亚马逊云科技

用户指南

Amazon Health

Amazon Health: 用户指南

Amazon Web Services 文档中描述的 Amazon Web Services 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 Amazon Web Services 服务入门 (PDF)。

Table of Contents

什么是 Amazon Health？

Amazon Health 提供对您的资源绩效以及 Amazon Web Services 服务 和账户可用性的持续可见性。您可以使用 Amazon Health 事件来了解服务和资源更改会如何影响正在运行的应用程序 Amazon。Amazon Health 提供相关且及时的信息，以帮助您管理正在进行的活动。 Amazon Health 还可以帮助您了解计划中的活动并为之做好准备。该服务提供由 Amazon Web Services 资源运行状况变化触发的警报和通知，因此您可以获得近乎即时的事件可见性和指导，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 D oard Person Amazon al Health Dashboard。仪表板无需设置，可供经过身份验证的 Amazon Web Services 用户使用。有关更多服务亮点，请参阅控制面板详细信息页面。

Amazon Health 为所有客户提供名为 “控制 Amazon Health 面板” 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。

要了解有关服务的基础知识 Amazon Health 和在使用服务时会遇到的术语，请了解基本信息的概念 Amazon Health。 Amazon Health

> **备注**
>
> - 所有 Amazon Web Services 客户均可使用 Amazon Health 控制面板，无需支付额外费用。
> - 所有 Amazon 买家都可以通过 Amazon 接收 Amazon Health 活动 EventBridge ，无需支付额外费用。
> - 如果您有商业、企业入口或企业支持计划，则可以使用 Amazon Health API 与内部和第三方系统集成。有关更多信息，请参阅 Amazon Health API 参考。
> - 有关可用 Amazon Web Services 支持 计划的更多信息，请参阅Amazon Web Services 支持。

的概念 Amazon Health

了解 Amazon Health 概念并了解如何使用该服务来维护您的应用程序、服务和资源的运行状况 Amazon Web Services 账户。

主题

Amazon Health 事件

Amazon Health 事件，也称为 Health 事件，是代表其他 Amazon 服务 Amazon Health 发送的通知。您可以使用这些事件来了解即将发生或已经计划的可能影响您的账户的更改。例如，如果 Amazon Identity and Access Management (IAM) 计划弃用托管策略或 Amazon Config 计划弃用托管规则，则 Amazon Health 可以发送事件。 Amazon Health 当中存在服务可用性问题时，还会发送事件 Amazon Web Services 区域。您可以查看事件描述以了解问题、确定任何受影响的资源并采取任何建议的措施。

有两种运行状况事件类型：

目录

特定于账户的事件

特定于账户的事件对您 Amazon Web Services 账户 或您组织中的账户来说是本地的 Amazon 。例如，如果您使用的区域中的亚马逊弹性计算云 (Amazon EC2) 实例类型出现问题，请 Amazon Health 提供有关该事件的信息以及受影响资源的名称。

您可以从Amazon Health 控制面板、Amazon Health API 中查找特定于账户的事件，也可以使用 Amazon EventBridge 或Amazon 用户通知来接收通知。

公有事件

公有事件是不特定于账户的报告服务事件。例如，如果美国东部（俄亥俄州）地区的 Amazon Simple Storage Service (Amazon S3) 出现服务问题，即使您没有使用该服务或在该地区也没有 S3 存储桶，Amazon Health 也会提供有关该事件的信息。我们建议您先查看公有通知，然后再对其采取措施。

您可以从 Amazon Health 控制面板和控制面板（服务运行状况）中 Amazon Health 找到公共事件。

如果您拥有这一账户，请参阅Amazon Health Dashboard 入门。

如果您没有这一账户，请参阅Amazon Health 仪表板。

Amazon Health 仪表板

如果您有 Amazon Web Services 账户，您的 Amazon Health 控制面板会同时显示公共事件和特定于账户的事件。

我们建议您使用 Amazon Health 控制面板来了解可提供一般意识的事件，例如某个地区服务即将出现的维护问题。您还可以使用 Amazon Health 控制面板来了解可能直接影响您的事件，例如您账户中已弃用的资源。

您可以登录在https://health.aws.amazon.com/health/家中 Amazon Web Services Management Console 查看 Amazon Health 控制面板。

有关更多信息，请参阅 Amazon Health Dashboard 入门。

Amazon Health 控制面板-服务运行状况

如果您没有帐户，则可以使用 Amazon Health 控制面板-服务运行状况处于https://health.aws.amazon.com/health/状态来查看公共事件。公有事件是报告的 Amazon Web Services 的服

务问题，用于提供有关服务可用性的信息。本网站仅显示公有事件，而非特定于任何账户。您无需登录或拥有账户即可查看该页面。

有关更多信息，请参阅 Amazon Health 仪表板。

事件类型代码

运行状况事件中显示的事件类型代码包括受影响的服务和事件的类型。例如，如果您收到带有 AWS_EC2_SYSTEM_MAINTENANCE_EVENT 事件类型代码的运行状况事件，则表示该服务正在计划一个可能会影响您的维护事件。使用此信息提前计划或对您的账户采取措施。

事件类型的类别

所有运行状况事件都有一个关联的事件类型的类别。对于某些事件，事件类型的类别可能会在事件类型代码中显示，例如 AWS_RDS_MAINTENANCE_SCHEDULED 代码。在此示例中，类别为已计划。您可以使用这些信息从较高层面了解事件类别。

最佳做法是监控所有事件类型类别。请注意，每个类别针对不同类型的事件显示。您还可以使用 DescribeEventTypesAPI 操作来查找事件类型类别。

账户通知

这些事件提供有关您账户和服务的管理或安全性信息。这些事件可能会提供某些信息，或者可能需要您采取紧急措施。我们建议您注意这些类型的事件，并查看所有建议的措施。

以下是账户通知的事件类型代码示例：

- AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION – 您有一个可能允许公有访问的 Amazon S3 存储桶。
- AWS_BILLING_SUSPENSION_NOTICE – 您的账户有未付费用并已被暂停，或者您停用了账户。
- AWS_WORKSPACES_OPERATIONAL_NOTIFICATION— Amazon 存在服务问题 WorkSpaces。

事务

这些事件是影响 Amazon 服务或资源的意外事件。此类别中的常见事件包括有关导致服务质量下降的操作问题的通信，或提醒您注意的本地资源级别的问题。

以下是问题的事件类型代码示例：

- AWS_EC2_OPERATIONAL_ISSUE – 服务的操作问题，例如延迟使用服务。

- AWS_EC2_API_ISSUE – 服务 API 的操作问题，例如 API 操作的延迟时间增加。
- AWS_EBS_VOLUME_ATTACHMENT_ISSUE – 本地资源级别的问题，可能会影响您的 Amazon Elastic Block Store (Amazon EBS) 资源。
- AWS_ABUSE_PII_CONTENT_REMOVAL_REPORT – 此事件意味着，如果您不采取措施，您的账户可能会被暂停。

计划更改

这些事件提供了有关服务和资源即将发生的更改的信息。这些事件包括计划的生命周期事件，例如不同版本的 end-of-support通知和自动升级。有些事件可能会建议您采取措施以避免服务中断，而另一些事件则会自动发生，无需您采取任何措施。在执行计划的更改活动期间，您的资源可能暂时不可用。此类别中的所有事件均为账户特定事件。

以下是已计划更改的事件类型代码示例：

- AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED— Amazon EC2 实例需要重启。
- AWS_SAGEMAKER_SCHEDULED_MAINTENANCE— SageMaker AI 需要维护事件，例如修复服务问题。
- AWS_RDS_PLANNED_LIFECYCLE_EVENT— Amazon RDS 正在安排计划中的生命周期 end-of-support事件，例如其某个版本的事件，需要客户采取行动。

