Amazon Health

用户指南

Amazon Health: 用户指南

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆或者贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

AWS 文档中描述的 AWS 服务或功能可能因区域而异。要查看适用于中国区域的差异，请参阅中国的 AWS 服务入门。

Table of Contents

什么是 Amazon Health？ 1
您是 Amazon Health 新用户吗？ 1
Amazon Personal Health Dashboard入门 2
Dashboard 2
事件日志 2
事件类型 3
事件详细信息窗格 3
Amazon CloudWatch Events 4
组织视图 4
访问 Amazon Health API 5
Endpoints 5
使用高可用性终端演示 6
使用 Java 演示 6
使用 Python 演示 8
签署 Amazon Health API 请求 10
Amazon Health 中支持的操作 10
Java 代码示例 11
第 1 步：初始化凭据 11
第 2 步：初始化Amazon HealthAPI 客户端 11
第 3 步：使用Amazon HealthAPI 操作获取事件信息 11
安全性 14
数据保护 14
数据加密 15
互联网络流量隐私 15
Identity and Access Management 15
Audience 16
使用身份进行身份验证 16
使用策略管理访问 17
Amazon Health 如何与 IAM 协同工作 19
基于身份的策略示例 22
问题排查 30
使用服务相关角色 31
Amazon Health 中的日志记录和监控 32
合规性验证 32
恢复功能 33
基础设施安全性 33
配置和漏洞分析 33
安全最佳实践 34
授予 Amazon Health 用户可能的最低权限 34
查看 Amazon Personal Health Dashboard 34
集成Amazon Health与 Amazon Chime 或松弛 34
监控 Amazon Health 事件 34
聚合 Amazon Health 事件 35
Prerequisites 35
组织视图 (控制台) 35
启用组织视图 (控制台) 36
查看组织视图事件 (控制台) 36
查看受影响的帐户和资源（控制台） 37
禁用组织视图 (控制台) 38
组织视图 (CLI) 38
启用组织视图 (CLI) 39
查看组织视图事件 (CLI) 40
禁用组织视图 (CLI) 41
Amazon Health 组织视图 API 操作 41

监控Amazon Health事件与 CloudWatch 43
About (关于 Amazon Lumberyard)Amazon的区域Amazon Health 43
关于公共活动Amazon Health 44
为创建 CloudWatch Events 规则Amazon Health 44
为多个服务和类别创建规则 45
正在接收Amazon Health使用事件AmazonChatbot 46
Prerequisites 46
Amazon EC2 实例的自动化操作 47
Prerequisites 47
为 CloudWatch Events 创建规则 50
监控 Amazon Health 51
使用 Amazon CloudTrail 记录 Amazon Health API 调用 51
Amazon HealthCloudTrail 中的信息 51
示例：Amazon Health 日志文件条目 52
文档历史记录 54
早期更新 55
Amazon术语表 56
..... lvii

什么是 Amazon Health？

Amazon Health可持续查看您的资源性能和Amazon服务和帐户. 您可以使用Amazon Health 事件，了解服务和资源更改如何影响在Amazon。Amazon Health会及时提供相关信息，帮助您管理正在进行的事件。Amazon Health还可以帮助您了解计划的活动并做好准备。该服务会提供由 Amazon 资源运行状况变化触发的报警和通知，因此您可以近乎即时地了解事件和获得指导，以帮助加快故障排除。

所有客户都可以使用由 Amazon Health API 提供支持的 Amazon Personal Health Dashboard (PHD)。控制面板无需设置，可随时供用于身份验证Amazon用户 (p. 15)。有关服务亮点的更多信息，请参阅Amazon Personal Health Dashboard详细信息页面。

此外，拥有商业或企业支持计划的 Amazon Web Services Support 客户可以使用 Amazon Health API 集成内部和第三方系统。

主题

- 您是 Amazon Health 新用户吗？ (p. 1)

您是 Amazon Health 新用户吗？

如果您是第一次使用 Amazon Health 的用户，请从阅读以下部分开始：

- 什么是 Amazon Health？ (p. 1)-此部分描述了底层数据模型、它支持的操作，以及Amazon可以用来与服务交互的开发工具包。
- Amazon Personal Health Dashboard入门 (p. 2)— Amazon Personal Health Dashboard 部分将介绍使用 Amazon Personal Health Dashboard 查看事件和受影响的实体，并执行高级筛选。
- 访问 Amazon Health API (p. 5)— Amazon Health API 部分介绍检索事件和实体相关信息的操作。

Amazon Health 为所有客户提供名为 Amazon Personal Health Dashboard 的控制台。您无需写入代码或执行任何操作，即可设置控制面板。如果您拥有商业或企业 Support 计划，则可以编程方式访问显示在控制面板上的信息。可以使用Amazon命令行界面 (AmazonCLI) 或写入代码来发出请求，通过直接使用 REST API 或使用Amazon软件开发工具包。

有关使用的更多信息Amazon Health与AmazonCLI，请参阅Amazon适用于的 CLI 参考Amazon Health。有关安装AmazonCLI，请参阅。安装Amazon命令行界面。

Amazon Personal Health Dashboard 入门

您可以使用 Amazon Personal Health Dashboard 了解可能影响 Amazon 服务或账户的 Amazon Health 事件。Amazon Personal Health Dashboard 会以两种方式显示信息：显示按类别组织的最近和未来事件的控制面板，以及显示过去 90 天内所有事件的完整事件日志。

查看您的 Amazon Personal Health Dashboard

1. 登录 Amazon Web Services Management Console 并通过以下网址打开 Amazon Personal Health Dashboard：https://phd.aws.amazon.com/phd/home。
2. 选择 Dashboard (控制面板) 查看最近和未来事件，或选择 Event log (事件日志) 查看过去 90 天内的所有事件。

主题

- Dashboard (p. 2)
- 事件日志 (p. 2)
- Amazon CloudWatch Events (p. 4)
- 组织视图 (p. 4)

Dashboard

Amazon Personal Health Dashboard 会分三组管理问题：未处理问题、已计划更改和其他通知。默认情况下，未处理问题和其他通知仅限于开始时间在过去 7 天内的问题。已计划更改组包含正在进行或即将进行的项目。

在仪表板列表中选择事件时，事件详细信息窗格会显示，其中包含受事件影响的事件和资源的相关信息。有关更多信息，请参阅 事件详细信息窗格 (p. 3)。

通过从筛选条件列表选择选项，您可以筛选显示在任何组中的项目。例如，您可以按可用区、区域、事件结束时间或上次更新时间、Amazon 服务等条件缩小结果范围。

要查看所有事件，而不是在控制面板中显示的最近事件，请选择查看所有问题以打开事件日志 (p. 2)。

> **Note**
>
> 当前，您无法删除 Amazon Personal Health Dashboard 中显示的事件的通知。待 Amazon 服务解决事件后，通知自会从控制面板视图中删除。

事件日志

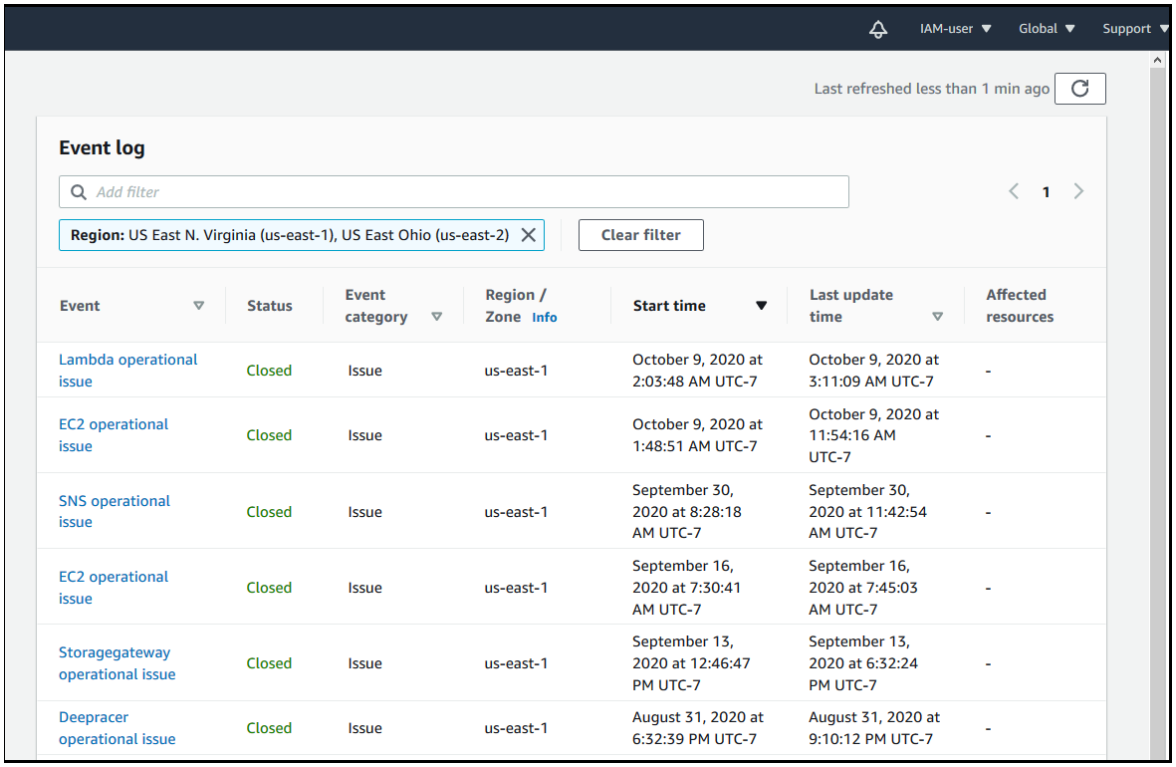
这些区域有：事件日志的页面Amazon Personal Health Dashboard显示所有Amazon Health适用于账户的事件。列布局和行为与控制面板相似，但日志页面包含适用于 Status (状态) 和 Event category (事件类别) 的其他列和筛选条件选项。

当您在事件日志列表中，事件详细信息窗格会显示，其中包含受事件影响的事件和资源的相关信息。有关更多信息，请参阅 事件详细信息窗格 (p. 3)。

通过从筛选条件列表选择选项，您可以筛选项目。例如，您可以按状态（已完结、未处理或即将到来）、事件类别（问题、通知或已计划更改）、可用区、区域、事件结束时间或上次更新时间、Amazon 服务等条件缩小结果范围。

Example：事件日志

以下屏幕截图仅显示了美国东部（弗吉尼亚北部）和美国东部（俄亥俄）区域的事件。



事件类型

有两种 Amazon Health 事件类型：

- 公有事件 是不特定于 Amazon 账户的服务事件。例如，如果存在与 Amazon Elastic Compute Cloud (Amazon EC2) 有关的问题，Amazon区域,Amazon Health提供有关事件的信息，即使您不使用该区域中的服务或资源也是如此。
- 特定于账户 的事件特定于您的 Amazon 账户或组织中的账户。例如，如果您使用的区域中存在与 Amazon EC2 实例有关的问题，则Amazon Health提供有关该事件和账户中受影响资源的信息。

您可以使用以下选项确定事件是公共事件还是特定于账户的事件：

- 在Amazon Personal Health Dashboard中，选择受影响的资源” 选项卡事件日志页. 具有资源的事件特定于您的账户。没有资源的事件是公开的，并不是特定于您的账户。有关更多信息，请参阅 Amazon Personal Health Dashboard入门 (p. 2)。
- 使用 Amazon Health API 返回 `eventScopeCode` 参数。事件可以具有 `PUBLIC`、`ACCOUNT_SPECIFIC` 或 `NONE` 值。有关更多信息，请参阅 。DescribeEventDetails中的操作Amazon HealthAPI 参考。

事件详细信息窗格

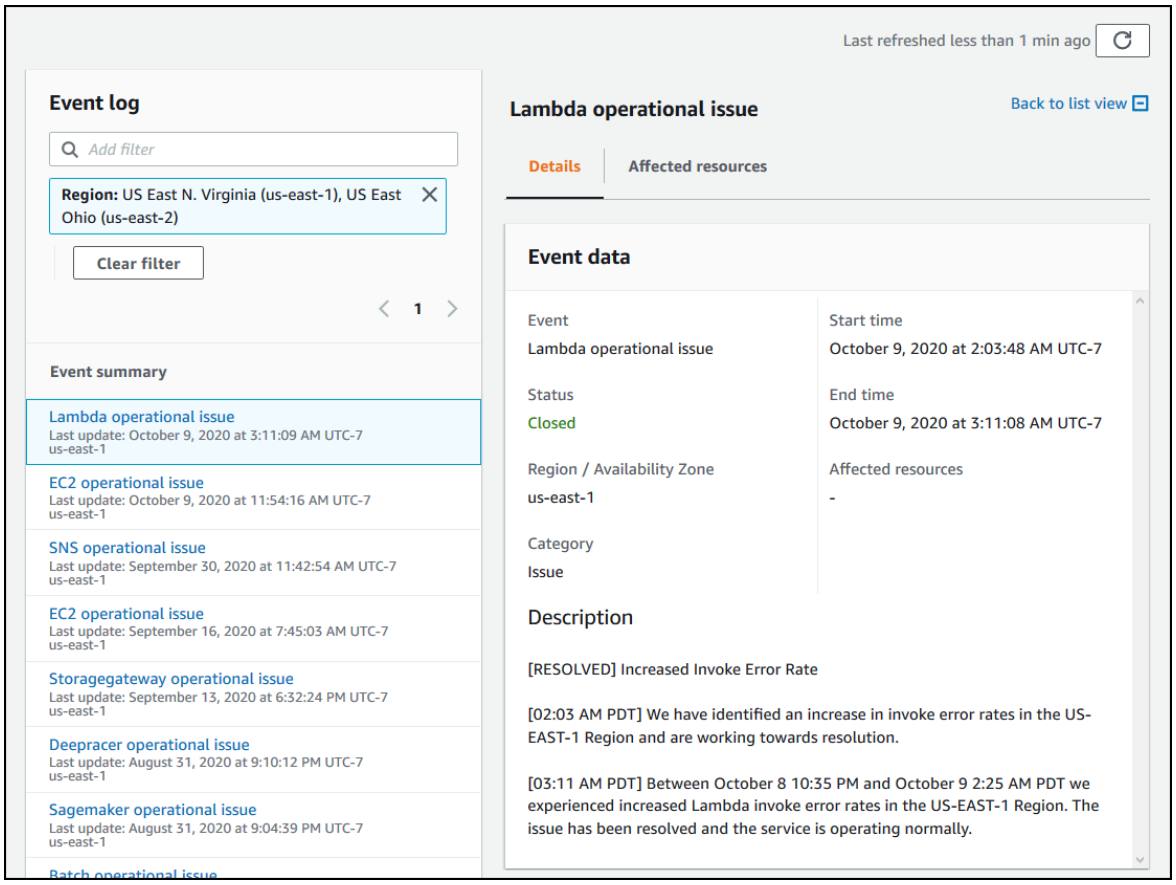
Event details (事件详细信息) 窗格有两个选项卡。Details 选项卡会显示事件的文本描述和事件的相关数据：事件名称、状态、区域和可用区、开始时间、结束时间和类别。这些区域有：受影响的资源选项卡显示有关任何Amazon受事件影响的资源：

- 资源 ID（例如，Amazon EBS 卷 ID）`vol-a1b2c34f`) 或 Amazon 资源名称 (ARN)。

通过从筛选条件列表选择选项，您可以筛选显示在资源列表中的项目。您可以按资源 ID 或 ARN 缩小结果范围.

