- `AWS::EC2::VPNConnection`
- `AWS::EC2::VPNGateway`
- `AWS::EC2::Volume`
- `AWS::ElasticLoadBalancingV2::LoadBalancer`
- `AWS::IAM::Group`
- `AWS::IAM::Policy`
- `AWS::IAM::Role`
- `AWS::IAM::User`
- `AWS::RDS::DBInstance`
- `AWS::RDS::DBSecurityGroup`
- `AWS::RDS::DBSnapshot`
- `AWS::RDS::DBSubnetGroup`
- `AWS::RDS::EventSubscription`

- AWS::Redshift::Cluster
- AWS::Redshift::ClusterParameterGroup
- AWS::Redshift::ClusterSecurityGroup
- AWS::Redshift::ClusterSnapshot
- AWS::Redshift::ClusterSubnetGroup
- AWS::Redshift::EventSubscription
- AWS::S3::Bucket

Amazon EventBridge format for Amazon Config

The EventBridge event for Amazon Config has the following format:

```
{
   "version": "0",
   "id": "cd4d811e-ab12-322b-8255-872ce65b1bc8",
   "detail-type": "event type",
   "source": "aws.config",
   "account": "111122223333",
   "time": "2018-03-22T00:38:11Z",
   "region": "us-east-1",
   "resources": [
      resources
   ],
   "detail": {
      specific message type
   }
}
```

Creating Amazon EventBridge Rule for Amazon Config

Use the following steps to create an EventBridge rule that triggers on an event emitted by Amazon Config. Events are emitted on a best effort basis.

1. In the navigation pane, choose **Rules**.
2. Choose **Create rule**.
3. Enter a name and description for the rule.

A rule can't have the same name as another rule in the same Region and on the same event bus.

> **Note**
>
> An event bus receives events from a source, uses rules to evaluate them, applies any configured input transformation, and routes them to the appropriate target(s). Your account's default event bus receives events from Amazon Web Services services. A custom event bus can receive events from your custom applications and services. A partner event bus receives events from an event source created by an SaaS partner. These events come from the partners services or applications. For more information, see Event buses in Amazon EventBridge in the *Amazon EventBridge User Guide*.

4. For **Rule type**, choose **Rule with an event pattern**.
5. For **Event source**, choose **Amazon events or EventBridge partner events**.
6. (Optional) For **Sample event type**, choose **Amazon events**.
7. (Optional) For **Sample events**, choose the event type that triggers the rule:
   - Choose **Amazon API Call from CloudTrail** to base rules on API calls made to this service. For more information about creating this type of rule, see Tutorial: Create an Amazon EventBridge rule for Amazon CloudTrail API calls.
   - Choose **Config Configuration Item Change** to get notifications when a resource in your account changes.

     As described in these support articles, you can use EventBridge to receive custom email notifications when a resource is created or deleted, How can I receive custom email notifications when a resource is created in my Amazon Web Services account using Amazon Config service? and How can I receive custom email notifications when a resource is deleted in my Amazon Web Services account using Amazon Config service?.
   - Choose **Config Rules Compliance Change** to get notifications when a compliance check to your rules fails.

     As described in this support article, you can use EventBridge to receive custom email notifications when a resource is noncompliant, How can I be notified when an Amazon resource is noncompliant using Amazon Config?.
   - Choose **Config Rules Re-evaluation Status** to get reevaluation status notifications.

- Choose **Config Configuration Snapshot Delivery Status** to get configuration snapshot delivery status notifications.
- Choose **Config Configuration History Delivery Status** to get configuration history delivery status notifications.

8. For **Creation method**, choose **Use pattern form**.
9. For **Event source**, choose **Amazon services**.
10. For **Amazon service**, choose **Config**.
11. For **Event type**, choose the event type that triggers the rule:
    - Choose **All Events** to make a rule that applies to all Amazon services. If you choose this option, you cannot choose specific message types, rule names, resource types, or resource IDs.
    - Choose **Amazon API Call from CloudTrail** to base rules on API calls made to this service. For more information about creating this type of rule, see Tutorial: Create an Amazon EventBridge rule for Amazon CloudTrail API calls.
    - Choose **Config Configuration Item Change** to get notifications when a resource in your account changes.

      As described in these support articles, you can use EventBridge to receive custom email notifications when a resource is created or deleted, How can I receive custom email notifications when a resource is created in my Amazon Web Services account using Amazon Config service? and How can I receive custom email notifications when a resource is deleted in my Amazon Web Services account using Amazon Config service?.
    - Choose **Config Rules Compliance Change** to get notifications when a compliance check to your rules fails.

      As described in this support article, you can use EventBridge to receive custom email notifications when a resource is noncompliant, How can I be notified when an Amazon resource is noncompliant using Amazon Config?.
    - Choose **Config Rules Re-evaluation Status** to get reevaluation status notifications.
    - Choose **Config Configuration Snapshot Delivery Status** to get configuration snapshot delivery status notifications.
    - Choose **Config Configuration History Delivery Status** to get configuration history delivery status notifications.
12. Choose **Any message type** to receive notifications of any type. Choose **Specific message type(s)** to receive the following types of notifications:

- If you choose **ConfigurationItemChangeNotification**, you receive messages when the configuration of a resource that Amazon Config evaluates has changed.
- If you choose **ComplianceChangeNotification**, you receive messages when the compliance type of a resource that Amazon Config evaluates has changed.
- If you choose **ConfigRulesEvaluationStarted**, you receive messages when Amazon Config starts evaluating your rule against the specified resources.
- If you choose **ConfigurationSnapshotDeliveryCompleted**, you receive messages when Amazon Config successfully delivers the configuration snapshot to your Amazon S3 bucket.
- If you choose **ConfigurationSnapshotDeliveryFailed**, you receive messages when Amazon Config fails to deliver the configuration snapshot to your Amazon S3 bucket.
- If you choose **ConfigurationSnapshotDeliveryStarted**, you receive messages when Amazon Config starts delivering the configuration snapshot to your Amazon S3 bucket.
- If you choose **ConfigurationHistoryDeliveryCompleted**, you receive messages when Amazon Config successfully delivers the configuration history to your Amazon S3 bucket.

13. If you chose a specific event type from the **Event Type** dropdown list, choose **Any resource type** to make a rule that applies to all Amazon Config supported resource types.

    Or choose **Specific resource type(s)**, and then type the Amazon Config supported resource type (for example, `AWS::EC2::Instance`).

14. If you chose a specific event type from the **Event Type** dropdown list, choose **Any resource ID** to include any Amazon Config supported resource ID.

    Or choose **Specific resource ID(s)**, and then type the Amazon Config supported resource ID (for example, `i-04606de676e635647`).

15. If you chose a specific event type from the **Event Type** dropdown list, choose **Any rule name** to include any Amazon Config supported rule.

    Or choose **Specific rule name(s)**, and then type the Amazon Config supported rule (for example, **required-tags**).

16. For **Select target(s)**, choose the type of target you have prepared to use with this rule, and then configure any additional options required by that type.

17. The fields displayed vary depending on the service you choose. Enter information specific to this target type as needed.

18. For many target types, EventBridge needs permissions to send events to the target. In these cases, EventBridge can create the IAM role needed for your rule to run.

- To create an IAM role automatically, choose **Create a new role for this specific resource**.
- To use an IAM role that you created earlier, choose **Use existing role**.

19. (Optional) Choose **Add target** to add another target for this rule.
20. (Optional) Enter one or more tags for the rule. For more information, see Amazon EventBridge tags.
21. Review your rule setup to make sure it meets your event-monitoring requirements.
22. Choose **Create** to confirm your selection.

Using Amazon Config with Interface Amazon VPC Endpoints

If you use Amazon Virtual Private Cloud (Amazon VPC) to host your Amazon resources, you can establish a private connection between your VPC and Amazon Config. You can use this connection to communicate with Amazon Config from your VPC without going through the public internet.

Amazon VPC is an Amazon service that you can use to launch Amazon resources in a virtual network that you define. With a VPC, you have control over your network settings, such the IP address range, subnets, route tables, and network gateways. Interface VPC endpoints are powered by Amazon PrivateLink, an Amazon technology that enables private communication between Amazon services using an elastic network interface with private IP addresses. To connect your VPC to Amazon Config, you define an *interface VPC endpoint* for Amazon Config. This type of endpoint enables you to connect your VPC to Amazon services. The endpoint provides reliable, scalable connectivity to Amazon Config without requiring an internet gateway, network address translation (NAT) instance, or VPN connection. For more information, see What is Amazon VPC in the *Amazon VPC User Guide*.

The following steps are for users of Amazon VPC. For more information, see Getting Started in the *Amazon VPC User Guide*.

Create a VPC Endpoint for Amazon Config

To start using Amazon Config with your VPC, create an interface VPC endpoint for Amazon Config. You do not need to change the settings for Amazon Config. Amazon Config calls other Amazon services using their public endpoints. For more information, see Creating an Interface Endpoint in the *Amazon VPC User Guide*.

Frequently Asked Questions

Unable to see my latest configuration changes

Can I expect to view my configuration changes right away?

Amazon Config usually records configuration changes to your resources right after a change is detected, or at the frequency that you specify. However, this is on a best effort basis and can take longer at times. If issues persist after sometime, contact Amazon Web Services Support and provide your Amazon Config metrics that are supported by Amazon CloudWatch. For information about these metrics, see Amazon Config Usage and Success Metrics.

Indirect Relationships in Amazon Config

Topics

- What is resource relationship?
- What is a direct and an indirect relationship with respect to a resource?
- Which indirect relationships does Amazon Config support?
- Which scenarios uses indirect relationship?
- How are the configuration items created due to direct and indirect relationship?
- What are the configuration items generated due to indirect relationships?
- How do I disable indirect relationship?
- How do I retrieve configuration data related to indirect relationships?

What is resource relationship?

In Amazon, resources refer to entities that are manageable, such as an Amazon Elastic Compute Cloud (Amazon EC2) instance, an Amazon CloudFormation stack, or an Amazon S3 bucket. Amazon Config is a service that tracks and monitors resources by creating configuration items (CIs) whenever a change to a recorded resource type is detected, or at the recording frequency that you set. For instance, when Amazon Config is set up to track Amazon EC2 instances, it creates a configuration item every time an instance is created, updated, or deleted. Each configuration item created by Amazon Config has several fields, including `accountId`, `arn` (Amazon Resource Name), `awsRegion`, `configuration`, `tags`, and `relationships`. The relationships field of a CI enables

Amazon Config to display how resources are linked to one another. For instance, a relationship may indicate that an Amazon EBS volume with ID `vol-123ab45d` is attached to an Amazon EC2 instance with ID `i-a1b2c3d4`, which is associated with security group `sg-ef678hk`.

What is a direct and an indirect relationship with respect to a resource?

Amazon Config derives the relationships for most resource types from the configuration field, which are called "direct" relationships. A direct relationship is a one-way connection (A→B) between a resource (A) and another resource (B), typically obtained from the describe API response of resource (A). In the past, for some resource types that Amazon Config initially supported, it also captured relationships from the configurations of other resources, creating "indirect" relationships that are bidirectional (B→A). For example, the relationship between an Amazon EC2 instance and its security group is direct because the security groups are included in the describe API response for the Amazon EC2 instance. On the other hand, the relationship between a security group and an Amazon EC2 instance is indirect because describing a security group does not return any information about the instances it is associated with.

For example, indirect relationships can help answer the following questions:

- When a NAT Gateway fails, which EC2 instances in private subnets are affected?
- If a route table is modified, which EC2 instance might experience connectivity issues?
- Which security group was never used?
- Which secondary ENI attached to an EC2 instance is associated with the security group?

As a result, when a resource configuration change is detected, Amazon Config not only creates a CI for that resource, but also generates CIs for any related resources, including those with indirect relationships. For example, when Amazon Config detects changes in an Amazon EC2 instance, it creates a CI for the instance and a CI for the security group that is associated with the instance.

Which indirect relationships does Amazon Config support?

The following indirect resource relationships are supported in Amazon Config.

Resource type	is indirectly related to the resource type		
`AWS::EC2::RouteTable`	`AWS::EC2::Instance`		

Resource type	is indirectly related to the resource type		
	,AWS::EC2::NetworkInterface , AWS::EC2::Subnet , AWS::EC2::VPNGateway , AWS::EC2::VPC		
AWS::EC2::EIP	AWS::EC2::Instance , AWS::EC2::NetworkInterface		
AWS::EC2::Instance	AWS::EC2::SecurityGroup ,AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::NetworkInterface	AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::NetworkACL	AWS::EC2::Subnet , AWS::EC2::VPC		

Resource type	is indirectly related to the resource type		
AWS::EC2::VPNConnection	AWS::EC2::VPNGateway ,AWS::EC2::CustomerGateway		
AWS::EC2::InternetGateway	AWS::EC2::VPC		
AWS::EC2::SecurityGroup	AWS::EC2::VPC		
AWS::EC2::Subnet	AWS::EC2::VPC		
AWS::EC2::VPNGateway	AWS::EC2::VPC		

Which scenarios uses indirect relationship?

Below are the Amazon services and the service's feature using indirect relationship.

Amazon feature	Scenario
Amazon Config managed rule	ec2-security-group-attached-to-eni rule checks whether non-default security groups are attached to Elastic Network Interfaces (ENI). Without an indirect relationship, you would need to create a custom rule to check if non-default security groups are attached to an ENI.

Amazon feature	Scenario
Amazon Firewall Manager	Usage Audit Security Group policy uses indirect relationship to understand when a security group was last used. Without an indirect relationship, you would need to build and associate a security group to new resources at the same time to avoid triggering the rule with Amazon Firewall Manager.

Default resources	• Default resources when a non-default VPC is created:
	  • Default security group, default network ACL, and default route table.
	• Default resources when a default VPC is created:
	  • Everything that is created with non-defau lt VPC, an internet gateway, and default subnet in each Availability Zone that you have access to.
	• Default VPC creation itself when an account calls EC2 for first time ever.
	  • Default subnet created for accounts in a newly launched Availability Zone.
	
	Without an indirect relationship, you would need to wait up to 12 hours for anti-entropy to record changes to default resources.

How are the configuration items created due to direct and indirect relationship?

For a direct relationship between resources (A→B), any configuration change to the resource B will initiate a configuration item (CI) for the resource A as well. Similarly, for an indirect relationship (B→A), when there is a configuration change to resource A a new CI will be generated for resource B. For example, Amazon EC2 instance to security group is a direct relationship so any configuration change to a security group would generate a CI for the security group as well as a CI for the EC2 instance. Similarly, security group to Amazon EC2 instance is an indirect relationship so any configuration change to an EC2 instance would generate a CI for the Amazon EC2 instance as well as a CI for the security group.

What are the configuration items generated due to indirect relationships?

Below are the additional configuration items (CIs) generated due to indirect resource relationships.

Configuration changes to the following resource types	will generate CIs for the following resources types		
AWS::EC2::RouteTable	AWS::EC2::Instance , AWS::EC2::NetworkInterface , AWS::EC2::Subnet , AWS::EC2::VPNGateway , and AWS::EC2::VPC		
AWS::EC2::EIP	AWS::EC2::Instance , AWS::EC2:		

Configuration changes to the following resource types	will generate CIs for the following resources types		
	:NetworkInterface		
AWS::EC2::Instance	AWS::EC2::SecurityGroup ,AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::NetworkInterface	AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::NetworkACL	AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::VPNConnection	AWS::EC2::VPNGateway ,AWS::EC2::CustomerGateway		
AWS::EC2::InternetGateway	AWS::EC2::VPC		
AWS::EC2::SecurityGroup	AWS::EC2::VPC		

Configuration changes to the following resource types	will generate CIs for the following resources types		
AWS::EC2::Subnet	AWS::EC2::VPC		
AWS::EC2::VPNGateway	AWS::EC2::VPC		

How do I disable indirect relationship?

Complete the following steps to disable indirect relationship:

1. Open an Amazon Web Services Support case from your account or from the management account for multiple accounts.
2. Select **Technical** for the support type.
3. For Service, select **Amazon Config**.
4. For Category, select **Other**.
5. Select appropriate severity level.
6. Enter **Disable Indirect Relationship** in the subject line.
7. In the description:
   - Confirm you have read this FAQ and want to proceed.
   - List the regions where you want to disable indirect relationship.
   - If submitting from a management account, include account IDs and their associated regions.
   - For multiple accounts, you may attach a CSV file with account IDs and regions.

An Amazon Web Services Support engineer will provide next steps and status updates. We recommend that you maintain a list of Amazon accounts and regions where indirect relationship is disabled. For new accounts, submit a new Amazon Web Services Support case to disable indirect relationship.

How do I retrieve configuration data related to indirect relationships?

You can run Structured Query Language (SQL) queries in Amazon Config Advanced Queries to retrieve configuration data related to indirect resource relationships. For example, if you want to retrieve the list of Amazon EC2 instances related to a security group, use the following query:

```
SELECT
    resourceId,
    resourceType
    WHERE
    resourceType ='AWS::EC2::Instance'
    AND
    relationships.resourceId = 'sg-234213'
```

Code examples for Amazon Config using Amazon SDKs

The following code examples show how to use Amazon Config with an Amazon software development kit (SDK).

Actions are code excerpts from larger programs and must be run in context. While actions show you how to call individual service functions, you can see actions in context in their related scenarios.

For a complete list of Amazon SDK developer guides and code examples, see Using Amazon Config with an Amazon SDK. This topic also includes information about getting started and details about previous SDK versions.

Code examples

- Basic examples for Amazon Config using Amazon SDKs
  - Actions for Amazon Config using Amazon SDKs
    - Use DeleteConfigRule with an Amazon SDK or CLI
    - Use DescribeComplianceByConfigRule with a CLI
    - Use DescribeComplianceByResource with a CLI
    - Use DescribeConfigRuleEvaluationStatus with a CLI
    - Use DescribeConfigRules with an Amazon SDK or CLI
    - Use DescribeConfigurationRecorderStatus with a CLI
    - Use DescribeConfigurationRecorders with a CLI
    - Use DescribeDeliveryChannels with a CLI
    - Use GetComplianceDetailsByConfigRule with a CLI
    - Use GetComplianceDetailsByResource with a CLI
    - Use GetComplianceSummaryByConfigRule with a CLI
    - Use GetComplianceSummaryByResourceType with a CLI
    - Use PutConfigRule with an Amazon SDK or CLI
    - Use PutDeliveryChannel with a CLI

Basic examples for Amazon Config using Amazon SDKs

The following code examples show how to use the basics of Amazon Config with Amazon SDKs.

Examples

- Actions for Amazon Config using Amazon SDKs
  - Use DeleteConfigRule with an Amazon SDK or CLI
  - Use DescribeComplianceByConfigRule with a CLI
  - Use DescribeComplianceByResource with a CLI
  - Use DescribeConfigRuleEvaluationStatus with a CLI
  - Use DescribeConfigRules with an Amazon SDK or CLI
  - Use DescribeConfigurationRecorderStatus with a CLI
  - Use DescribeConfigurationRecorders with a CLI
  - Use DescribeDeliveryChannels with a CLI
  - Use GetComplianceDetailsByConfigRule with a CLI
  - Use GetComplianceDetailsByResource with a CLI
  - Use GetComplianceSummaryByConfigRule with a CLI
  - Use GetComplianceSummaryByResourceType with a CLI
  - Use PutConfigRule with an Amazon SDK or CLI
  - Use PutDeliveryChannel with a CLI

Actions for Amazon Config using Amazon SDKs

The following code examples demonstrate how to perform individual Amazon Config actions with Amazon SDKs. Each example includes a link to GitHub, where you can find instructions for setting up and running the code.

The following examples include only the most commonly used actions. For a complete list, see the Amazon Config API Reference.