> **Tip**
>
> 如果您使用 Amazon Health API 或 Amazon Command Line Interface (Amazon CLI) 返回事件详细信息，则`Event`对象将包含带有`ACCOUNT_SPECIFIC`值的`eventScopeCode`字段。有关更多信息，请参阅 Amazon Health API 参考。

事件状态

事件状态会告知您运行状况事件是打开、关闭还是即将到来。您可以在 Amazon Health 控制面板或 Amazon Health API 中查看最长 90 天的健康事件。

受影响的实体

受影响的实体是指可能受事件影响的 Amazon 资源。例如，如果您收到账户中使用的特定实例类型的亚马逊 EC2 维护计划事件，则可以使用 Health 事件来确定受影响实例的 ID。使用此信息来解决任何潜在的服务问题，例如创建或弃用资源。

Amazon Health 亚马逊上的活动 EventBridge

您可以为账户设置 Amazon EventBridge 规则，以便在账户收到相应 Amazon Health 事件后自动执行操作。这些操作可以是常规操作，例如将所有已计划生命周期事件消息发送到聊天界面。或者，它们也可以是特定的操作，例如在 IT 服务管理工具中触发一个工作流程。

有关更多信息，请参阅 通过 Amaz Amazon Health on 监控事件 EventBridge。

Amazon Health API

您可以使用 Amazon Health API 以编程方式访问Amazon Health 控制面板中显示的信息，例如：

- 获取有关可能影响您的 Amazon 服务和资源的事件的信息
- 为您的 Amazon 组织启用或禁用组织视图功能
- 按特定服务、事件类型的类别和事件类型代码来筛选您的事件

有关更多信息，请参阅 Amazon Health API 参考。

> **Note**
>
> 要使用 Amazon Health API，您必须拥有商业、企业入口或企业支持计划。Amazon Web Services 支持如果您使用没有商业、企业入口或企业支持计划的账户调用 Amazon Health API，则会收到`SubscriptionRequiredException`错误消息。

组织视图

您可以使用此功能将您 Amazon 账户的所有健康事件汇总 Amazon Organizations 到 Amazon Health 控制面板中的单个视图中。然后，您可以登录组织的管理账户或使用 Amazon Health API 查看可能影响不同账户和资源的所有事件。您可以通过 Amazon Health 控制台或 API 启用此功能。有关更多信息，请参阅 跨账号聚合 Amazon Health 事件。

Amazon 用户通知服务

Amazon Health 与集成，Amazon 用户通知服务因此您可以轻松接收和控制有关影响您 Amazon Web Services 账户 和服务的事件的通知。 用户通知服务 默认情况下为 Amazon Health 事件提供托管通知。您可以将这些订阅配置为控制通过基于时间的聚合接收消息的频率、收到通知 Amazon Health

的事件类型以及通知的发送地点。要开始使用，请在 用户通知服务 中打开Amazon Web Services Management Console。有关更多信息，请参阅 ???

Amazon Health Dashboard 入门

您可以使用 Amazon Health 控制面板来了解 Amazon Health 事件。这些事件可能会影响您的 Amazon Web Services 服务 或 Amazon Web Services 账户。登录账户后， Amazon Health 控制面板将通过以下方式显示信息：

- 您的账户事件 – 此页面显示特定于您账户的事件。您可以查看未完成的更改、最近更改和已计划的更改。您还可以查看通知和显示过去 90 天内所有事件的事件日志。
- 您的组织事件 – 此页面显示 Amazon Organizations中特定于您组织的事件。您可以查看组织中未完成的更改、最近更改和已计划的更改。您还可以查看通知以及显示过去 90 天内所有组织事件的事件日志。

> **Note**
>
> 如果您没有 Amazon Web Services 账户，则可以使用Amazon Health 仪表板来了解一般服务的可用性。
> 如果您有帐户，我们建议您登录 Amazon Health 控制面板，以更深入地了解可能影响您的服务和资源的事件和即将发生的变化。

主题

设置您的 Amazon 账户

在启用之前 Amazon Health，必须有一个 Amazon Web Services 账户。如果您没有 Amazon 帐户，请完成以下步骤来创建一个帐户。

注册获取 Amazon Web Services 账户

如果您没有 Amazon Web Services 账户，请完成以下步骤来创建一个。

报名参加 Amazon Web Services 账户

1. 打开https://portal.aws.amazon.com/billing/注册。
2. 按照屏幕上的说明操作。

   在注册时，将接到电话，要求使用电话键盘输入一个验证码。

   当您注册时 Amazon Web Services 账户，就会创建Amazon Web Services 账户根用户一个。根用户有权访问该账户中的所有 Amazon Web Services 服务 和资源。作为最佳安全实践，请为用户分配管理访问权限，并且只使用根用户来执行需要根用户访问权限的任务。

Amazon 注册过程完成后会向您发送一封确认电子邮件。您可以随时前往 https://aws.amazon.com/并选择 “我的账户”，查看您当前的账户活动并管理您的账户。

保护 IAM 用户

注册后 Amazon Web Services 账户，开启多重身份验证 (MFA)，保护您的管理用户。有关说明，请参阅《IAM 用户指南》中的 为 IAM 用户启用虚拟 MFA 设备（控制台）。

要允许其他用户访问您的 Amazon Web Services 账户 资源，请创建 IAM 用户。为了保护您的 IAM 用户，请启用 MFA 并仅向 IAM 用户授予执行任务所需的权限。

有关创建和保护 IAM 用户的更多信息，请参阅《IAM 用户指南》中的以下主题：

- 在你的 IAM 用户中创建 Amazon Web Services 账户
- 适用于 Amazon 资源的访问权限管理
- 基于 IAM 身份的策略示例

在 Amazon Health 控制面板中查看您的账户事件

您可以登录自己的账户，以获取个性化事件和建议。

在 Amazon Health 控制面板中查看账户事件

1. 在https://health.aws.amazon.com/health/家中打开 Amazon Health 控制面板。
2. 在导航窗格中，对于您的账户运行状况，您可以选择以下选项：

   a. 未决问题和近期问题 – 查看最近打开和关闭的事件。

b. 已计划的更改 – 查看即将发生的可能影响您的服务和资源的事件。
c. 其他通知 – 查看过去七天内可能影响您账户的所有其他通知和持续发生的事件。
d. 事件日志 – 查看过去 90 天发生的所有事件。

未决问题和近期问题

使用未决问题和近期问题选项卡，查看过去七天内所有可能影响您账户的持续事件。

在控制面板中选择事件时，系统会显示详细信息窗格，其中包含事件和受影响资源的相关信息。有关更多信息，请参阅 事件详细信息。

通过从筛选条件列表选择选项，您可以筛选在任何选项卡中显示的事件。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 Web Services 服务等来缩小结果范围。

要查看所有事件，而不是控制面板中最近显示的事件，请选择 事件日志 选项卡。

> **Note**
>
> 当前，您无法删除 Amazon Health 控制面板中显示的事件的通知。事件 Amazon Web Services 服务 解决后，该通知将从您的控制面板视图中删除。

已计划的更改

使用已计划的更改选项卡，查看即将发生的可能影响您的账户的事件。这些事件可能包括已为服务计划的维护活动和需要采取行动才能解决的已计划生命周期事件。为了帮助您计划这些活动，我们提供了日历视图，以便您可以将这些已计划的更改映射到月度日历中。筛选条件可用。有关生命周期事件的更多信息，请参阅 Amazon Health已计划的生命周期事件。