Example ：Amazon Health的事件Amazon Lambda

以下屏幕截图显示了 Lambda 的示例事件和问题的描述。



Amazon CloudWatch Events

使用 Amazon CloudWatch Events 检测和响应Amazon Health事件. 您可以监控特定的Amazon Health事件中发生的Amazon帐户，然后设置规则，以便在事件发生变化时收到通知或采取措施。

组织视图

Amazon Health已与 集成Amazon Organizations，以便查看属于组织一部分的所有账户的事件。这为您提供了组织中显示的事件的集中式视图。您可以使用这些事件来监控资源、服务和应用程序中的更改。

有关更多信息，请参阅 使用组织视图跨账户聚合 Amazon Health 事件 (p. 35)。

访问 Amazon Health API

Amazon Health是一种 RESTful Web 服务，它使用 HTTPS 进行传输，并采用 JSON 作为消息序列化格式。您的应用程序代码可以直接向 Amazon Health API 发送请求。在您直接使用 REST API 时，您必须编写必要的代码来对您的请求签名以及验证您的请求。有关的更多信息Amazon Health操作和参数，请参阅Amazon HealthAPI 参考。

> Note
>
> 您必须拥有商业或企业支持计划来自Amazon Web Services Support要使用的Amazon HealthAPI。如果您调用Amazon Health使用的 APIAmazon帐户中没有商业或企业支持计划时，您会收到`SubscriptionRequiredException`错误。

您可以使用Amazon软件开发工具包来包装Amazon HealthREST API 调用，这可以简化您的应用程序开发。您可以指定您的Amazon凭证，这些库会为您处理身份验证和请求签名。

Amazon Health还提供了一个Amazon Personal Health Dashboard中的Amazon Web Services Management Console，您可以使用它查看并搜索事件和受影响的实体。请参阅 Amazon Personal Health Dashboard入门 (p. 2)。

Endpoints

这些区域有：Amazon HealthAPI 遵循多区域应用程序架构，并在主动-被动配置中具有两个区域终端节点。要支持主动-被动 DNS 故障转移，Amazon Health提供单个全局终端节点。您可以在全局终端节点上执行 DNS 查找以确定活动终端节点和相应的签名Amazon区域。这有助于您知道要在代码中使用哪个端点，以便您可以从Amazon Health。

当您向全局终端节点发出请求时，必须指定Amazon访问您目标的区域终端节点的凭据，并为您的区域配置签名。否则，您的身份验证可能会失败。有关更多信息，请参阅 签署 Amazon Health API 请求 (p. 10)。

下表列出了默认配置。

描述	签名区域	终端节点	协议
处于活动状态	cn-northwest-1	健康.cn-west-1.amazonaws.com.cn	HTTPS
被动	cn-north-1	健康.cn-北1.amazonaws.com.cn	HTTPS
服务全球	cn-northwest-1 Note 这是当前活动终端节点的签名区域。	全球健康	HTTPS

要确定终端节点是否是活跃终端节点，请在全球终端节点别名记录，然后提取Amazon来自已解析名称的区域。

Example ：全局终端节点上的 DNS 查找

以下命令在全球健康终端节点。然后，该命令将返回cn-northwest-1区域终端节点。此输出告诉你应该使用哪个端点Amazon Health。

```
dig global.health.amazonaws.com.cn  | grep CNAME
global.health.amazonaws.com.cn. 10 IN CNAME health.cn-northwest-1.amazonaws.com.cn
```

Tip

主动和被动端点都返回Amazon Health数据。然而，最新的Amazon Health数据仅可从活动端点获得。来自被动端点的数据最终将与主动端点保持一致。我们建议您在活动终端节点发生变化时重新启动任何工作流。

使用高可用性终端演示

在以下代码示例中，Amazon Health使用针对全局终端节点的 DNS 查找来确定活动的区域终端节点和签名区域。然后，如果活动终端节点发生更改，代码将重新启动工作流。

主题

- 使用 Java 演示 (p. 6)
- 使用 Python 演示 (p. 8)

使用 Java 演示

Prerequisite

您必须安装Gradle。

使用 Java 示例

1. 下载Amazon Health高可用性终端节点演示从 GitHub 中获取。
2. 导航到演示项目high-availability-endpoint/java目录。
3. 在命令行窗口中，输入以下命令。

```
gradle build
```

4. 输入以下命令以指定Amazon凭证。

```
export AWS_ACCESS_KEY_ID="AKIAIOSFODNN7EXAMPLE"
export AWS_SECRET_ACCESS_KEY="wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
export AWS_SESSION_TOKEN="your-aws-token"
```

5. 输入以下命令以运行演示。

```
gradle run
```

Example ：Amazon Health事件输出

代码示例返回最近的Amazon Health的过去七天内的事件Amazonaccount. 在下面的示例中，输出包含Amazon Health适用于的Amazon Config服务。

```
> Task :run
[main] INFO aws.health.high.availability.endpoint.demo.HighAvailabilityV2Workflow
 - EventDetails(Event=Event(Arn=arn:aws:health:global::event/CONFIG/
AWS_CONFIG_OPERATIONAL_NOTIFICATION/AWS_CONFIG_OPERATIONAL_NOTIFICATION_88a43e8a-
e419-4ca7-9baa-56bcde4dba3,
```

```
Service=CONFIG, EventTypeCode=AWS_CONFIG_OPERATIONAL_NOTIFICATION,
 EventTypeCategory=accountNotification, Region=global,
 StartTime=2020-09-11T02:55:49.899Z, LastUpdatedTime=2020-09-11T03:46:31.764Z,
StatusCode=open, EventScopeCode=ACCOUNT_SPECIFIC),
 EventDescription=EventDescription(LatestDescription=As part of our ongoing efforts
 to optimize costs associated with recording changes related to certain ephemeral
 workloads,
Amazon Config is scheduled to release an update to relationships modeled within
 ConfigurationItems (CI) for 7 EC2 resource types on August 1, 2021.
Examples of ephemeral workloads include changes to Amazon Elastic Compute Cloud (Amazon
 EC2) Spot Instances, Amazon Elastic MapReduce jobs, and Amazon EC2 Autoscaling.
This update will optimize CI models for EC2 Instance, SecurityGroup, Network Interface,
 Subnet, VPC, VPN Gateway, and Customer Gateway resource types to record direct
 relationships and deprecate indirect relationships.

A direct relationship is defined as a one-way relationship (A->B) between a resource
 (A) and another resource (B), and is typically derived from the Describe API response
 of resource (A).
An indirect relationship, on the other hand, is a relationship that Amazon Config
 infers (B->A), in order to create a bidirectional relationship.
For example, EC2 instance -> Security Group is a direct relationship, since security
 groups are returned as part of the describe API response for an EC2 instance.
But Security Group -> EC2 instance is an indirect relationship, since EC2 instances are
 not returned when describing an EC2 Security group.

Until now, Amazon Config has recorded both direct and indirect relationships. With
 the launch of Advanced queries in March 2019, indirect relationships can easily be
 answered by running Structured Query Language (SQL) queries such as:

SELECT
 resourceId,
 resourceType
WHERE
 resourceType ='AWS::EC2::Instance'
AND
 relationships.resourceId = 'sg-234213'

By deprecating indirect relationships, we can optimize the information contained within
 a
Configuration Item while reducing Amazon Config costs related to relationship changes.
This is especially useful in case of ephemeral workloads where there is a high volume
 of configuration changes for EC2 resource types.

Which resource relationships are being removed?

Resource Type: Related Resource Type
1 AWS::EC2::CustomerGateway: AWS::VPN::Connection
2 AWS::EC2::Instance: AWS::EC2::EIP, AWS::EC2::RouteTable
3 AWS::EC2::NetworkInterface: AWS::EC2::EIP, AWS::EC2::RouteTable
4 AWS::EC2::SecurityGroup: AWS::EC2::Instance, AWS::EC2::NetworkInterface
5 AWS::EC2::Subnet: AWS::EC2::Instance, AWS::EC2::NetworkACL,
 AWS::EC2::NetworkInterface, AWS::EC2::RouteTable
6 AWS::EC2::VPC: AWS::EC2::Instance, AWS::EC2::InternetGateway, AWS::EC2::NetworkACL,
 AWS::EC2::NetworkInterface, AWS::EC2::RouteTable, AWS::EC2::Subnet,
 AWS::EC2::VPNGateway, AWS::EC2::SecurityGroup
7 AWS::EC2::VPNGateway: AWS::EC2::RouteTable, AWS::EC2::VPNConnection

Alternate mechanism to retrieve this relationship information:
The SelectResourceConfig API accepts a SQL SELECT command, performs the corresponding
 search, and returns resource configurations matching the properties. You can use this
 API to retrieve the same relationship information.
For example, to retrieve the list of all EC2 Instances related to a particular VPC
 vpc-1234abc, you can use the following query:

SELECT
 resourceId,
```

```
 resourceType
WHERE
 resourceType ='AWS::EC2::Instance'
AND
 relationships.resourceId = 'vpc-1234abc'

If you have any questions regarding this deprecation plan, please contact Amazon
 Web Services Support [1]. Additional sample queries to retrieve the relationship
 information for the resources listed above is provided in [2].

[1] https://aws.amazon.com/support
[2] https://docs.aws.amazon.com/config/latest/developerguide/
examplerelationshipqueries.html),
EventMetadata={})
```

Java 资源

- 有关更多信息，请参阅 。界面健康客户端中的AmazonSDK for Java API 参考和源代码。
- 有关 DNS 查找演示中使用的库的更多信息，请参阅dnsjava，开发工 GitHub 的。

使用 Python 演示

Prerequisite

您必须安装Python 3。

使用 Python 示例

1. 下载Amazon Health高可用性终端节点演示从 GitHub 中获取。
2. 导航到演示项目`high-availability-endpoint/python`目录。
3. 在命令行窗口中，输入以下命令。

```
pip3 install virtualenv
virtualenv -p python3 v-aws-health-env
```

> **Note**
>
> 对于 Python 3.3 及更高版本，您可以使用内置的`venv`模块来创建虚拟环境，而不是安装`virtualenv`。有关更多信息，请参阅 。venv-创建虚拟环境在 Python 网站上。

```
python3 -m venv v-aws-health-env
```

4. 输入以下命令激活虚拟环境。

```
source v-aws-health-env/bin/activate
```

5. 输入以下命令以安装依赖关系。

```
pip install -r requirements.txt
```

6. 输入以下命令以指定Amazon凭证。

```
export AWS_ACCESS_KEY_ID="AKIAIOSFODNN7EXAMPLE"
export AWS_SECRET_ACCESS_KEY="wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
```

```
export AWS_SESSION_TOKEN="your-aws-token"
```

7. 输入以下命令以运行演示。

```
python3 main.py
```

Example ：Amazon Health事件输出

代码示例返回最近的Amazon Health的过去七天内的事件Amazonaccount. 以下输出返回Amazon Health适用于的事件Amazon安全通知功能.

```
INFO:botocore.credentials:Found credentials in environment variables.
INFO:root:Details: {'arn': 'arn:aws:health:global::event/SECURITY/
AWS_SECURITY_NOTIFICATION/AWS_SECURITY_NOTIFICATION_0e35e47e-2247-47c4-
a9a5-876544042721',
'service': 'SECURITY', 'eventTypeCode': 'AWS_SECURITY_NOTIFICATION',
 'eventTypeCategory': 'accountNotification', 'region': 'global', 'startTime':
 datetime.datetime(2020, 8, 19, 23, 30, 42, 476000,
tzinfo=tzlocal()), 'lastUpdatedTime': datetime.datetime(2020, 8, 20, 20, 44, 9, 547000,
 tzinfo=tzlocal()), 'statusCode': 'open', 'eventScopeCode': 'PUBLIC'}, description:
{'latestDescription': 'This is the second notice regarding TLS requirements on FIPS
 endpoints.\n\nWe
are in the process of updating all Amazon Federal Information Processing Standard
 (FIPS) endpoints across all Amazon regions
to Transport Layer Security (TLS) version 1.2 by March 31, 2021 . In order to avoid an
 interruption in service, we encourage you to act now, by ensuring that you connect to
 Amazon FIPS endpoints at a TLS version of 1.2.
If your client applications fail to support TLS 1.2 it will result in connection
 failures when TLS versions below 1.2 are no longer supported.\n\nBetween now and March
 31, 2021 Amazon will remove TLS 1.0 and TLS 1.1 support from each FIPS endpoint where
 no connections below TLS 1.2 are detected over a 30-day period.
After March 31, 2021 we may deploy this change to all Amazon FIPS endpoints, even if
 there continue
to be customer connections detected at TLS versions below 1.2. \n\nWe will provide
 additional updates and reminders on the Amazon Security Blog, with a ‘TLS’ tag [1].
 If you need further guidance or assistance, please contact Amazon Web Services Support
 [2] or your Technical Account Manager (TAM).
Additional information is below.\n\nHow can I identify clients that are connecting with
 TLS
1.0/1.1?\nFor customers using S3 [3], Cloudfront [4] or Application Load Balancer [5]
 you can use
your access logs to view the TLS connection information for these services, and
 identify client
connections that are not at TLS 1.2. If you are using the Amazon Developer Tools on
 your clients,
you can find information on how to properly configure your client’s TLS versions by
 visiting Tools to Build on Amazon [7] or our associated Amazon Security Blog has a
 link for each unique code language [7].\n\nWhat is Transport Layer Security (TLS)?
\nTransport Layer Security (TLS Protocols) are cryptographic protocols designed to
 provide secure communication across a computer network
[6].\n\nWhat are Amazon FIPS endpoints? \nAll Amazon services offer Transport Layer
 Security (TLS) 1.2 encrypted endpoints that can be used for all API calls. Some Amazon
 services also offer FIPS 140-2 endpoints [9] for customers that require use of FIPS
 validated cryptographic libraries. \n\n[1] https://aws.amazon.com/blogs/security/tag/
tls/\n[2] https://aws.amazon.com/support\n[3]
https://docs.aws.amazon.com/AmazonS3/latest/dev/LogFormat.html\n[4] https://
docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html\n[5]
 https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-
access-logs.html\n[6] https://aws.amazon.com/tools\n[7] https://aws.amazon.com/blogs/
security/tls-1-2-to-become-the-minimum-for-all-aws-fips-endpoints\n[8]
https://en.wikipedia.org/wiki/Transport_Layer_Security\n[9] https://aws.amazon.com/
compliance/fips'}
```

8. 当您完成后，输入以下命令停用虚拟机。

```
deactivate
```

Python 资源

- 有关的更多信息`Health. Client`，请参阅Amazon适用 SDK for Python (Boto3) API 参考。
- 有关 DNS 查找演示中使用的库的更多信息，请参阅第三次马拉松工具包和源代码（位于 GitHub 上）。

签署 Amazon Health API 请求

当您使用Amazon开发工具包或Amazon命令行界面 (AmazonCLI) 发出请求Amazon时，这些工具会自动使用您在配置工具时指定的访问密钥为您签署请求。例如，如果您使用AmazonSDK for Java 进行之前的高可用性终端演示，您不必亲自签署请求。

Java 代码示例

有关如何使用Amazon Health使用的 APIAmazonSDK for Java，请参阅示例代码 (p. 11)。

当您提出请求时，我们强烈建议您不要使用Amazon根帐户凭据，以便常规访问Amazon Health。您可以使用 IAM 用户的凭证。有关更多信息，请参阅 。隐藏您的Amazon账户根用户访问密钥中的IAM 用户指南。

如果您没有使用Amazon开发工具包或AmazonCLI，那么您必须亲自签署您的请求。建议使用Amazon签名版本 4。有关更多信息，请参阅 。签名AmazonAPI 请求中的Amazon一般参考。

Amazon Health 中支持的操作

Amazon Health 支持以下获取会影响 Amazon 账户的事件相关信息的操作：

- Amazon Health 支持的事件类型。
- 有关匹配特定筛选条件的一个或多个事件的信息。
- 有关受一个或多个事件影响的实体的信息。
- 匹配特定筛选条件的事件或实体的分类计数。

所有操作均为非更改操作。也就是说，它们会检索数据，但不会进行修改。以下部分概述了 Amazon Health 操作：

事件类型

DescribeEventTypes 操作会检索匹配可选指定筛选条件的事件类型。事件类型是事件的Amazon服务、事件类型代码和类别。事件类型和事件与面向对象编程中的类和对象相似。Amazon Health 支持的事件类型数随时间增长。

Events

DescribeEvents 操作会检索有关 Amazon 账户关联事件的摘要信息。事件可与 Amazon 操作问题、Amazon 基础设施的已计划更改或安全性和账单通知关联。DescribeEventDetails 操作会检索有关一个或多个事件的详细信息，例如 Amazon 服务、区域、可用区、事件开始和结束时间以及文本描述。

受影响的实体

DescribeAffectedEntities 操作会检索有关受一个或多个事件影响的实体的信息。结果可以按其他条件进行筛选，包括可为 Amazon 资源分配的状态。

Aggregation

DescribeEventAggregates 操作会检索每个事件类型类别中的事件计数，也可由其他条件筛选。DescribeEntityAggregates 操作会检索受一个或多个指定事件影响的实体 (资源) 计数。

DescribeHealthServiceStatusForOrganization

DescribeHealthServiceStatusForOrganization操作提供有关启用或禁止的状态信息Amazon Health与您的组织合作

有关这些操作的更多信息，请参阅Amazon HealthAPI 参考。

适用于 Amazon Health API 的 Java 代码示例

以下 Java 代码示例将演示如何初始化 Amazon Health 客户端，并检索有关事件和实体的信息。

第 1 步：初始化凭据

需要有效凭证，才可以与 Amazon Health API 进行通信。您 key pair 以使用与Amazonaccount.