Examples

- Use DeleteConfigRule with an Amazon SDK or CLI
- Use DescribeComplianceByConfigRule with a CLI
- Use DescribeComplianceByResource with a CLI
- Use DescribeConfigRuleEvaluationStatus with a CLI
- Use DescribeConfigRules with an Amazon SDK or CLI
- Use DescribeConfigurationRecorderStatus with a CLI

- Use DescribeConfigurationRecorders with a CLI
- Use DescribeDeliveryChannels with a CLI
- Use GetComplianceDetailsByConfigRule with a CLI
- Use GetComplianceDetailsByResource with a CLI
- Use GetComplianceSummaryByConfigRule with a CLI
- Use GetComplianceSummaryByResourceType with a CLI
- Use PutConfigRule with an Amazon SDK or CLI
- Use PutDeliveryChannel with a CLI

Use `DeleteConfigRule` with an Amazon SDK or CLI

The following code examples show how to use `DeleteConfigRule`.

CLI

Amazon CLI

To delete an Amazon Config rule

The following command deletes an Amazon Config rule named `MyConfigRule`:

```
aws configservice delete-config-rule --config-rule-name MyConfigRule
```

- For API details, see DeleteConfigRule in *Amazon CLI Command Reference*.

Python

SDK for Python (Boto3)

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
class ConfigWrapper:
```

```
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def delete_config_rule(self, rule_name):
        """
        Delete the specified rule.

        :param rule_name: The name of the rule to delete.
        """
        try:
            self.config_client.delete_config_rule(ConfigRuleName=rule_name)
            logger.info("Deleted rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't delete rule %s.", rule_name)
            raise
```

- For API details, see DeleteConfigRule in *Amazon SDK for Python (Boto3) API Reference*.

For a complete list of Amazon SDK developer guides and code examples, see Using Amazon Config with an Amazon SDK. This topic also includes information about getting started and details about previous SDK versions.

Use `DescribeComplianceByConfigRule` with a CLI

The following code examples show how to use `DescribeComplianceByConfigRule`.

CLI

Amazon CLI

To get compliance information for your Amazon Config rules

The following command returns compliance information for each Amazon Config rule that is violated by one or more Amazon resources:

```
aws configservice describe-compliance-by-config-rule --compliance-
types NON_COMPLIANT
```

In the output, the value for each `CappedCount` attribute indicates how many resources do not comply with the related rule. For example, the following output indicates that 3 resources do not comply with the rule named `InstanceTypesAreT2micro`.

Output:

```
{
    "ComplianceByConfigRules": [
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "InstanceTypesAreT2micro"
        },
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "RequiredTagsForVolumes"
        }
    ]
}
```

- For API details, see DescribeComplianceByConfigRule in *Amazon CLI Command Reference*.

PowerShell

Tools for PowerShell V4

Example 1: This example retrieves compliances details for the rule ebs-optimized-instance, for which there is no current evaluation results for the rule, hence it returns INSUFFICIENT_DATA

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

Output:

```
ComplianceContributorCount ComplianceType
-------------------------- --------------
                           INSUFFICIENT_DATA
```

Example 2: This example returns the number of non-compliant resources for the rule ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK.

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

Output:

```
CapExceeded CappedCount
----------- -----------
False       2
```

- For API details, see DescribeComplianceByConfigRule in *Amazon Tools for PowerShell Cmdlet Reference (V4)*.

Tools for PowerShell V5

Example 1: This example retrieves compliances details for the rule ebs-optimized-instance, for which there is no current evaluation results for the rule, hence it returns INSUFFICIENT_DATA

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

Output:

```
ComplianceContributorCount ComplianceType
-------------------------- --------------
                           INSUFFICIENT_DATA
```

Example 2: This example returns the number of non-compliant resources for the rule ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK.

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

Output:

```
CapExceeded CappedCount
----------- -----------
False       2
```

- For API details, see DescribeComplianceByConfigRule in *Amazon Tools for PowerShell Cmdlet Reference (V5)*.

For a complete list of Amazon SDK developer guides and code examples, see Using Amazon Config with an Amazon SDK. This topic also includes information about getting started and details about previous SDK versions.

Use `DescribeComplianceByResource` with a CLI

The following code examples show how to use `DescribeComplianceByResource`.

CLI

Amazon CLI

To get compliance information for your Amazon resources

The following command returns compliance information for each EC2 instance that is recorded by Amazon Config and that violates one or more rules:

```
aws configservice describe-compliance-by-resource --resource-
type AWS::EC2::Instance --compliance-types NON_COMPLIANT
```

In the output, the value for each `CappedCount` attribute indicates how many rules the resource violates. For example, the following output indicates that instance `i-1a2b3c4d` violates 2 rules.

Output:

```
{
    "ComplianceByResources": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-1a2b3c4d",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 2,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        },
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-2a2b3c4d ",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        }
    ]
}
```

- For API details, see DescribeComplianceByResource in *Amazon CLI Command Reference*.

PowerShell

Tools for PowerShell V4

Example 1: This example checks the `AWS::SSM::ManagedInstanceInventory` resource type for 'COMPLIANT' compliance type.

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

Output:

```
Compliance                              ResourceId          ResourceType
----------                              ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- For API details, see DescribeComplianceByResource in *Amazon Tools for PowerShell Cmdlet Reference (V4)*.

Tools for PowerShell V5

Example 1: This example checks the `AWS::SSM::ManagedInstanceInventory` resource type for 'COMPLIANT' compliance type.

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

Output:

```
Compliance                              ResourceId          ResourceType
----------                              ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- For API details, see DescribeComplianceByResource in *Amazon Tools for PowerShell Cmdlet Reference (V5)*.

For a complete list of Amazon SDK developer guides and code examples, see Using Amazon Config with an Amazon SDK. This topic also includes information about getting started and details about previous SDK versions.

Use `DescribeConfigRuleEvaluationStatus` with a CLI

The following code examples show how to use `DescribeConfigRuleEvaluationStatus`.

CLI

Amazon CLI

To get status information for an Amazon Config rule

The following command returns the status information for an Amazon Config rule named `MyConfigRule`:

```
aws configservice describe-config-rule-evaluation-status --config-rule-
names MyConfigRule
```

Output:

```
{
    "ConfigRulesEvaluationStatus": [
        {
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "FirstActivatedTime": 1450311703.844,
            "ConfigRuleId": "config-rule-abcdef",
            "LastSuccessfulInvocationTime": 1450314643.156,
            "ConfigRuleName": "MyConfigRule"
        }
    ]
}
```

- For API details, see DescribeConfigRuleEvaluationStatus in *Amazon CLI Command Reference*.

PowerShell

Tools for PowerShell V4

Example 1: This sample returns the status information for the given config rules.

```
Get-CFGConfigRuleEvaluationStatus -ConfigRuleName root-account-mfa-enabled, vpc-
flow-logs-enabled
```

Output:

```
ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-kvq1wk
ConfigRuleId                 : config-rule-kvq1wk
ConfigRuleName               : root-account-mfa-enabled
FirstActivatedTime           : 8/27/2019 8:05:17 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 8:12:03 AM
LastSuccessfulInvocationTime : 12/13/2019 8:12:03 AM

ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-z1s23b
ConfigRuleId                 : config-rule-z1s23b
ConfigRuleName               : vpc-flow-logs-enabled
FirstActivatedTime           : 8/14/2019 6:23:44 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 7:12:01 AM
LastSuccessfulInvocationTime : 12/13/2019 7:12:01 AM
```

- For API details, see DescribeConfigRuleEvaluationStatus in *Amazon Tools for PowerShell Cmdlet Reference (V4)*.

Tools for PowerShell V5

Example 1: This sample returns the status information for the given config rules.

```
Get-CFGConfigRuleEvaluationStatus -ConfigRuleName root-account-mfa-enabled, vpc-
flow-logs-enabled
```

Output:

```
ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-kvq1wk
ConfigRuleId                 : config-rule-kvq1wk
ConfigRuleName               : root-account-mfa-enabled
FirstActivatedTime           : 8/27/2019 8:05:17 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 8:12:03 AM
LastSuccessfulInvocationTime : 12/13/2019 8:12:03 AM

ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-z1s23b
ConfigRuleId                 : config-rule-z1s23b
ConfigRuleName               : vpc-flow-logs-enabled
FirstActivatedTime           : 8/14/2019 6:23:44 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 7:12:01 AM
LastSuccessfulInvocationTime : 12/13/2019 7:12:01 AM
```

- For API details, see DescribeConfigRuleEvaluationStatus in *Amazon Tools for PowerShell Cmdlet Reference (V5)*.

For a complete list of Amazon SDK developer guides and code examples, see Using Amazon Config with an Amazon SDK. This topic also includes information about getting started and details about previous SDK versions.

Use `DescribeConfigRules` with an Amazon SDK or CLI

The following code examples show how to use `DescribeConfigRules`.

CLI

Amazon CLI

To get details for an Amazon Config rule

The following command returns details for an Amazon Config rule named `InstanceTypesAreT2micro`:

```
aws configservice describe-config-rules --config-rule-
names InstanceTypesAreT2micro
```

Output:

```
{
    "ConfigRules": [
        {
            "ConfigRuleState": "ACTIVE",
            "Description": "Evaluates whether EC2 instances are the t2.micro
 type.",
            "ConfigRuleName": "InstanceTypesAreT2micro",
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "Source": {
                "Owner": "CUSTOM_LAMBDA",
                "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
                "SourceDetails": [
                    {
                        "EventSource": "aws.config",
                        "MessageType": "ConfigurationItemChangeNotification"
                    }
                ]
            },
            "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}",
            "Scope": {
                "ComplianceResourceTypes": [
                    "AWS::EC2::Instance"
                ]
            },
            "ConfigRuleId": "config-rule-abcdef"
        }
    ]
}
```

- For API details, see DescribeConfigRules in *Amazon CLI Command Reference*.

PowerShell

Tools for PowerShell V4

Example 1: This sample lists config rules for the account, with selected properties.

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

Output:

```
ConfigRuleName                                  ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                  ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                           config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                             config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required      config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- For API details, see DescribeConfigRules in *Amazon Tools for PowerShell Cmdlet Reference (V4)*.

Tools for PowerShell V5

Example 1: This sample lists config rules for the account, with selected properties.

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

Output:

```
ConfigRuleName                                  ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
```

```
--------------                                      ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                               config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                                 config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required          config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- For API details, see DescribeConfigRules in *Amazon Tools for PowerShell Cmdlet Reference (V5)*.

Python

SDK for Python (Boto3)

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def describe_config_rule(self, rule_name):
        """
        Gets data for the specified rule.
```

```
        :param rule_name: The name of the rule to retrieve.
        :return: The rule data.
        """
        try:
            response = self.config_client.describe_config_rules(
                ConfigRuleNames=[rule_name]
            )
            rule = response["ConfigRules"]
            logger.info("Got data for rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't get data for rule %s.", rule_name)
            raise
        else:
            return rule
```

- For API details, see DescribeConfigRules in *Amazon SDK for Python (Boto3) API Reference*.

For a complete list of Amazon SDK developer guides and code examples, see Using Amazon Config with an Amazon SDK. This topic also includes information about getting started and details about previous SDK versions.

Use `DescribeConfigurationRecorderStatus` with a CLI

The following code examples show how to use `DescribeConfigurationRecorderStatus`.

CLI

Amazon CLI

To get status information for the configuration recorder

The following command returns the status of the default configuration recorder:

```
aws configservice describe-configuration-recorder-status
```

Output:

```
{
    "ConfigurationRecordersStatus": [
```

```
        {
            "name": "default",
            "lastStatus": "SUCCESS",
            "recording": true,
            "lastStatusChangeTime": 1452193834.344,
            "lastStartTime": 1441039997.819,
            "lastStopTime": 1441039992.835
        }
    ]
}
```

- For API details, see DescribeConfigurationRecorderStatus in *Amazon CLI Command Reference*.

PowerShell

Tools for PowerShell V4

Example 1: This sample returns status of the configuration recorders.

```
Get-CFGConfigurationRecorderStatus
```

Output:

```
LastErrorCode        :
LastErrorMessage     :
LastStartTime        : 10/11/2019 10:13:51 AM
LastStatus           : Success
LastStatusChangeTime : 12/31/2019 6:14:12 AM
LastStopTime         : 10/11/2019 10:13:46 AM
Name                 : default
Recording            : True
```

- For API details, see DescribeConfigurationRecorderStatus in *Amazon Tools for PowerShell Cmdlet Reference (V4)*.

Tools for PowerShell V5

Example 1: This sample returns status of the configuration recorders.

```
Get-CFGConfigurationRecorderStatus
```

Output:

```
LastErrorCode        :
LastErrorMessage     :
LastStartTime        : 10/11/2019 10:13:51 AM
LastStatus           : Success
LastStatusChangeTime : 12/31/2019 6:14:12 AM
LastStopTime         : 10/11/2019 10:13:46 AM
Name                 : default
Recording            : True
```

- For API details, see DescribeConfigurationRecorderStatus in *Amazon Tools for PowerShell Cmdlet Reference (V5)*.

For a complete list of Amazon SDK developer guides and code examples, see Using Amazon Config with an Amazon SDK. This topic also includes information about getting started and details about previous SDK versions.

Use `DescribeConfigurationRecorders` with a CLI

The following code examples show how to use `DescribeConfigurationRecorders`.

CLI

Amazon CLI

To get details about the configuration recorder

The following command returns details about the default configuration recorder:

```
aws configservice describe-configuration-recorders
```

Output:

```
{
    "ConfigurationRecorders": [
        {
            "recordingGroup": {
                "allSupported": true,
                "resourceTypes": [],
                "includeGlobalResourceTypes": true
```

```
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-ConfigRole-
A1B2C3D4E5F6",
            "name": "default"
        }
    ]
}
```

- For API details, see DescribeConfigurationRecorders in *Amazon CLI Command Reference*.

PowerShell

Tools for PowerShell V4

Example 1: This example returns the details of configuration recorders.

```
Get-CFGConfigurationRecorder | Format-List
```

Output:

```
Name           : default
RecordingGroup : Amazon.ConfigService.Model.RecordingGroup
RoleARN        : arn:aws:iam::123456789012:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig
```

- For API details, see DescribeConfigurationRecorders in *Amazon Tools for PowerShell Cmdlet Reference (V4)*.

Tools for PowerShell V5

Example 1: This example returns the details of configuration recorders.

```
Get-CFGConfigurationRecorder | Format-List
```

Output:

```
Name           : default
RecordingGroup : Amazon.ConfigService.Model.RecordingGroup
RoleARN        : arn:aws:iam::123456789012:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig
```

- For API details, see DescribeConfigurationRecorders in *Amazon Tools for PowerShell Cmdlet Reference (V5)*.

For a complete list of Amazon SDK developer guides and code examples, see Using Amazon Config with an Amazon SDK. This topic also includes information about getting started and details about previous SDK versions.

Use `DescribeDeliveryChannels` with a CLI

The following code examples show how to use `DescribeDeliveryChannels`.

CLI

Amazon CLI

To get details about the delivery channel

The following command returns details about the delivery channel:

```
aws configservice describe-delivery-channels
```

Output:

```
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

- For API details, see DescribeDeliveryChannels in *Amazon CLI Command Reference*.

PowerShell

Tools for PowerShell V4

Example 1: This example retrieves the delivery channel for the region and displays details.

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

Output:

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- ----------------
default config-bucket-NA my          TwentyFour_Hours
```

- For API details, see DescribeDeliveryChannels in *Amazon Tools for PowerShell Cmdlet Reference (V4)*.

Tools for PowerShell V5

Example 1: This example retrieves the delivery channel for the region and displays details.

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

Output:

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- ----------------
default config-bucket-NA my          TwentyFour_Hours
```

- For API details, see DescribeDeliveryChannels in *Amazon Tools for PowerShell Cmdlet Reference (V5)*.

For a complete list of Amazon SDK developer guides and code examples, see Using Amazon Config with an Amazon SDK. This topic also includes information about getting started and details about previous SDK versions.

Use `GetComplianceDetailsByConfigRule` with a CLI

The following code examples show how to use `GetComplianceDetailsByConfigRule`.

CLI

Amazon CLI

To get the evaluation results for an Amazon Config rule

The following command returns the evaluation results for all of the resources that don't comply with an Amazon Config rule named `InstanceTypesAreT2micro`:

```
aws configservice get-compliance-details-by-config-rule --config-rule-
name InstanceTypesAreT2micro --compliance-types NON_COMPLIANT
```

Output:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-2a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.18,
            "ConfigRuleInvokedTime": 1450314642.902,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
```

```
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-3a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.346,
            "ConfigRuleInvokedTime": 1450314643.124,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- For API details, see GetComplianceDetailsByConfigRule in *Amazon CLI Command Reference*.

PowerShell

Tools for PowerShell V4

Example 1: This example obtains the evaluation results for the rule access-keys-rotated and returns the output grouped by compliance-type

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

Output:

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

Example 2: This example queries compliance details for the rule access-keys-rotated for COMPLIANT resources.

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

Output:

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- For API details, see GetComplianceDetailsByConfigRule in *Amazon Tools for PowerShell Cmdlet Reference (V4)*.

Tools for PowerShell V5

Example 1: This example obtains the evaluation results for the rule access-keys-rotated and returns the output grouped by compliance-type

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

Output:

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

Example 2: This example queries compliance details for the rule access-keys-rotated for COMPLIANT resources.

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

Output:

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- For API details, see GetComplianceDetailsByConfigRule in *Amazon Tools for PowerShell Cmdlet Reference (V5)*.

For a complete list of Amazon SDK developer guides and code examples, see Using Amazon Config with an Amazon SDK. This topic also includes information about getting started and details about previous SDK versions.

Use `GetComplianceDetailsByResource` with a CLI

The following code examples show how to use `GetComplianceDetailsByResource`.

CLI

Amazon CLI

To get the evaluation results for an Amazon resource

The following command returns the evaluation results for each rule with which the EC2 instance `i-1a2b3c4d` does not comply:

```
aws configservice get-compliance-details-by-resource --resource-
type AWS::EC2::Instance --resource-id i-1a2b3c4d --compliance-types NON_COMPLIANT
```

Output:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
```

```
            },
            "ResultRecordedTime": 1450314643.288,
            "ConfigRuleInvokedTime": 1450314643.034,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "RequiredTagForEC2Instances"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- For API details, see GetComplianceDetailsByResource in *Amazon CLI Command Reference*.

PowerShell

Tools for PowerShell V4

Example 1: This example evaulation results for the given resource.

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

Output:

```
Annotation                :
ComplianceType            : COMPLIANT
ConfigRuleInvokedTime     : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime        : 8/25/2019 11:34:56 PM
ResultToken               :
```

- For API details, see GetComplianceDetailsByResource in *Amazon Tools for PowerShell Cmdlet Reference (V4)*.

Tools for PowerShell V5

Example 1: This example evaulation results for the given resource.

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

Output:

```
Annotation                :
ComplianceType            : COMPLIANT
ConfigRuleInvokedTime     : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime        : 8/25/2019 11:34:56 PM
ResultToken               :
```

- For API details, see GetComplianceDetailsByResource in *Amazon Tools for PowerShell Cmdlet Reference (V5)*.

For a complete list of Amazon SDK developer guides and code examples, see Using Amazon Config with an Amazon SDK. This topic also includes information about getting started and details about previous SDK versions.

Use `GetComplianceSummaryByConfigRule` with a CLI

The following code examples show how to use `GetComplianceSummaryByConfigRule`.

CLI

Amazon CLI

To get the compliance summary for your Amazon Config rules

The following command returns the number of rules that are compliant and the number that are noncompliant:

```
aws configservice get-compliance-summary-by-config-rule
```

In the output, the value for each CappedCount attribute indicates how many rules are compliant or noncompliant.

Output:

```
{
    "ComplianceSummary": {
        "NonCompliantResourceCount": {
            "CappedCount": 3,
            "CapExceeded": false
        },
        "ComplianceSummaryTimestamp": 1452204131.493,
        "CompliantResourceCount": {
            "CappedCount": 2,
            "CapExceeded": false
        }
    }
}
```

- For API details, see GetComplianceSummaryByConfigRule in *Amazon CLI Command Reference*.

PowerShell

Tools for PowerShell V4

Example 1: This sample returns the number of Config rules that are non-compliant.

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

Output:

```
CapExceeded CappedCount
----------- -----------
False       9
```

- For API details, see GetComplianceSummaryByConfigRule in *Amazon Tools for PowerShell Cmdlet Reference (V4)*.

Tools for PowerShell V5

Example 1: This sample returns the number of Config rules that are non-compliant.

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

Output:

```
CapExceeded CappedCount
----------- -----------
False       9
```

- For API details, see GetComplianceSummaryByConfigRule in *Amazon Tools for PowerShell Cmdlet Reference (V5)*.

For a complete list of Amazon SDK developer guides and code examples, see Using Amazon Config with an Amazon SDK. This topic also includes information about getting started and details about previous SDK versions.

Use `GetComplianceSummaryByResourceType` with a CLI

The following code examples show how to use `GetComplianceSummaryByResourceType`.

CLI

Amazon CLI

To get the compliance summary for all resource types

The following command returns the number of Amazon resources that are noncompliant and the number that are compliant:

```
aws configservice get-compliance-summary-by-resource-type
```

In the output, the value for each `CappedCount` attribute indicates how many resources are compliant or noncompliant.

Output:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 16,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1453237464.543,
                "CompliantResourceCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

To get the compliance summary for a specific resource type

The following command returns the number of EC2 instances that are noncompliant and the number that are compliant:

```
aws configservice get-compliance-summary-by-resource-type --resource-
types AWS::EC2::Instance
```

In the output, the value for each CappedCount attribute indicates how many resources are compliant or noncompliant.

Output:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1452204923.518,
                "CompliantResourceCount": {
```

```
                    "CappedCount": 7,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

- For API details, see GetComplianceSummaryByResourceType in *Amazon CLI Command Reference*.

PowerShell

Tools for PowerShell V4

Example 1: This sample returns the number of resources that are compliant or noncompliant and converts the output to json.

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- For API details, see GetComplianceSummaryByResourceType in *Amazon Tools for PowerShell Cmdlet Reference (V4)*.

Tools for PowerShell V5

Example 1: This sample returns the number of resources that are compliant or noncompliant and converts the output to json.

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
```

```
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- For API details, see GetComplianceSummaryByResourceType in *Amazon Tools for PowerShell Cmdlet Reference (V5)*.

For a complete list of Amazon SDK developer guides and code examples, see Using Amazon Config with an Amazon SDK. This topic also includes information about getting started and details about previous SDK versions.

Use `PutConfigRule` with an Amazon SDK or CLI

The following code examples show how to use `PutConfigRule`.

CLI

Amazon CLI

To add an Amazon managed Config rule

The following command provides JSON code to add an Amazon managed Config rule:

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

`RequiredTagsForEC2Instances.json` is a JSON file that contains the rule configuration:

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
```

```
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

For the `ComplianceResourceTypes` attribute, this JSON code limits the scope to resources of the `AWS::EC2::Instance` type, so Amazon Config will evaluate only EC2 instances against the rule. Because the rule is a managed rule, the `Owner` attribute is set to `AWS`, and the `SourceIdentifier` attribute is set to the rule identifier, `REQUIRED_TAGS`. For the `InputParameters` attribute, the tag keys that the rule requires, `CostCenter` and `Owner`, are specified.

If the command succeeds, Amazon Config returns no output. To verify the rule configuration, run the describe-config-rules command, and specify the rule name.

To add a customer managed Config rule

The following command provides JSON code to add a customer managed Config rule:

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

`InstanceTypesAreT2micro.json` is a JSON file that contains the rule configuration:

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
    "SourceDetails": [
```

```
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

For the `ComplianceResourceTypes` attribute, this JSON code limits the scope to resources of the `AWS::EC2::Instance` type, so Amazon Config will evaluate only EC2 instances against the rule. Because this rule is a customer managed rule, the `Owner` attribute is set to `CUSTOM_LAMBDA`, and the `SourceIdentifier` attribute is set to the ARN of the Amazon Lambda function. The `SourceDetails` object is required. The parameters that are specified for the `InputParameters` attribute are passed to the Amazon Lambda function when Amazon Config invokes it to evaluate resources against the rule.

If the command succeeds, Amazon Config returns no output. To verify the rule configuration, run the describe-config-rules command, and specify the rule name.

- For API details, see PutConfigRule in *Amazon CLI Command Reference*.

Python

SDK for Python (Boto3)

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the Amazon Code Examples Repository.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
```

```
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
publicly
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- For API details, see PutConfigRule in *Amazon SDK for Python (Boto3) API Reference*.

For a complete list of Amazon SDK developer guides and code examples, see Using Amazon Config with an Amazon SDK. This topic also includes information about getting started and details about previous SDK versions.

Use `PutDeliveryChannel` with a CLI

The following code examples show how to use `PutDeliveryChannel`.

CLI

Amazon CLI

To create a delivery channel

The following command provides the settings for the delivery channel as JSON code:

```
aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

The `deliveryChannel.json` file specifies the delivery channel attributes:

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

This example sets the following attributes:

`name` - The name of the delivery channel. By default, Amazon Config assigns the name `default` to a new delivery channel.You cannot update the delivery channel name with the `put-delivery-channel` command. For the steps to change the name, see Renaming the Delivery Channel.`s3BucketName` - The name of the Amazon S3 bucket to which Amazon Config delivers configuration snapshots and configuration history files.If you specify a bucket that belongs to another Amazon account, that bucket must have policies that grant access permissions to Amazon Config. For more information, see Permissions for the Amazon S3 Bucket.

`snsTopicARN` - The Amazon Resource Name (ARN) of the Amazon SNS topic to which Amazon Config sends notifications about configuration changes.If you choose a topic from another account, the topic must have policies that grant access permissions to Amazon Config. For more information, see Permissions for the Amazon SNS Topic.

`configSnapshotDeliveryProperties` - Contains the `deliveryFrequency` attribute, which sets how often Amazon Config delivers configuration snapshots and how often it invokes evaluations for periodic Config rules.

If the command succeeds, Amazon Config returns no output. To verify the settings of your delivery channel, run the describe-delivery-channels command.

- For API details, see PutDeliveryChannel in *Amazon CLI Command Reference*.

PowerShell

Tools for PowerShell V4

Example 1: This example changes the deliveryFrequency property of an existing delivery channel.

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 amzn-s3-demo-bucket -DeliveryChannel_S3KeyPrefix my
```

- For API details, see PutDeliveryChannel in *Amazon Tools for PowerShell Cmdlet Reference (V4)*.

Tools for PowerShell V5

Example 1: This example changes the deliveryFrequency property of an existing delivery channel.

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 amzn-s3-demo-bucket -DeliveryChannel_S3KeyPrefix my
```

- For API details, see PutDeliveryChannel in *Amazon Tools for PowerShell Cmdlet Reference (V5)*.

For a complete list of Amazon SDK developer guides and code examples, see Using Amazon Config with an Amazon SDK. This topic also includes information about getting started and details about previous SDK versions.

Document History

The following table describes the important changes to the documentation for Amazon Config. For notification about updates to this documentation, you can subscribe to an RSS feed.

- **API version**: 2014-11-12
- **Latest documentation update**: June 24, 2025

Change	Description	Date
Security IAM updates	The `AWS_ConfigRole` policy and `AWSConfig ServiceRolePolicy` policy now grants additiona l permissions for Amazon Backup gateway, Amazon Billing and Cost Managemen t, Amazon Bedrock, Amazon CloudFormation, Amazon CloudFront, Amazon Entity Resolution, Amazon IoT Core Device Advisor, Amazon Lambda, Amazon Network Manager, Amazon Private Certificate Authority, Amazon Redshift, Amazon S3 Tables, Amazon Systems Manager Quick Setup. For more information, see Amazon managed policies for Amazon Config.	June 18, 2025
Amazon Config supports new resource types	With this release, you can use Amazon Config to record configuration changes to new Amazon Bedrock resource	June 17, 2025

	types. For more information, see Supported resource types.	
Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • cloudfront-ssl-policy-check • cognito-identity-pool-unauth-access-check • ec2-enis-source-destination-check-enabled • elbv2-listener-encryption-in-transit • lambda-function-xray-enabled • msk-cluster-public-access-disabled • msk-connect-connector-logging-enabled • msk-unrestricted-access-check • aurora-mysql-cluster-audit-logging • redshift-cluster-multi-az-enabled • s3express-dir-bucket-lifecycle-rules-check • ssm-automation-logging-enabled • ssm-automation-block-public-sharing	June 13, 2025

Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Bedrock. For more information, see Amazon managed policies for Amazon Config.	May 27, 2025
Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new Amazon App Integrations, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Inspector, Amazon Macie, Amazon Route 53 Profiles, Amazon OpenSearch Serverless, Amazon Simple Storage Service (Amazon S3), Amazon Security Hub, and Amazon SageMaker AI resource types. For more information, see Supported Resource Types.	April 30, 2025
Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rule: redshift-serverless-default-db-name-check	April 22, 2025
Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rule: redshift-serverless-default-admin-check	April 17, 2025

Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon B2B Data Interchange, Amazon Bedrock, Amazon Clean Rooms, Amazon CodeConnections, Amazon Direct Connect, Amazon Database Migration Service (Amazon DMS), Amazon CloudWatch Logs, Amazon Macie, Amazon Managed Blockchain, Amazon Q Business, Route 53 Profiles, Amazon Simple Storage Service (Amazon S3), Amazon SageMaker AI, Amazon Security Hub, and Amazon Systems Manager Incident Manager, Amazon Systems Manager Incident Manager Contacts, and Amazon Systems Manager. For more information, see Amazon managed policies for Amazon Config.	April 8, 2025

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • s3-bucket-tagged • ecr-repository-tagged • sagemaker-feature-group-tagged • sagemaker-domain-tagged • cognito-user-pool-tagged	April 1, 2025

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • nlb-cross-zone-load-balancing-enabled • redshift-serverless-publish-logs-to-cloudwatch • rds-instance-subnet-igw-check • ec2-spot-fleet-request-ct-encryption-at-rest • redshift-serverless-workgroup-encrypted-in-transit • redshift-serverless-workgroup-no-public-access • redshift-serverless-namespace-cmk-encryption • event-data-store-cmk-encryption-enabled • ecs-task-definition-network-mode-not-host • rds-proxy-tls-encryption • nlb-logging-enabled • redshift-audit-logging-enabled • s3-lifecycle-policy-check • sagemaker-image-tagged • redshift-cluster-parameter-group-tagged • ec2-dhcp-options-tagged • sagemaker-app-image-config-tagged	March 22, 2025

- mariadb-publish-logs-to-cloudwatch-logs
- docdb-cluster-encrypted-in-transit
- rds-sqlserver-encrypted-in-transit
- ec2-traffic-mirror-session-tagged
- ec2-launch-template-tagged
- ec2-traffic-mirror-target-tagged
- transfer-certificate-tagged
- batch-managed-compute-env-compute-resources-tagged
- lightsail-disk-tagged
- transfer-profile-tagged
- amplify-app-tagged
- ec2-prefix-list-tagged
- amplify-branch-tagged
- transfer-agreement-tagged
- datasync-task-tagged
- transfer-workflow-tagged
- sagemaker_notebook_instance_platform_version
- ec2-traffic-mirror-filter-tagged
- aurora-mysql-cluster-audit-logging
- ssm-document-tagged
- transfer-connector-tagged

- rds-mariadb-instance-encrypted-in-transit
- iam-saml-provider-tagged
- ec2-fleet-tagged
- iam-server-certificate-tagged
- iam-oidc-provider-tagged
- alb-listener-tagged
- glb-listener-tagged
- ec2-network-insights-access-scope-tagged
- lightsail-certificate-tagged
- ec2-capacity-reservation-tagged
- ec2-transit-gateway-multicast-domain-tagged
- dms-endpoint-tagged
- ec2-carrier-gateway-tagged
- dms-replication-task-tagged
- ec2-client-vpn-endpoint-tagged
- lightsail-bucket-tagged
- ec2-network-insights-access-scope-analysis-tagged
- nlb-listener-tagged
- ec2-network-insights-path-tagged

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • docdb-cluster-encrypted-in-transit • mariadb-publish-logs-to-cloudwatch-logs • aurora-mysql-cluster-audit-logging • rds-mariadb-instance-encrypted-in-transit • rds-sqlserver-encrypted-in-transit • sagemaker-notebook-instance-platform-version • appstream-fleet-multi-az • apprunner-vpc-connector-multi-az • mq-broker-general-logging-enabled • mq-active-single-instance-broker-storage-type-efs • mq-active-broker-ldap-authentication • iottwinmaker-component-type-tagged	March 19, 2025

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • fsx-openzfs-deployment-type-check • fsx-ontap-deployment-type-check • fsx-windows-deployment-type-check • redshift-serverless-workgroup-routes-within-vpc	March 18, 2025
Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: ec2-instance-launched-with-allowed-ami	March 11, 2025

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • connect-instance-logging-enabled • ecr-repository-cmk-encryption-enabled • elbv2-predefined-security-policy-ssl-check • glue-spark-job-supported-version • guardduty-runtime-monitoring-enabled • guardduty-ecs-protection-runtime-enabled • guardduty-ec2-protection-runtime-enabled • netfw-subnet-change-protection-enabled • rds-sql-server-logs-to-cloudwatch • sqs-queue-no-public-access • transfer-connector-logging-enabled	March 7, 2025

Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Elastic Compute Cloud (Amazon EC2). For more information, see Amazon managed policies for Amazon Config.	March 4, 2025

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • athena-workgroup-description • amplify-app-tagged • sagemaker-app-image-config-tagged • elasticbeanstalk-application-version-description • amplify-branch-performance-mode-enabled • athena-workgroup-engine-version-auto-upgrade • sagemaker-image-description • devicefarm-instance-profile-tagged • transfer-workflow-description • ec2-traffic-mirror-session-tagged • appstream-fleet-in-vpc • transfer-agreement-tagged • ec2-traffic-mirror-target-description • transfer-agreement-description • athena-prepared-statement-description	February 8, 2025

- batch-managed-compute-env-compute-resources-tagged
- codedeploy-deployment-group-auto-rollback-enabled
- batch-managed-compute-environment-using-launch-template
- ec2-prefix-list-tagged
- ec2-traffic-mirror-filter-tagged
- athena-workgroup-enforce-workgroup-configuration
- transfer-certificate-tagged
- batch-compute-environment-managed
- lightsail-disk-tagged
- transfer-profile-tagged
- ec2-traffic-mirror-target-tagged
- appintegrations-event-integration-tagged
- datasync-task-tagged
- batch-compute-environment-enabled
- appconfig-configuration-profile-validators-not-empty
- elasticbeanstalk-application-description

- codedeploy-deployment-group-outdated-instances-update
- ec2-launch-template-tagged
- fis-experiment-template-tagged
- ivs-channel-playback-authorization-enabled
- redshift-cluster-parameter-group-tagged
- ec2-traffic-mirror-filter-description
- appintegrations-event-integration-description
- athena-data-catalog-description
- fis-experiment-template-log-configuration-exists
- amplify-app-description
- amplify-branch-tagged
- batch-job-queue-enabled
- elasticbeanstalk-environment-description
- amplify-app-branch-auto-deletion-enabled
- appconfig-hosted-configuration-version-description
- appconfig-freeform-profile-config-storage
- datasync-task-data-verification-enabled

	• apprunner-service-observability-enabled • transfer-certificate-description • appconfig-deployment-strategy-replicate-to-ssm • transfer-workflow-tagged • transfer-connector-tagged • ec2-traffic-mirror-session-description • customerprofiles-object-type-allow-profile-creation • sagemaker-image-tagged	
Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new Amazon Simple Storage Service (Amazon S3) resource types. For more information, see Supported Resource Types.	February 6, 2025
Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new Amazon Simple Storage Service (Amazon S3) resource types. For more information, see Supported Resource Types.	January 29, 2025

Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Clean Rooms, Amazon Comprehend, Amazon Elastic Compute Cloud (Amazon EC2), Amazon HealthOmics, Amazon Simple Storage Service (Amazon S3), and Amazon Simple Email Service (Amazon SES). For more information, see Amazon managed policies for Amazon Config.	January 16, 2025

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • appmesh-mesh-deny-tcp-forwarding • sagemaker-model-isolation-enabled • evidently-project-description • alb-internal-scheme-check • evidently-segment-description • appconfig-environment-description • apprunner-service-in-vpc • sagemaker-domain-in-vpc • nlb-internal-scheme-check • emr-security-configuration-encryption-rest • apprunner-service-no-public-access • sagemaker-model-in-vpc • appconfig-deployment-strategy-description • evidently-launch-description • iot-authorizer-token-signing-enabled	January 9, 2025

Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new Amazon Elastic Compute Cloud (Amazon EC2) resource types. For more informati on, see Supported Resource Types.	January 9, 2025

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • batch-job-queue-tagged • iottwinmaker-sync-job-tagged • codeguruprofiler-profiling-group-tagged • ivs-recording-configuration-tagged • iottwinmaker-entity-tagged • iottwinmaker-workspace-tagged • iottwinmaker-scene-tagged • acmpca-certificate-authority-tagged • appflow-flow-tagged • iotevents-detector-model-tagged • appmesh-virtual-node-logging-file-path-exists • apprunner-vpc-connector-tagged • apprunner-service-tagged • iotwireless-fuota-task-tagged • appmesh-virtual-node-backend-defaults-tls-on • codegurureviewer-repository-association-tagged • iotevents-input-tagged	January 8, 2025

- appmesh-virtual-gateway-logging-file-path-exists
- batch-compute-environment-tagged
- batch-scheduling-policy-tagged
- customerprofiles-object-type-tagged
- emr-security-configuration-encryption-transit
- iotwireless-service-profile-tagged
- ivs-playback-key-pair-tagged
- cassandra-keyspace-tagged
- iotevents-alarm-model-tagged
- appconfig-application-description
- appmesh-virtual-gateway-backend-defaults-tls
- ivs-channel-tagged
- iotwireless-multicast-group-tagged

Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new Amazon Elastic Compute Cloud (Amazon EC2), Amazon Cognito, AWS Elemental MediaConnect, and Amazon OpenSearch Service resource types. For more informati on, see Supported Resource Types.	December 19, 2024
Security IAM update	The `AWSConfigServiceRo lePolicy` policy now grants additional permissio ns for Amazon Organizations. For more information, see Amazon managed policies for Amazon Config.	December 18, 2024
Amazon Config supports service-linked configuration recorders	With this release, Amazon Config supports service-l inked configuration recorders . You enable a service-linked configuration recorder in the supported service or using the Amazon CLI, and the recorder records the resource types needed for the linked service on your behalf. You can view details of a service-linked configuration recorder using the Amazon Config console or Amazon CLI. For more information, see Working with the configuration recorder.	November 27, 2024

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • appconfig-application-tagged • appconfig-configuration-profile-tagged • appconfig-environment-tagged • appconfig-extension-association-tagged • appmesh-gateway-route-tagged • appmesh-mesh-tagged • appmesh-route-tagged • appmesh-virtual-gateway-tagged • appmesh-virtual-node-tagged • appmesh-virtual-router-tagged • appmesh-virtual-service-tagged • evidently-launch-tagged • evidently-project-tagged • evidently-segment-tagged • frauddetector-entity-type-tagged • frauddetector-label-tagged • frauddetector-outcome-tagged	November 12, 2024

- frauddetector-variable-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged

Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon AppConfig, Amazon CloudTrail, Amazon Connect, Amazon DataZone, Amazon DevOps Guru, Amazon Glue, Identity Store, Amazon IoT, Amazon IoT FleetWise, Amazon IoT Wireless, Amazon Interactive Video Service (Amazon IVS), Amazon CloudWatch Logs, Amazon CloudWatch Observability Access Manager, Amazon Payment Cryptography, Amazon Relational Database Service (Amazon RDS), Amazon Rekognition, Amazon Simple Storage Service (Amazon S3), Amazon EventBridge Scheduler, Amazon Systems Manager, and Amazon VPC Lattice. For more information, see Amazon managed policies for Amazon Config.	November 8, 2024
Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rule: cognito-user-pool-advanced-security-enabled	November 6, 2024