其他通知

使用通知选项卡，查看过去七天内可能影响您账户的所有其他通知和持续发生的事件。这可能包括证书轮换、账单通知和安全漏洞等事件。

事件日志

使用事件日志选项卡查看所有 Amazon Health 事件。日志表包含其他列，因此您可以按状态和开始时间进行筛选。

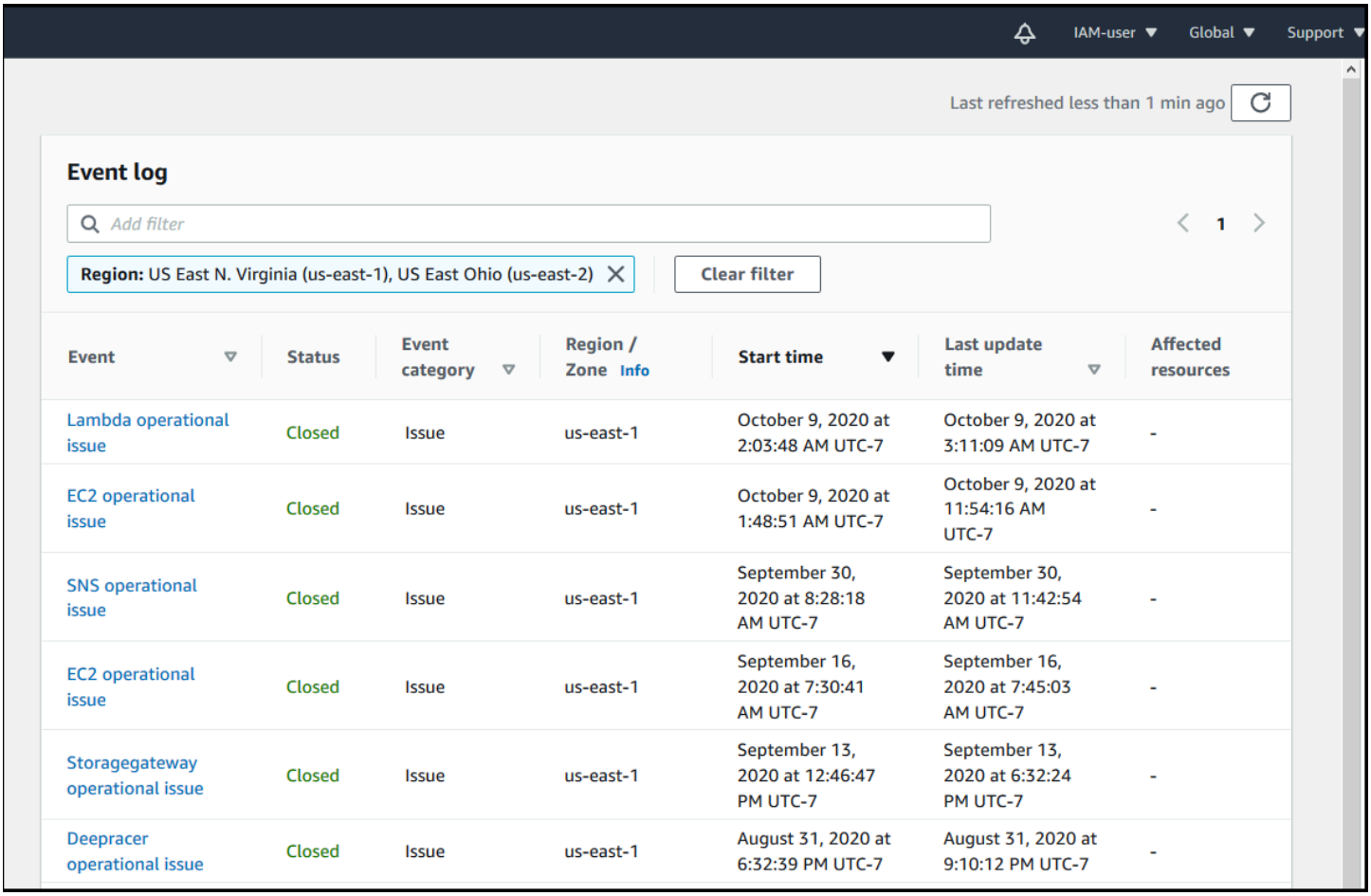
在事件日志表中选择事件时，系统会显示详细信息窗格，其中包含事件和受影响资源列表的相关信息。有关更多信息，请参阅 事件详细信息。

要缩小结果范围，可以选择以下筛选选项：

- 可用区
- 结束时间
- 事件
- 事件 ARN
- 事件类别
- 上次更新时间
- 区域
- 资源 ID /ARN
- 服务
- 开始时间
- 状态

Example ：事件日志

下图显示了美国东部（弗吉尼亚州北部）和美国东部（俄亥俄州）地区最近发生的事件。



事件详细信息

当您选择一个事件时，会出现两个关于该事件的选项卡。详细信息选项卡显示以下信息：

- 服务
- 状态
- 区域/可用区
- 事件是否特定于账户
- 开始和结束时间
- 类别
- 受影响资源的数量
- 事件的描述和更新的时间表

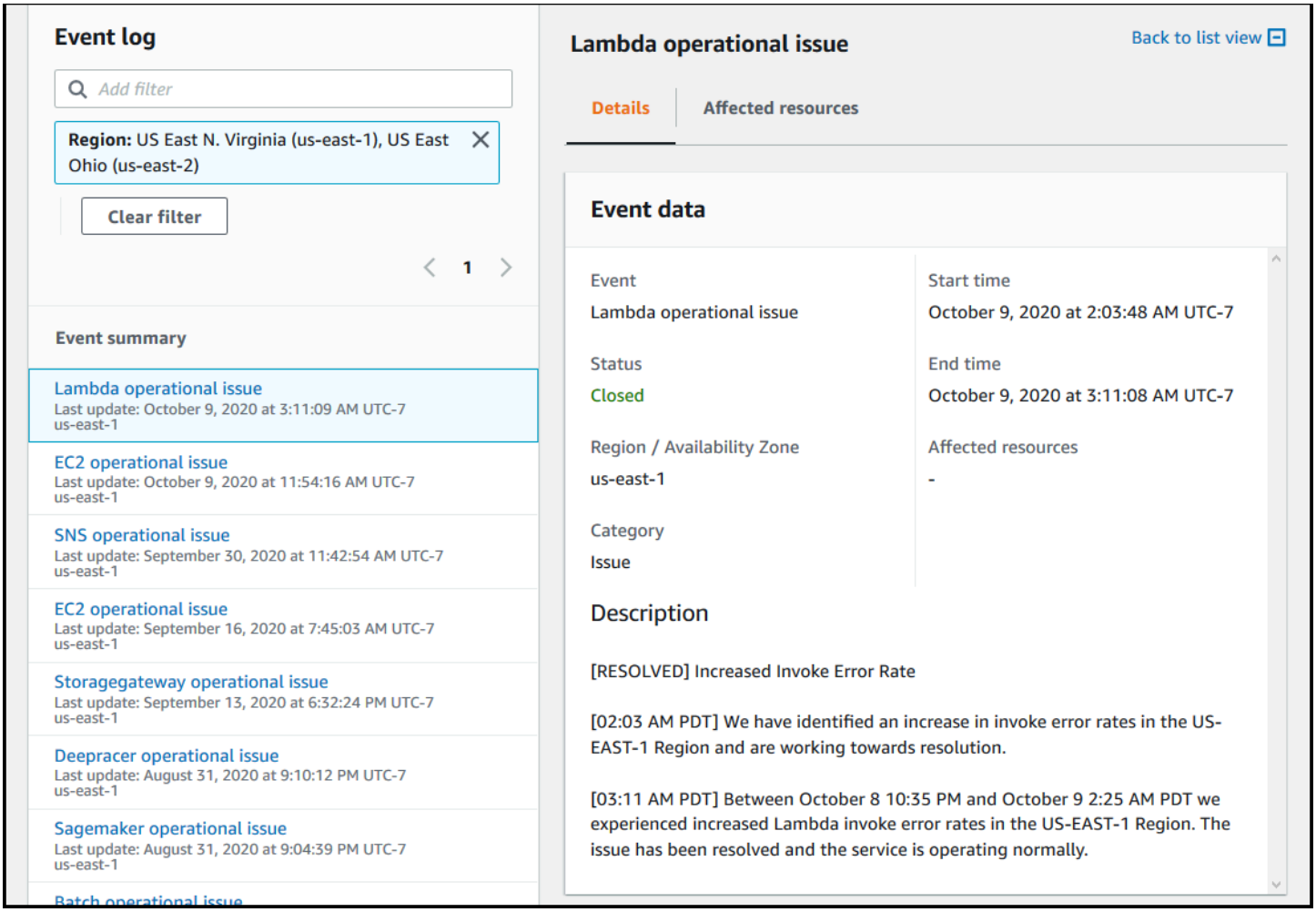
“受影响的资源” 选项卡显示有关受该事件影响的所有 Amazon Web Services 资源的以下信息：