创建并初始化 AWSCredentials 实例：

```
AWSCredentials credentials = null;
try {
       credentials = new ProfileCredentialsProvider("default").getCredentials();
} catch (Exception e) {
throw new AmazonClientException(
   "Cannot load the credentials from the credential profiles file. "
   + "Please make sure that your credentials file is at the correct "
   + "location (/home/username/.aws/credentials), and is in valid format.", e);
}
```

第 2 步：初始化Amazon HealthAPI 客户端

使用上一步中的初始化凭证对象来创建 Amazon Health 客户端：

```
import com.amazonaws.services.health.AWSHealthClient;

AWSHealth awsHealthClient = new AWSHealthClient(credentials);
```

第 3 步：使用Amazon HealthAPI 操作获取事件信息

DescribeEvents

```
import com.amazonaws.services.health.model.DescribeEventsRequest;
import com.amazonaws.services.health.model.DescribeEventsResult;
import com.amazonaws.services.health.model.Event;
import com.amazonaws.services.health.model.EventFilter;

DescribeEventsRequest request = new DescribeEventsRequest();

EventFilter filter = new EventFilter();
```

```
// Filter on any field from the supported Amazon Health EventFilter model.
// Here is an example for Region cn-northwest-1 events from the EC2 service.
filter.setServices(singletonList("EC2"));
filter.setRegions(singletonList("cn-northwest-1"));
request.setFilter(filter);

DescribeEventsResult response = awsHealthClient.describeEvents(request);
List<Event> resultEvents = response.getEvents();

Event currentEvent = null;
for (Event event : resultEvents) {
    // Display result event data; here is a subset.
    System.out.println(event.getArn());
    System.out.println(event.getService());
    System.out.println(event.getRegion());
    System.out.println(event.getAvailabilityZone());
    System.out.println(event.getStartTime());
    System.out.println(event.getEndTime());
 }
```

DescribeEventAggregates

```
import com.amazonaws.services.health.model.DescribeEventAggregatesRequest;
import com.amazonaws.services.health.model.DescribeEventAggregatesResult;
import com.amazonaws.services.health.model.EventAggregate;
import com.amazonaws.services.health.model.EventFilter;

DescribeEventAggregatesRequest request = new DescribeEventAggregatesRequest();
// set the aggregation field
request.setAggregateField("eventTypeCategory");

// filter more on result if needed
EventFilter filter = new EventFilter();
filter.setRegions(singleton("cn-northwest-1"));
request.setFilter(filter);

DescribeEventAggregatesResult response = awsHealthClient.describeEventAggregates(request);

// print event count for each eventTypeCategory
for (EventAggregate aggregate: response.getEventAggregates()) {
    System.out.println("Event Category:" + aggregate.getAggregateValue());
    System.out.println("Event Count:" + aggregate.getCount());
 }
```

DescribeEventDetails

```
import com.amazonaws.services.health.model.DescribeEventDetailsRequest;
import com.amazonaws.services.health.model.DescribeEventDetailsResult;
import com.amazonaws.services.health.model.Event;
import com.amazonaws.services.health.model.EventDetails;


DescribeEventDetailsRequest describeEventDetailsRequest = new
 DescribeEventDetailsRequest();
// set event ARN and local value

describeEventDetailsRequest.setEventArns(singletonList("arn:aws:health:cn-
northwest-1::event/service/eventTypeCode/eventId"));
describeEventDetailsRequest.setLocale("en-US");
filter.setEventArns
DescribeEventDetailsResult describeEventDetailsResult =
 awsHealthClient.describeEventDetails(request);
EventDetails eventDetail = describeEventDetailsResult.getSuccessfulSet().get(0);
```

```
// check event-related fields
Event event = eventDetail.getEvent();
System.out.println(event.getService());
System.out.println(event.getRegion());
System.out.println(event.getAvailabilityZone());
System.out.println(event.getStartTime());
System.out.println(event.getEndTime());

// print out event description
System.out.println(eventDetail.getEventDescription().getLatestDescription());
```

DescribeAffectedEntities

```
import com.amazonaws.services.health.model.AffectedEntity;
import com.amazonaws.services.health.model.DateTimeRange;
import com.amazonaws.services.health.model.DescribeAffectedEntitiesRequest;
import
 com.amdescribeEventDetailsRequestazonaws.services.health.model.DescribeAffectedEntitiesResult;

DescribeAffectedEntitiesRequest request = new DescribeAffectedEntitiesRequest();
EntityFilter filter = new EntityFilter();

filter.setEventArns(singletonList("arn:aws:health:cn-
northwest-1::event/service/eventTypeCode/eventId"));

DescribeAffectedEntitiesResult response =
 awsHealthClient.describeAffectedEntities(request);

for (AffectedEntity affectedEntity: response.getEntities()) {
    System.out.println(affectedEntity.getEntityValue());
    System.out.println(affectedEntity.getAwsAccountId());
    System.out.println(affectedEntity.getEntityArn());
 }
```

DescribeEntityAggregates

```
import com.amazonaws.services.health.model.DescribeEntityAggregatesRequest;
import com.amazonaws.services.health.model.DescribeEntityAggregatesResult;
import com.amazonaws.services.health.model.EntityAggregate;

DescribeEntityAggregatesRequest request = new DescribeEntityAggregatesRequest();

request.setEventArns(singletonList("arn:aws:health:cn-
northwest-1::event/service/eventTypeCode/eventId"));

DescribeEntityAggregatesResult response =
 awsHealthClient.describeEntityAggregates(request);

for (EntityAggregate entityAggregate : response.getEntityAggregates()) {
    System.out.println(entityAggregate.getEventArn());
    System.out.println(entityAggregate.getCount());
 }
```

Amazon Health 中的安全性

Amazon 的云安全性的优先级最高。为了满足对安全性最敏感的组织的需求，我们打造了具有超高安全性的数据中心和网络架构。作为 Amazon 客户，您也将从这些数据中心和网络架构受益。

安全性是 Amazon 和您的共同责任。责任共担模式将其描述为云的安全性和云中的安全性：

- 云的安全性–Amazon负责保护运行Amazon中的服务Amazon云。Amazon还向您提供可安全使用的服务。作为 Amazon 合规性计划的一部分，第三方审计人员将定期测试和验证安全性的有效性。要了解适用于 Amazon Health，请参阅Amazon合规性计划范围内的服务。
- 云中的安全性— 您的责任由Amazon服务。您是还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

该文档帮助您了解如何在使用 Amazon Health 时应用责任共担模式。以下主题说明如何配置 Amazon Health 以实现您的安全性和合规性目标。您还会了解如何使用其他 Amazon 服务以帮助您监控和保护 Amazon Health 资源。

主题

- Amazon Health 中的数据保护 (p. 14)
- 适用于 Amazon Health 的 Identity and Access Management (p. 15)
- Amazon Health 中的日志记录和监控 (p. 32)
- Amazon Health 的合规性验证 (p. 32)
- Amazon Health 中的恢复功能 (p. 33)
- Amazon Health 中的基础设施安全性 (p. 33)
- Amazon Health 中的配置和漏洞分析 (p. 33)
- Amazon Health 的安全最佳实践 (p. 34)

Amazon Health 中的数据保护

这些区域有：Amazon 责任共担模式适用于中的数据保护Amazon Health。如本模型所述,Amazon负责保护运行所有Amazon云。您负责维护对托管在此基础设施上的内容的控制。此内容包括安全配置和管理任务。Amazon使用的服务。有关数据隐私的更多信息，请参阅数据隐私常见问题。

出于数据保护目的，我们建议您保护Amazon账户凭证并使用 AWS Identity and Access Management (IAM) 设置单独的用户账户。这仅向每个用户授予履行其工作职责所需的权限。我们还建议您通过以下方式保护您的数据：

- 对每个账户使用 Multi-Factor Authentication (MFA)。
- 使用 SSL/TLS 与 Amazon 资源进行通信。建议使用 TLS 1.2 或更高版本。
- 使用 Amazon CloudTrail 设置 API 和用户活动日志记录。
- 使用 Amazon 加密解决方案以及 Amazon 服务中的所有默认安全控制。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的个人数据。
- 如果在通过命令行界面或 API 访问 Amazon 时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 终端节点。有关可用的 FIPS 终端节点的更多信息，请参阅美国联邦信息处理标准 (FIPS) 第 140-2 版。

我们强烈建议您切勿将敏感的可识别信息（例如您客户的账号）放入自由格式字段（例如 Name (名称) 字段）。这包括使用时Amazon Health或其他Amazon服务使用控制台、API、AmazonCLI 或Amazon开发工具

包。您输入到 Amazon Health 或其他服务中的任何数据都可能被选取以包含在诊断日志中。当您向外部服务器提供 URL 时，请勿在 URL 中包含凭证信息来验证您对该服务器的请求。

数据加密

请参阅以下有关 Amazon Health 如何加密数据的信息。

数据加密是指在传输过程中（当数据从服务传输到您的 Amazon 账户时）和静态数据（当数据存储在 Amazon 服务中时）保护数据。您可以使用传输层安全性 (TLS) 保护传输中的数据，或使用客户端加密保护静态数据。

Amazon Health 不会在事件中记录个人身份信息 (PII)，例如电子邮件地址或客户名称。

静态加密

由 Amazon Health 存储的所有数据都是静态加密的。

传输中加密

通过 Amazon Health 收发的所有数据都会在传输过程中加密。

密钥管理

Amazon Health 不支持将客户托管的加密密钥用于 Amazon 云中加密的数据。

互联网络流量隐私

请参阅以下有关 Amazon Health 如何处理流量隐私的信息。

您可以启用 Amazon Health 来处理 Amazon Organizations，以便查看属于组织一部分的各个 Amazon 账户中的事件。此功能为您提供所有 Amazon Health 事件的集中视图，其中包括操作问题、计划维护和账户通知。

为此，您必须使用组织的管理账户登录并从Amazon Web Services Management Console或使用EnableHealthServiceAccessForOrganizationAPI 操作。

有关更多信息，请参阅 使用组织视图跨账户聚合 Amazon Health 事件 (p. 35)。

适用于 Amazon Health 的 Identity and Access Management

AWS Identity and Access Management (IAM) 是Amazon服务，可以帮助管理员安全地控制对Amazon资源的费用。IAM 管理员控制谁可以身份验证(已登录) 和Augency（具有权限）使用Amazon Health资源的费用。IAM 是一个Amazon服务，您可以免费使用。

主题

- Audience (p. 16)
- 使用身份进行身份验证 (p. 16)
- 使用策略管理访问 (p. 17)
- Amazon Health 如何与 IAM 协同工作 (p. 19)
- Amazon Health 基于身份的策略示例 (p. 22)

- 对 Amazon Health 身份和访问进行故障排除 (p. 30)
- 将服务相关角色用于 Amazon Health (p. 31)

Audience

您使用 AWS Identity and Access Management (IAM) 的方式有所不同，具体取决于您在中完成的工作。Amazon Health。

服务用户— 如果您使用Amazon Health服务来完成工作，然后您的管理员会为您提供所需的凭证和权限。当您使用更多 Amazon Health 功能来完成工作时，您可能需要额外权限。了解如何管理访问权限可帮助您向管理员请求适合的权限。如果您无法访问 Amazon Health 中的一项功能，请参阅对 Amazon Health 身份和访问进行故障排除 (p. 30)。

服务管理员— 如果你负责Amazon Health资源，则您可能具有的完全访问权限。Amazon Health。您有责任确定您的员工应访问哪些 Amazon Health 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要了解有关您的公司如何将 IAM 与 Amazon Health 搭配使用的更多信息，请参阅Amazon Health 如何与 IAM 协同工作 (p. 19)。

IAM 管理员— 如果您是 IAM 管理员，您可能希望了解有关您可以如何编写策略以管理访问权限的详细信息。Amazon Health。要查看您可在 IAM 中使用的 Amazon Health 基于身份的策略示例，请参阅 Amazon Health 基于身份的策略示例 (p. 22)。

使用身份进行身份验证

身份验证是您使用身份凭证登录 Amazon 的方法。有关如何使用Amazon Web Services Management Console，请参阅登录到Amazon Web Services Management Console作为 IAM 用户或根用户中的IAM 用户指南。

您必须是身份验证（登录到Amazon）作为Amazon账户根用户、IAM 用户或代入 IAM 角色。您还可以使用公司的单一登录身份验证方法，甚至使用 Google 或 Facebook 登录。在这些情况下，您的管理员以前使用 IAM 角色设置了联合身份验证。在您使用来自其他公司的凭证访问 Amazon 时，您间接地代入了角色。

要直接登录到Amazon Web Services Management Console中，请将您的密码与您的根用户电子邮件地址或 IAM 用户名一起使用。您可以访问Amazon以编程方式使用根用户或 IAM 用户访问密钥。Amazon提供了开发工具包和命令行工具，以使用您的凭证对您的请求进行加密签名。如果您不使用 Amazon 工具，则必须自行对请求签名。使用签名版本 4（用于对入站 API 请求进行验证的协议）完成此操作。有关验证请求的更多信息，请参阅。签名版本 4 签名过程中的Amazon一般参考。

无论使用何种身份验证方法，您可能还需要提供其他安全信息。例如，Amazon 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅在中使用多重身份验证 (MFA)Amazon中的IAM 用户指南。

Amazon 账户根用户

当您首次创建 Amazon 账户时，最初使用的是一个对账户中所有 Amazon 服务和资源有完全访问权限的单点登录身份。此身份称为Amazon账户根用户，可使用您创建账户时所用的电子邮件地址和密码登录来访问。强烈建议您不使用根用户执行日常任务，即使是管理任务。相反，请遵循仅使用根用户创建您的第一个 IAM 用户的最佳实践。然后请妥善保存根用户凭证，仅用它们执行少数账户和服务管理任务。

IAM 用户和组

一个IAM 用户是您的Amazon账户具有某个人员或应用程序的特定权限。IAM 用户可能具有长期凭证，例如用户名和密码或一组访问密钥。要了解如何生成访问密钥，请参阅管理 IAM 用户的访问密钥中的IAM 用户指南。为 IAM 用户生成访问密钥时，请确保查看并安全保存密钥对。您以后无法找回秘密访问密钥，而是必须生成新的访问密钥对。

IAM 组 是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅何时创建 IAM 用户（而不是角色）中的IAM用户指南。