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • active-mq-supported-version • rabbit-mq-supported-version • ec2-vpn-connection-logging-enabled • appsync-cache-ct-encryption-at-rest • appsync-cache-ct-encryption-in-transit • vpc-endpoint-enabled • efs-filesystem-ct-encrypted • redshift-cluster-subnet-group-multi-az • sns-topic-no-public-access • rabbit-mq-supported-version • kms-key-policy-no-public-access • rds-mysql-instance-encrypted-in-transit • rds-postgres-instance-encrypted-in-transit • rds-sql-server-logs-to-cloudwatch • ec2-launch-template-imdsv2-check	October 21, 2024

Amazon Config supports new conformance packs	With this release, Amazon Config supports the following conformance packs: • Operational Best Practices for PCI DSS 4.0 (Excluding global resource types) • Operational Best Practices for PCI DSS 4.0 (Including global resource types)	September 23, 2024
Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon OpenSearch Service Severless, Amazon AppStream, Amazon Backup, Amazon CloudTrail, Amazon Glue, EC2 Image Builder, Amazon IoT, Amazon Interactive Video Service (Amazon IVS), AWS Elemental MediaConnect, AWS Elemental MediaTailor, Amazon HealthOmics, and Amazon EventBridge Scheduler. For more information, see Amazon managed policies for Amazon Config.	September 16, 2024

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • ec2-resources-in-logically-air-gapped-vault • ebs-resources-in-logically-air-gapped-vault • aurora-resources-in-logically-air-gapped-vault • efs-resources-in-logically-air-gapped-vault • s3-resources-in-logically-air-gapped-vault • storagegateway-resources-in-logically-air-gapped-vault • virtualmachine-resources-in-logically-air-gapped-vault	September 3, 2024
Amazon Config supports new conformance packs	With this release, Amazon Config supports the following conformance packs: • Operational Best Practices for FedRAMP (High Part 1) • Operational Best Practices for FedRAMP (High Part 2)	August 27, 2024

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • athena-workgroup-logging-enabled • codebuild-report-group-encrypted-at-rest • cognito-user-pool-advanced-security-enabled • datasync-task-logging-enabled • efs-automatic-backups-enabled • glue-job-logging-enabled • glue-ml-transform-encrypted-at-rest • kinesis-stream-backup-retention-check • rds-aurora-postgresql-logs-to-cloudwatch • rds-postgresql-logs-to-cloudwatch • workspaces-root-volume-encryption-enabled • workspaces-user-volume-encryption-enabled	July 22, 2024

Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Elastic File System (Amazon EFS), Amazon Redshift and Amazon Systems Manager for SAP. For more information, see Amazon managed policies for Amazon Config.	June 17, 2024
Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • cloudtrail-s3-bucket-public-access-prohibited • cloudtrail-s3-bucket-access-logging	May 8, 2024
Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rule: iam-external-access-analyzer-enabled	May 2, 2024

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • guardduty-malware-protection-enabled • guardduty-rds-protection-enabled • guardduty-s3-protection-enabled • inspector-lambda-standard-scan-enabled	April 26, 2024
Amazon Config simplifies usage analysis with Amazon CloudWatch	With this release, the Amazon CloudWatch metrics for monitoring Amazon Config data usage will display only billable usage. This means, non-billable usage will no longer be displayed in both the Amazon CloudWatch metrics emitted to Amazon Config and the Amazon Config console. This allows you to validate Amazon Config setup and usage using Amazon CloudWatch metrics and correlate billable usage with associated costs. For more information, see Amazon Config Usage and Success Metrics.	April 26, 2024

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rule: iam-server-certificate-expiration-check	April 23, 2024
Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • vpc-sg-port-restriction-check • cloudtrail-all-write-s3-data-event-check • cloudtrail-all-read-s3-data-event-check	April 17, 2024
Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • guardduty-eks-protection-audit-enabled • guardduty-eks-protection-runtime-enabled • guardduty-lambda-protection-enabled • inspector-ec2-scan-enabled • inspector-ecr-scan-enabled • inspector-lambda-code-scan-enabled • redshift-unrestricted-port-access	April 16, 2024

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rule: efs-mount-target-public-accessible	March 20, 2024
Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • dms-neptune-iam-authorization-enabled • dms-mongo-db-authentication-enabled • dms-redis-tls-enabled • dax-tls-endpoint-encryption • eks-cluster-secrets-encrypted • kinesis-firehose-delivery-stream-encrypted • mq-cloudwatch-audit-log-enabled • mq-cloudwatch-audit-log-enabled • opensearch-primary-node-fault-tolerance • sagemaker-endpoint-config-prod-instance-count • service-catalog-shared-within-organization • transfer-family-server-no-ftp	February 26, 2024

Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Managed Service for Prometheus, Amazon CloudWatch, Amazon Cognito, Amazon ElastiCache, Amazon FSx, Amazon Glue, Amazon Identity and Access Management (IAM), Amazon Lambda, Amazon RAM, Amazon Redshift Serverless, Amazon SageMaker AI, and Amazon Simple Notification Service (Amazon SNS). For more information, see Amazon managed policies for Amazon Config.	February 22, 2024
Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rule: s3-bucket-cross-region-replication-enabled	February 12, 2024

Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new Amazon AppConfig, Amazon CloudWatch Evidently, Amazon Identity and Access Management (IAM), Amazon MemoryDB (MemoryDB), Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Redshift, and Amazon Transfer Family resource types. For more information, see Supported Resource Types.	February 6, 2024
Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rule: macie-auto-sensitive-data-discovery-check	January 29, 2024

Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new Amazon AppStream, Amazon Key Managemen t Service (Amazon KMS), Amazon Relational Database Service (Amazon RDS), Amazon Cognito, Amazon Elastic Compute Cloud (Amazon EC2), EC2 Image Builder, Amazon Ground Station, Amazon Mainframe Modernization, Amazon QuickSight, Amazon Redshift, and Amazon Systems Manager resource types. For more information, see Supported Resource Types.	January 3, 2024

Service limits increase for the maximum number of Amazon Config Rules per Region per account	With this release, Amazon Config supports 1000 Amazon Config rules per Amazon Region per account. This increase applies to the total of all deployed rules including Amazon Config managed rules, Amazon Config custom rules, Amazon Config conformance packs, Amazon Security Hub controls, Amazon Firewall Manager policies, and Amazon Backup backup plans per Region per account. For more information, see Service Limits.	December 19, 2023

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • s3-meets-restore-time-target • ebs-meets-restore-time-target • ec2-meets-restore-time-target • rds-meets-restore-time-target • efs-meets-restore-time-target • fsx-meets-restore-time-target • aurora-meets-restore-time-target • dynamodb-meets-restore-time-target	December 19, 2023

Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon AppConfig, Amazon Managed Service for Prometheus, Amazon Database Migration Service (Amazon DMS), (Amazon Identity and Access Management) IAM, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon CloudWatch Logs, Amazon Organizations, and Amazon Simple Storage Service (Amazon S3). For more information, see Amazon managed policies for Amazon Config.	December 5, 2023

Preview release: Natural language query processor for advanced queries	With this release, you can use the natural language query processor for advanced queries, which uses generative artificial intelligence (generative AI) capabilities that allow you to ask questions in plain English and convert them into a ready-to-use query format. With the natural language query processor, you can query your Amazon Web Services account or across an Amazon organization. For more information, see Natural language query processor for advanced queries.	November 26, 2023

Periodic recording	With this release, Amazon Config supports periodic recording. Periodic recording provides you with the ability to capture the latest configuration changes for your resources over a fixed period of time. You can now set the default frequency for the configuration recorder to Daily, allowing you to receive a configuration item (CI) representing the most recent state of your resources over the last 24-hour period, only if it's different from the previous CI recorded. The Amazon Config console also introduces a new recording strategy experience, where you can also override the recording frequency for specific resource types or exclude specific resource types from recording. This can help make your settings fit your granular requirements. The following data types are added: • RecordingMode • RecordingModeOverride The following data types are updated:	November 26, 2023

- PutConfigurationRecorder
- ConfigurationRecorder
- BaseConfigurationItem
- ConfigurationItem

The following pages in the developer guide are updated:

- Recoding Amazon Resources
- Setting up Amazon Config with the Amazon Config Console | 1-click setup
- Setting up Amazon Config with the Amazon Config Console | Manual setup
- Setting up Amazon Config with the Amazon CLI

Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Cognito, Amazon Connect, Amazon EMR, Amazon Ground Station, Amazon Mainframe Modernization, Amazon MemoryDB, Amazon Organizations, Amazon QuickSight, Amazon Relational Database Service (Amazon RDS), Amazon Redshift, Amazon Route 53, Amazon Service Catalog, and Amazon Transfer Family. The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy also now add security identifiers (SID) for `AWSConfigServiceRolePolicyStatementID`, `AWSConfigSLRLogStatementID`, `AWSConfigSLRLogEventStatementID`, `AWSConfigSLRApiGatewayStatementID`, and `AWSConfigServiceRolePolicy` policy.	November 17, 2023

	For more information, see Amazon managed policies for Amazon Config.	
Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • acm-pca-root-ca-disabled • dynamodb-table-deletion-protection-enabled • ec2-client-vpn-connection-log-enabled • eks-cluster-log-enabled • emr-block-public-access • fsx-windows-audit-log-configured • fsx-openzfs-copy-tags-enabled • fsx-lustre-copy-tags-to-backups • msk-enhanced-monitoring-enabled • mq-auto-minor-version-upgrade-enabled • neptune-cluster-multi-az-enabled • opensearch-update-check • s3-access-point-in-vpc-only • s3-access-point-public-access-blocks • s3-bucket-mfa-delete-enabled	November 9, 2023

Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new Amazon Identity and Access Management (IAM), Amazon Network Manager, Amazon Private Certificate Authority (Amazon Private CA), Amazon App Mesh, Amazon Connect, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Service (Amazon ECS), Amazon IoT, Amazon IoT TwinMaker, Amazon Managed Streaming for Apache Kafka Connect (Amazon MSK Connect), Amazon Lambda, and Amazon Resource Explorer resource types. For more information, see Supported Resource Types.	November 3, 2023
Amazon Config supports new conformance packs	With this release, Amazon Config updates the following conformance pack: Operational Best Practices for BNM RMiT	October 26, 2023

Compliance and Inventory Dashboards for Aggregators	With this release, Amazon Config adds a compliance dashboard page and an inventory dashboard page to the aggregated view in the Amazon Config console. For the compliance dashboard page, you can view automated dashboards with widgets that summarize insights on resource compliance within your aggregator, such as Top 10 resource types by noncompliant resources, Top 10 account level conformance packs by noncompliant rules, and more. For the inventory dashboard page, you can view automated dashboard with widgets that summarize insights on resource configuration data within your aggregator, such as Top 10 resource types by resource count, Top 10 accounts by resource count, and more. For information on the graph and charts, see Compliance dashboard and Inventory dashboard.	October 23, 2023

Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Private CA, Amazon App Mesh, Amazon Connect, Amazon Elastic Container Service (Amazon ECS), Amazon CloudWatch Evidently, Amazon Managed Grafana, Amazon GuardDuty , Amazon Inspector, Amazon IoT, Amazon IoT TwinMaker, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Lambda, Amazon Network Manager, Amazon Organizations, and Amazon SageMaker AI. For more information, see Amazon managed policies for Amazon Config.	October 4, 2023

Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new Amazon IoT, Amazon IoT TwinMaker, Amazon IoT Wireless, Amazon Personalize Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon SageMaker AI, Amazon CodeBuild, Amazon AppStream, and Amazon Inspector resource types. For more information, see Supported Resource Types.	October 4, 2023

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • docdb-cluster-deletion-protection-enabled • docdb-cluster-audit-logging-enabled • docdb-cluster-snapshot-public-prohibited • mq-active-deployment-mode • mq-rabbit-deployment-mode • dms-auto-minor-version-upgrade-check • dms-replication-task-target db-logging • dms-replication-task-source db-logging • dms-endpoint-ssl-configured • custom-eventbus-policy-attached • global-endpoint-event-replication-enabled • route53-query-logging-enabled • rds-aurora-mysql-audit-logging-enabled • rds-cluster-auto-minor-version-upgrade-enable • appsync-authorization-check	September 21, 2023

	• netfw-deletion-protection-enabled • wafv2-rulegroup-logging-enabled • msk-in-cluster-node-require-tls	
Amazon Config supports new conformance packs	With this release, Amazon Config updates the following conformance packs: • Operational Best Practices for Amazon S3 • Operational Best Practices for EC2	September 8, 2023
Security IAM update	The `AWSConfigServiceRolePolicy` policy now removes permissions for Amazon Systems Manager (Systems Manager). For more information, see Amazon managed policies for Amazon Config.	September 6, 2023

Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new Amazon CodeGuru Profiler, AWS Elemental MediaConnect, Amazon Transfer Family, Amazon Managed Service for Prometheus, Amazon Batch, Amazon Cloud Map, and Amazon Route 53 Resolver resource types. For more information, see Supported Resource Types.	September 6, 2023

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • athena-workgroup-encrypted-at-rest • neptune-cluster-iam-database-authentication • neptune-cluster-copy-tags-to-snapshot-enabled • neptune-cluster-cloudwatch-log-export-enabled • neptune-cluster-deletion-protection-enabled • neptune-cluster-snapshot-encrypted • neptune-cluster-backup-retention-check • neptune-cluster-encrypted • neptune-cluster-snapshot-public-prohibited • docdb-cluster-backup-retention-check • docdb-cluster-encrypted • rds-cluster-encrypted-at-rest	August 10, 2023

Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new Amazon Amplify, Amazon AppIntegrations, Amazon App Mesh, Amazon Athena, Amazon Elastic Compute Cloud (Amazon EC2), Amazon CloudWatch Evidently, Amazon Forecast, Amazon IoT Greengrass Version 2, Amazon Ground Station, AWS Elemental MediaConvert, AWS Elemental MediaTailor, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Personali ze, Amazon Pinpoint, and Amazon Resilience Hub resource types. For more information, see Supported Resource Types.	August 3, 2023

Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Managed Workflows for Amazon App Mesh, Amazon AppStream 2.0, Amazon CloudFormation, Amazon CloudFront Amazon CodeArtifact, Amazon CodeBuild, Amazon Connect, Amazon Glue, Amazon GuardDuty, Amazon Identity and Access Management (IAM), Amazon Inspector, Amazon IoT, Amazon IoT TwinMaker, Amazon IoT Wireless, Amazon Managed Streaming for Apache Kafka, Amazon Macie, AWS Elemental MediaConnect, Amazon Network Manager, Amazon Organizations, Amazon Resource Explorer, Amazon Route 53, Amazon Simple Storage Service (Amazon S3), Amazon Simple Notification Service (Amazon SNS), and Amazon EC2 Systems Manager (SSM). For more information, see Amazon managed policies for Amazon Config.	July 28, 2023

Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new Amazon Kinesis, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Pinpoint, Amazon Simple Storage Service (Amazon S3), Amazon Virtual Private Cloud (Amazon VPC), Amazon Kendra, Amazon Connect, Amazon CloudFormation, Amazon AppConfig, Amazon App Mesh, Amazon App Runner, and Amazon Database Migration Service (Amazon DMS) resource types. For more information, see Supported Resource Types.	July 10, 2023
Service limits increase for organization conformance packs	With this release, Amazon Config supports 350 Amazon Config rules per region per account across all conformance packs and 350 organizational Amazon Config rules per organization. For more information, see Service Limits.	June 13, 2023

Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Managed Workflows for Amazon Amplify, Amazon Connect, Amazon App Mesh, Amazon Managed Service for Prometheus, Amazon Athena, Amazon Batch, Amazon CloudFormation, Amazon CloudTrail, Amazon CodeArtifact, Amazon CodeGuru, Amazon Directory Service, Amazon DynamoDB, Amazon Elastic Compute Cloud (Amazon EC2), Amazon CloudWatch Evidently, Amazon Forecast, Amazon Organizations, Amazon IoT Greengrass, Amazon Ground Station, Amazon Identity and Access Management (IAM), Amazon Managed Streaming for Apache Kafka(Amazon MSK), Amazon Lightsail, Amazon CloudWatch Logs, AWS Elemental MediaConnect, AWS Elemental MediaTailor, Amazon Pinpoint, Amazon Virtual Private Cloud (Amazon VPC), Amazon Personalize, Amazon QuickSight, Amazon Migration Hub Refactor Spaces, Amazon Simple	June 13, 2023

Storage Service (Amazon S3), Amazon SageMaker AI, and Amazon Transfer Family. For more information, see Amazon managed policies for Amazon Config.

Amazon Config Recording Exclusions by Resource Type	With this release, Amazon Config allows you to exclude specific types of Amazon resources from inventory tracking and compliance monitoring while still tracking all other supported resource types currently available in Amazon Config, including those that will be added in the future. You can use this feature to concentrate on critical resources that are subject to your compliance and governance standards. The updates to the API for the configuration recorder and recording group are backward compatible, meaning that they work with previous versions of the PutConfigurationRecorder API. You can continue to manage which resource types are recorded in the exact same way as before without using the updated or new APIs. The following data types are added: • RecordingStrategy • ExclusionByResourceTypes The following data types are updated:	June 9, 2023

	• PutConfigurationRecorder • ConfigurationRecorder • RecordingGroup The following page in the developer guide is updated: • Selecting Which Resources are Recorded	
Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new Amazon Elastic Container Service (Amazon ECS), Amazon Keyspaces (for Apache Cassandra) (Amazon Keyspaces), Amazon Signer, Amazon Amplify, Amazon App Mesh, Amazon App Runner, Amazon AppStream 2.0, Amazon CodeArtifact, Amazon Elastic Compute Cloud (Amazon EC2), Amazon CloudWatch Evidently, Amazon Forecast, Amazon Identity and Access Management (IAM), Amazon Pinpoint, Amazon SageMaker AI, Amazon Transfer Family, Amazon Data Firehose resource types. For more information, see Supported Resource Types.	June 5, 2023

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • cloudfront-s3-origin-access-control-enabled • custom-schema-registry-policy-attached • ec2-client-vpn-not-authorize-all • elasticache-supported-engine-version • macie-status-check • mq-automatic-minor-version-upgrade-enabled • mq-cloudwatch-audit-logging-enabled • netfw-logging-enabled • opensearch-encrypted-at-res • step-functions-state-machine-logging-enabled	May 10, 2023

Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new Amazon Route 53 Resolver, Amazon Elastic Compute Cloud (Amazon EC2), Amazon IoT Wireless, Amazon Network Manager, Amazon Device Farm, Amazon Ground Station, Amazon AppFlow, Amazon Redshift, Amazon Pinpoint, Amazon IoT, Amazon AppConfig, EC2 Image Builder, Amazon CloudWatch, Amazon Panorama, Amazon SageMaker Runtime, Amazon ECR, and Amazon Audit Manager resource types. For more information, see Supported Resource Types.	May 5, 2023
Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to `AWS::NetworkFirewall::TLSInspectionConfiguration` . For more information, see Supported Resource Types.	May 1, 2023

Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Managed Workflows for Amazon Amplify, Amazon App Mesh, Amazon App Runner, Amazon CloudFront, Amazon CodeArtifact, Amazon Elastic Compute Cloud, Amazon Kendra, Amazon Macie, Amazon Route 53, Amazon SageMaker AI, Amazon Transfer Family, Amazon Pinpoint, Amazon Migration Hub, Amazon Resilience Hub, Amazon CloudWatch, Amazon Directory Service, and Amazon WAF. For more information, see Amazon managed policies for Amazon Config.	April 13, 2023

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • elasticache-auto-minor-version-upgrade-check • elasticache-repl-grp-auto-failover-enabled • elasticache-repl-grp-encrypted-at-rest • elasticache-repl-grp-encrypted-in-transit • elasticache-repl-grp-redis-auth-enabled • elasticache-subnet-group-check • cloudfront-s3-origin-non-existent-bucket	April 10, 2023
Service limits increase for organization conformance packs	With this release, Amazon Config supports 350 Amazon Config rules per account across all organization conformance packs. For more information, see Service Limits.	April 3, 2023

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • acm-certificate-rsa-check • appsync-associated-with-waf • appsync-logging-enabled • elasticache-rbac-auth-enabled • mq-no-public-access • netfw-multi-az-enabled • ses-malware-scanning-enabled • eks-cluster-logging-enabled • appsync-cache-encryption-at-rest	April 3, 2023

Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new Amazon AppStream 2.0, Amazon Auto Scaling, Amazon Connect Amazon Elastic Compute Cloud, Amazon EventBridge, HealthLak e, Kinesis video stream, Amazon IoT TwinMaker, Lookout for Vision, Network Manager, Amazon Pinpoint, Amazon Application Recovery Controller (ARC), and Amazon RoboMaker resource types. For more information, see Supported Resource Types.	April 3, 2023

Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Managed Workflows for Amazon AppFlow, Amazon App Runner, Amazon AppStream 2.0, Amazon CloudFormation, Amazon CloudFront, Amazon CloudWatch, Amazon CodeArtifact, Amazon CodeCommit, Amazon Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon CloudWatch Evidently, Amazon Forecast, Amazon Ground Station, Amazon Identity and Access Management (IAM), Amazon IoT, Amazon MemoryDB, Amazon Pinpoint, Amazon Network Manager, Amazon Panorama, Amazon Relational Database Service (Amazon RDS), Amazon Redshift, and Amazon SageMaker AI. For more information, see Amazon managed policies for Amazon Config.	March 30, 2023

Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Audit Manager. For more information, see Amazon managed policies for Amazon Config.	March 3, 2023
Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new AWS Elemental MediaPackage, Amazon EventBridge, Amazon IoT, (Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Amazon Lookout for Metrics, Amazon Lex, Amazon Budgets, Amazon Device Farm, Amazon CodeGuru Reviewer, Amazon Route 53 Resolver, and Amazon RoboMaker resource types. For more information, see Supported Resource Types.	March 2, 2023
Security IAM update	Amazon Config now tracks changes to the `AWSConfigMultiAccountSetupPolicy` policy. For more information, see Amazon managed policies for Amazon Config.	February 27, 2023

Amazon Config Resource Coverage by Region Availability	With this release, Amazon Config provides Region information for each supported resource type. For information on which resource types are supported in which Regions, see Resource Coverage by Region Availability.	February 20, 2023
Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new Amazon Interactive Video Service (Amazon IVS), Amazon Simple Storage Service (Amazon S3), Amazon Glue, Amazon Elastic Kubernetes Service (Amazon EKS), Amazon IoT, Amazon Relational Database Service (Amazon RDS), and Managed Service for Apache Flink resource types. For more information, see Supported Resource Types.	February 7, 2023

Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Managed Workflows for Apache Airflow, Amazon IoT, Amazon AppStream 2.0, Amazon CodeGuru Reviewer, Amazon HealthLake, Amazon Kinesis Video Streams, Amazon Application Recovery Controller (ARC), Amazon Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Pinpoint, Amazon Identity and Access Management (IAM), Amazon GuardDuty, and Amazon CloudWatch Logs. For more information, see Amazon managed policies for Amazon Config.	February 1, 2023
Security IAM update	As a security best practice, the `ConfigConformsServiceRolePolicy` policy now removes broad resource-level permission for `config:DescribeConfigRules` . For more information, see Amazon managed policies for Amazon Config.	January 12, 2023

Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Managed Service for Prometheus, Amazon Audit Manager, Amazon Device Farm, Amazon Database Migration Service (Amazon DMS), Amazon Directory Service, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Glue, Amazon IoT, Amazon Lightsail, AWS Elemental MediaPackage, Amazon Network Manager, Amazon QuickSight, Amazon Resource Access Manager, Amazon Application Recovery Controller (ARC), Amazon Simple Storage Service (Amazon S3), and Amazon Timestream. For more information, see Amazon managed policies for Amazon Config.	January 10, 2023

Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new Amazon MQ, Amazon AppConfig, Amazon Cloud9, Amazon EventBridge schemas, Amazon Fraud Detector, Amazon IoT, Amazon IoT Analytics, Amazon Lightsail , AWS Elemental MediaPack age (MediaPackage), Amazon Application Recovery Controller (ARC), Amazon Resilience Hub, and Amazon Transfer Family resource types. For more informati on, see Supported Resource Types.	January 5, 2023
Amazon Config rule resource coverage	With this release, Amazon Config displays the resource type coverage for an increased number of Amazon Config managed rules.	December 21, 2022
Amazon Config rule discovera bility	With this release, Amazon Config supports pages for List of Amazon Config Managed Rules by Evaluation Mode, List of Amazon Config Managed Rules by Trigger Type, and List of Amazon Config Managed Rules by Region Availability.	December 21, 2022

Amazon Config supports new conformance packs	With this release, Amazon Config updates the following conformance packs: • Operational Best Practices for K-ISMS • Operational Best Practices for NIST 800 171 • Operational Best Practices for PCI DSS 3.2.1 • Operational Best Practices for Esquema Nacional de Seguridad (ENS) High • Operational Best Practices for Esquema Nacional de Seguridad (ENS) Medium • Operational Best Practices for Esquema Nacional de Seguridad (ENS) Low • Operational Best Practices for NZISM • Operational Best Practices for NIST 800-53 rev 5	December 19, 2022

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • api-gwv2-access-logs-enabled • api-gwv2-authorization-type-configured • cloudfront-security-policy-check • ec2-launch-template-public-ip-disabled • elastic-beanstalk-logs-to-cloudwatch • sagemaker-notebook-instance-inside-vpc • sagemaker-notebook-instance-root-access-check • security-account-information-provided • storagegateway-resources-protected-by-backup-plan • wafv2-rulegroup-not-empty • wafv2-webacl-not-empty	December 9, 2022

Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new Amazon CloudWatch RUM, Amazon EventBridge, Amazon GuardDuty, Amazon Simple Email Service (Amazon SES), Amazon Backup, Amazon DataSync, and Amazon Fault Injection Service (Amazon FIS) resource types. For more information, see Supported Resource Types.	December 9, 2022

Amazon Config Proactive Compliance	With this release, Amazon Config supports the ability to proactively check for compliance with Amazon Config rules before resource provisioning. This allows you to evaluate the configuration settings of your resources before they are created or updated. Use Amazon Config to track the configuration changes made to your resources, either pre-provisioning or post-provisioning, and check if your resources match your desired configurations. The following data types are added: • GetResourceEvaluationSummary • StartResourceEvaluation • ListResourceEvaluations The following data types are updated: • DescribeConfigRulesFilters • GetComplianceDetailsByResource • EvaluationResultQualifier • EvaluationModeConfiguration	November 28, 2022

The following pages in the developer guide are updated:

- Components of an Amazon Config Rule
- Evaluation Mode and Trigger Types for Amazon Config Rules
- Amazon Config Managed Rules
- Amazon Config Custom Rules
- Managing Your Amazon Config Rules

Drift Detection as Configuration Item (CI) for the Amazon Config Configuration Recorder	With this release, Amazon Config tracks all changes to the configuration recorder to indicate if the state of the configuration recorder differs, or has *drifted*, from its previous state; for example, if there are updates to resource types that you have enabled Amazon Config to track, if you have stopped or started the configuration recorder, or if you have deleted or uninstalled the configuration recorder. The `AWS::Config::ConfigurationRecorder` resource type is a system resource type of Amazon Config and recording of this resource type is enabled by default in all supported Regions. Recording for the `AWS::Config::ConfigurationRecorder` resource type comes with no additional charge. For more information, see Drift Detection for the Configuration Recorder.	November 18, 2022

Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new Amazon IoT Events, Amazon Cloud Map, EC2 Image Builder, Amazon DataSync, Amazon Glue, Amazon Application Recovery Controller (ARC), and Amazon Elastic Container Registry (Amazon ECR) resource types. For more information, see Supported Resource Types.	November 8, 2022
Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon CloudFormation. For more information, see Amazon managed policies for Amazon Config.	November 7, 2022

Amazon Config supports new conformance packs	With this release, Amazon Config supports the following conformance packs: • Operational Best Practices for Criminal Justice Information Services (CJIS) • Security Best Practices for Amazon SageMaker AI • Security Best Practices for Amazon Elastic Container Registry The following conformance packs are updated: • Operational Best Practices for MAS TRMG • Operational Best Practices for NCSC Cyber Assesment Framework • Operational Best Practices for NCSC Cloud Security Principles	October 27, 2022

Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Certificate Manager, Amazon Managed Workflows for Apache Airflow, Amazon Amplify, Amazon AppConfig , Amazon Keyspaces, Amazon CloudWatch, Amazon Connect, Amazon Glue DataBrew, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service (Amazon EKS), Amazon EventBridge, Amazon Fault Injection Service, Amazon Fraud Detector, Amazon FSx, Amazon GameLift Servers, Amazon Location Service, Amazon IoT, Amazon Lex, Amazon Lightsail, Amazon Pinpoint, Amazon OpsWorks, Amazon Panorama, Amazon Resource Access Manager, Amazon QuickSight, Amazon Relational Database Service (Amazon RDS), Amazon Rekognition, Amazon RoboMaker, Amazon Resource Groups, Amazon Route 53, Amazon Simple Storage Service (Amazon S3), Amazon Cloud Map, and Amazon	October 19, 2022

	Security Token Service. For more information, see Amazon managed policies for Amazon Config.	
Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Email Service (Amazon SES), Amazon AppConfig , Amazon Cloud Map, and Amazon DataSync resource types. For more informati on, see Supported Resource Types.	October 6, 2022
Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new Amazon GuardDuty , Amazon SageMaker AI, Amazon AppSync, Amazon Cloud Map, and Amazon DataSync resource types. For more information, see Supported Resource Types.	October 4, 2022
Amazon Config supports new conformance pack	With this release, Amazon Config updates the Operation al Best Practices for SWIFT CSP conformance pack.	October 4, 2022

Amazon Config supports new conformance packs	With this release, Amazon Config supports the following conformance packs: • Operational Best Practices for CMMC 2.0 Level 1 • Operational Best Practices for CMMC 2.0 Level 2 The following conformance packs are updated: • Operational Best Practices for Amazon API Gateway • Operational Best Practices for Amazon Well-Architected Framework Reliability Pillar • Operational Best Practices for Amazon Well-Architected Framework Security Pillar • Operational Best Practices for CMMC Level 1 • Operational Best Practices for CMMC Level 2 • Operational Best Practices for CMMC Level 3 • Operational Best Practices for CMMC Level 4 • Operational Best Practices for CMMC Level 5 • Operational Best Practices for FFIEC	September 30, 2022

	• Operational Best Practices for FedRAMP(Low) • Operational Best Practices for MAS Notice 655 • Operational Best Practices for NBC TRMG • Operational Best Practices for NIST 800 172	
Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Glue. For more information, see Amazon managed policies for Amazon Config.	September 14, 2022
Amazon Config supports new conformance pack	With this release, Amazon Config supports the Operational Best Practices for SWIFT CSP conformance pack.	September 9, 2022

Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon AppFlow, Amazon CloudWatch, Amazon CloudWatch RUM, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon DevOps Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon EventBridge, Amazon EventBridge Schemas, Amazon FinSpace, Amazon Fraud Detector, Amazon GameLift Servers, Amazon Interactive Video Service (Amazon IVS), Amazon Managed Service for Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon QuickSight, Amazon Application Recovery Controller (ARC), Amazon Route 53	September 7, 2022

Resolver, Amazon Simple Storage Service (Amazon S3), Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream, Amazon AppConfig, Amazon AppSync, Amazon Auto Scaling, Amazon Backup, Amazon Budgets, Amazon Cost Explorer, Amazon Cloud9, Amazon Directory Service, Amazon DataSync, AWS Elemental MediaPack age, Amazon Glue, Amazon IoT, Amazon IoT Analytics, Amazon IoT Events, Amazon IoT SiteWise, Amazon IoT TwinMaker, Amazon Lake Formation, Amazon License Manager, Amazon Resilienc e Hub, Amazon Signer, and Amazon Transfer Family. For more information, see Amazon managed policies for Amazon Config.

Amazon Config supports new conformance packs	With this release, Amazon Config supports the following conformance packs: • Operational Best Practices for Amazon CloudWatch • Operational Best Practices for Germany Cloud Computing Compliance Controls Catalog (C5) • Operational Best Practices for IRS 1075 The following conformance packs are updated: • Amazon Control Tower Detective Guardrails Conformance Pack • Operational Best Practices for CISA Cyber Essentials • Operational Best Practices for ENISA Cybersecurity guide for SMEs • Operational Best Practices for FDA Title 21 CFR Part 11 • Operational Best Practices for FedRAMP(Moderate) • Operational Best Practices for HIPAA Security • Operational Best Practices for NIST Privacy Framework v1.0 • Operational Best Practices for NYDFS 23	August 31, 2022

	• Operational Best Practices for RBI Cyber Security Framework for UCBs • Operational Best Practices for RBI MD-ITF	
Getting Started with Amazon Config and Custom Conformance Pack updates	With this release, Amazon Config updates the Getting Started with Amazon Config and Setting Up Amazon Config with the Console pages, introducing a 1-click setup and Manual setup page. Amazon Config also updates the Custom Conformance Pack page with a walkthrough on how to create a conformance pack YAML file from scratch.	August 25, 2022

Amazon Systems Manager Document (SSM document) Integration with Conformance Packs	With this release, you can create a conformance pack template with an SSM document. For more informati on on SSM documents, see Amazon Systems Manager Documents in the Amazon Systems Manager User Guide. The following data types are updated: • PutConformancePack • ConformancePackDetail • TemplateSSMDocumen tDetails The following pages in the developer guide are updated: • Deploying a Conforman ce Pack Using the Amazon Config Console • Deploying a Conforman ce Pack Using the Amazon Command Line Interface	August 24, 2022

Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Simple Email Service (Amazon SES), Amazon DataSync, and Amazon Cloud Map. For more information, see Amazon managed policies for Amazon Config.	August 22, 2022
Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new Amazon Athena, Amazon Detective, Amazon SageMaker AI, Amazon Route 53, Amazon Database Migration Service (Amazon DMS), Amazon Glue, Amazon Key Management Service (Amazon KMS), and Amazon Simple Email Service (Amazon SES) resource types. For more information, see Supported Resource Types.	August 16, 2022

Amazon Config supports new conformance packs	With this release, Amazon Config updates the following conformance packs: • Operational Best Practices for NIST 1800 25 • Operational Best Practices for NIST 800 181 • Operational Best Practices for ABS CCIG 2.0 Standard Workloads • Operational Best Practices for ABS CCIG 2.0 Material Workloads • Operational Best Practices for ACSC Essential 8 • Operational Best Practices for ACSC ISM • Operational Best Practices for APRA CPG 234 • Operational Best Practices for CIS Amazon Foundations Benchmark v1.4 Level 1 • Operational Best Practices for CIS Amazon Foundations Benchmark v1.4 Level 2 • Operational Best Practices for BNM RMiT • Operational Best Practices for NIST CSF	August 1, 2022

Compliance score for conformance packs	With this release, Amazon Config introduces compliance score for conformance packs, which provides you with a high-level view of the compliance state of your conformance packs. You can use it to identify, investigate, and understand the level of compliance in your conformance packs. A compliance score is the percentage of the number of compliant rule-resource combinations in a conformance pack compared to the number of total possible rule-resource combinations in the conformance pack. The following data types are updated: • ListConformancePackComplianceScores • ConformancePackComplianceScore The following pages in the developer guide are updated: • Viewing the Amazon Config Dashboard • Viewing Compliance Data in the Conformance Packs Dashboard	July 26, 2022

	• Managing Conformance Packs (API)	
Security IAM update	The `ConfigConformsServiceRolePolicy` policy now grants permission to publish metric data points to Amazon CloudWatch. For more information, see Amazon managed policies for Amazon Config.	July 25, 2022

Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Elastic Container Service (Amazon ECS), Amazon ElastiCache, Amazon EventBridge, Amazon FSx, Amazon Managed Service for Apache Flink, Amazon Location Service, Amazon Managed Streaming for Apache Kafka, Amazon QuickSight, Amazon Rekognition, Amazon RoboMaker, Amazon Simple Storage Service (Amazon S3), Amazon Simple Email Service (Amazon SES), Amazon Amplify, Amazon AppConfig, Amazon AppSync, Amazon Billing Conductor, Amazon DataSync, Amazon Firewall Manager, Amazon Glue, Amazon IAM Identity Center (IAM Identity Center), EC2 Image Builder, and Elastic Load Balancing. For more information, see Amazon managed policies for Amazon Config.	July 15, 2022

Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new Amazon Elastic Compute Cloud (Amazon EC2) resource types. For more informati on, see Supported Resource Types.	July 8, 2022
Amazon Config supports new resources type	With this release, you can use Amazon Config to record configuration changes to new Amazon Global Accelerat or resource types. For more information, see Supported Resource Types.	July 5, 2022
Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • autoscaling-launch-template • ecs-task-definition-log-con figuration • ecs-awsvpc-networking-enabled	July 1, 2022

Amazon Config supports new conformance packs	With this release, Amazon Config supports the following conformance packs: • Operational Best Practices for Canadian Centre for Cyber Security (CCCS) Medium Cloud Control Profile • Operational Best Practices for Gramm Leach Bliley Act (GLBA) • Operational Best Practices for GxP EU Annex 11 • Security Best Practices for Amazon Elastic Kubernetes Service (Amazon EKS) • Security Best Practices for Amazon Relational Database Service (Amazon RDS) • Security Best Practices for Amazon Lambda The following conformance packs are updated: • Operational Best Practices for AI and ML • Operational Best Practices for Amazon DynamoDB • Operational Best Practices for CIS Critical Security Controls v8 IG1	June 30, 2022

	• Operational Best Practices for CIS Critical Security Controls v8 IG2 • Operational Best Practices for CIS Critical Security Controls v8 IG3 • Operational Best Practices for HIPAA Security • Operational Best Practices for NIST 800-53 rev 5 • Operational Best Practices for NIST CSF	
Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new Amazon SageMaker AI resource types. For more information, see Supported Resource Types.	June 29, 2022

Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Route 53, Amazon WorkSpaces, Amazon Batch, Amazon Identity and Access Management Access Analyzer (IAM Access Analyzer), Amazon Database Migration Service (Amazon DMS), Amazon Step Functions , and Elastic Load Balancing resource types. For more information, see Supported Resource Types.	June 14, 2022

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • aurora-last-backup-recovery-point-created • dynamodb-last-backup-recovery-point-created • ebs-last-backup-recovery-point-created • ec2-last-backup-recovery-point-created • efs-last-backup-recovery-point-created • fsx-last-backup-recovery-point-created • rds-last-backup-recovery-point-created • s3-last-backup-recovery-point-created • storagegateway-last-backup-recovery-point-created • virtualmachine-last-backup-recovery-point-created	June 13, 2022

Amazon Config Integration with Amazon Security Hub	With this release, you can see the results of Amazon Config managed and custom rule evaluations as findings in Amazon Security Hub. Security Hub transform s rule evaluations into findings, which provide more information about the impacted resources, such as the Amazon Resource Name (ARN) and creation date. These findings can be viewed alongside other Security Hub findings, providing a comprehensive overview of your security posture. For more information, see Sending Rule Evaluations to Security Hub	June 7, 2022

Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Athena, Amazon Detective, Amazon GuardDuty, Amazon Macie, Amazon Simple Email Service (Amazon SES), Amazon Glue, Amazon Resource Access Manager (Amazon RAM), and Amazon IAM Identity Center. For more information, see Amazon managed policies for Amazon Config.	May 31, 2022
Amazon Config supports new conformance packs	With this release, Amazon Config supports the following conformance packs: • Security Best Practices for Amazon Elastic Container Service (Amazon ECS) • Security Best Practices for Amazon Elastic File System (Amazon EFS) • Security Best Practices for Amazon CloudFront • Security Best Practices for Amazon Auto Scaling • Security Best Practices for Amazon Network Firewall • Security Best Practices for Amazon Secrets Manager	May 31, 2022

Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new Amazon SageMaker AI and Amazon Step Functions resource types. For more information, see Supported Resource Types.	May 26, 2022
Amazon Config supports new conformance pack	With this release, Amazon Config updates the Operational Best Practices for NERC CIP BCSI conformance pack.	May 20, 2022
Components of an Amazon Config Rule	With this release, Amazon Config introduces a Components of an Amazon Config Rule page. The page discusses the structure of rule definitions, rule metadata, and best practices on how to write rules with Python using the Amazon Config Rules Development Kit (RDK) and Amazon Config Rules Development Kit Library (RDKlib).	May 9, 2022
Service limits increase for organization conformance packs	With this release, Amazon Config supports 180 Amazon Config rules per account across all organization conformance packs. For more information, see Service Limits.	May 6, 2022