- 如果可用或相关，资源 ID（例如，Amazon EBS 卷 ID `vol-a1b2c34f`）或 Amazon 资源名称（ARN）。
- 对于已计划的生命周期事件，此受影响的资源列表还包含资源的最新状态（待处理、未知或已解决）。此列表通常每 24 小时更新一次。

您可以筛选资源中显示的项目。您可以按资源 ID 或 ARN 缩小结果范围。

Example : Amazon Health 活动用于 Amazon Lambda

以下屏幕截图显示 Lambda 的一个示例事件。



事件类型

有两种类型 Amazon Health 的事件：

- 公有事件是不特定于账户的服务事件。例如，如果某处的 Amazon EC2 出现问题 Amazon Web Services 区域，即使您未在该地区使用服务或资源，也会 Amazon Health 提供有关该事件的信息。

- 特定于账户的事件特定于您的账户或您组织中的账户。例如，如果您使用的区域中的某个 Amazon EC2 实例出现问题，请 Amazon Health 提供有关该事件的信息以及受影响的 Amazon EC2 实例列表。

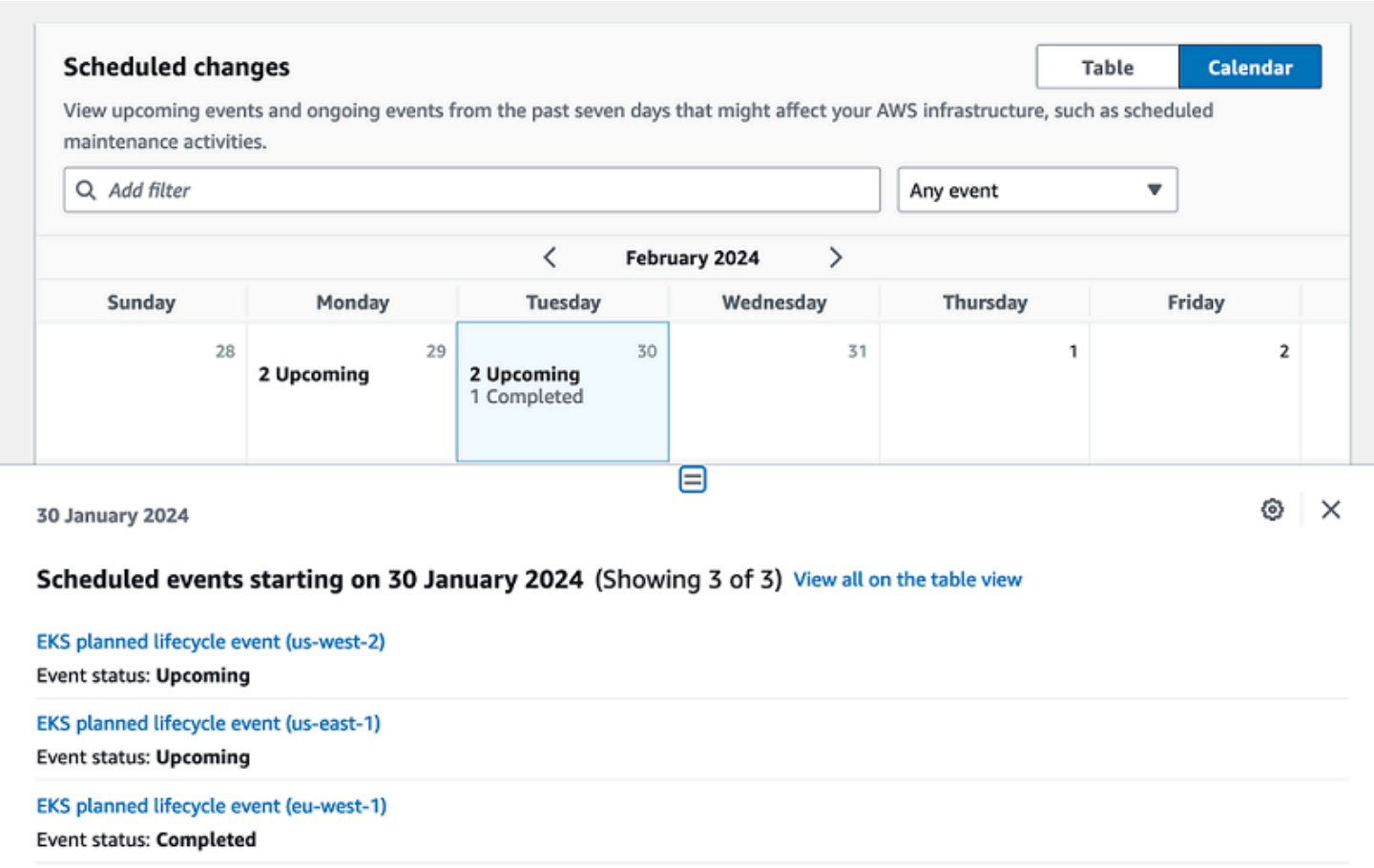
使用以下选项确定事件是公有事件还是特定于账户的事件：

- 在 Amazon Health 控制面板中，为事件选择受影响资源选项卡。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 Health Dashboard 入门。
- 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 Amazon Health API 参考中的DescribeEventDetails操作。

日历视图

日历视图在 “计划更改” 选项卡中可用，用于将 Amazon Health 事件投射到月度日历中。此视图允许您查看过去 3 个月和未来一年内的计划更改。

Amazon Health 事件按日期显示。选择日期以显示包含 Amazon Health 活动更多详细信息的侧面板。即将到来的和持续进行的事件以黑色显示。已完成的事件以灰色显示。如果一个日期中有两个以上的事件，则仅显示黑色和灰色事件的数量。选择一个日期，在侧面板中显示 Amazon Health 事件列表。您可以在侧面板中选择一个事件，以显示有关该事件的信息。侧面板上有页面导览痕迹，可以导航到较早的视图。