IAM 角色

一个IAM 角色是您的Amazon具有特定权限的账户。它类似于 IAM 用户，但与特定人员不关联。您可以在Amazon Web Services Management Console由切换角色。您可以调用AmazonCLI 或AmazonAPI 操作或使用自定义 URL。有关使用角色的方法的更多信息，请参阅。使用 IAM 角色中的IAM 用户指南。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 临时 IAM 用户权限 – IAM 用户可以代入 IAM 角色，以暂时获得不同的权限以执行特定的任务。
- 联合身份用户访问— 您可以不创建 IAM 用户，而是使用来自Amazon Directory Service、您的企业用户目录或 Web 身份提供商。它们被称为联合身份用户。Amazon在请求访问权限时，将为联合身份用户分配角色。身份提供商。有关联合身份用户的更多信息，请参阅。联合身份用户和角色中的IAM 用户指南。
- 跨账户访问 – 您可以使用 IAM 角色以允许不同账户中的某个人（可信委托人）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些 Amazon 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅IAM 角色与基于资源的策略的差异中的IAM 用户指南。
- 跨服务访问— 一段时间Amazon服务使用其他Amazon服务。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 Amazon S3 中存储对象。服务可能会使用发出调用的委托人的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 委托人权限— 当您使用 IAM 用户或角色在Amazon，您将被视为委托人。策略向委托人授予权限。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中触发另一个操作。在这种情况下，您必须具有执行这两个操作的权限。要查看某个操作是否需要策略中的其他相关操作，请参阅的操作、资源和条件键Amazon Health中的服务授权参考。
  - 服务角色 – 服务角色是服务代表您执行操作的 IAM 角色。服务角色只在您的账户内提供访问权限，不能用于为访问其他账户中的服务授权。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅 。创建向委派权限的角色Amazon服务中的IAM 用户指南。
  - 服务相关角色— 服务相关角色是一种服务角色，它与Amazon服务。服务可以代入代表您执行操作的角色。服务相关角色显示在您的 IAM 账户中，并归该服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 Amazon EC2 上运行的应用程序— 您可以使用 IAM 角色管理在 EC2 实例上运行的应用程序的临时凭证并使AmazonCLI 或AmazonAPI 请求。这优先于在 EC2 实例中存储访问密钥。要将 Amazon 角色分配给 EC2 实例并使其对该实例的所有应用程序可用，您可以创建一个附加到实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅 。使用 IAM 角色向 Amazon EC2 实例上运行的应用程序授予权限中的IAM 用户指南。

要了解使用 IAM 角色还是 IAM 用户，请参阅何时创建 IAM 角色（而不是用户）中的IAM 用户指南。

使用策略管理访问

您可以控制Amazon创建策略并将其附加到 IAM 身份或Amazon资源的费用。策略是 Amazon中的对象；在与标识或资源相关联时，策略定义它们的权限。您可以通过 root 用户或 IAM 用户身份登录，也可以代入 IAM 角色。当您提出请求时，Amazon评估相关的基于身份或基于资源的策略。策略中的权限确定是允许还是拒绝请求。大多数策略在 Amazon 中存储为 JSON 文档。有关 JSON 策略文档的结构和内容的更多信息，请参阅JSON 策略概述中的IAM 用户指南。

管理员可以使用AmazonJSON 策略来指定谁可以访问哪些内容。也就是说，这委托人可以执行操作上的resources，并根据什么条件。

每个 IAM 实体（用户或角色）最初没有任何权限。换言之，默认情况下，用户什么都不能做，甚至不能更改他们自己的密码。要为用户授予执行某些操作的权限，管理员必须将权限策略附加到用户。或者，管理员可以将用户添加到具有预期权限的组中。当管理员为某个组授予访问权限时，该组内的全部用户都会获得这些访问权限。

IAM 策略定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设您有一个允许 `iam:GetRole` 操作的策略。具有该策略的用户可以从Amazon Web Services Management Console，AmazonCLI 或 AmazonAPI。

基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅。创建 IAM 策略中的IAM 用户指南。

基于身份的策略可以进一步归类为内联策略或托管策略。内联策略直接嵌入单个用户、组或角色中。托管策略是可以附加到 Amazon 账户中的多个用户、组和角色的独立策略。托管策略包括 Amazon 托管策略和客户托管策略。要了解如何在托管策略或内联策略之间选择，请参阅在托管策略与内联策略之间进行选择中的IAM 用户指南。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略 和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定委托人可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定委托人。委托人可以包括账户、用户、角色、联合身份用户或Amazon服务。

基于资源的策略是位于该服务中的内联策略。您不能使用Amazon托管策略中的权限。

Amazon Health 支持基于资源的条件。您可以指定用户可以查看的 Amazon Health 事件。例如，您可以创建一个策略，该策略仅允许 IAM 用户访问Amazon Personal Health Dashboard。

有关更多信息，请参阅 Resources (p. 20)。

访问控制列表

访问控制列表 (ACL) 控制哪些委托人（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Amazon S3Amazon WAF和 Amazon VPC 是支持 ACL 的服务示例。要了解有关 ACL 的更多信息，请参阅访问控制列表 (ACL) 概述中的Amazon Simple Storage Service 开发人员指南。

Amazon Health 不支 ACL。

其他策略类型

Amazon 支持额外的、不太常用的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界 – 权限边界是一个高级功能，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体的基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅。IAM 实体的权限边界中的IAM 用户指南。
- 服务控制策略 (SCP)— SCP 是指定组织或组织单位 (OU) 的最大权限的 JSON 策略。Amazon Organizations。Amazon Organizations是用于分组和集中管理多个服务Amazon您的企业拥有的账户。如果在组织内启用了所有功能，则可对任意或全部账户应用服务控制策略 (SCP)。SCP 限制成员账户中实体

的权限，包括每个Amazon账户根用户。有关 Organizations 和 SCP 的更多信息，请参阅。SCP 的工作方式中的Amazon Organizations用户指南。

- 会话策略 – 会话策略是当您以编程方式为角色或联合身份用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅 。会话策略中的IAM 用户指南。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解如何操作Amazon确定在涉及多种策略类型时是否允许请求，请参阅策略评估逻辑中的IAM 用户指南。

Amazon Health 如何与 IAM 协同工作

在您使用 IAM 管理对的访问Amazon Health，您应该了解哪些 IAM 功能可与协同工作。Amazon Health。要获取简要视图，请了解Amazon Health和其他Amazon服务与 IAM 配合使用，请参阅Amazon与 IAM 结合使用的服务中的IAM 用户指南。

主题

- Amazon Health 基于身份的策略 (p. 19)
- Amazon Health 基于资源的策略 (p. 21)
- 基于 Amazon Health 标签的授权 (p. 21)
- Amazon HealthIAM 角色 (p. 22)

Amazon Health 基于身份的策略

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。Amazon Health支持特定的操作、资源和条件键。要了解在 JSON 策略中使用的所有元素，请参阅IAM JSON 策略元素参考中的IAM 用户指南。

Actions

管理员可以使用AmazonJSON 策略来指定谁可以访问哪些内容。也就是说，这委托人可以执行操作上的resources，并根据什么条件。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 Amazon API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 操作。还有一些操作要求在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行相关操作的权限。

中的策略操作Amazon Health在操作前使用以下前缀：`health:`。 例如，要授予某人查看有关指定事件的详细信息的权限。DescribeEventDetailsAPI 操作时，您可以包含`heath:DescribeEventDetails`在策略中的操作。

策略语句必须包括 `Action` 或 `NotAction` 元素。Amazon Health 定义了自己的一组操作，这些操作描述了可使用该服务执行的任务。

要在单个语句中指定多项操作，请使用逗号将它们隔开，如下所示。

```
"Action": [
      "health:action1",
      "health:action2"
```

您也可以使用通配符 (*) 指定多个操作。例如，要指定以单词 `Describe` 开头的所有操作，请包括以下操作。

```
"Action": "health:Describe*"
```

要查看的列表Amazon Health操作，请参阅定义的操作Amazon Health中的IAM 用户指南。

Resources

管理员可以使用AmazonJSON 策略来指定谁可以访问哪些内容。也就是说，这委托人可以执行操作上的resources，并根据什么条件。

`Resource` JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 `Resource` 或 `NotResource` 元素。作为最佳实践，请使用其 Amazon 资源名称 (ARN)指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符 (*) 指示语句应用于所有资源。

```
"Resource": "*"
```

Amazon Health 事件具有以下 Amazon 资源名称 (ARN) 格式。

```
arn:${Partition}:health:*::event/service/event-type-code/event-ID
```

例如，要在语句中指定 `EC2_INSTANCE_RETIREMENT_SCHEDULED_ABC123-DEF456` 事件，请使用以下 ARN。

```
"Resource": "arn:aws:health:*::event/EC2/EC2_INSTANCE_RETIREMENT_SCHEDULED/
EC2_INSTANCE_RETIREMENT_SCHEDULED_ABC123-DEF456"
```

要指定所有Amazon Health事 Amazon EC2 请使用通配符 (*)。

```
"Resource": "arn:aws:health:*::event/EC2/*/*"
```

有关 ARN 格式的更多信息，请参阅 Amazon 资源名称 (ARN) 和 Amazon 服务命名空间。

无法对特定资源执行某些 Amazon Health 操作。在这些情况下，您必须使用通配符 (*)。

```
"Resource": "*"
```

Amazon Health API 操作可能涉及多种资源。例如，DescribeEvents 操作返回有关满足指定筛选条件的事件的信息。这意味着 IAM 用户必须具有查看此事件的权限。

要在单个语句中指定多个资源，请使用逗号分隔 ARN。

```
"Resource": [
      "resource1",
      "resource2"
```

Amazon Health 对于运行状况事件仅支持资源级权限，并且对于 DescribeAffectedEntities 和 DescribeEventDetails API 操作仅支持资源级权限。有关更多信息，请参阅 基于资源和基于操作的条件 (p. 28)。

要查看的列表Amazon Health资源类型及其 ARN 的信息，请参阅定义的资源Amazon Health中的IAM 用户指南。要了解您可以在哪些操作中指定每个资源的 ARN，请参阅 Amazon Health 定义的操作。

条件键

管理员可以使用AmazonJSON 策略来指定谁可以访问哪些内容。也就是说，这委托人可以执行操作上的resources，并根据什么条件。

在 `Condition` 元素（或 `Condition` 块）中，可以指定语句生效的条件。`Condition` 元素是可选的。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 `Condition` 元素，或在单个 `Condition` 元素中指定多个键，则 Amazon 使用逻辑 `AND` 运算评估它们。如果您为单个条件键指定多个值，则 Amazon 使用逻辑 `OR` 运算来评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅 。IAM 策略元素：变量和标签中的IAM 用户指南。

Amazon支持全局条件键和特定于服务的条件键。要查看所有Amazon全局条件键，请参阅Amazon全局条件上下文键中的IAM 用户指南。

Amazon Health 定义了自己的一组条件键，还支持使用一些全局条件键。要查看所有Amazon全局条件键，请参阅Amazon全局条件上下文键中的IAM 用户指南。

DescribeAffectedEntities 和 DescribeEventDetails API 操作支持 `health:eventTypeCode` 和 `health:service` 条件键。

要查看的列表Amazon Health条件键，请参阅的条件键Amazon Health中的IAM 用户指南。要了解您可以对哪些操作和资源使用条件键，请参阅 Amazon Health 定义的操作。

Examples

要查看 Amazon Health 基于身份的策略的示例，请参阅Amazon Health 基于身份的策略示例 (p. 22)。

Amazon Health 基于资源的策略

基于资源的策略是 JSON 策略文档，它们指定了指定委托人可在 Amazon Health 资源上执行的操作以及在什么条件下可执行这些操作。Amazon Health 对于运行状况事件支持基于资源的权限策略。基于资源的策略允许您基于资源向其他账户授予使用权限。您也可以使用基于资源的策略以允许 Amazon 服务访问您的 Amazon Health 事件。

要启用跨账户访问，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的委托人。将跨账户委托人添加到基于资源的策略只是建立信任关系工作的一半而已。当委托人和资源位于不同的 Amazon 账户中时，还必须授予委托人实体对资源的访问权限。通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的委托人授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅 。IAM 角色与基于资源的策略有何不同中的IAM 用户指南。

Amazon Health 对于 DescribeAffectedEntities 和 DescribeEventDetails API 操作仅支持基于资源的策略。您可以在策略中指定这些操作，以定义哪些委托人实体（账户、用户、角色和联合用户）可以对 Amazon Health 事件执行操作。

Examples

要查看 Amazon Health 基于资源的策略的示例，请参阅基于资源和基于操作的条件 (p. 28)。

基于 Amazon Health 标签的授权

Amazon Health 不支持标记资源或基于标签控制访问。

Amazon HealthIAM 角色

一个IAM 角色是您的Amazon具有特定权限的账户。

将临时凭证用于 Amazon Health

您可以使用临时凭证进行联合身份登录，担任 IAM 角色或担任跨账户角色。您可以通过调用AmazonSTS API 操作，如AssumeRole或者GetFederationToken。

Amazon Health 支持使用临时凭证。

服务相关角色

服务相关角色允许 Amazon 服务访问其他服务中的资源以代表您完成操作。服务相关角色显示在您的 IAM 账户中，并归该服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

Amazon Health 支持服务相关角色以与 Amazon Organizations 集成。该角色命名为 Health_OrganizationsServiceRolePolicy，它允许 Amazon Health 从组织中的其他 Amazon 账户访问运行状况事件。

您可以使用 EnableHealthServiceAccessForOrganization 操作在账户中创建服务相关角色。但是，如果要禁用此功能，则必须首先调用 DisableHealthServiceAccessForOrganization 操作。然后，您可以通过 IAM 控制台、IAM API 或Amazon命令行界面 (AmazonCLI) 。有关更多信息，请参阅 。使用服务相关角色中的IAM 用户指南。

有关更多信息，请参阅 使用组织视图跨账户聚合 Amazon Health 事件 (p. 35)。

服务角色

此功能允许服务代表您代入服务角色。此角色允许服务访问其他服务中的资源以代表您完成操作。服务角色显示在您的 IAM 账户中，并归该账户所有。这意味着，IAM 管理员可以更改该角色的权限。但是，这样做可能会中断服务的功能。

Amazon Health 不支持服务角色。

Amazon Health 基于身份的策略示例

默认情况下，IAM 用户和角色没有创建或修改权限Amazon Health资源的费用。它们还无法使用Amazon Web Services Management Console、AmazonCLI 或AmazonAPI。IAM 管理员必须创建 IAM 策略，以便为用户和角色授予权限以对所需的指定资源执行特定的 API 操作。然后，管理员必须将这些策略附加到需要这些权限的 IAM 用户或组。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅在“JSON”选项卡上创建策略中的IAM 用户指南。

主题

- 策略最佳实践 (p. 22)
- 使用 Amazon Health 控制台 (p. 23)
- 允许用户查看他们自己的权限 (p. 24)
- 访问 Amazon Personal Health Dashboard 和 Amazon Health API (p. 25)
- 基于资源和基于操作的条件 (p. 28)

策略最佳实践

基于身份的策略非常强大。它们确定某个人是否可以创建、访问或删除您账户中的 Amazon Health 资源。这些操作可能会使 Amazon 账户产生成本。创建或编辑基于身份的策略时，请遵循以下准则和建议：

- 入门Amazon托管策略— 开始使用Amazon Health快速、使用Amazon托管策略，以便为您的员工授予所需的权限。这些策略已在您的账户中提供，并由 Amazon 维护和更新。有关更多信息，请参阅 。入门Amazon托管策略中的IAM 用户指南。
- 授予最低权限 – 创建自定义策略时，仅授予执行任务所需的许可。最开始只授予最低权限，然后根据需要授予其他权限。这样做比起一开始就授予过于宽松的权限而后再尝试收紧权限来说更为安全。有关更多信息，请参阅 。授予最低权限中的IAM 用户指南。
- 为敏感操作启用 MFA – 为了提高安全性，要求 IAM 用户使用多重验证 (MFA) 访问敏感资源或 API 操作。有关更多信息，请参阅 。在中使用多重身份验证 (MFA)Amazon中的IAM 用户指南。
- 使用策略条件来增强安全性 – 在切实可行的范围内，定义基于身份的策略在哪些情况下允许访问资源。例如，您可编写条件来指定请求必须来自允许的 IP 地址范围。您也可以编写条件，以便仅允许指定日期或时间范围内的请求，或者要求使用 SSL 或 MFA。有关更多信息，请参阅 。IAM JSON 策略元素：Condition中的IAM 用户指南。