Amazon Config supports new conformance packs	With this release, Amazon Config supports the following conformance packs: • Security Best Practices for Amazon OpenSearch Service • Security Best Practices for Amazon Redshift • Security Best Practices for Amazon CloudTrail • Security Best Practices for Amazon CodeBuild • Security Best Practices for Amazon WAF	April 29, 2022
Amazon Config updates managed rule	With this release, Amazon Config supports the s3-resources-protected-by-backup-plan managed rule.	April 11, 2022

Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions to get information about all or a specified Amazon CloudTrail event data store (EDS), get information about all or a specified Amazon CloudFormation resource, get a list of a DynamoDB Accelerator (DAX) parameter group or subnet group, get information about Amazon Database Migration Service (Amazon DMS) replication tasks for your account in the current region being accessed, and get a list all policies in an Amazon Organizations of a specified type. For more information, see Amazon managed policies for Amazon Config.	April 7, 2022

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • alb-desync-mode-check • autoscaling-capacity-rebalancing • autoscaling-launchconfig-requires-imdsv2 • autoscaling-launch-config-hop-limit • autoscaling-multiple-instance-types • clb-desync-mode-check • ecs-container-insights-enabled • ecs-fargate-latest-platform-version • netfw-policy-default-action-fragment-packets • netfw-policy-default-action-full-packets • netfw-policy-rule-group-associated • redshift-audit-logging-enabled • s3-lifecycle-policy-check • waf-regional-rule-not-empty • waf-regional-rulegroup-not-empty • waf-regional-webacl-not-empty	April 4, 2022

- vpc-peering-dns-resolution-check

Amazon Config Custom Policy rules	With this release, Amazon Config allows you to create Amazon Config Custom Policy rules using Amazon CloudFormation Guard (guard). Guard is a policy-as-code language that allows you to write policies that are enforced by Amazon Config without the need to create Lambda functions to manage your custom rules. Rules written using Guard policy can be created from the Amazon Config console or by using the Amazon Config rule APIs. The following pages in the developer guide are updated: • Amazon Config Custom Rules • Creating Amazon Config Custom Rules with Guard The following data types are updated: • Source • CustomPolicyDetails • ConfigRuleEvaluationStatus • GetCustomRulePolicy • GetOrganizationCustomRulePolicy	April 4, 2022

	• OrganizationCustomPolicyRuleMetadata	
Amazon Config supports new resources type	With this release, you can use Amazon Config to record configuration changes to the new Amazon EMR SecurityConfiguration resource type. For more information, see Supported Resource Types.	March 31, 2022
Amazon Config updates managed rule	With this release, Amazon Config supports the virtualmachine-resources-protected-by-backup-plan managed rule.	March 29, 2022

Amazon Config Integration with Amazon CloudWatch Metrics	With this release, Amazon Config now supports tracking of your Amazon Config usage and success metrics with Amazon CloudWatch in the Amazon Config Dashboard page. CloudWatch metrics is a monitoring service which provides data about the performance of your systems, including the ability to search, graph, and build alarms on metrics about Amazon resources. From the Amazon Config Dashboard, you can see what traffic is driving your Amazon Config usage and key metrics for failures that have occured in your workflow. The following page is updated: • Viewing the Amazon Config Dashboard	March 29, 2022
Amazon Config supports new resources type	With this release, you can use Amazon Config to record configuration changes to new Amazon GuardDuty Detector resource type. For more information, see Supported Resource Types.	March 24, 2022

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • clb-multiple-az • cloudfront-no-deprecated-ssl-protocols • cloudfront-traffic-to-origin-encrypted • cloudwatch-alarm-action-enabled-check • ec2-no-amazon-key-pair • ec2-paravirtual-instance-check • ec2-token-hop-limit-check • ec2-transit-gateway-auto-vpc-attach-disabled • ecr-private-lifecycle-policy-configured • efs-access-point-enforce-root-directory • efs-access-point-enforce-user-identity • elbv2-multiple-az • kinesis-stream-encrypted • redshift-default-db-name-check • s3-event-notifications-enabled • sns-topic-message-delivery-notification-enabled	March 23, 2022

	• waf-global-rulegroup-not-empty • waf-global-rule-not-empty	
Amazon Config supports new conformance packs	With this release, Amazon Config updates the following conformance packs: • Operational Best Practices for CIS Critical Security Controls v8 IG1 • Operational Best Practices for CIS Critical Security Controls v8 IG2 • Operational Best Practices for CIS Critical Security Controls v8 IG3 • Operational Best Practices for Amazon Well-Arch itected Framework Security Pillar • Operational Best Practices for Esquema Nacional de Seguridad (ENS) Low • Operational Best Practices for Esquema Nacional de Seguridad (ENS) Medium • Operational Best Practices for Esquema Nacional de Seguridad (ENS) High • Operational Best Practices for MAS Notice 655 • Operational Best Practices for NIST 1800-25	March 16, 2022

Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon CloudFormation. For more information, see Amazon managed policies for Amazon Config.	March 14, 2022
Amazon Config updates managed rules	With this release, Amazon Config updates the following managed rules: • aurora-resources-protected-by-backup-plan • dynamodb-resources-protected-by-backup-plan • ebs-resources-protected-by-backup-plan • ec2-resources-protected-by-backup-plan • efs-resources-protected-by-backup-plan • fsx-resources-protected-by-backup-plan • rds-resources-protected-by-backup-plan	March 10, 2022

Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new Amazon Elastic Container Registry Public resource types. For more informati on, see Supported Resource Types.	March 4, 2022
Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new Amazon Elastic Compute Cloud resource types. For more information, see Supported Resource Types.	February 28, 2022
Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • codedeploy-auto-rollback-monitor-enabled • codedeploy-ec2-minimum-healthy-hosts-configured • codedeploy-lambda-allatonce-traffic-shift-disabled	February 25, 2022

Logging and Monitoring in Amazon Config Update	With this release, Amazon Config updates the Monitoring Amazon Config with Amazon EventBridge Events page to replace references to Amazon CloudWatch Events. Amazon EventBridge is the preferred way to manage your events. CloudWatch Events and EventBridge are the same underlying service and API, but EventBridge provides more features. Changes you make in either CloudWatch or EventBridge will appear in each console. For more informance, see Amazon EventBridge.	February 24, 2022
Amazon SDK Page for Amazon Config	With this release, Amazon Config introduces a Using Amazon Config with an Amazon SDK page. Amazon software development kits (SDKs) are available for many popular programming languages. Each SDK provides an API, code examples, and documentation that make it easier for developers to build applications in their preferred language.	February 24, 2022

Security IAM Role Trust policy update	With this release, Amazon Config updates the IAM trust policy statement to include security protections in the trust policy that restrict access with `sourceARN` and/or `sourceAccountId` for the Amazon Security Token Service (Amazon STS) operation. This helps make sure that the IAM role trust policy is accessing your resources on behalf of expected users and scenarios only. The following page is updated: • Adding an IAM Trust Policy to your Role	February 18, 2022

Changes to Global Resource Type Recording	Amazon Config now changes how new global resource types are recorded in Amazon Config Recording. Global resource types are Amazon resources that do not require you to specify a region at creation. Before this change, you could enable the recording of global resource types in all supported regions in Amazon Config. After this change, new global resource types onboarded to Amazon Config recording can only be recorded in the service's home region for the commercia l partition, and Amazon GovCloud (US-West) for the Amazon GovCloud (US) partition. You will now be able to view the configuration items for these new global resource types only in their home region and Amazon GovCloud (US-West). For a list of home regions for global resource types onboarded after February 2022, see the table on the Recording All Supported Resource Types page.	February 18, 2022

Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant permission to get details about Elastic Beanstalk environments and a description of the settings for the specified Elastic Beanstalk configuration set, get a map of OpenSearch or Elasticsearch versions, describe the available Amazon RDS option groups for a database, and get information about a CodeDeploy deployment configuration. This policy also now grants permission to retrieve the specified alternate contact attached to an Amazon Web Services account, retrieve information about an Amazon Organizations policy, retrieve an Amazon ECR repository policy, retrieve information about an archived Amazon Config rule, retrieve a list of Amazon ECS task definition families, list the root or parent organizational units (OUs) of the specified child OU or account, and list the policies that are attached to the specified target root, organizational unit, or account. For more information, see Amazon	February 10, 2022

managed policies for Amazon Config.

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • autoscaling-multiple-az • codebuild-project-artifact-encryption • codebuild-project-environment-privileged-check • codebuild-project-logging-enabled • codebuild-project-s3-logs-encrypted • ec2-security-group-attached-to-eni-periodic • ecr-private-image-scanning-enabled • ecr-private-tag-immutability-enabled • ecs-containers-nonprivileged • ecs-containers-readonly-access • ecs-no-environment-secrets • ecs-task-definition-memory-hard-limit • ecs-task-definition-nonroot-user • ecs-task-definition-pid-mode-check • eks-cluster-oldest-supported-version	February 10, 2022

	• eks-cluster-supported-version • lambda-vpc-multi-az-check • nacl-no-unrestricted-ssh-rdp • netfw-stateless-rule-group-not-empty • rds-cluster-default-admin-check • rds-db-security-group-not-allowed • rds-instance-default-admin-check • redshift-default-admin-check • s3-bucket-acl-prohibited • s3-version-lifecycle-policy-check • waf-global-webacl-not-empty	
Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant permission to create Amazon CloudWatch log groups and streams and to write logs to created log streams. For more information, see Amazon managed policies for Amazon Config.	February 2, 2022

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • opensearch-access-control-enabled • opensearch-audit-logging-enabled • opensearch-data-node-fault-tolerance • opensearch-encrypted-at-rest • opensearch-https-required • opensearch-in-vpc-only • opensearch-logs-to-cloudwatch • opensearch-node-to-node-encryption-check	January 31, 2022
Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to Amazon CodeDeploy resource types. For more informati on, see Supported Resource Types.	January 5, 2022
Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new Amazon SageMaker AI resource types. For more information, see Supported Resource Types.	December 20, 2021

Amazon Config supports new conformance packs	With this release, Amazon Config supports the following conformance packs: • Operational Best Practices for ENISA Cybersecurity guide for SMEs	December 20, 2021
Amazon Config supports new conformance packs	With this release, Amazon Config supports the following conformance packs: • Operational Best Practices for NIST 800 172 • Operational Best Practices for NIST 800 181 The following conformance pack is updated: • Operational Best Practices for K-ISMS	November 18, 2021

Amazon Config supports new conformance packs	With this release, Amazon Config supports the following conformance packs: • Operational Best Practices for Amazon API Gateway • Operational Best Practices for Amazon Backup • Operational Best Practices for CISA Cyber Essentials • Operational Best Practices for DevOps • Operational Best Practices for NIST Privacy Framework v1.0 The following conformance packs are updated: • Operational Best Practices for FedRAMP(Low) • Operational Best Practices for FedRAMP(Moderate)	October 29, 2021
Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new Amazon OpenSearch Service resource types. For more information, see Supported Resource Types.	October 12, 2021

Amazon Config supports new conformance packs	With this release, Amazon Config updates the following conformance pack: • Operational Best Practices for MAS TRMG	October 12, 2021

Amazon Config supports new conformance packs	With this release, Amazon Config updates the following conformance packs: • Operational Best Practices for ABS CCIG 2.0 Material Workloads • Operational Best Practices for ABS CCIG 2.0 Standard Workloads • Operational Best Practices for ACSC Essential 8 • Operational Best Practices for ACSC ISM • Operational Best Practices for BNM RMiT • Operational Best Practices for CMMC Level 1 • Operational Best Practices for CMMC Level 2 • Operational Best Practices for CMMC Level 3 • Operational Best Practices for CMMC Level 4 • Operational Best Practices for CMMC Level 5 • Operational Best Practices for FDA Title 21 CFR Part 11 • Operational Best Practices for FFIEC • Operational Best Practices for MAS Notice 655 • Operational Best Practices for NBC TRMG	September 30, 2021

	• Operational Best Practices for NERC CIP • Operational Best Practices for NIST 800-53 rev 5	
Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant permission to get details about an Amazon OpenSearch Service (OpenSearch Service) domain/domains and to get a detailed parameter list for a particular Amazon Relational Database Service (Amazon RDS) DB parameter group. This policy also grants permission to get details about Amazon ElastiCache snapshots. For more information, see Amazon managed policies for Amazon Config.	September 8, 2021
Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to new Amazon Elastic Compute Cloud resource types. For more information, see Supported Resource Types.	September 7, 2021

Amazon Config supports new conformance packs	With this release, Amazon Config updates the following conformance packs: • Operational Best Practices for APRA CPG 234 • Operational Best Practices for CIS Amazon Foundations Benchmark v1.4 Level 1 • Operational Best Practices for CIS Amazon Foundations Benchmark v1.4 Level 2 • Operational Best Practices for NCSC Cloud Security Principles • Operational Best Practices for NCSC Cyber Assesment Framework • Operational Best Practices for NIST 800 171 • Operational Best Practices for NIST CSF • Operational Best Practices for RBI Cyber Security Framework for UCBs • Operational Best Practices for RBI MD-ITF • Operational Best Practices for NYDFS 23 • Operational Best Practices for PCI DSS 3.2.1	August 30, 2021

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • aurora-resources-protected-by-backup-plan • backup-plan-min-frequency-and-min-retention-check • backup-recovery-point-encrypted • backup-recovery-point-manual-deletion-disabled • backup-recovery-point-minimum-retention-check • dynamodb-resources-protected-by-backup-plan • ebs-resources-protected-by-backup-plan • ec2-resources-protected-by-backup-plan • efs-resources-protected-by-backup-plan • fsx-resources-protected-by-backup-plan • rds-resources-protected-by-backup-plan	August 20, 2021
Amazon Config supports new conformance packs	With this release, Amazon Config supports the following conformance pack: • Operational Best Practices for NZISM	August 20, 2021

Security Amazon SNS policy update	With this release, Amazon Config updates the IAM policy statement for the Amazon SNS topic when using service-linked roles to include security protectio ns that restrict access with `sourceARN` and/or `sourceAccountId` in the topic policy. This helps make sure Amazon SNS is accessing your resources on behalf of expected users and scenarios only. The following page is updated: • Permissions for the Amazon SNS Topic	August 17, 2021

Security Amazon Lambda policy update	With this release, Amazon Config updates the Amazon Lambda resource-based policy for Amazon Config custom rules to include security protections that restrict access with `sourceARN` and/or `sourceAccountId` in the invoke request. This helps make sure Amazon Lambda is accessing your resources on behalf of expected users and scenarios only. The following pages are updated: • AWS::Config::ConfigRule • Developing a Custom Rule for Amazon Config	August 12, 2021
Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to Amazon Kinesis resource types. For more informati on, see Supported Resource Types.	August 6, 2021

Amazon Config supports new conformance packs	With this release, Amazon Config supports the following conformance pack: • Operational Best Practices for Esquema Nacional de Seguridad (ENS) High The following conformance packs are updated: • Operational Best Practices for Amazon Well-Architected Framework Reliability Pillar • Operational Best Practices for Amazon Well-Architected Framework Security Pillar • Operational Best Practices for Esquema Nacional de Seguridad (ENS) Low • Operational Best Practices for Esquema Nacional de Seguridad (ENS) Medium • Operational Best Practices for HIPAA Security	July 30, 2021
Example Amazon Lambda Functions for Amazon Config Custom Rules	With this release, Amazon Config provides Python example functions in Example Amazon Lambda Functions for Amazon Config Rules (Python).	July 29, 2021

Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant permission to list tags for a log group, list tags for a state machine, and list all state machines. These policies now grant permission to get details about a state machine. These policies also now support additional permission for Amazon EC2 Systems Manager (SSM), Amazon Elastic Container Registry, Amazon FSx, Amazon Data Firehose, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Relational Database Service (Amazon RDS), Amazon Route 53, Amazon SageMaker AI, Amazon Simple Notification Service, Amazon Database Migration Service, Amazon Global Accelerator, and Amazon Storage Gateway. For more information, see Amazon managed policies for Amazon Config.	July 28, 2021

Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to Amazon Backup resource types. For more informati on, see Supported Resource Types.	July 14, 2021
Amazon Config supports new conformance packs	With this release, Amazon Config supports the following conformance packs: • Operational Best Practices for CIS Critical Security Controls v8 IG1 • Operational Best Practices for CIS Critical Security Controls v8 IG2 • Operational Best Practices for CIS Critical Security Controls v8 IG3 • Operational Best Practices for NIST 1800 25	July 9, 2021
Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • ssm-document-not-public • s3-account-level-public-acc ess-blocks-periodic	June 25, 2021

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • ec2-instance-multiple-eni-check • elbv2-acm-certificate-required • autoscaling-launch-config-public-ip-disabled	June 10, 2021

Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant permission to view the permissions of Amazon Systems Manager documents and information about IAM Access Analyzer. These policies now support additional Amazon resource types for Amazon Kinesis, Amazon ElastiCache, Amazon EMR, Amazon Network Firewall, Amazon Route 53, and Amazon Relational Database Service (Amazon RDS). These permission changes allow Amazon Config to invoke the read-only APIs required to support these resource types. These policies also now support filtering Lambda@Edge functions for the lambda-inside-vpc Amazon Config managed rule. For more information, see Amazon managed policies for Amazon Config.	June 8, 2021

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • elasticsearch-logs-to-cloudwatch • rds-cluster-multi-az-enabled • api-gw-associated-with-waf • iam-policy-no-statements-with-full-access	May 19, 2021
Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to Amazon Elastic File System resource types. For more information, see Supported Resource Types.	May 13, 2021

Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grants permission that allow Amazon Config to make read-only GET calls to API Gateway to support a Config Rule for API Gateway. These policies also adds permissions that allow Amazon Config to invoke Amazon Simple Storage Service (Amazon S3) read-only APIs, which are required to support the new `AWS::S3::AccessPoint` resource type. For more information, see Amazon managed policies for Amazon Config.	May 10, 2021
Amazon Config Custom Rules	The following pages in the developer guide are updated: • Getting Started with Custom Rules for Amazon Config • Developing a Custom Rule for Amazon Config	April 30, 2021

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • aurora-mysql-backtracking-enabled • ec2-instance-profile-attached • ecs-task-definition-user-for-host-mode-check • no-unrestricted-route-to-igw • rds-automatic-minor-version-upgrade-enabled • redshift-enhanced-vpc-routing-enabled	April 15, 2021

Security IAM update	The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant permission to view information about Amazon Systems Manager specified documents. These policies also now support additional Amazon resource types for Amazon Backup, Amazon Elastic File System, Amazon ElastiCache, Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Amazon Kinesis, Amazon SageMaker AI, Amazon Database Migration Service, and Amazon Route 53. These permission changes allow Amazon Config to invoke the read-only APIs required to support these resource types. For more information, see Amazon managed policies for Amazon Config.	April 14, 2021

Conformance Pack Compliance as Configuration Items (CIs)	With this release, Amazon Config supports conformance pack compliance as configuration items. This enables you to: • View a timeline of changes to the compliance state of your conformance packs • Aggregate conformance packs compliance across multiple accounts and regions • Use advanced queries to check the compliance of your conformance packs The following data types are updated: • DescribeAggregateComplianceByConformancePacks • GetAggregateConformancePackComplianceSummary The following pages in the developer guide are updated: • Viewing Compliance Data in the Conformance Packs Dashboard • Viewing Compliance History Timeline for Conformance Packs	March 30, 2021

	• Viewing Compliance Data in the Aggregator Dashboard • Querying the Current Configuration State of Amazon Resources • Supported Resource Types	
Pagination update	With this release, Amazon Config advanced queries feature now supports pagination for queries that contain aggregate functions , such as COUNT and SUM. You can now use advanced queries to get complete results for your aggregate queries through paginatio n, which were previously limited to 500 rows. For more information, see Querying the Current Configuration State of Amazon Resources	March 26, 2021
Region support	With this release, Amazon Config and Amazon Config Rules is now supported in Asia Pacific (Osaka) Region.	March 4, 2021

Amazon Config supports new resources types	With this release, you can use Amazon Config to record configuration changes to Amazon Elastic Container Registry, Amazon Elastic Container Service, and Amazon Elastic Kubernetes Service resource types. For more information, see Supported Resource Types.	February 25, 2021
KMS encryption support	With this release, Amazon Config allows you to use KMS-based encryption on objects delivered by Amazon Config for S3 bucket delivery. The following data types are updated: • DeliveryChannel • PutDeliveryChannel The following pages in the developer guide are updated: • Permissions for the KMS Key • Permissions for the IAM Role Assigned to Amazon Config	February 16, 2021

Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • secretsmanager-secret-periodic-rotation • secretsmanager-secret-unused • secretsmanager-using-cmk	February 16, 2021
Saved Query Region support	With this release, saved query is now supported in Amazon GovCloud (US-East) and Amazon GovCloud (US-West) Regions.	February 15, 2021
Advanced queries Region support	With this release, advanced queries is now supported in Africa (Cape Town) and Europe (Milan) Regions. For more information, see Querying the Current Configuration State of Amazon Resources.	February 15, 2021
Amazon Config documentation history notification available through RSS feed	You can now receive notification about updates to the Amazon Config documentation by subscribing to an RSS feed.	January 1, 2021

Earlier Updates

The following table describes the documentation release history of Amazon Config prior to Dec 31, 2020.