受影响的资源视图

Amazon Health 事件可能会指定受影响的确切资源。您可以在 Amazon Health 事件的受影响资源选项卡中查看受影响的资源。要查看状态，请选择 Amazon Health 事件。状态显示在侧面板的受影响资源选项卡中。对于计划的生命周期 Amazon Health 事件，事件提供受影响资源状态的每日更新。

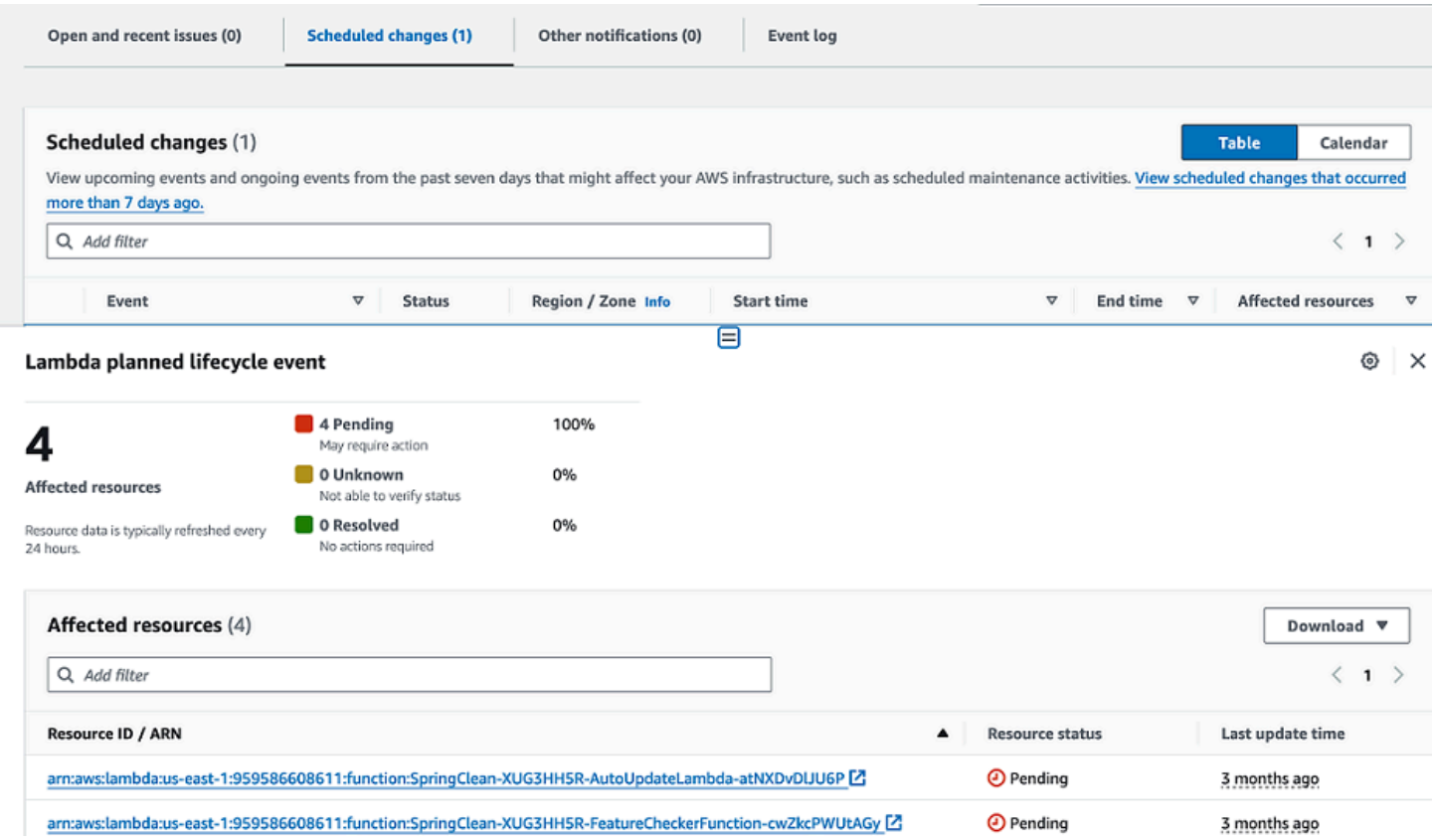
账户级 Amazon Health 事件在 “受影响资源” 选项卡的顶部显示受影响资源状态的摘要。受影响资源的列表以及相应的状态在表中显示。计划生命周期事件是使用资源状态字段的事件类型的一个示例。要了解有关计划生命周期事件的更多信息，请参阅 Amazon Health已计划的生命周期事件。

当您访问组织视图时， Amazon Health 事件会显示包含的所有账户的所有受影响资源的状态摘要。摘要后面是受影响账户的列表以及该账户的待处理资源数量。选择账号或待处理资源的数量以显示账户视图摘要。账户视图摘要包含页面导览痕迹，可以导航回受影响账户的组织列表。受影响资源状态的摘要显示在拆分窗格的顶部。

您可以在“受影响资源”选项卡中以 CSV 或 JSON 格式下载受影响资源列表。在组织视图中，下载的文件包括所列账户中的所有资源。在组织视图中导航到账户级别，以便在下载的文件中仅包含该账户的资

源。下载文件中每个受影响的资源都包括资源的 Amazon Web Services 账户 ID、EventArn、实体名称、EntityArn、状态和上次更新时间。如果激活了筛选条件，则下载的文件将仅包含筛选后的结果。

一次只能下载一个文件。这些文件会自动下载到浏览器的默认下载文件夹，并具有基于活动标题 Amazon Web Services 区域、活动开始日期和下载日期的预设文件名。



时区设置

您可以在 Amazon Health 控制面板中按当地时区或 UTC 查看事件。如果您在控制面板中更改时区，则 Amazon Health 控制面板中的所有时间戳和公共事件都会更新为您指定的时区。

要更新您的时区设置

1. 在https://health.aws.amazon.com/health/家中打开 Amazon Health 控制面板。
2. 在页面底部，选择 Cookie 首选项。
3. 对于功能性 Cookie，选择已允许。然后选择保存首选项。
4. 在 Amazon Health 控制面板的导航窗格中，选择时区设置。
5. 为您的 Amazon Health 控制面板会话选择一个时区。然后选择保存更改。

您的组织运行状况

Amazon Health 与集成， Amazon Organizations 因此您可以查看属于您的组织的所有账户的事件。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 跨账号聚合 Amazon Health 事件。

配置亚马逊 EventBridge

EventBridge 用于检测 Amazon Health 事件的变化并做出反应。您可以监控账户中发生的特定 Amazon Health 事件，然后设置规则，以便在事件发生变化时 Amazon Health 通知您或您采取行动。

EventBridge 搭配使用 Amazon Health

1. 在https://health.aws.amazon.com/health/家中打开 Amazon Health 控制面板。
2. 要导航到 EventBridge 控制台以创建规则，请执行以下任一操作：
   - 在导航窗格的 “健康集成” 下，选择 Amazon EventBridge。
   - 在 “配置” 下 EventBridge，选择 “转到” EventBridge。
3. 按照该步骤为事件创建规则和监控。请参阅 通过 Amaz Amazon Health on 监控事件 EventBridge。

Amazon Health 仪表板

您可以使用 Amazon Health 控制面板-服务运行状况来查看所有人的运行状况 Amazon Web Services 服务。此页面显示了 Amazon Web Services 区域中各服务报告的服务事件。您无需登录或拥有即可 Amazon Web Services 账户 访问 Amazon Health 控制面板-服务运行状况页面。