使用 Amazon Health 控制台

要访问 Amazon Health 控制台，您必须拥有一组最低的权限。这些权限必须允许您列出和查看有关您的 Amazon 账户中的 Amazon Health 资源的详细信息。如果您创建的基于身份的策略比所需的最低权限更严格，则无法为具有该策略的实体（IAM 用户或角色）正常运行控制台。

为了确保这些实体仍然可以使用 Amazon Health 控制台，您可以附加以下 Amazon 托管策略 AWSHealthFullAccess。

AWS ShealthAccess 策略授予实体对以下内容的完全访问权限：

- 启用或禁用Amazon Health组织视图功能中的所有帐户Amazon组织
- 这些区域有：Amazon Personal Health Dashboard中的Amazon Health控制台
- Amazon Health API 操作和通知
- 查看属于您的账户的信息。Amazon组织
- 查看管理帐户的组织单位 (OU)

Example ：AWSHealthFullAccess

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "health.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "health:*",
                "organizations:DescribeAccount",
                "organizations:ListAccounts",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListParents"
            ],
```

```
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "health.amazonaws.com"
                }
            }
        }
    ]
}
```

Note

您还可以使用 Amazon 托管角色 `Health_OrganizationsServiceRolePolicy`，以便 Amazon Health 可以查看组织中其他账户的事件。有关更多信息，请参阅 将服务相关角色用于 Amazon Health (p. 31)。

对于只需要调用的用户，无需为其提供最低控制台权限。AmazonCLI 或AmazonAPI。相反，只允许访问与您尝试执行的 API 操作相匹配的操作。

有关更多信息，请参阅 。向用户添加权限中的IAM 用户指南。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管策略。此策略包括在控制台上完成此操作或者以编程方式使用AmazonCLI 或AmazonAPI。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws: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": "*"
        }
    ]
```

```
}
```

访问 Amazon Personal Health Dashboard 和 Amazon Health API

Amazon Personal Health Dashboard 适用于所有 Amazon 账户。Amazon Health API 仅适用于具有商业或企业支持计划的账户。有关更多信息，请参阅 Amazon Web Services Support。

您可以使用 IAM 创建实体（用户、组或角色），然后为这些实体授予权限，以访问Amazon Personal Health Dashboard和Amazon HealthAPI。

默认情况下，IAM 用户无权访问Amazon Personal Health Dashboard或Amazon HealthAPI。通过将 IAM 策略附加到单一用户、一组用户或角色，您可为用户授予对账户的 Amazon Health 信息的访问权限。有关更多信息，请参阅身份 (用户、组和角色) 和 IAM 策略概述。

创建 IAM 用户以后，您可以为这些用户提供单独的密码。然后，他们可以使用特定于账户的登录页面登录账户并查看 Amazon Health 信息。有关更多信息，请参阅 用户如何登录您的 账户。

> Note
>
> 具有查看权限的 IAM 用户Amazon Personal Health Dashboard具有对所有运行状况信息的只读访问权限Amazon服务的账户，这可能包括但不限于，Amazon资源 ID，例如 Amazon EC2 实例 ID、EC2 实例 IP 地址和常规安全通知。
> 例如，如果 IAM 策略仅授予对Amazon Personal Health Dashboard和Amazon HealthAPI，则策略应用到的用户或角色可以访问关于Amazon服务和相关资源，即使其他 IAM 策略不允许访问。

- 个人帐户 — 您可以使用诸如DescribeEvents和DescribeEventDetails以获取有关的信息Amazon Health为您账户提供的事件。
- 组织帐户 — 您可以使用诸如DescribeEventsForOrganization和DescribeEventDetailsForOrganization以获取有关的信息Amazon Health属于您组织的账户的事件。

有关可用 API 操作的更多信息，请参阅Amazon HealthAPI 参考。

单个操作

描述访问权限

此策略语句授予对 Amazon Personal Health Dashboard 和任何 `Describe*` Amazon Health API 操作的访问权限。例如，具有此策略的权限的 IAM 用户可以访问Amazon Personal Health Dashboard中的Amazon Web Services Management Console并调用Amazon Health `DescribeEvents`API 操作。

Example ：描述访问权限

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "health:Describe*"
    ],
    "Resource": "*"
  }]
}
```

拒绝访问

此策略语句拒绝访问 Amazon Personal Health Dashboard 和 Amazon Health API。具有此策略的 IAM 用户无法查看Amazon Personal Health Dashboard中的Amazon Web Services Management Console并且不能调用任何Amazon HealthAPI 操作。

Example ：拒绝访问

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Effect": "Deny",
    "Action": [
      "health:*"
    ],
    "Resource": "*"
  }]
}
```

组织视图

如果要启用组织视图Amazon Health，则必须允许访问Amazon Health和Amazon Organizations操作。

这些区域有：`Action`元素必须包含以下权限：

- `iam:CreateServiceLinkedRole`
- `organizations:EnableAWSServiceAccess`
- `organizations:DescribeAccount`
- `organizations:DisableAWSServiceAccess`
- `organizations:ListAccounts`
- `organizations:ListDelegatedAdministrators`
- `organizations:ListParents`

要了解每个 API 所需的确切权限，请参阅定义的操作Amazon HealthAPI 和通知中的IAM 用户指南。

> **Note**
>
> 您必须使用来自组织的管理账户的凭证来访问Amazon Health用于 的 APIAmazon Organizations。有关更多信息，请参阅 使用组织视图跨账户聚合 Amazon Health 事件 (p. 35)。

允许访问Amazon Health组织视图

此策略语句授予对所有的访问权限Amazon Health和Amazon Organizations组织视图功能所需的操作。

Example ：允许 Amazon Health 组织视图访问

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "health.amazonaws.com"
                }
            }
        },
        {
```

```
            "Effect": "Allow",
            "Action": [
                "health:*",
                "organizations:DescribeAccount",
                "organizations:ListAccounts",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListParents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/health.amazonaws.com/
AWSServiceRoleForHealth*"
        }
    ]
}
```

拒绝对 的访问Amazon Health组织视图

此策略语句拒绝访问Amazon Organizations操作，但允许访问Amazon Health单个账户的操作。

Example ：拒绝 Amazon Health 组织视图访问

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "health:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "health.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": [
                "organizations:DescribeAccount",
                "organizations:ListAccounts",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListParents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/health.amazonaws.com/
AWSServiceRoleForHealth*"
        }
```

```
    ]
}
```

Note

如果您想要授予权限的用户或组已拥有 IAM 策略，则可将Amazon Health特定于该策略的政策声明。

基于资源和基于操作的条件

Amazon Health支持IAM 条件(对于)DescribeAffectedEntities和DescribeEventDetailsAPI 操作。您可以使用基于资源和操作的条件来限制Amazon HealthAPI 发送至用户、组或角色。

为此，请更新`Condition`块或设置`Resource`元素。您可以使用字符串条件基于某些 Amazon Health 事件字段来限制访问。

当您指定一个Amazon Health事件：

- `eventTypeCode`
- `service`

Notes

- 这些区域有：DescribeAffectedEntities和DescribeEventDetailsAPI 操作支持资源级权限。例如，您可以创建策略以允许或拒绝特定的Amazon Health事件.
- 这些区域有：DescribeAffectedEntitiesForOrganization和DescribeEventDetailsForOrganizationAPI 操作不支持资源级权限。
- 有关更多信息，请参阅 。的操作、资源和条件键Amazon HealthAPI 和通知中的服务授权参考。

Example ：基于操作的条件

此策略语句授予对Amazon Personal Health Dashboard和Amazon Health `Describe*`API 操作，但拒绝访问任何Amazon Health与 Amazon EC2 相关的事件。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "health:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "health:DescribeAffectedEntities",
                "health:DescribeEventDetails"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "health:service": "EC2"
                }
            }
        }
    ]
```

```
}
```

Example ：基于资源的条件

以下策略具有相同的效果，但使用 `Resource` 元素。

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "health:Describe*"
    ],
    "Resource": "*",
  },
  {
    "Effect": "Deny",
    "Action": [
      "health:DescribeEventDetails",
      "health:DescribeAffectedEntities"
    ],
    "Resource": "arn:aws:health:*::event/EC2/*/*",
  }]
}
```

Example ：eventTypeCode 条件

此策略语句授予对 Amazon Personal Health Dashboard 和 Amazon Health `Describe*` API 操作的访问权限，但拒绝访问 `eventTypeCode` 与 `AWS_EC2_*` 匹配的任何 Amazon Health 事件。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "health:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "health:DescribeAffectedEntities",
                "health:DescribeEventDetails"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "health:eventTypeCode": "AWS_EC2_*"
                }
            }
        }
    ]
}
```

> **Important**
>
> 如果调用 DescribeAffectedEntities 和 DescribeEventDetails 操作但没有访问 Amazon Health 事件的权限，则会出现 `AccessDeniedException` 错误。有关更多信息，请参阅 对 Amazon Health 身份和访问进行故障排除 (p. 30)。

对 Amazon Health 身份和访问进行故障排除

使用以下信息可诊断和修复在使用时可能遇到的常见问题。Amazon Health和 IAM。

主题

- 我无权在 Amazon Health 中执行操作 (p. 30)
- 未授权我执行 iam:PassRole (p. 30)
- 我想要查看我的访问密钥 (p. 30)
- 我是管理员并希望允许其他人访问 Amazon Health (p. 31)
- 我希望允许我的 Amazon 账户之外的人员访问我的 Amazon Health 资源 (p. 31)

我无权在 Amazon Health 中执行操作

如果 Amazon Web Services Management Console 告诉您，您无权执行某个操作，则必须联系您的管理员寻求帮助。您的管理员是指为您提供用户名和密码的那个人。

当用户没有使用 Amazon Personal Health Dashboard 或 Amazon Health API 操作的权限时，会出现 `AccessDeniedException` 错误。

在这种情况下，用户的管理员必须更新策略以允许用户访问。

Amazon Health API 需要 Amazon Web Services Support 提供的商业或企业支持计划。
如果您通过没有商业或企业支持计划的账户调用 Amazon Health API，则返回以下错误代码：`SubscriptionRequiredException`。

未授权我执行 iam:PassRole

如果您收到错误消息，提示您无权执行 `iam:PassRole` 操作，则必须联系您的管理员寻求帮助。您的管理员是指为您提供用户名和密码的那个人。请求该人员更新您的策略，以便允许您将角色传递给 Amazon Health。

有些 Amazon 服务允许您将现有角色传递到该服务，而不是创建新服务角色或服务相关角色。为此，您必须具有将角色传递给该服务的权限。

当名为 `marymajor` 的 IAM 用户尝试使用控制台在 Amazon Health 中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform: iam:PassRole
```

在这种情况下，Mary 请求她的管理员来更新其策略，以允许她执行 `iam:PassRole` 操作。

我想要查看我的访问密钥

在创建 IAM 用户访问密钥后，您可以随时查看您的访问密钥 ID。但是，您无法再查看您的秘密访问密钥。如果您丢失了私有密钥，则必须创建一个新的访问密钥对。

访问密钥包含两部分：访问密钥 ID（例如 `AKIAIOSFODNN7EXAMPLE`）和秘密访问密钥（例如 `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`）。与用户名和密码一样，您必须同时使用访问密钥 ID 和秘密访问密钥对请求执行身份验证。像对用户名和密码一样，安全地管理访问密钥。

> **Important**
>
> 请不要向第三方提供访问密钥，甚至为了帮助找到您的规范用户 ID 也是如此。如果您这样做，可能会向某人提供对您的账户的永久访问权限。

当您创建访问密钥对时，系统会提示您将访问密钥 ID 和秘密访问密钥保存在一个安全位置。秘密访问密钥仅在您创建它时可用。如果丢失了您的秘密访问密钥，您必须为 IAM 用户添加新的访问密钥。您最多可拥有两个访问密钥。如果您已有两个密钥，则必须删除一个密钥对，然后再创建新的密钥。要查看说明，请参阅管理访问密钥中的IAM 用户指南。

我是管理员并希望允许其他人访问 Amazon Health

允许其他人访问Amazon Health中，您必须为需要访问权限的人员或应用程序创建 IAM 实体（用户或角色）。他们（它们）将使用该实体的凭证访问 Amazon。然后，您必须将策略附加到实体，以便在 Amazon Health 中为这些实体授予正确的权限。

要立即开始，请参阅创建您的第一个 IAM 委派用户和组中的IAM 用户指南。

我希望允许我的 Amazon 账户之外的人员访问我的 Amazon Health 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以代入角色。对于支持基于资源的策略或访问控制列表 (ACL) 的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解 Amazon Health 是否支持这些功能，请参阅Amazon Health 如何与 IAM 协同工作 (p. 19)。
- 要了解如何跨Amazon您拥有的帐户，请参阅在另一个中向 IAM 用户提供访问权限Amazon您拥有的账户中的IAM 用户指南。
- 了解如何向第三方提供对资源的访问权限Amazon帐户，请参阅提供对的访问权限Amazon第三方拥有的账户中的IAM 用户指南。
- 要了解如何通过身份联合提供访问权限，请参阅向经过外部身份验证的用户（联合身份验证）提供访问权限中的IAM 用户指南。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅IAM 角色与基于资源的策略的差异中的IAM 用户指南。

将服务相关角色用于 Amazon Health

Amazon Health使用 AWS Identity and Access Management (IAM)服务相关角色。服务相关角色是一种独特类型的 IAM 角色，它与 Amazon Health 直接相关。服务相关角色由 Amazon Health 预定义，并包含该服务代表您调用其他 Amazon 服务所需的一切权限。

服务相关角色使 Amazon Health 的设置更轻松，因为您不必手动添加必要的权限。Amazon Health 定义其服务相关角色的权限，除非另行定义，否则仅 Amazon Health 可以代入其角色。定义的权限包括信任策略和权限策略，以及不能附加到任何其他 IAM 实体的权限策略。