Change	Description	Release Date
Saved Query support	With this release, Amazon Config allows you to save your queries. After you save the query, you can search it, copy it to the query editor, edit it, or delete it. For more information about how to save a query, see the Query Using the SQL Query Editor for Amazon Config (Console) and Query Using the SQL Query Editor for Amazon Config (Amazon CLI). For more information about APIs, see the *Amazon Config API Reference* : • PutStoredQuery • GetStoredQuery • ListStoredQueries • DeleteStoredQuery Also see Service Limits for Amazon Config.	December 21, 2020
Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • api-gw-ssl-enabled • api-gw-xray-enabled • beanstalk-enhanced-health-reporting-enabled • cloudfront-accesslogs-enabled • cloudfront-associated-with-waf	December 17, 2020

Change	Description	Release Date
	• cloudfront-custom-ssl-certificate • elastic-beanstalk-managed-updates-enabled • rds-cluster-iam-authentication-enabled • redshift-cluster-kms-enabled • s3-bucket-level-public-access-prohibited • subnet-auto-assign-public-ip-disabled • vpc-network-acl-unused-check	
Amazon Config supports Amazon Network Firewall	With this release, you can use Amazon Config to record configuration changes to your Amazon Network Firewall FirewallPolicy, RuleGroup, and Firewall resource types. For more information, see Supported Resource Types for Amazon Config.	December 4, 2020

Change	Description	Release Date
Documentation update	Amazon Config added support for organization-wide resource data aggregation in a delegated administrator account. You can now use a delegated administr ator account to aggregate resource configuration and compliance data from all member accounts of an organization in Amazon Organizat ions. For more information, see PutConfig urationAggregator, Creating Aggregators for Amazon Config and Registering a Delegated Administr ator for Amazon Config.	December 4, 2020
Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • iam-customer-policy-blocked-kms-actions • iam-inline-policy-blocked-kms-actions	September 17, 2020
Amazon Config supports Amazon WAFv2	With this release, you can use Amazon Config to record configura tion changes to your Amazon WAFv2 WebACL, IPSet, RegexPatternSet, RuleGroup, and ManagedRuleSet resource types. For more informati on, see Supported Resource Types for Amazon Config.	September 1, 2020

Change	Description	Release Date
Documentation update	A note has been added to Full access to Amazon Config about creating custom permissions that grant full access. The documentation has been updated for the following rules: • s3-bucket-server-side-encryption-enabled • ec2-instance-detailed-monitoring-enabled • ec2-managedinstance-platform-check	August 24, 2020
Documentation update	??? and ??? templates are updated.	August 14, 2020
Documentation update	Example relationship queries are added. For more information, see Example Relationship Queries for Amazon Config.	July 30, 2020

Change	Description	Release Date
Documentation update	The following data types are updated: • ConfigurationAggregator • RemediationConfiguration • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRuleStatuses • DescribeOrganizationConformancePacks • DescribeOrganizationConformancePackStatuses • GetOrganizationConformancePackDetailedStatus	July 23, 2020
Amazon Config supports Amazon Systems Manager resource type	With this release, you can use Amazon Config to record configuration changes to the Amazon Systems Manager file data resource type. For more information, see Supported Resource Types for Amazon Config.	July 9, 2020

Change	Description	Release Date
Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • ??? • alb-http-drop-invalid-header-enabled • alb-waf-enabled • ??? • ??? • ??? • ??? • cloudtrail-security-trail-enabled • cw-loggroup-retention-period-check • dax-encryption-enabled • dynamodb-in-backup-plan • ebs-in-backup-plan • ec2-imdsv2-check • efs-in-backup-plan • eks-endpoint-no-public-access • eks-secrets-encrypted • elasticsearch-node-to-node-encryption-check • elb-cross-zone-load-balancing-enabled • elb-tls-https-listeners-only • iam-no-inline-policy-check • ??? • rds-in-backup-plan	July 9, 2020

Change	Description	Release Date
	• rds-instance-deletion-protection-enabled • rds-instance-iam-authentication-enabled • rds-logging-enabled • redshift-backup-enabled • ??? • wafv2-logging-enabled For more information, see List of Amazon Config Managed Rules.	
Multi-account multi-region data aggregation Region support	With this release, multi-account multi-region data aggregation is now supported in Asia Pacific (Hong Kong) and Middle East (Bahrain) Regions. For more information, see Multi-Account Multi-Region Data Aggregation and Troubleshooting for Multi-Account Multi-Region Data Aggregation for Amazon Config.	July 1, 2020
Advanced queries Region support	With this release, advanced queries is now supported in Asia Pacific (Hong Kong) and Middle East (Bahrain) Regions. For more information, see Querying the Current Configuration State of Amazon Resources with Amazon Config.	July 1, 2020

Change	Description	Release Date
Documentation update	The documentation has been updated for the following rules: • ec2-managedinstance-association-compliance-status-check • iam-policy-no-statements-with-admin-access • required-tags • restricted-common-ports • rds-snapshots-public-prohibited • s3-bucket-policy-grantee-check	June 30, 2020
Documentation update	The documentation has been updated with information about security for Amazon Config. See Security in Amazon Config.	June 24, 2020

Change	Description	Release Date
Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • dynamodb-pitr-enabled • dynamodb-table-encrypted-kms • ec2-ebs-encryption-by-default • rds-snapshot-encrypted • redshift-require-tls-ssl • s3-bucket-default-lock-enabled • s3-default-encryption-kms • securityhub-enabled • sns-encrypted-kms For more information, see List of Amazon Config Managed Rules.	May 28, 2020

Change	Description	Release Date
Delegated administrator support	With this release, you can deploy Amazon Config rules and conformance packs from any delegated member account in your organization, in addition to the management account. For more information about APIs, see the *Amazon Config API Reference*: • PutOrganizationConfigRule • PutOrganizationConformancePack • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRuleStatuses • DeleteOrganizationConfigRule • DeleteOrganizationConformancePack • DescribeOrganizationConformancePacks • DescribeOrganizationConformancePackStatuses • GetOrganizationConformancePackDetailedStatus For more information, see Service Limits for Amazon Config.	May 27, 2020

Change	Description	Release Date
Amazon Config rules Region support	With this release, few Amazon Config rules are supported in Africa (Cape Town) and Europe (Milan) regions. For a detailed list of rules and the regions they are supported in, see List of Amazon Config Managed Rules.	April 28, 2020
Amazon Config supports Amazon Secrets Manager	With this release, you can use Amazon Config to record configuration changes to your Secrets Manager secret. For more information, see Supported Resource Types for Amazon Config.	April 20, 2020
Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • secretsmanager-rotation-enabled-check • secretsmanager-scheduled-rotation-success-check For more information, see List of Amazon Config Managed Rules.	April 16, 2020
Documentation update	Amazon Config limits are available in this developer guide. For more information, see Service Limits for Amazon Config.	April 8, 2020

Change	Description	Release Date
Documentation update	Third-party resources that are managed (that is, created/updated/deleted) through Amazon CloudFormation registry are automatically tracked in Amazon Config as configuration items. For more information, see Recording Configurations with Amazon Config for Third-Party Resources using the Amazon CLI.	March 30, 2020
Documentation update	The Amazon Config Managed Rules are updated to include Amazon Web Services Region information. For more information, see List of Amazon Config Managed Rules.	March 27, 2020
Amazon Config supports Amazon SNS resource type	With this release, you can use Amazon Config to record configuration changes to your Amazon SNS topic. For more information, see Supported Resource Types for Amazon Config.	March 6, 2020
Multi-account multi-region data aggregation Region support	With this release, multi-account multi-region data aggregation is now supported in Europe (Stockholm) Region. For more information, see Multi-Account Multi-Region Data Aggregation.	March 5, 2020

Change	Description	Release Date
Advanced queries Region support	With this release, advanced queries is now supported in Europe (Stockholm) Region. For more information, see Querying the Current Configuration State of Amazon Resources with Amazon Config.	March 5, 2020
Amazon Config allows you to run advanced queries with configuration aggregators	With this release, Amazon Config adds support to run advanced queries based on resource configuration properties with configuration aggregators, enabling you to run the same queries across multiple accounts and Regions. For more information, see Querying the Current Configuration State of Amazon Resources with Amazon Config. With this release, Amazon Config adds `SelectAggregateResourceConfig` API. For more information, see SelectAggregateResourceConfig in the *Amazon Config API Reference*:	February 28, 2020
Amazon Config supports Amazon SQS resource type	With this release, you can use Amazon Config to record configuration changes to your Amazon SQS queue. For more information, see Supported Resource Types for Amazon Config.	February 13, 2020

Change	Description	Release Date
Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • api-gw-execution-logging-enabled • ec2-stopped-instance • elasticache-redis-cluster-automatic-backup-check • emr-master-no-public-ip • guardduty-non-archived-findings • rds-enhanced-monitoring-enabled • s3-account-level-public-access-blocks • sagemaker-endpoint-configuration-kms-key-configured • service-vpc-endpoint-enabled For more information, see List of Amazon Config Managed Rules.	December 20, 2019

Change	Description	Release Date
Record configurations for custom resource types	With this release, Amazon Config introduces support to record configurations for custom resource types. You can publish the configuration data of third-party resources into Amazon Config and view and monitor the resource inventory and configuration history using Amazon Config console and APIs. For more information, see Recording Configurations with Amazon Config for Third-Party Resources using the Amazon CLI. For more information about APIs, see the *Amazon Config API Reference* : • DeleteResourceConfig • PutResourceConfig	November 20, 2019
Amazon Config supports Amazon OpenSearch Service and Amazon Key Management Service resource types	With this release, you can use Amazon Config to record configuration changes to your Amazon OpenSearch Service domain and Amazon Key Management Service key. For more information, see Supported Resource Types for Amazon Config.	November 11, 2019

Change	Description	Release Date
Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • dms-replication-not-public • emr-kerberos-enabled • internet-gateway-authorized-vpc-only • kms-cmk-not-scheduled-for-deletion • sagemaker-notebook-no-direct-internet-access • sagemaker-notebook-instance-kms-key-configured • ??? For more information, see List of Amazon Config Managed Rules.	October 10, 2019
Amazon Config supports Amazon RDS resource type	With this release, you can use Amazon Config to record configuration changes to your Amazon Relational Database Service (Amazon RDS) DBCluster and DBClusterSnapshot. For more information, see Supported Resource Types for Amazon Config.	September 17, 2019

Change	Description	Release Date
Amazon Config supports Amazon QLDB resource type	With this release, you can use Amazon Config to record configuration changes to Amazon Quantum Ledger Database (QLDB) ledger resource type. For more information, see Supported Resource Types for Amazon Config.	September 10, 2019
Amazon Config allows you to apply auto remediation on noncompliant resources as evaluated by Amazon Config Rules	With this release, Amazon Config introduces support to apply auto remediation using Amazon Systems Manager automation documents on noncompliant resources as evaluated by Amazon Config Rules. For more information, see Remediating Noncompliant Resources with Amazon Config. With this release, Amazon Config adds the following new APIs. For more information, see the *Amazon Config API Reference* : • PutRemediationExceptions • DescribeRemediationExceptions • DeleteRemediationExceptions	September 5, 2019

Change	Description	Release Date
Amazon Config updates managed rules	With this release, Amazon Config supports the following managed rules: • alb-http-to-https-redirection-check • api-gw-cache-enabled-and-encrypted • api-gw-endpoint-type-check • cloudtrail-s3-dataevents-enabled • cloudwatch-log-group-encrypted • ebs-snapshot-public-restorable-check • elb-deletion-protection-enabled • ??? • ??? • ??? • ??? • ??? For more information, see List of Amazon Config Managed Rules.	August 22, 2019

Change	Description	Release Date
Amazon Config updates managed rules	With this release, Amazon Config updates the following managed rules: • ??? • ec2-instance-no-public-ip • ec2-security-group-attached-to-eni • efs-encrypted-check • elasticsearch-encrypted-at-rest • elasticsearch-in-vpc-only • redshift-cluster-public-access-check • vpc-sg-open-only-to-authorized-ports For more information, see List of Amazon Config Managed Rules.	July 31, 2019
Amazon Config supports Amazon EC2 resource types	With this release, you can use Amazon Config to record configuration changes to the following Amazon EC2 resources; VPCEndpoint, VPCEndpointService, and VPCPeeringConnection. For more information, see Supported Resource Types for Amazon Config.	July 12, 2019

Change	Description	Release Date
Amazon Config supports Amazon S3 and Amazon EC2 resource types	With this release, you can use Amazon Config to record configuration changes to the Amazon S3 AccountPublicAccessBlock resource and the following Amazon EC2 resources; NatGateway, EgressOnlyInternetGateway, and FlowLog. For more information, see Supported Resource Types for Amazon Config.	May 17, 2019
Amazon Config updates managed rules	With this release, Amazon Config updates the following managed rules: • s3-bucket-public-read-prohibited • s3-bucket-public-write-prohibited For more information, see List of Amazon Config Managed Rules.	May 7, 2019
Amazon Config allows you to delete a remediation action using Amazon Web Services Management Console.	With this release, Amazon Config introduces support to delete a remediation action using Amazon Web Services Management Console. For more information, see Remediating Noncompliant Resources with Amazon Config.	April 24, 2019

Change	Description	Release Date
Amazon Config supports new managed rules	This release supports a new managed rule: ???. For more information, see List of Amazon Config Managed Rules.	April 7, 2019
Amazon Config supports Amazon API Gateway resource type	With this release, you can use Amazon Config to record configuration changes to the following Amazon API Gateway resources; Api (WebSocket API), RestApi (REST API), Stage (WebSocket API stage), and Stage (REST API stage). For more information, see Supported Resource Types for Amazon Config.	March 20, 2019
Amazon Config allows you to run advanced queries	With this release, Amazon Config adds support to run advanced queries based on resource configuration properties. For more information, see Querying the Current Configuration State of Amazon Resources with Amazon Config. With this release, Amazon Config adds `SelectResourceConfig` API. For more information, see SelectResourceConfig in the *Amazon Config API Reference*:	March 19, 2019

Change	Description	Release Date
Amazon Config allows you to assign tags your Amazon Config resources	With this release, Amazon Config introduces support for tag based access control for three Amazon Config resources—`ConfigRule`, `ConfigurationAggregator`, and `AggregationAuthorization` . For more information, see Tagging Your Amazon Config Resources. With this release, you can add, remove or list tags from your Amazon Config resources using the following data types. For more information, see the *Amazon Config API Reference*: • ListTagsForResource • TagResource • UntagResource	March 14, 2019

Change	Description	Release Date
Amazon Config allows you to apply remediation on noncompliant resources as evaluated by Amazon Config Rules	With this release, Amazon Config introduces support to apply remediation using Amazon Systems Manager automation documents on noncompliant resources as evaluated by Amazon Config Rules. For more information, see Remediating Noncompliant Resources with Amazon Config. With this release, Amazon Config adds the following new APIs. For more information, see the *Amazon Config API Reference* : • DeleteRemediationConfiguration • DescribeRemediationConfigurations • DescribeRemediationExecutionStatus • PutRemediationConfigurations • StartRemediationExecution	March 12, 2019

Change	Description	Release Date
Amazon Config supports Amazon Config Rules in China (Ningxia) Region	This release only supports 54 Amazon Config Rules in the China (Ningxia) Region. For more informati on, see List of Amazon Config Managed Rules. However, Amazon Config does not currently support the following rules in the China (Ningxia) Region: • acm-certificate-expiration-check • cmk-backing-key-rotation-en abled • cloudformation-stack-drift- detection-check • cloudformation-stack-notifi cation-check • cloud-trail-encryption-enabled • cloud-trail-log-file-validation- enabled • codebuild-project-envvar-aw scred-check • codebuild-project-source-repo- url-check • codepipeline-deployment-count- check • codepipeline-region-fanout-check • dynamodb-table-encryption-e nabled • elb-acm-certificate-required • encrypted-volumes • fms-webacl-resource-policy-check	March 12, 2019

Change	Description	Release Date
	• fms-webacl-rulegroup-association-check • guardduty-enabled-centralized • lambda-function-public-access-prohibited • lambda-function-settings-check • rds-storage-encrypted • root-account-mfa-hardware-mfa-enabled • root-account-mfa-enabled • s3-bucket-blacklisted-actions-prohibited • s3-bucket-policy-grantee-check • s3-bucket-policy-not-more-permissive • s3-bucket-public-read-prohibited • s3-bucket-public-write-prohibited • s3-bucket-server-side-encryption-enabled • s3-bucket-ssl-requests-only	
Amazon Config supports new managed rules	This release supports the following new managed rules: • iam-user-mfa-enabled For more information, see List of Amazon Config Managed Rules.	January 21, 2019

Change	Description	Release Date
Amazon Config supports Service Catalog resource type	With this release, you can use Amazon Config to record configuration changes to the following Service Catalog resources; CloudFromation product, provisioned product, and portfolio. For more information, see Supported Resource Types for Amazon Config.	January 11, 2019
Service-linked Amazon Config rules support	With this release, Amazon Config adds a new managed config rule that supports other Amazon services to create Amazon Config Rules in your account. For more information, see Service-Linked Amazon Config Rules.	November 20, 2018

Change	Description	Release Date
Amazon Config allows you to aggregate configuration data of Amazon resources	With this release, Amazon Config introduces support for aggregating the configuration data of Amazon resources. For more information, see Viewing Compliance and Inventory Data in the Aggregator Dashboard for Amazon Config. With this release, Amazon Config adds the following new APIs. For more information, see the *Amazon Config API Reference* : • BatchGetAggregateResourceConfig • GetAggregateDiscoveredResourceCounts • GetAggregateResourceConfig • ListAggregateDiscoveredResources	November 19, 2018
Amazon Config supports new managed rules	This release supports the following new managed rules: • cloudformation-stack-drift-detection-check • ??? • ??? For more information, see List of Amazon Config Managed Rules.	November 19, 2018

Change	Description	Release Date
Amazon Config supports new managed rules	This release supports the following new managed rules: • access-keys-rotated • cloud-trail-cloud-watch-logs-enabled • cloud-trail-encryption-enabled • cloud-trail-log-file-validation-enabled • cmk-backing-key-rotation-enabled • iam-policy-no-statements-with-admin-access • iam-role-managed-policy-check • iam-root-access-key-check • iam-user-unused-credentials-check • mfa-enabled-for-iam-console-access • multi-region-cloudtrail-enabled • ??? • vpc-flow-logs-enabled For more information, see List of Amazon Config Managed Rules.	November 12, 2018