> **Tip**
>
> 本网站仅显示公共活动，这些活动并不特定于 Amazon Web Services 账户. 如果您已经有一个帐户，我们建议您登录以查看 Amazon Health 控制面板，并随时了解可能影响您的账户和服务的事件。有关更多信息，请参阅 Amazon Health Dashboard 入门。

查看 Amazon Health 控制面板-服务运行状况

1. 导航到https://health.aws.amazon.com/health/状态页面。

   > **Note**
   >
   > 如果您已经登录到您的页面 Amazon Web Services 账户，您将被重定向到Amazon Health 控制面板-您的账户健康状况页面。

2. 在服务运行状况下，选择未决问题和近期问题以查看最近报告的事件。您可以查看有关事件的以下信息：

   - 事件名称和受影响区域。例如，操作问题 – Amazon Elastic Compute Cloud（弗吉尼亚北部）
   - 服务名称
   - 事件的严重性，例如 “受影响” 或 “已降级”
   - 最近更新的事件时间表
   - 也受 Amazon Web Services 服务 此事件影响的名单

   > **Note**
   >
   > 您可以按当地时区或 UTC 查看事件。有关更多信息，请参阅时区设置。

3. （可选）在事件旁边，选择 RSS 以订阅该事件的 RSS 源。您将在指定中收到有关此特定服务的通知 Amazon Web Services 区域。

4. 选择服务历史记录，以查看服务历史记录表。此表显示了过去 12 个月的所有 Amazon Web Services 服务 中断情况。

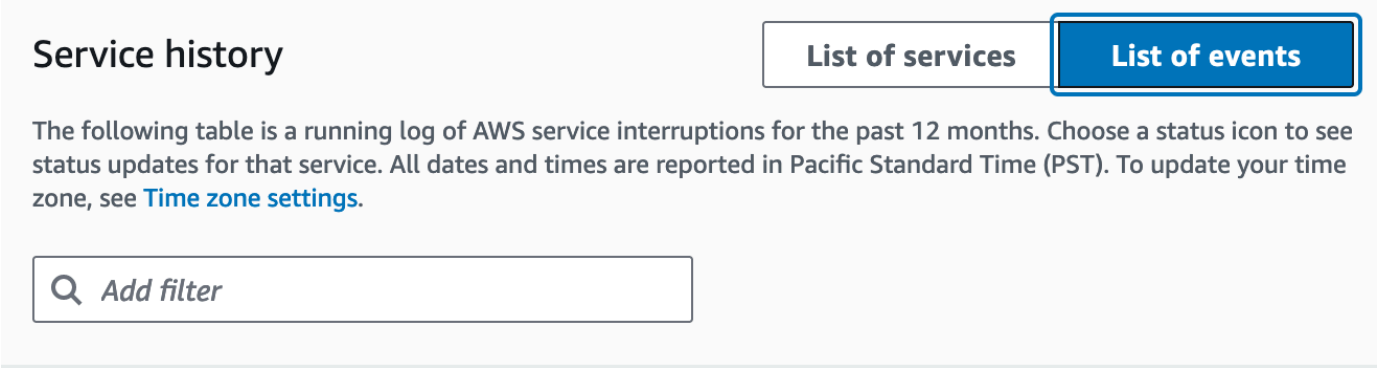
> **Tip**
>
> 您可以按服务、Amazon Web Services 区域 和日期进行筛选。

5. 在进行中的服务事件旁边，选择状态图标

( )

以查看有关该事件的更多信息。

6. （可选）要以历史事件列表的形式查看此信息，请选择事件列表按钮。选中事件列中的任何事件，即可在弹出的侧面板中查看有关该特定事件的更多信息。



> **Note**
>
> 如果选择 2023 年 9 月之后的任何公共事件，都将在浏览器的 URL 中填充指向该公共 Amazon Health 事件的链接。选择此链接后，您会导航到将弹出该事件的事件列表视图。

7. （可选）选择 RSS 源，以订阅 RSS 源。您将收到指定 Amazon Web Services 区域的有关此特定服务的通知。
8. （可选）您可以按当地时区或 UTC 查看事件。有关更多信息，请参阅 时区设置。
9. （可选）如果您有一个账户，请选择打开账户运行状况以便登录。登录后，您可以查看特定于您账户的事件。有关更多信息，请参阅 Amazon Health Dashboard 入门。

Amazon Health已计划的生命周期事件

了解计划的生命周期事件 Amazon Health。

主题

什么是已计划的生命周期事件？

Amazon Health 传达可能影响应用程序可用性的重要更改。在 Amazon 分担责任模式中， Amazon 采取措施使支持您的资源的底层硬件和基础设施保持最新且安全。但是，某些更改需要客户采取行动或进行协调，以免对您的应用程序产生影响。 Amazon Health 会提前针对重要更改发出通知，如：

- 开源软件终止支持-有些软件 Amazon Web Services 服务 运行开源版本。如果开源社区终止对软件版本的支持，则会 Amazon 通知您何时需要采取措施进行升级并避免对应用程序造成影响。
  - Amazon RDS for MySQL 引擎版本终止支持
  - Amazon EKS Kubernetes 版本终止支持
- 影响 Amazon自有资源的更改，可能需要您采取行动。
  - Amazon RDS 证书颁发机构证书到期。
  - Amazon C WorkDocs ompanion 即将到期，不再可用。

> **Note**
>
> 所有符合此标准的通知都将 Amazon Health 作为计划生命周期事件进行报告。

- 动态资源消耗和改进的元数据：从您收到通知到 Amazon Health 事件的生命周期，您受影响的资源作为具有特定实体状态的受影响实体与 Amazon Health 事件相关联。以 ARN 格式指定受影响资源（如果适用）。如果受影响资源需要客户采取行动，则以“PENDING（待处理）”状态列出。如果受影响资源执行必要操作或资源被删除，则状态更新为“RESOLVED（已解决）”。

> **Note**
>
> - 异步定期执行资源状态更新，在极少数情况下延迟可能长达 72 小时。
> - 在不提供动态更新的例外情况下，资源不会处于“待处理”或“已解决”状态，也不会分配任何状态。
> - Amazon GovCloud (US) 和中国区域不支持资源状态更新。

当收到已计划的生命周期事件通知时，将会发生什么?