Amazon Health 的服务相关角色权限

Amazon Health 使用名为 `Health_OrganizationsServiceRolePolicy` 的服务相关角色。

服务相关角色信任 `health.amazonaws.com` 服务来代入角色。

此角色使用以下权限策略允许 Amazon Health 在 Amazon Organizations 中列出账户。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Action": "organizations:ListAccounts",
            "Resource": "*"
        },
        {
            "Sid": "ListAWSServiceAccessForOrganization0",
            "Effect": "Allow",
            "Action": "organizations:ListAWSServiceAccessForOrganization",
            "Resource": "*"
        }
    ]
}
```

为 Amazon Health 创建服务相关角色

您无需手动创建服务相关角色。当调用 EnableHealthServiceAccessForOrganization 操作时，Amazon Health 会在账户中为您创建服务相关角色。

为 Amazon Health 编辑服务相关角色

Amazon Health 不允许您编辑服务相关角色。在创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。不过，您可以使用 IAM 编辑角色的说明。有关更多信息，请参阅 。编辑服务相关角色中的IAM 用户指南。

删除 Amazon Health 的服务相关角色

如果要删除此角色，必须首先调用 DisableHealthServiceAccessForOrganization 操作。然后，您可以通过 IAM 控制台、IAM API 或Amazon命令行界面 (AmazonCLI) 。有关更多信息，请参阅 。使用服务相关角色中的IAM 用户指南。

Amazon Health 中的日志记录和监控

监控是保持可靠性、可用性和性能的重要环节。Amazon Health和您的其他Amazon解决方案。Amazon提供以下监控工具监视Amazon Health，在出现错误时进行报告，并在适当的时候采取措施：

- Amazon CloudWatch监控Amazon资源以及您在上运行的应用程序Amazon实时操作。您可以收集和跟踪指标，创建自定义的控制面板，以及设置警报以在指定的指标达到您指定的阈值时通知您或采取措施。例如，您可以具有亚马逊 Elastic Compute Cloud (Amazon EC2) 实例的 CloudWatch 跟踪 CPU 使用率或其他指标并且在需要时自动启动新实例。有关更多信息，请参阅 Amazon CloudWatch 用户指南。
- Amazon CloudWatch Events会提供近乎实时的系统事件流，这些系统事件描述Amazon资源的费用。CloudWatch 事件支持自动事件驱动型计算。您可以编写规则，以监控某些事件和在这些事件发生时在其他 Amazon 服务中触发自动操作。有关更多信息，请参阅 Amazon CloudWatch Events 用户指南。
- Amazon CloudTrail捕获由您的或代表该人发出或代表该人发出的 API 调用和相关事件。Amazon账户，并将日志文件传送到您指定的 Amazon Simple Storage Service (Amazon S3) 存储桶。您可以标识哪些用户和账户调用了 Amazon、从中发出调用的源 IP 地址以及调用的发生时间。有关更多信息，请参阅 Amazon CloudTrail 用户指南。

有关更多信息，请参阅 监控 Amazon Health (p. 51)。

Amazon Health 的合规性验证

第三方审计员评估的安全性和合规性。Amazon服务作为多个Amazon合规性计划，例如SOC、PCI、FedRAMP 和 HIPAA。

要了解Amazon Health或其他Amazon服务在特定的合规性计划范围内，请参阅。Amazon合规性计划范围内的服务。有关常规信息，请参阅 Amazon 合规性计划。

您可以使用 Amazon Artifact 下载第三方审计报告。有关更多信息，请参阅下载 Amazon Artifact 中的报告。

您在使用 Amazon 服务时的合规性责任由您数据的敏感性、贵公司的合规性目标以及适用的法律法规决定。Amazon 提供以下资源来帮助满足合规性：

- 安全性与合规性快速入门指南安全性与合规性快速入门指南— 这些部署指南讨论了架构注意事项，并提供了在Amazon以安全性和合规性为中心。
- HIPAA 安全性和合规性架构设计白皮书— 本白皮书介绍了公司如何使用Amazon以创建符合 HIPAA 要求的应用程序。

  Note

  并非所有服务都符合 HIPAA 的要求。
- Amazon合规性资源— 此业务手册和指南集合可能适用于您的行业和位置。
- 使用规则评估资源中的Amazon Config开发人员指南—Amazon Config服务评估您的资源配置对内部实践、行业指南和法规的遵循情况。
- Amazon Security Hub— 此Amazon服务向您提供中安全状态的全面视图。Amazon，可帮助您检查是否符合安全行业标准和最佳实践。

Amazon Health 中的恢复功能

这些区域有：Amazon全球基础设施围绕Amazon区域和可用区。Amazon区域提供多个在物理上独立且隔离的可用区，这些可用区通过延迟低、吞吐量高且冗余性高的网络连接在一起。利用可用区，您可以设计和操作在可用区之间无中断地自动实现故障转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

Amazon Health 事件跨多个可用区进行存储和复制。此方法确保您可以通过 Amazon Personal Health Dashboard 或 Amazon Health API 操作访问它们。您最多可以在 Amazon Health 事件发生后 90 天内查看这些事件。

有关 Amazon 区域和可用区的更多信息，请参阅 Amazon 全球基础设施。

Amazon Health 中的基础设施安全性

作为托管服务，Amazon Health受Amazon全局网络安全过程，请参阅Amazon Web Services：安全过程概述白皮书。

您可以使用 Amazon 发布的 API 调用通过网络访问 Amazon Health。客户端必须支持传输层安全性 (TLS) 1.0 或更高版本。建议使用 TLS 1.2 或更高版本。客户端还必须支持具有完全向前保密 (PFS) 的密码套件，例如 Ephemeral Diffie-Hellman (DHE) 或 Elliptic Curve Ephemeral Diffie-Hellman (ECDHE)。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 Amazon Security Token Service (Amazon STS) 生成临时安全凭证来对请求进行签名。

Amazon Health 中的配置和漏洞分析

配置和 IT 控制是 Amazon 和您（我们的客户）之间的共同责任。有关更多信息，请参阅 Amazon 责任共担模式。

Amazon Health 的安全最佳实践

请参阅以下使用 Amazon Health 的最佳实践。

授予 Amazon Health 用户可能的最低权限

通过对 用户和组使用最小访问策略权限集，遵循最低权限原则。例如，您可能允许 AWS Identity and Access Management (IAM) 用户访问Amazon Personal Health Dashboard。但是，您可能不允许同一用户启用或禁用对 Amazon Organizations 的访问。

有关更多信息，请参阅 Amazon Health 基于身份的策略示例 (p. 22)。

查看 Amazon Personal Health Dashboard

经常检查 Amazon Personal Health Dashboard，以确定可能影响您的账户或应用程序的事件。例如，您可能会收到有关资源的事件通知，如需要更新的 Amazon Elastic Compute Cloud (Amazon EC2) 实例。

有关更多信息，请参阅 Amazon Personal Health Dashboard入门 (p. 2)。

集成Amazon Health与 Amazon Chime 或松弛

您可以将 Amazon Health 与聊天工具相集成。此集成可让您和您的团队实时获得有关 Amazon Health 事件的通知。有关更多信息，请参阅 GitHub 中的 Amazon Health 工具。

监控 Amazon Health 事件

您可以将其集成Amazon Health，以便为特定事件创建规则。当 CloudWatch Events 检测到与您的规则匹配的事件时，系统会通知您，然后可以采取措施。CloudWatch 事件特定于区域，因此您必须在应用程序或基础设施所在的区域中配置此服务。

在某些情况下，无法确定 Amazon Health 事件的区域。如果出现这种情况，默认情况下，事件将出现在美国东部（弗吉尼亚北部）区域。您可以在此区域中设置 CloudWatch 事件，以确保监视这些事件。

有关更多信息，请参阅 监控Amazon HealthAmazon CloudWatch Events (p. 43)。

使用组织视图跨账户聚合 Amazon Health 事件

默认情况下，您可以使用Amazon Health查看Amazon Health单个Amazonaccount. 如果您使用 Amazon Organizations，也可以在组织中集中查看 Amazon Health 事件。使用此功能可以访问与单个账户操作相同的信息。您可以使用筛选条件查看特定 Amazon 区域、账户和服务中的事件。

您可以聚合事件，确定组织中受操作事件影响的账户，或获得安全漏洞通知。然后，您可以使用此信息在组织内主动管理和自动化资源维护事件。使用此功能可随时了解即将发生的 Amazon 服务更改，这些更改可能需要您更新或更改代码。

Important

- Amazon Health 不会记录您启用组织视图之前组织中发生的事件。例如，如果您的组织中的成员账户 (111122223333) 在启用此功能之前收到了亚马逊 Elastic Compute Cloud (Amazon EC2) 的事件，则此事件将不会显示在您的组织视图中。
- Amazon Health为组织中的帐户发送的事件将显示在组织视图中，只要事件可用，长达 90 天，即使其中一个或多个帐户离开您的组织也是如此。
- 组织事件将在 90 天后这些事件将被删除。这个配额不能提高。

Prerequisites

在使用组织视图之前，您必须：

- 成为已启用所有功能的组织的一员。
- 以 AWS Identity or Access Management (IAM) 用户的身份登录到管理账户，或代入 IAM 角色。

  您还可以在组织的管理账户中以根用户的身份登录（不推荐）。有关更多信息，请参阅 。隐藏您的Amazon账户根用户访问密钥中的IAM 用户指南。
- 如果您以 IAM 用户的身份登录，请使用 IAM 策略，授予对Amazon Health和 “Organizations” 操作，例如AWSHealthFullAccess策略。有关更多信息，请参阅 Amazon Health 基于身份的策略示例 (p. 22)。

Topics

- 组织视图 (控制台) (p. 35)
- 组织视图 (CLI) (p. 38)

组织视图 (控制台)

您可以将Amazon Health控制台以获取运行状况事件的集中视图Amazon组织。

组织视图位于Amazon Health控制台Amazon Web Services Support计划，没有任何额外费用。

Note

如果要允许用户在管理帐户中访问此功能，则他们必须具有AWSHealthFullAccess策略。有关更多信息，请参阅 Amazon Health 基于身份的策略示例 (p. 22)。

目录

- 启用组织视图 (控制台) (p. 36)
- 查看组织视图事件 (控制台) (p. 36)
    - Dashboard (p. 37)
    - 事件日志 (p. 37)
- 查看受影响的帐户和资源（控制台） (p. 37)
- 禁用组织视图 (控制台) (p. 38)

启用组织视图 (控制台)

您可以从Amazon Health控制台。您必须登录您的Amazon组织。

查看Amazon Personal Health Dashboard适用于组织

1. 登录 Amazon Web Services Management Console 并通过以下网址打开 Amazon Personal Health Dashboard：https://phd.aws.amazon.com/phd/home。
2. 在导航窗格中，选择组织视图，然后选择配置。
3. 在存储库的启用组织视图页面上，选择启用组织视图。
4. （可选）如果您希望更改Amazon组织（例如创建组织单位 (OU)），请选择ManageAmazon Organizations。

   有关更多信息，请参阅 。开始使用Amazon Organizations中的Amazon Organizations用户指南。

   Notes

   - 启用此功能是一个异步过程，需要花点时间才能完成。根据组织中账户的数量，可能需要几分钟才能加载账户。您可以离开并检查Amazon Health控制台更高版本。
   - 如果您有商业或企业支持计划，那么您可以调用DescribeHealthServiceStatusForOrganizationAPI 操作以检查该过程的状态。
   - 启用此功能后，`AWSServiceRoleForHealth_Organizations`服务相关角色`Health_OrganizationsServiceRolePolicy`策略应用于组织中的管理帐户。有关更多信息，请参阅 将服务相关角色用于 Amazon Health (p. 31)。

查看组织视图事件 (控制台)

启用组织视图后，Amazon Health显示组织中所有账户的运行状况事件。

当某个账户加入您的组织时，Amazon Health 会自动将该账户添加到组织视图中。当某个账户离开您的组织时，该账户中的新事件将不再记录到组织视图中。但是，现有事件将保留，您仍可以查询它们，直到达到 90 天限制。

Note

启用此功能后，Amazon Health控制台可以从服务运行状况控制面板的过去 7 天。这些公有事件并非特定于组织中的账户。服务运行状况控制面板中的事件则会提供有关Amazon服务。

您可以在控制面板或事件日志页.

Topics

- 控制面板 (p. 37)

- 事件日志 (p. 37)

Dashboard

您可以将控制面板页面查看可能影响Amazon基础架构，例如更改Amazon服务和资源。

在仪表板页面中查看组织视图事件

1. 登录 Amazon Web Services Management Console 并通过以下网址打开 Amazon Personal Health Dashboard：https://phd.aws.amazon.com/phd/home。
2. 在导航窗格中，选择组织视图，然后选择控制面板查看最近和即将发生的活动。
3. 您可以选择未决问题、已安排更改，或者其他通知选项卡，然后选择事件名称。
4. 在存储库的详细信息选项卡上，您可以查看有关事件的以下信息：

   - 事件名称
   - 状态
   - 地区/可用区
   - 受影响的账户
   - 开始时间
   - End Time
   - 类别
   - 描述

事件日志

您也可以使用事件日志页面查看Amazon Health组织视图的事件。列的布局和行为类似于控制面板页面，只是事件日志页面包含其他列和过滤器选项，例如事件类别、状态, 和开始时间。

在事件日志页中查看组织视图事件

1. 登录 Amazon Web Services Management Console 并通过以下网址打开 Amazon Personal Health Dashboard：https://phd.aws.amazon.com/phd/home。
2. 在导航窗格中，选择组织视图，然后选择事件日志。
3. Untes事件日志，选择事件名称。您可以查看有关事件的以下信息：

   - 事件名称
   - 状态
   - 地区/可用区
   - 受影响的账户
   - 开始时间
   - End Time
   - 类别
   - 描述

查看受影响的帐户和资源（控制台）

在活动详细信息中控制面板和事件日志页面上，您可以查看组织中受事件影响的账户以及任何相关资源。例如，如果即将进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例维护事件，那么您组织中具有 Amazon EC2 实例的账户可以显示在详细信息选项卡。您可以确定特定资源，然后联系帐户所有者。

查看受影响的帐户和资源

1. 在控制面板或者事件日志页面上，选择一个具有受影响的账户。
2. 选择受影响的账户选项卡。
3. 选择显示账户详细信息查看账户的以下信息：
   - 账户 ID
   - 账户名称
   - 主要电子邮件
   - 组织部门 (OU)
4. 展开账户以查看受影响的资源。
5. 如果资源超过 10 个，请选择查看所有资源以查看它们。
6. 要按帐户 ID 筛选此特定事件，请执行以下操作：
   a. 在存储库的受影响的账户选项卡上，选择添加筛选器中，选择账户 ID，然后输入帐户 ID。您一次只能输入一个账户 ID。
   b. 选择 Apply。您输入的账户显示在列表中。

禁用组织视图 (控制台)

如果您不想聚合组织的事件，可以从管理帐户关闭此功能。

Amazon Health停止聚合组织中所有其他账户的事件。您可以继续查看组织中以前的事件，直到它们被删除。

禁用组织视图

1. 登录 Amazon Web Services Management Console 并通过以下网址打开 Amazon Personal Health Dashboard：https://phd.aws.amazon.com/phd/home。
2. 在导航窗格中，选择组织视图，然后选择配置。
3. 在存储库的启用组织视图页面上，选择禁用组织视图。

关闭此功能后，Amazon Health不再聚合来自组织的事件。但是，服务链接的角色将保留在管理账户中，直到您通过 AWS Identity and Access Management (IAM) 控制台、IAM API 或Amazon命令行界面 (AmazonCLI)。有关更多信息，请参阅 。删除服务相关角色中的IAM 用户指南。

组织视图 (CLI)

您也可以从Amazon命令行界面 (AmazonCLI) 而不是Amazon Health控制台。要使用控制台，请参阅 启用组织视图 (控制台) (p. 36)。

> Note
>
> 如果要允许用户访问组织视图功能的管理帐户，他们必须具有AWSHealthFullAccess策略。有关更多信息，请参阅 Amazon Health 基于身份的策略示例 (p. 22)。

主题

- 启用组织视图 (CLI) (p. 39)
- 查看组织视图事件 (CLI) (p. 40)
- 禁用组织视图 (CLI) (p. 41)

- Amazon Health 组织视图 API 操作 (p. 41)

启用组织视图 (CLI)

您可以通过使用EnableHealthServiceAccessForOrganizationAPI 操作。

您可以使用Amazon命令行界面 (AmazonCLI) 或您自己的代码来调用此操作。

Note

- 您必须具有业务或者企业支持计划调用Amazon HealthAPI。
- 您必须使用美国东部 (弗吉尼亚北部) 区域终端节点。

Example

以下AmazonCLI 命令从Amazonaccount. 您可以从管理账户或从可担任具有所需权限的角色的账户使用此命令。

```
aws health enable-health-service-access-for-organization --region us-east-1
```

以下代码示例调用EnableHealthServiceAccessForOrganizationAPI 操作。

Python

```
import boto3

client = boto3.client('health')

response = client.enable_health_service_access_for_organization()

print(response)
```

Java

您可以在以下示例中使用适用于 Java 2.0 版的 Amazon 开发工具包。

```
import software.amazon.awssdk.services.health.HealthClient;
import software.amazon.awssdk.services.health.HealthClientBuilder;

import software.amazon.awssdk.services.health.model.ConcurrentModificationException;
import
 software.amazon.awssdk.services.health.model.EnableHealthServiceAccessForOrganizationRequest;
import
 software.amazon.awssdk.services.health.model.EnableHealthServiceAccessForOrganizationResponse;
import
 software.amazon.awssdk.services.health.model.DescribeHealthServiceStatusForOrganizationRequest;
import
 software.amazon.awssdk.services.health.model.DescribeHealthServiceStatusForOrganizationResponse;

import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;

import software.amazon.awssdk.regions.Region;

public class EnableHealthServiceAccessDemo {
    public static void main(String[] args) {
        HealthClient client = HealthClient.builder()
            .region(Region.US_EAST_1)
            .credentialsProvider(
                DefaultCredentialsProvider.builder().build()
```