Change	Description	Release Date
Amazon Config supports new managed rules	This release supports the following new managed rules: • ??? • elb-logging-enabled • rds-instance-public-access-check • vpc-default-security-group-closed For more information, see List of Amazon Config Managed Rules.	October 24, 2018
Compliance history support	With this release, Amazon Config now supports storing compliance history of resources as evaluated by Amazon Config Rules. For more information, see Viewing Compliance History Timeline for Resources and Rules.	October 18, 2018
Multi-account multi-region Data Aggregation Region support	With this release, multi-account multi-region Data Aggregation is now supported in six new Regions. For more information, see Multi-Account Multi-Region Data Aggregation.	October 4, 2018
Amazon Config supports resource-level permissions for Amazon Config Rules APIs actions	With this release, Amazon Config supports resource-level permissions for certain Amazon Config Rules API actions. For more information about the supported APIs, see Supported Resource-Level Permissions for Amazon Config Rule API Actions.	October 1, 2018

Change	Description	Release Date
Amazon Config supports CodePipeline resource type	With this release, you can use Amazon Config to record configuration changes to the Amazon CodePipeline resource type. For more information, see Supported Resource Types for Amazon Config.	September 12, 2018
Amazon Config supports new managed rules	This release supports the following new managed rules: • ec2-instance-managed-by-systems-manager • ec2-managedinstance-association-compliance-status-check • ec2-managedinstance-patch-compliance-status-check • guardduty-enabled-centralized • rds-snapshots-public-prohibited • s3-bucket-blacklisted-actions-prohibited • s3-bucket-policy-not-more-permissive For more information, see List of Amazon Config Managed Rules.	September 5, 2018

Change	Description	Release Date
Amazon Config supports Amazon Systems Manager resource type	With this release, you can use Amazon Config to record configuration changes to the Amazon Systems Manager patch compliance and association compliance resource types. For more information, see Supported Resource Types for Amazon Config.	August 9, 2018
Amazon Config allows you to delete your Amazon Config data using Amazon Web Services Management Console	With this release, Amazon Config introduces support for retention period using Amazon Web Services Management Console. In the Amazon Web Services Management Console, you can select a custom data retention period for your `ConfigurationItems` . For more information, see Deleting Amazon Config Data.	August 7, 2018
Amazon Config supports Amazon Shield resource type	With this release, you can use Amazon Config to record configuration changes to the Amazon Shield Protection resource type. For more information, see Supported Resource Types for Amazon Config.	August 7, 2018

Change	Description	Release Date
Amazon Config supports Amazon PrivateLink	With this release, Amazon Config supports Amazon PrivateLink, enabling you to route data between your Amazon Virtual Private Cloud (VPC) and Amazon Config entirely within the Amazon network. For more information, see Using Amazon Config with Interface Amazon VPC Endpoints.	July 31, 2018
Amazon Config allows you to delete your Amazon Config data	With this release, Amazon Config introduces support for retention period. Amazon Config allows you to delete your data by specifyin g a retention period for your `ConfigurationItems` . For more information, see Deleting Amazon Config Data. With this release, Amazon Config adds the following new APIs. For more information, see the *Amazon Config API Reference* : • PutRetentionConfiguration • DescribeRetentionConfigurations • DeleteRetentionConfiguration	May 25, 2018

Change	Description	Release Date
Amazon Config supports new managed rules	This release supports the following two new managed rules: • ??? • s3-bucket-replication-enabled • iam-policy-blacklisted-check For more information, see List of Amazon Config Managed Rules.	May 10, 2018
Amazon Config supports Amazon X-Ray resource type	With this release, you can use Amazon Config to record configuration changes to the Amazon X-Ray EncryptionConfig resource type. For more information, see Supported Resource Types for Amazon Config.	May 1, 2018
Amazon Config supports Amazon Lambda resource type and one new managed rule	With this release, you can use Amazon Config to record configuration changes to the Amazon Lambda function resource type. For more information, see Supported Resource Types for Amazon Config. This release also supports the ??? managed rule. For more information, see Amazon Config Managed Rules.	April 25, 2018

Change	Description	Release Date
Amazon Config supports Amazon Elastic Beanstalk resource type	With this release, you can use Amazon Config to record configuration changes to the Amazon Elastic Beanstalk Application, Application Version, and Environment resources. For more information, see Supported Resource Types for Amazon Config.	April 24, 2018
Amazon Config supports new managed rules	This release supports the following two new managed rules: • fms-webacl-resource-policy-check • fms-webacl-rulegroup-association-check For more information, see List of Amazon Config Managed Rules.	April 4, 2018

Change	Description	Release Date
Multi-account multi-region data aggregation	With this release, Amazon Config introduces multi-account multi-region data aggregation. This feature allows you to aggregate Amazon Config data from multiple accounts or an organization and multiple regions into an aggregator account. For more information, see Multi-Account Multi-Region Data Aggregation. With this release, Amazon Config adds the following new APIs. For more information, see the *Amazon Config API Reference* : • PutConfigurationAggregator • DescribePendingAggregationRequests • DeletePendingAggregationRequest • PutAggregationAuthorization • DescribeAggregationAuthorizations • GetAggregateConfigRuleComplianceSummary • DescribeAggregateComplianceByConfigRules • GetAggregateComplianceDetailsByConfigRule • DescribeConfigurationAggregators • DescribeConfigurationAggregatorSourcesStatus	April 4, 2018

Change	Description	Release Date
	• DeleteAggregationAuthorization • DeleteConfigurationAggregator	
Monitoring Amazon Config with Amazon CloudWatch Events	With this release, use Amazon CloudWatch Events to detect and react to changes in the status of Amazon Config events. For more information, see Monitoring Amazon Config with Amazon EventBridge.	March 29, 2018
New API operation	With this release, Amazon Config adds support for BatchGetResourceConfig API, allowing you to batch-retrieve the current state of one or more of your resources.	March 20, 2018
Amazon Config supports Amazon WAF RuleGroup resource type	With this release, you can use Amazon Config to record configuration changes to the Amazon WAF RuleGroup and Amazon WAF RuleGroup Regional resources. For more information, see Supported Resource Types for Amazon Config.	February 15, 2018

Change	Description	Release Date
Amazon Config supports new managed rules	This release supports the following new managed rules: • elb-acm-certificate-required • elb-custom-security-policy-ssl-check • elb-predefined-security-policy-ssl-check • codebuild-project-envvar-awscred-check • codebuild-project-source-repo-url-check • iam-group-has-users-check • s3-bucket-server-side-encryption-enabled For more information, see List of Amazon Config Managed Rules.	January 25, 2018
Amazon Config supports Elastic Load Balancing resource type	With this release, you can use Amazon Config to record configuration changes to your Elastic Load Balancing classic load balancers. For more information, see Supported Resource Types for Amazon Config.	November 17, 2017

Change	Description	Release Date
Amazon Config supports the Amazon CloudFront and Amazon WAF resource type	With this release, you can use Amazon Config to record configuration changes to your CloudFront distribution and streaming distribution. With this release, you can use Amazon Config to record configuration changes to the following Amazon WAF and Amazon WAF Regional resources; rate based rule, rule, and Web ACL. For more information, see Supported Resource Types for Amazon Config.	November 15, 2017
Amazon Config supports the Amazon CodeBuild resource type	With this release, you can use Amazon Config to record configuration changes to your Amazon CodeBuild projects. For more information, see Supported Resource Types for Amazon Config.	October 20, 2017

Change	Description	Release Date
Amazon Config supports Auto Scaling resources and one new managed rule	With this release, you can use Amazon Config to record configuration changes to the following Auto Scaling resources; groups, launch configuration, scheduled action, and scaling policy. For more information, see Supported Resource Types for Amazon Config. This release also supports the following managed rule: • autoscaling-group-elb-healthcheck-required For more information, see Amazon Config Managed Rules.	September 18, 2017
Amazon Config supports the Amazon CodeBuild resource type	With this release, you can use Amazon Config to record configuration changes to your Amazon CodeBuild projects. For more information, see Supported Resource Types for Amazon Config.	October 20, 2017

Change	Description	Release Date
Amazon Config supports Auto Scaling resources and one new managed rule	With this release, you can use Amazon Config to record configuration changes to the following Auto Scaling resources; groups, launch configuration, scheduled action, and scaling policy. For more information, see Supported Resource Types for Amazon Config. This release also supports the following managed rule: • autoscaling-group-elb-healthcheck-required For more information, see Amazon Config Managed Rules.	September 18, 2017
Amazon Config supports the DynamoDB table resource type and one new managed rule	With this release, you can use Amazon Config to record configuration changes to your DynamoDB tables. For more information, see Supported Resource Types for Amazon Config. This release supports the following managed rule: • dynamodb-autoscaling-enabled For more information, see Amazon Config Managed Rules.	September 8, 2017

Change	Description	Release Date
Amazon Config supports two new managed rules for Amazon S3	This release supports two new managed rules: • s3-bucket-public-read-prohibited • s3-bucket-public-write-prohibited For more information, see Amazon Config Managed Rules.	August 14, 2017
New page in the Amazon Config console	You can use the **Dashboard** in the Amazon Config console to see the following: • Total number of resources • Total number of rules • Number of noncompliant resources • Number of noncompliant rules For more information, see Viewing the Amazon Config Dashboard.	July 17, 2017
New API operation	You can use the GetDiscoveredResourceCounts operation to return the number of resource types, the number of each resource type, and the total number of resources that Amazon Config is recording in a Region for your Amazon Web Services account.	July 17, 2017

Change	Description	Release Date
Amazon Config supports the Amazon CloudFormation stack resource type and one new managed rule	With this release, you can use Amazon Config to record configuration changes to your Amazon CloudFormation stacks. For more information, see Supported Resource Types for Amazon Config. This release supports the following managed rule: • cloudformation-stack-notification-check For more information, see Amazon Config Managed Rules.	July 6, 2017
New and updated content	This release adds support for Amazon Config Rules in the Canada (Central) Region and South America (São Paulo) Region. For all regions that support Amazon Config and Config Rules, see Amazon Web Services Regions and Endpoints in the *Amazon Web Services General Reference*.	July 5, 2017

Change	Description	Release Date
New and updated content	Amazon Config Rules is available in the Amazon GovCloud (US) Region. For more information, see the Amazon GovCloud (US) User Guide. For regions that support Amazon Config, see Amazon Web Services Regions and Endpoints in the *Amazon Web Services General Reference*.	June 8, 2017
Amazon Config supports the Amazon CloudWatch alarm resource type and three new managed rules	With this release, you can use Amazon Config to record configuration changes to your Amazon CloudWatch alarms. For more information, see Supported Resource Types for Amazon Config. This release supports three new managed rules: • cloudwatch-alarm-action-check • cloudwatch-alarm-resource-check • cloudwatch-alarm-settings-check For more information, see Amazon Config Managed Rules.	June 1, 2017

Change	Description	Release Date
New and updated content	This release supports specifying the application version number for the following managed rules: • ec2-managedinstance-applications-blacklisted • ec2-managedinstance-applications-required For more information, see Amazon Config Managed Rules.	June 1, 2017
New and updated content	This release adds support for Amazon Config Rules in the Asia Pacific (Mumbai) Region. For more information, see Amazon Web Services Regions and Endpoints in the *Amazon Web Services General Reference*.	April 27, 2017

Change	Description	Release Date
New and updated content	This release supports an updated console experience for adding Amazon Config managed rules to your account for the first time. When you set up Amazon Config Rules for the first time or in a new Region, you can search for Amazon managed rules by name, description, or label. You can choose **Select all** to select all rules or choose **Clear all** to clear all rules. For more information, see Add, View, Update and Delete Rules (Console).	April 5, 2017
Amazon Config supports new managed rules	This release supports the following new managed rules: • acm-certificate-expiration-check • ec2-instance-detailed-monitoring-enabled • ec2-managedinstance-inventory-blacklisted • ec2-volume-inuse-check • iam-user-group-membership-check • iam-user-no-policies-check • s3-bucket-ssl-requests-only For more information, see List of Amazon Config Managed Rules.	February 21, 2017

Change	Description	Release Date
New and updated content	This release adds support for Amazon Config Rules in the Europe (London) Region. For more informati on, see Amazon Web Services Regions and Endpoints in the *Amazon Web Services General Reference*.	February 21, 2017
New and updated content	This release adds Amazon CloudFormation templates for Amazon Config managed rules. You can use the templates to create managed rules for your account. For more information, see Creating Amazon Config Managed Rules With Amazon CloudFormation Templates.	February 16, 2017
New and updated content	This release adds support for a new test mode for the `PutEvalua tions` API. Set the `TestMode` parameter to true in your custom rule to verify whether your Amazon Lambda function will deliver evaluation results to Amazon Config. No updates occur to your existing evaluations, and evaluation results are not sent to Amazon Config. For more information, see PutEvalua tions in the *Amazon Config API Reference*.	February 16, 2017

Change	Description	Release Date
New and updated content	This release adds support for Amazon Config Rules in the Asia Pacific (Seoul), and US West (N. California) Regions. For more information, see Amazon Web Services Regions and Endpoints in the *Amazon Web Services General Reference*.	December 21, 2016
New and updated content	This release adds support for Amazon Config in the Europe (London) Region. For more informati on, see Amazon Web Services Regions and Endpoints in the *Amazon Web Services General Reference*.	December 13, 2016
New and updated content	This release adds support for Amazon Config in the Canada (Central) Region. For more informati on, see Amazon Web Services Regions and Endpoints in the *Amazon Web Services General Reference*.	December 8, 2016

Change	Description	Release Date
Amazon Config supports Amazon Redshift resource types and two new managed rules	With this release, you can use Amazon Config to record configuration changes to your Amazon Redshift clusters, cluster parameter groups, cluster security groups, cluster snapshots, cluster subnet groups, and event subscriptions. For more information, see Supported Resource Types for Amazon Config. This release supports two new managed rules: • redshift-cluster-configuration-check • redshift-cluster-maintenancesettings-check For more information, see List of Amazon Config Managed Rules.	December 7, 2016
New and updated content	This release adds support for a new managed rule: • dynamodb-throughput-limit-check For more information, see List of Amazon Config Managed Rules.	December 7, 2016

Change	Description	Release Date
New and updated content	This release adds support for creating up to 50 rules per Region in an account. For more informati on, see Amazon Config Limits in the *Amazon Web Services General Reference*.	December 7, 2016
Amazon Config supports the managed instance inventory resource type for Amazon EC2 Systems Manager and three new managed rules	With this release, you can use Amazon Config to record software configuration changes on your managed instances with support for managed instance inventory. For more information, see Recording Software Configuration for Managed Instances. This release supports three new managed rules: • ec2-managedinstance-inventory-blacklisted • ec2-managedinstance-applica tions-required • ec2-managedinstance-platform-check For more information, see List of Amazon Config Managed Rules.	December 1, 2016
New and updated content	Amazon Config is available in the China (Beijing) Region.	October 24, 2016

Change	Description	Release Date
Amazon Config supports the Amazon S3 bucket resource and two new managed rules	With this release, you can use Amazon Config to record configuration changes to your Amazon S3 buckets. For more information, see Supported Resource Types for Amazon Config. This release supports two new managed rules: • s3-bucket-logging-enabled • s3-bucket-versioning-enabled For more information, see Amazon Config Managed Rules.	October 18, 2016
New and updated content	This release adds support for Amazon Config and Amazon Config Rules in the US East (Ohio) Region. For more information, see Amazon Web Services Regions and Endpoints in the *Amazon Web Services General Reference*.	October 17, 2016

Change	Description	Release Date
New and updated managed rules	This update adds support for eight new managed rules: • approved-amis-by-id • approved-amis-by-tag • db-instance-backup-enabled • desired-instance-type • ebs-optimized-instance • iam-password-policy • rds-multi-az-support • rds-storage-encrypted You can specify multiple parameter values for the following rules: • desired-instance-tenancy • required-tags For more information, see List of Amazon Config Managed Rules.	October 4, 2016
New and updated content for the Amazon Config console	This update adds support for viewing Amazon CloudTrail API activity in the Amazon Config timeline. If CloudTrail is logging for your account, you can view create, update, and delete API events for configuration changes to your resources. For more information, see Viewing Compliance History for your Amazon Resources with Amazon Config.	September 06, 2016

Change	Description	Release Date
Amazon Config supports Elastic Load Balancing resource type	With this release, you can use Amazon Config to record configuration changes to your Elastic Load Balancing application load balancers. For more information, see Supported Resource Types for Amazon Config.	August 31, 2016
New and updated content	This release adds support for Amazon Config Rules in the Asia Pacific (Singapore), and Asia Pacific (Sydney) Regions. For more information, see Amazon Web Services Regions and Endpoints in the *Amazon Web Services General Reference*.	August 18, 2016

Change	Description	Release Date
New and updated content for Amazon Config Rules	This update adds support for creating a rule that can be triggered by both configuration changes and at a periodic frequency that you choose. For more information, see Components of an Amazon Config Rule. This update also adds support for manually evaluating your resources against your rule and deleting evaluation results. For more information, see Evaluating Your Resources with Amazon Config Rules. This update also adds support for evaluating additional resource types using custom rules.	July 25, 2016
Amazon Config supports Amazon RDS and Amazon Certificate Manager (ACM) resource types	With this release, you can use Amazon Config to record configuration changes to your Amazon Relational Database Service (Amazon RDS) DB instances, DB security groups, DB snapshots, DB subnet groups, and event subscriptions. You can also use Amazon Config to record configuration changes to certificates provided by ACM. For more information, see Supported Resource Types for Amazon Config.	July 21, 2016

Change	Description	Release Date
Updated information about managing the configura tion recorder	This update adds steps for renaming and deleting the configuration recorder to Working with the configuration recorder.	July 07, 2016
Simplified role creation and updated policies	With this update, creating an IAM role for Amazon Config is simplifie d. This enhancement is available in regions that support Config rules. To support this enhancement, the steps in Setting Up Amazon Config with the Console are updated, the example policy in Permissions for the Amazon S3 Bucket for the Amazon Config Delivery Channel is updated, and the example policy in Identity-based policy examples for Amazon Config is updated.	March 31, 2016
Example functions and events for Config rules	This update provides updated example functions.	March 29, 2016
Amazon Config Rules GitHub repository	This update adds information about the Amazon Config Rules GitHub repository to Evaluating Resources with Amazon Config Rules. This repository provides sample functions for custom rules that are developed and contributed by Amazon Config users.	March 1, 2016

Change	Description	Release Date
Amazon Config Rules	This release introduces Amazon Config Rules. With rules, you can use Amazon Config to evaluate whether your Amazon resources comply with your desired configurations. For more information, see Evaluating Resources with Amazon Config Rules.	December 18, 2015
Amazon Config supports IAM resource types	With this release, you can use Amazon Config to record configuration changes to your IAM users, groups, roles, and customer managed policies. For more information, see Supported Resource Types for Amazon Config.	December 10, 2015
Amazon Config supports EC2 Dedicated host	With this release, you can use Amazon Config to record configuration changes to your EC2 Dedicated hosts. For more information, see Supported Resource Types for Amazon Config.	November 23, 2015

Change	Description	Release Date
Updated permissions information	This update adds information about the following Amazon managed policies for Amazon Config: • `AWS_ConfigRole` – Grants Amazon Config permission to get configuration details about your resources. For more information, see IAM Role Policy for Getting Configuration Details. • `AWSConfigUserAccess` – Grants read-only access to an Amazon Config user. For more information, see Read-only access to Amazon Config.	October 19, 2015
Amazon Config Rules preview	This release introduces the Amazon Config Rules preview. With rules, you can use Amazon Config to evaluate whether your Amazon resources comply with your desired configurations. For more informati on, see Evaluating Resources with Amazon Config Rules.	October 7, 2015
New and updated content	This release adds the ability to look up resources that Amazon Config has discovered. For more informati on, see Looking Up Resources That Are Discovered by Amazon Config.	August 27, 2015

Change	Description	Release Date
New and updated content	This release adds the ability to select which resource types Amazon Config records. For more information, see Recording Amazon Resources with Amazon Config.	June 23, 2015
New and updated content	This release adds support for the following regions: Asia Pacific (Tokyo), Asia Pacific (Singapore), Europe (Frankfurt), South America (São Paulo), and US West (N. California). For more information, see Amazon Web Services Regions and Endpoints.	April 6, 2015
New guide	This release introduces Amazon Config.	November 12, 2014