计划生命周期事件的 Amazon Health 体验可帮助您的团队了解即将发生的生命周期变化并跟踪操作的完成情况。

类型类别：已计划的更改

事件类型代码： Amazon_{SERVICE}_PLANNED_LIFECYCLE_EVENT

事件开始时间：事件开始时间是您的资源受到更改影响的最快日期。

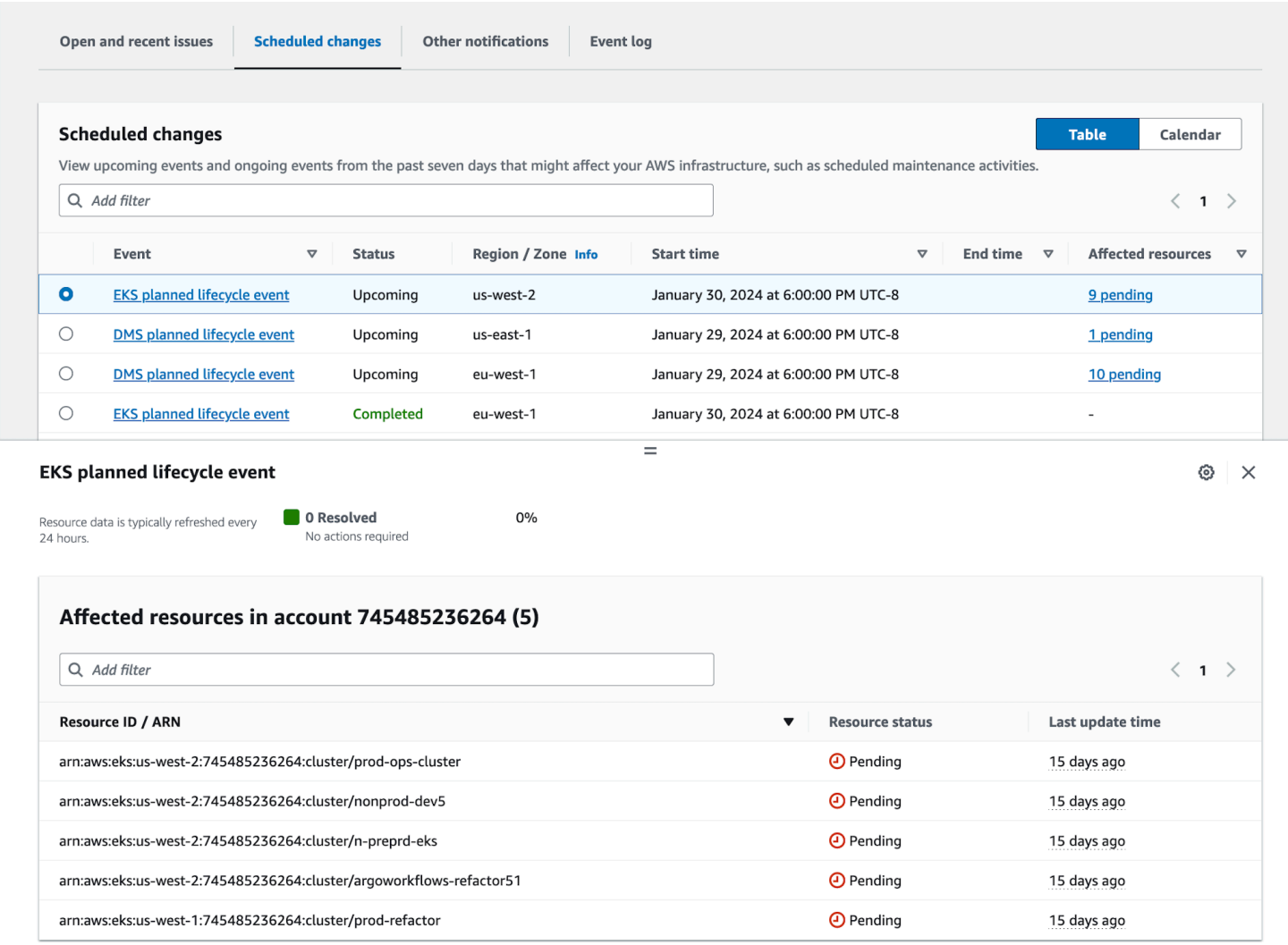
活动结束时间：事件结束时间是指所有 Amazon 资源完成更改的日期。请注意，并不总是指定结束时间。将开始时间视为更改日期非常重要。

> **Note**
>
> 组织可以针对每个计划生命周期事件接收单个事件 ARN，事件按区域分组，其中包含受影响的资源。但是， ARNs 如果组织有大量受影响 Amazon Web Services 账户 或资源，他们可能会获得多个。

尽早了解计划中的生命周期事件：如果可能，计划中的生命周期事件的交付时间至少为 versions/changes and 90 days for minor versions/changes 180 天。

动态资源消耗和改进的元数据：从您收到通知到 Amazon Health 事件的生命周期，您受影响的资源作为具有特定实体状态的受影响实体与 Amazon Health 事件相关联。以 ARN 格式指定受影响资源（如果适用）。如果受影响资源需要客户采取行动，则以“PENDING（待处理）”状态列出。如果受影响资源执行必要操作或资源被删除，则状态更新为“RESOLVED（已解决）”。

> **Note**
>
> - Amazon Health 通知会尽可能提供一段时间内的状态更新，但 Amazon GovCloud (US) 和中国地区除外。
> - 异步定期执行资源状态更新，在极少数情况下延迟可能长达 72 小时。

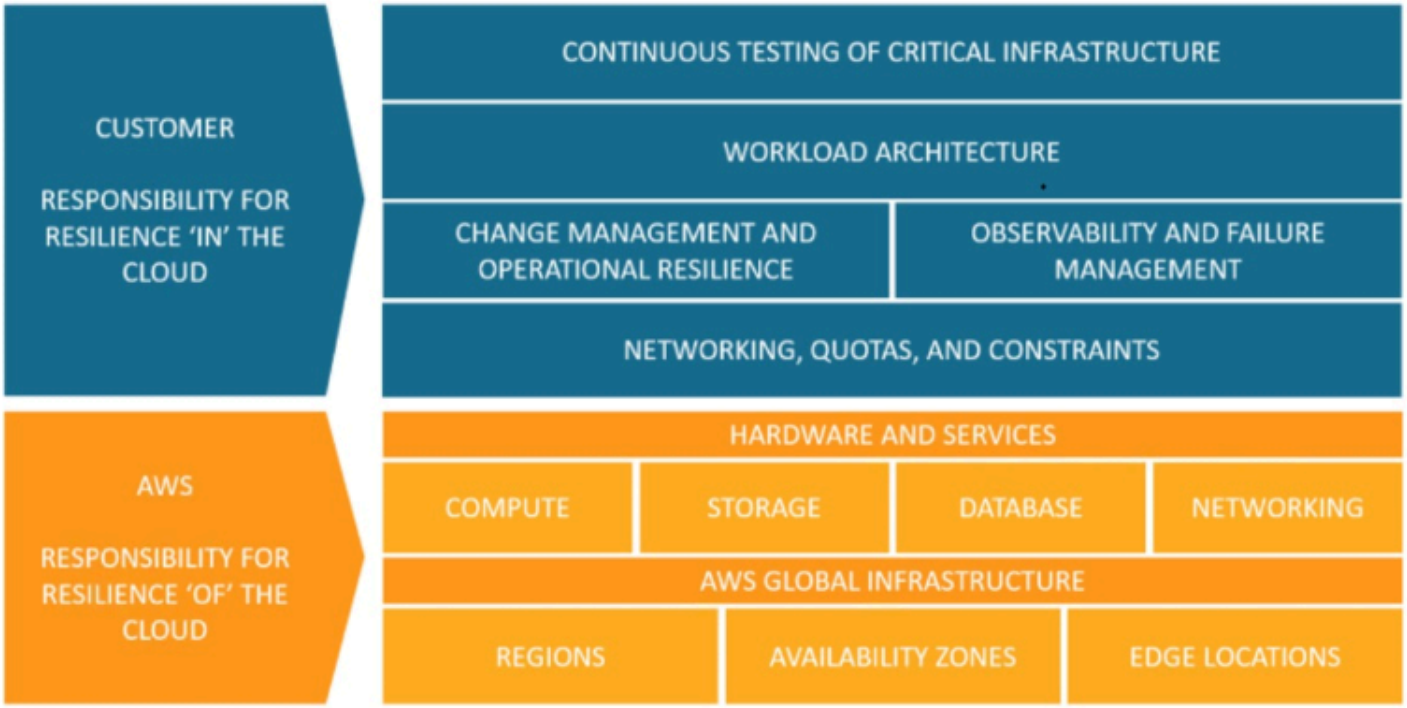


超出计划事件日期：

1. 如果适用，服务可能会在事件开始日期后的任意时间对您的资源实施描述的更改。
2. 如果您在支持终止日期之前解决了所有资源，则您的 Amazon Health 活动将更改为 “已关闭” 状态。
3. 如果在该日期结束后仍存在未完成资源未得到解析，则 Amazon Health 事件将在开始或结束日期后的 90 天内保持开放状态。然后，将删除事件。