```
            )
            .build();

        try {
            DescribeHealthServiceStatusForOrganizationResponse statusResponse =
client.describeHealthServiceStatusForOrganization(
                DescribeHealthServiceStatusForOrganizationRequest.builder().build()
            );

            String status = statusResponse.healthServiceAccessStatusForOrganization();
            if ("ENABLED".equals(status)) {
                System.out.println("EnableHealthServiceAccessForOrganization already
enabled!");
                return;
            }

            client.enableHealthServiceAccessForOrganization(
                EnableHealthServiceAccessForOrganizationRequest.builder().build()
            );

            System.out.println("EnableHealthServiceAccessForOrganization is in
progress");
        } catch (ConcurrentModificationException cme) {
            System.out.println("EnableHealthServiceAccessForOrganization is already in
progress. Wait for the action to complete before trying again.");
        } catch (Exception e) {
            System.out.println("EnableHealthServiceAccessForOrganization FAILED: " +
e);
        }
    }
}
```

有关更多信息，请参阅适用于 Java 2.0 的 Amazon 开发工具包开发人员指南。

启用此功能后，AWSServiceRoleForHealth_Organizations 服务相关角色（单反相机）与Health_OrganizationsServiceRolePolicy策略应用于组织中的管理帐户。

Note

启用此功能是一个异步过程，需要花点时间才能完成。您可以调用DescribeHealthServiceStatusForOrganization操作来检查该过程的状态。

查看组织视图事件 (CLI)

启用此功能后，Amazon Health 会开始记录影响组织中账户的事件。当某个账户加入您的组织时，Amazon Health 会自动将该账户添加到组织视图中。当某个账户离开您的组织时，该账户中的新事件将不再记录到组织视图中。但是，现有事件将保留，您仍可以查询它们，直到达到 90 天限制。

Note

Amazon Health 不会记录您启用组织视图之前组织中发生的事件。

您可以使用 Amazon Health API 操作从组织视图返回事件。

Example ：描述组织视图事件

以下AmazonCLI 命令返回Amazon组织中的账户。

```
aws health describe-events-for-organization --region us-east-1
```

有关其他 Amazon Health API 操作，请参阅以下部分。

禁用组织视图 (CLI)

您可以通过使用DisableHealthServiceAccessForOrganizationAPI 操作。

Example

以下AmazonCLI 命令从账户禁用此功能。

```
aws health disable-health-service-access-for-organization --region us-east-1
```

> Note
>
> 您也可以通过使用 Organizations 功能来禁用组织功能DisableAWSServiceAccessAPI 操作。调用此操作后，Amazon Health 会停止聚合组织中所有其他账户的事件。如果您为组织视图调用 Amazon Health API 操作，则 Amazon Health 会返回错误。Amazon Health 会继续为 Amazon 账户聚合运行状况事件。

禁用此功能后，Amazon Health 不再聚合来自组织的事件。但是，服务链接的角色将保留在管理账户中，直到您通过 AWS Identity and Access Management (IAM) 控制台、IAM API 或AmazonCLI。有关更多信息，请参阅 。删除服务相关角色中的IAM 用户指南。

Amazon Health 组织视图 API 操作

您可以将以下 Amazon Health API 操作用于组织视图：

- DescribeEventsForOrganization— 返回有关组织中事件的摘要信息。
- DescribeAffectedAccountsForOrganization— 返回Amazon组织中受指定事件影响的账户。
- DescribeEventDetailsForOrganization— 返回有关组织中一个或多个账户的指定事件的详细信息。
- DescribeAffectedEntitiesForOrganization— 返回组织中一个或多个账户受到一个或多个事件影响的实体列表。

您可以使用以下操作来启用或禁止Amazon Health与 Organizations 合作：

- EnableHealthServiceAccessForOrganization— 授权Amazon Health权限与 Organizations 交互并将 SLR 应用于组织中的管理账户。
- DisableHealthServiceAccessForOrganization— 撤销权限Amazon Health与 Organizations 进行互动。
- DescribeHealthServiceStatusForOrganization— 返回状态信息，说明是否Amazon Health已为您的组织启用。

您必须拥有商业或企业支持计划才能调用这些 API 操作。如果您从至少具有商业支持计划的账户调用 `DescribeEventForOrganization` 和 `DescribeAffectedAccountsForOrganization` 操作，则可以返回有关组织中任何账户的信息，而不必考虑各个账户的支持级别。请见以下示例。

Example 示例：组织包含具有商业和开发人员支持计划的账户

- 您的组织中有三个账户。管理账户具有商业支持计划，而另两个账户具有开发人员支持计划。
- 您可以调用`DescribeEventForOrganization`API 操作从管理账户或从可担任具有所需权限的角色的账户。
- Amazon Health 返回所有三个账户的信息。

如果您从至少具有商业支持计划的账户调用 `DescribeEventDetailsForOrganization` 和 `DescribeAffectedEntitiesForOrganization` API 操作，则只能返回有关组织中具有商业或企业支持级别计划的账户的信息。

Example 示例：组织包含具有商业、商业和开发人员支持计划的账户

- 您的组织中有五个账户。管理账户具有商业支持计划，两个账户具有商业支持计划，而另两个账户具有开发人员支持计划。
- 您可以调用`DescribeEventDetailsForOrganization`API 操作。
- Amazon Health 仅返回具有企业或商业支持计划的账户的信息。具有开发人员支持计划的账户将显示在响应的 `failedSet` 中。

监控Amazon HealthAmazon CloudWatch Events

您可以使用 Amazon CloudWatch Events 检测和响应Amazon Health事件. 然后，CloudWatch Event 会根据您创建的规则，在事件匹配您在规则中指定的值时调用一个或多个目标操作。根据事件的类型，您可以发送通知、捕获事件信息、采取纠正措施、启动事件或采取其他操作。例如，您可以使用Amazon Health以接收电子邮件通知，如果您有Amazon中的资源Amazon账户（例如 Amazon Elastic Compute Compute Cloud (Amazon EC2) 实例）。

Notes

- 本主题使用 CloudWatch 事件控制台创建规则。您还可以使用 Amazon EventBridge 控制台创建规则。有关更多信息，请参阅 。为创建规则Amazon服务中的Amazon EventBridge 用户指南。
- 对于这两项服务,Amazon Health尽最大努力提供事件。事件并不总是保证传送到 CloudWatch 事件或 EventBridge。

您可以在以下类型的目标：将 CloudWatch Events 用于您的Amazon Health工作流程：

- Amazon Lambda 函数
- Amazon Kinesis Data Streams
- Amazon Simple Queue Service (Amazon SQS) 队列
- 内置目标（CloudWatch 警报操作）
- Amazon Simple Notification Service (Amazon SNS) 主题

例如，您可以使用 Lambda 函数，以在Amazon Health事件发生。或者，您也可以使用 Lambda 和 CloudWatch 事件 Amazon SNS 在Amazon Health事件发生。

主题

- About (关于 Amazon Lumberyard)Amazon的区域Amazon Health (p. 43)
- 关于公共活动Amazon Health (p. 44)
- 为创建 CloudWatch Events 规则Amazon Health (p. 44)
- 正在接收Amazon Health使用事件AmazonChatbot (p. 46)
- Amazon EC2 实例的自动化操作 (p. 47)

About (关于 Amazon Lumberyard)Amazon的区域Amazon Health

您必须为要接收通知的每个区域创建 CloudWatch 事件规则Amazon Health事件. 如果您没有创建规则，则不会收到事件。例如，要接收来自中国（北京）区域的事件，您必须为此区域创建规则。

一段时间Amazon Health事件不是区域特定的，而是全局事件，例如为 AWS Identity and Access Management (IAM) 发送的事件。要接收全球事件，您必须为中国（宁夏）区域创建规则。

关于公共活动Amazon Health

仅限Amazon Health事件特定于Amazon帐户发送到 CloudWatch 事件。例如，这可能包括对 Amazon EC2 实例的必需更新以及其他可能影响您的账户和资源的计划更改事件等事件。

目前，您无法使用 CloudWatch Events 返回公有来自的事件服务运行状况控制面板。服务运行状况控制面板中的事件会提供有关服务的区域可用性的公有信息。这些事件不特定于Amazon帐户，因此不会被传输到 CloudWatch Events。

相反，您可以使用Amazon Health控制台和DescribeEventDetailsoperation. 您可以使用任一选项返回有关事件的信息，然后确定该事件是 Service Health Dashboard 中的公共事件还是影响您账户的账户特定事件。

您可以使用以下选项确定事件是公共事件还是特定于账户的事件：

- 在Amazon Personal Health Dashboard中，选择受影响的资源选项卡事件日志页. 具有资源的事件特定于您的账户。没有资源的事件是公开的，并不是特定于您的账户。有关更多信息，请参阅 Amazon Personal Health Dashboard入门 (p. 2)。
- 使用 Amazon Health API 返回 `eventScopeCode` 参数。事件可以具有 `PUBLIC`、`ACCOUNT_SPECIFIC` 或 `NONE` 值。有关更多信息，请参阅 。DescribeEventDetails中的Amazon HealthAPI 参考。

您也可以使用Amazon HealthService Health Dashboard 通知程序工具，以获取公共事件的通知。有关更多信息，请参阅 。aws-健康工具在 GitHub 网站上。

为创建 CloudWatch Events 规则Amazon Health

您可以创建一个 CloudWatch 事件规则，以获得Amazon Health事件。在为 Amazon Health 创建事件规则之前，您应该先执行以下操作：

- 熟悉 CloudWatch Events 中的事件、规则和目标。有关更多信息，请参阅 。什么是 Amazon CloudWatch Events？中的Amazon CloudWatch Events 用户指南和CloudWatch Svents-跟踪和响应对您的Amazon资源。
- 创建要在您的事件规则中使用的目标。

为创建 CloudWatch Events 规则Amazon Health

1. 通过以下网址打开 CloudWatch 控制台：https://console.aws.amazon.com/cloudwatch/。
2. 要更改 Amazon 区域，请使用页面右上角的 Region selector (区域选择器)。选择要在其中跟踪 Amazon Health 事件的区域。
3. 在导航窗格中的事件中，选择Rule。
4. 选择 Create rule，然后在 Event Source 下，对于 Service Name，选择 Health。
5. 适用于事件类型下，选择以下选项之一。
   - 选择所有事件创建应用到所有Amazon服务。此规则监视所有来自Amazon Health。如果您选择此选项，则无法指定事件类型类别或事件类型代码。
   - 选择具体 Health 事件、特定服务，然后从列表中选择服务名称。此示例创建了一个规则，用于监视EC2，以便 CloudWatch 事件仅监控 Amazon EC2 事件。
6. 如果您选择特定服务，则选择以下选项之一。
   - 选择任何事件类型类别创建适用于所有事件类型类别的规则。
   - 选择特定事件类型类别，然后从列表中选择一个值。这将创建一个仅应用于一个事件类型类别的规则，例如scheduledChange。

Tip

- 监控所有Amazon Health事件，建议选择任何事件类型类别和任何资源。这可确保您的规则监视任何Amazon Health事件（包括指定服务的任何新事件类型代码）。有关示例规则，请参阅。所有 Amazon EC2 事件 (p. 45)。
- 您可以创建一个规则来监视多个服务或事件类型类别。为此，您必须手动更新规则的事件模式。有关更多信息，请参阅 为多个服务和类别创建规则 (p. 45)。

7. 如果选择了特定的服务和事件类型类别，请为事件类型代码选择以下选项之一。
   - 选择任何事件类型代码创建适用于所有事件类型代码的规则。
   - 选择特定事件类型代码，然后从列表中选择一个或多个值。这将创建一个仅适用于特定事件类型代码的规则。例如，如果您选择**AWS_EC2_INSTANCE_STOP_SCHEDULED**和**AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED**，则您的规则仅适用于这些事件发生在您的帐户中时。
8. 为受影响的资源选择以下一个选项。
   - 选择任何资源创建适用于所有资源的规则。
   - 选择具体资源并输入一个或多个资源的 ID。例如，您可以指定 Amazon EC2 实例 ID，例如`i-EXAMPLEa1b2c3de4`来监视仅影响此资源的事件。
9. 审查您的规则设置以满足事件监控要求。
10. 在 Targets 区域，选择 Add target*。
11. 在选择目标类型列表中，选择您准备为此规则使用的目标类型，然后配置该类型所需的任何其他选项。
12. 选择 Configure details。
13. 在存储库的配置规则详细信息页面上，输入规则的名称和描述，然后选择州复选框以在创建规则后立即启用它。
14. 选择 Create rule (创建规则)。

Example ：针对特定 Amazon EC2 事件的规则

以下示例创建一个规则，以便 CloudWatch 事件监视以下内容：

- Amazon EC2 服务
- 这些区域有：scheduledChange事件类型类别
- 事件类型代码`AWS_EC2_INSTANCE_TERMINATION_SCHEDULED`和`AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED`
- 具有`i-EXAMPLEa1b2c3de4`ID

为多个服务和类别创建规则

上一步骤中的示例说明了如何为单个服务和事件类型类别创建规则。您还可以为多个服务和事件类型类别创建规则。这意味着，您不必为您要监控的每个服务和类别创建单独的规则。为此，您必须编辑事件模式，然后手动输入更改。

您可以使用以下任意选项。

为现有规则添加服务和类别

1. 在 CloudWatch 事件控制台中，在Rule页面上，选择规则名称。
2. 在右上角，选择操作，然后选择编辑。
3. 适用于事件模式中，在文本字段中输入您的更改。

4. 选择配置详细信息，然后选择更新规则保存您的更改。

为新规则添加服务和类别

1. 按照中过程操作为创建 CloudWatch Events 规则Amazon Health (p. 44)到步骤 6 (p. 44)。
2. 而不是从列表中选择单个服务或类别，事件模式预览中，选择编辑。
3. 在文本字段中输入您的更改，然后选择Save。请参阅以下信息示例模式 (p. 46)。
4. 查看您的事件模式，然后按照为创建 CloudWatch Events 规则Amazon Health (p. 44)创建您的规则。

使用 API 或Amazon命令行界面 (AmazonCLI)

对于新规则或现有规则，请使用PutRuleAPI 操作或`aws events put-rule`命令更新事件模式。例如，AmazonCLI 命令，请参阅推出规则中的AmazonCLI 命令参考。

Example 示例：多种服务和事件类型

以下事件模式创建了一个规则来监视`issue`、`accountNotification`, 和`scheduledChange`事件类型类别和三个Amazon服务。

```
{
  "detail": {
    "eventTypeCategory": [
      "issue",
      "accountNotification",
      "scheduledChange"
    ],
    "service": [
      "AUTOSCALING",
      "VPC",
      "EC2"
    ]
  },
  "detail-type": [
    "AWS Health Event"
  ],
  "source": [
    "aws.health"
  ]
}
```

正在接收Amazon Health使用事件AmazonChatbot

您可以接收Amazon Health事件，例如 Slack 和 Amazon Chime。使用此事件可以识别最近Amazon服务问题可能影响Amazon应用程序和基础设施. 然后，您可以登录到Amazon Personal Health Dashboard以了解有关更新的更多信息。例如，如果您正在监控`AWS_EC2_INSTANCE_STOP_SCHEDULED`事件类型Amazon帐户，Amazon Health事件可以直接显示在您的 Slack 频道中。

Prerequisites

在开始之前，您必须具有以下内容：

- 聊天客户端配置为AmazonChatbot 您可以配置 Amazon Chime 和松弛。有关更多信息，请参阅 。开始使用AmazonChatbot中的AmazonChatbot 管理员指南。

- 您创建并订阅的 Amazon SNS 主题。如果您已有 SNS 主题，则可以使用现有主题。有关更多信息，请参阅 。Amazon SNS 入门中的Amazon Simple Notification Service 开发人员指南。

要接收Amazon Health使用事件AmazonChatbot

1. 按照为创建 CloudWatch Events 规则Amazon Health (p. 44)中过程操作。
   a. 当您选择步骤 11 (p. 45)下，选择 SNS 主题。您将使用此 SNS 主题在AmazonChatbot 控制台
   b. 完成创建规则的剩余步骤。
2. 导航到AmazonChatbot。
3. 选择您的聊天客户端，例如您的 Slack 频道名称，然后选择编辑。
4. 在通知-可选部分，用于主题中，选择您指定的相同 SNS 主题。
5. 选择保存。

   何时Amazon Health将事件发送到与您的规则匹配的 CloudWatch 事件，Amazon Health事件将出现在您的聊天客户端中。
6. 选择事件名称，以查看Amazon Personal Health Dashboard。

Amazon EC2 实例的自动化操作

您可以自动执行操作以响应 Amazon EC2 实例的计划事件。何时Amazon Health将事件发送到Amazon帐户，您的 CloudWatch 事件规则随后可以调用目标，例如Amazon Web Services Systems Manager自动化文档，代表您实现自动化操作。

例如，在为 Amazon 弹性块存储 (Amazon EBS) 支持的 EC2 实例计划 Amazon EC2 实例停用事件时，Amazon Health将发送`AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED`事件类型为 Amazon Personal Health Dashboard。当您的规则检测到此事件类型时，您可以自动执行实例的停止和启动操作。这样，您无需手动执行这些操作。

Notes

- 此过程使用 CloudWatch 事件控制台创建规则。您还可以使用 EventBridge 控制台创建规则。有关更多信息，请参阅 。为创建规则Amazon服务中的Amazon EventBridge 用户指南。
- 要自动执行 Amazon EC2 实例的操作，必须由 Systems Manager 管理这些实例。

有关更多信息，请参阅 。使用 EventBridge 自动化 Amazon EC2中的适用于 Linux 实例的 Amazon EC2 用户指南。

Prerequisites

您必须先创建 AWS Identity and Access Management (IAM) 策略、创建 IAM 角色并更新信任策略，然后才能创建规则。

创建 IAM 策略

按照以下步骤为您的角色创建客户托管策略。此策略授予角色代表您执行操作的权限。此过程使用 IAM 控制台中的 JSON 策略编辑器。

创建 IAM 策略

1. 登录 Amazon Web Services Management Console，单击 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
2. 在导航窗格中，选择 Policies。

3. 选择创建策略。
4. 选择 JSON 选项卡。
5. 复制以下 JSON，然后替换编辑器中的默认 JSON。

   a. 在Resource参数，对于 Amazon 资源名称 (ARN)，输入您的Amazon账户 ID。
   b. 您还可以替换角色名称或使用默认名称。此示例使用*### CWT ##*。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:DescribeInstanceStatus"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "sns:Publish"
      ],
      "Resource": [
        "arn:aws:sns:*:*:Automation*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::123456789012:role/AutomationCWRole"
    }
  ]
}
```

6. 选择 Next:。标签。
7. （可选）您可以使用标签作为键值对以向策略添加元数据。
8. 选择 Next:。审核。
9. 在存储库的查看策略页面上，输入名称例如*#######*和说明（可选）。
10. 查看摘要页面以查看策略允许的权限，然后选择创建策略。

此策略定义角色可以执行的操作。有关更多信息，请参阅 。创建 IAM 策略（控制台）中的IAM 用户指南。

创建 IAM 角色

创建策略后，您必须创建 IAM 角色，然后将策略附加到该角色。

为创建角色Amazon服务

1. 登录 Amazon Web Services Management Console，单击 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
2. 在导航窗格中，选择角色，然后选择创建角色。
3. 对于选择受信任实体的类型，选择 Amazon 服务。
4. 选择EC2对于您希望允许其承担此角色的服务。
5. 选择 Next:。Permissions (下一步：权限)。
6. 输入您创建的策略名称，例如*******，然后选中策略旁的复选框。
7. 选择 Next:。标签。
8. （可选）您可以使用标签作为键值对以向角色添加元数据。
9. 选择 Next:。审核。
10. 适用于Role name (角色名称)中，输入*### CWT ##*。此名称必须与您之前创建的 IAM 策略的 ARN 中显示的名称相同。
11. （可选）角色描述中，输入角色的描述。
12. 检查角色，然后选择 Create role。

有关更多信息，请参阅 。为创建角色Amazon服务中的IAM 用户指南。

更新信任策略

按照此过程更新您创建的角色的信任策略。您必须完成此过程，以便在 CloudWatch 事件控制台中选择此角色。

更新角色的信任策略

1. 登录 Amazon Web Services Management Console，单击 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
2. 在导航窗格中，选择 Roles。
3. 在角色列表中Amazon帐户中，选择您创建的角色的名称，例如*### CWT ##*。
4. 选择 Trust relationships 选项卡，然后选择 Edit trust relationship。
5. 适用于策略文档，复制以下 JSON，然后替换默认策略。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "ssm.amazonaws.com",
                    "events.amazonaws.com"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

6. 选择 Update Trust Policy。

有关更多信息，请参阅 。修改角色信任策略（控制台）中的IAM 用户指南。

为 CloudWatch Events 创建规则

按照此步骤在 CloudWatch Event 控制台中创建规则，这样就可以自动完成计划停用的 EC2 实例的停止和启动。

为 Systems Manager 自动操作的 CloudWatch 事件创建规则

1. 通过以下网址打开 CloudWatch 控制台：https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中的事件中，选择Rule。
3. 选择 Create rule，然后在 Event Source 下，对于 Service Name，选择 Health。
4. 适用于事件类型中，选择具体 Health 事件。
5. 选择特定服务，然后选择EC2。
6. 选择特定事件类型类别，然后选择scheduledChange。
7. 选择特定事件类型代码，然后选择事件类型代码。例如，对于 Amazon EC2 EBS 支持的实例，请选择**AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED**。对于 Amazon EC2 实例存储支持的实例，选择**AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED**。
8. 选择任何资源。

   您的事件模式预览可能与以下示例类似。

   Example

```
{
  "source": [
    "aws.health"
  ],
  "detail-type": [
    "AWS Health Event"
  ],
  "detail": {
    "service": [
      "EC2"
    ],
    "eventTypeCategory": [
      "scheduledChange"
    ],
    "eventTypeCode": [
      "AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED"
    ]
  }
}
```

9. 添加 Systems Manager Automation 文档目标。在目标中，选择添加目标 *，然后选择SSM 自动化。
10. 适用于文档 *中，选择Amazon-RestartEC2Instance。
11. 展开配置自动化参数，然后选择输入转换器。
12. 对于输入路径字段中，输入{"Instances":"$.resources"}。
13. 对于第二个字段，输入{"InstanceId": <Instances>}。
14. 选择使用现有角色，然后选择您创建的 IAM 角色，例如*### CWT ##*。

    Note

    如果您没有具备所需 EC2 和 Systems Manager 权限和可信关系的现有 IAM 角色，则您的角色将不会显示在列表中。有关更多信息，请参阅 Prerequisites (p. 47)。
15. 选择 Configure details。
16. 为您的规则输入名称和描述。保留州选项。
17. 选择 Create rule (创建规则)。

监控 Amazon Health

监控是保持可靠性、可用性和性能的重要环节。Amazon Health和您的其他Amazon解决方案。Amazon提供以下监控工具监视Amazon Health，在出现错误时进行报告，并在适当的时候采取措施：

- Amazon CloudWatch 可监控您的Amazon资源以及您在上运行的应用程序Amazon实时操作。您可以收集和跟踪指标，创建自定义的控制面板，以及设置警报以在指定的指标达到您指定的阈值时通知您或采取措施。有关更多信息，请参阅 Amazon CloudWatch 用户指南。

  您可以使用 Amazon CloudWatch Events，以便您收到Amazon Health事件，这可能影响服务和资源。例如，如果Amazon Health发布有关 Amazon EC2 实例的事件，您可以使用这些通知采取措施并根据需要更新或替换资源。有关更多信息，请参阅 监控Amazon HealthAmazon CloudWatch Events (p. 43)。
- Amazon CloudTrail捕获由您的或代表该地区发出的 API 调用和相关事件。Amazon账户，并将日志文件传送到您指定的 Amazon S3 存储桶。您可以标识哪些用户和账户调用了 Amazon、从中发出调用的源 IP 地址以及调用的发生时间。有关更多信息，请参阅 Amazon CloudTrail 用户指南。

主题

- 使用 Amazon CloudTrail 记录 Amazon Health API 调用 (p. 51)

使用 Amazon CloudTrail 记录 Amazon Health API 调用

Amazon Health 与 Amazon CloudTrail 集成，后者是在 Amazon Health 中记录用户、角色或 Amazon 服务所执行操作的服务。CloudTrail 捕获 API 调用Amazon Health作为事件。捕获的调用包含来自 Amazon Health 控制台和代码的 Amazon Health API 操作调用。如果您创建跟踪，则可以使 CloudTrail 事件持续传送到 Amazon S3 存储桶（包括Amazon Health。如果您不配置跟踪，则仍可在 CloudTrail 控制台中的 Event history (事件历史记录) 中查看最新事件。通过使用 CloudTrail 收集的信息，可以确定已对发出的请求。Amazon Health、发出请求的源 IP 地址、用户、时间以及其他详细信息。

要了解有关 CloudTrail 的更多信息（包括如何对其进行配置和启用），请参阅Amazon CloudTrail用户指南。

Amazon HealthCloudTrail 中的信息

CloudTrail 已在您的Amazon创建账户时，即可。当受支持的事件活动发生在Amazon Health，该活动将记录在 CloudTrail 事件中，并与其他Amazon中的服务事件事件历史记录。您可以在 Amazon 账户中查看、搜索和下载最新事件。有关更多信息，请参阅使用 CloudTrail 事件历史记录查看事件。

要持续记录 Amazon 账户中的事件（包括 Amazon Health 的事件），请创建跟踪。通过 trail (跟踪)，CloudTrail 可将日志文件传送至 Amazon S3 存储桶。默认情况下，在控制台中创建跟踪时，此跟踪应用于所有 Amazon 区域。此跟踪记录中所有区域中的事件Amazon分区，并将日志文件传送到您指定的 Amazon S3 存储桶。此外，您还可以配置其他Amazon服务进一步分析在 CloudTrail 日志中收集的事件数据并采取措施。有关更多信息，请参阅下列内容：

- 创建跟踪概述
- CloudTrail 支持的服务和集成
- 为 CloudTrail 配置 Amazon SNS 通知
- 从多个账户中接收 CloudTrail 日志文件

全部Amazon HealthAPI 操作由 CloudTrail 记录，并记录在Amazon HealthAPI 参考。例如，对DescribeEvents、DescribeEventDetails, 和DescribeAffectedEntities操作将在 CloudTrail 日志文件中生成条目。

Amazon Health支持在 CloudTrail 日志文件中将以下操作记录为事件：

- 请求是使用根用户还是 IAM 凭证发出的
- 请求是使用角色还是联合身份用户的临时安全凭证发出的
- 请求是否由其他 Amazon 服务发出

有关更多信息，请参阅 CloudTrail userIdentity 元素。

您可以将日志文件在 Amazon S3 存储桶中存储任意长的时间。您也可以定义 Amazon S3 生命周期规则以自动存档或删除日志文件。默认情况下，将使用 Amazon S3 服务器端加密 (SSE) 对日志文件进行加密。

要获得日志文件传输的通知，可以将 CloudTrail 配置为在传输新日志文件时发布 Amazon SNS 通知。有关更多信息，请参阅为 CloudTrail 配置 Amazon SNS 通知。

您还可以聚合Amazon Health中的日志文件多个Amazon账户添加到单个 Amazon S3 存储桶。

有关更多信息，请参阅 。 接收多个账户中的 CloudTrail 日志文件。

示例：Amazon Health 日志文件条目

跟踪是一种配置，可用于将事件作为日志文件传送到您指定的 Amazon S3 存储桶。CloudTrail 日志文件包含一个或多个日志条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序显示。

下面的示例显示了一个 CloudTrail 日志条目，该条目演示了DescribeEntityAggregatesoperation.


```
{
   "Records": [
   {
   "eventVersion": "1.05",
   "userIdentity": {
      "type": "IAMUser",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE",
      "arn": "arn:aws:iam::123456789012:user/JaneDoe",
      "accountId": "123456789012",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "userName": "JaneDoe",
      "sessionContext": {"attributes": {
         "mfaAuthenticated": "false",
         "creationDate": "2016-11-21T07:06:15Z"
      }},
      "invokedBy": "Amazon Internal"
    },
   "eventTime": "2016-11-21T07:06:28Z",
   "eventSource": "health.amazonaws.com",
   "eventName": "DescribeEntityAggregates",
   "awsRegion": "cn-northwest-1",
   "sourceIPAddress": "203.0.113.0",
   "userAgent": "Amazon Internal",
   "requestParameters": {"eventArns": ["arn:aws:health:cn-northwest-1::event/EBS/
EBS_LOST_VOLUME/EBS_LOST_VOLUME_123"]},
   "responseElements": null,
   "requestID": "05b299bc-afb9-11e6-8ef4-c34387f40bd4",
   "eventID": "e4deb9dc-dbc2-4bdb-8515-73e8abcbc29b",
   "eventType": "AwsApiCall",
```

```
   "recipientAccountId": "123456789012"
   }
   ],
   ...
}
```

Amazon Health 的文档历史记录

下表介绍了此版本的 Amazon Health 的文档。

- API 版本： 2016-08-04
- 最近文档更新： 2021 年 5 月 7 日

下表介绍了对Amazon Health文档，从 2020 年 8 月 28 日开始。您可以订阅 RSS 源来接收有关更新的通知。

更新-历史记录-更改	更新-历史记录-描述	更新-历史记录-日期
有关 CloudWatch 事件的更新文档 (p. 54)	添加了有关如何为多个服务和事件类型类别创建规则的章节。有关更多信息，请参阅 。为多个服务和类别创建规则。	2021 年 5 月 7 日
有关 CloudWatch 事件的更新文档 (p. 54)	更新部分以实现自动化Amazon Web Services Systems ManagerAmazon CloudWatch Events 规则的操作。有关更多信息，请参阅 。针对 Amazon EC2 实例实现自动化操作。	2021 年 4 月 28 日
有关 CloudWatch 事件的更新文档 (p. 54)	添加了要接收的部分Amazon Health您的聊天客户端中的事件。有关更多信息，请参阅 。接收Amazon Health使用事件AmazonChatbot。	2021 年 3 月 16 日
更新的文档 (p. 54)	以下主题更新了： • 更新了聚合Amazon Health事件主题 • 重新整理和更新了的监控Amazon HealthAmazon CloudWatch Events 的事件主题 • 更新了基于资源和基于操作的条件部分	2021 年 1 月 29 日
在控制台中添加了用于组织视图	您可以将Amazon Health控制台以启用组织视图功能。然后，您可以在Amazon组织.	2020 年 12 月 14 日
高可用性终端演示	您可以使用示例代码来确定活动的区域终端节点并签名Amazon的区域Amazon Health。	2020 年 10 月 22 日
用户指南更新 (p. 54)	组织更新并添加了 RSS 源，以便您可以订阅Amazon Health文档中）。	2020 年 8 月 28 日

早期更新

变更	描述	日期
更新了组织视图主题以包含示例。	请参阅 使用组织视图跨账户聚合 Amazon Health 事件 (p. 35)。	2020 年 6 月 3 日
安全性和 Amazon Health	添加了有关使用 Amazon Health 时的安全注意事项的信息。请参阅 Amazon Health 中的安全性 (p. 14)。	2020 年 5 月 5 日
添加了新的部分，以说明如何使用组织视图跨 Amazon Organizations 中的所有账户聚合事件。	请参阅 使用组织视图跨账户聚合 Amazon Health 事件 (p. 35)。	2019 年 12 月 18 日
添加了新的部分“基于资源和基于操作的条件”，以解释 Amazon Health API 提供的事件限制。	请参阅 适用于 Amazon Health 的 Identity and Access Management (p. 15)。	2018 年 8 月 2 日
服务发布。	Amazon Health 已发布。	2019 年 12 月 18 日

Amazon术语表

最新的Amazon术语，请参阅Amazon术语表中的Amazon一般参考。

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。