通过责任共担模式增强恢复能力

安全和合规是客户共同承担 Amazon 的责任。此共担模式可根据所部署的服务帮助减轻客户的操作负担。这是因为 Amazon 操作、管理和控制从主机操作系统和虚拟化层到服务运行设施的物理安全的组件。除了配置 Amazon提供的安全组防火墙外，客户还负责管理访客操作系统（包括更新和安全补丁）和其他相关的应用程序软件。有关更多信息，请参阅责任共担模式。



访问已计划的生命周期事件

计划生命周期事件可以使用多种通道进行访问和监控：

- 使用亚马逊 EventBridge
- 使用 Amazon Health 控制面板
  - 日历视图
  - 受影响的资源视图
- 使用 Amazon Health API

使用 Amazon Health API Amazon Health 与其他系统集成

Amazon Health 是一项 RESTful Web 服务，它使用 HTTPS 作为传输，使用 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 Amazon Health 操作和参数的更多信息，请参阅 Amazon Health API 参考。

> **Note**
>
> 要使用 Amazon Health API，您必须拥有商业、企业入口或企业支持计划。Amazon Web Services 支持如果您使用没有商业、企业入口或企业支持计划的 Amazon 账户调用 Amazon Health API，则会收到`SubscriptionRequiredException`错误消息。

您可以使用 Amazon SDKs 来封装 Amazon Health REST API 调用，这样可以简化应用程序开发。您可以指定您的 Amazon 凭据，这些库会为您处理身份验证和请求签名。

Amazon Health 还在中提供了一个 Amazon Health 控制面板 Amazon Web Services Management Console ，可用于查看和搜索事件和受影响的实体。请参阅 Amazon Health Dashboard 入门。

主题

对 Amazon Health API 请求进行签名

当您使用 Amazon SDKs 或 Amazon Command Line Interface (Amazon CLI) 向发出请求时 Amazon，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，如果您在 适用于 Java 的 Amazon SDK 之前的高可用性终端节点演示中使用，则无需自己签署请求。

Java 代码示例

有关如何将 Amazon Health API 与一起使用的更多示例 适用于 Java 的 Amazon SDK，请参阅此示例代码。

当您提出请求时，我们强烈建议您不要使用 Amazon 根账户证书进行常规访问 Amazon Health。您可以使用 IAM 用户的凭证。有关更多信息，请参阅 IAM 用户指南中的锁定 Amazon 账户根用户访问密钥。

如果您不使用 Amazon SDKs 或 Amazon CLI，则必须自己签署请求。我们建议您使用 Amazon 签名版本 4。有关更多信息，请参阅中的签署 Amazon API 请求Amazon Web Services 一般参考。

为 Amazon Health API 请求选择终端节点

Amazon Health API 遵循多区域应用程序架构多区域应用程序架构，并且在主动-被动配置中具有两个区域端点。为了支持主动-被动 DNS 故障转移， Amazon Health 提供了一个全局端点。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。这可以帮助您知道要在代码中使用哪个端点，以便您可以从中获取最新信息 Amazon Health。

当您向全球终端节点发出请求时，必须指定您对目标区域终端节点的 Amazon 访问凭证，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 对 Amazon Health API 请求进行签名。

对于 IPv6仅限请求的请求，我们建议在全局终端节点上执行 DNS 查找以确定处于活动状态的请求，Amazon Web Services 区域 然后调用该区域 IPv6 支持的双栈终端节点。

下表列出了默认配置。

描述	签名区域	终端节点	协议
活动	cn-northwest-1	health.cn-northwest-1.amazonaws.com.cn	HTTPS
Passive	cn-north-1	health.cn-north-1.amazonaws.com.cn	HTTPS
Global	cn-northwest-1 Note 这是当前主动端点的签名区域。	global.health.amaws.com.cn	HTTPS

要确定终端节点是否为活动终端节点，请在全局终端节点 CNAME 上进行 DNS 查找，然后从解析的名称中提取 Amazon 区域。

Example ：在全局端点上查找 DNS

以下命令在 global.health.amazonaws.com.cn 端点上完成 DNS 查找。然后，该命令返回 cn-northwest-1 区域端点。此输出告诉您应该使用哪个端点 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**
>
> 主动端点和被动端点都返回 Amazon Health 数据。但是，最新 Amazon Health 数据只能从主动端点获得。来自被动端点的数据最终将与主动端点保持一致。我们建议您在主动端点发生变化时重新启动所有工作流程。

演示：以编程方式检索最近七天的 Amazon Health 事件数据

在以下代码示例中， Amazon Health 使用针对全球终端节点的 DNS 查询来确定有效的区域终端节点和签名区域。 Amazon Health 使用此信息检索最近七天的事件数据报告。如果主动端点发生变化，代码将重新启动工作流。

主题

- 演示：使用 Java 检索最近七天的 Amazon Health 事件数据
- 演示：使用 Python 检索最近七天的 Amazon Health 事件数据

演示：使用 Java 检索最近七天的 Amazon Health 事件数据

先决条件

您必须安装 Gradle。

要使用 Java 示例

1. 从下载Amazon Health 高可用性终端节点演示 GitHub。
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. 输入以下命令来指定您的 Amazon 凭据。

```
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

该代码示例返回您 Amazon 账户中最近七天内的近期 Amazon Health 事件。在以下示例中，输出包括 Amazon Config 服务 Amazon Health 的事件。

```
> 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 ## [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 适用于 Java 的 Amazon SDK API 参考 HealthClient中的接口和源代码。
- 有关此演示中用于 DNS 查找的库的更多信息，请参阅中的 dns java。 GitHub

演示：使用 Python 检索最近七天的 Amazon Health 事件数据

先决条件

您必须安装 Python 3。

要使用 Python 示例

1. 从下载Amazon Health 高可用性终端节点演示 GitHub。
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 venv 模块来创建虚拟环境，而无需安装 virtualenv。有关更多信息，请参阅 Python 网站上的 venv - 创建虚拟环境。
>
> ```
> python3 -m venv v-aws-health-env
> ```

4. 输入以下命令，以激活虚拟环境。

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

5. 运行以下命令，以安装依赖项。

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

6. 输入以下命令来指定您的 Amazon 凭据。

```
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

该代码示例返回您 Amazon 账户中最近七天内的近期 Amazon Health 事件。以下输出返回 Amazon 安全通知 Amazon Health 的事件。

```
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 ## [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. 您完成后，请输入以下命令来停用虚拟机。

```
deactivate
```

Python 资源

- 有关 `Health. Client` 的更多信息，请参阅 适用于 Python 的Amazon SDK (Boto3) API 参考。
- 有关此演示中用于 DNS 查找的库的更多信息，请参阅 dnspython 工具包和上的源代码。 GitHub

教程：使用 Amazon Health API 和 Java 示例

以下 Java 代码示例演示如何初始化 Amazon Health 客户端以及如何检索有关事件和实体的信息。

步骤 1：初始化凭证

需要有效的凭据才能与 Amazon Health API 通信。您可以使用与该 Amazon 账户关联的任何 IAM 用户的密钥对。

创建并初始化一个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);
}
```

步骤 2：初始化 Amazon Health API 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);
```

步骤 3：使用 Amazon Health API 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());
 }
```

安全性 Amazon Health

云安全 Amazon 是重中之重。作为 Amazon 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方共同承担 Amazon 的责任。责任共担模式将其描述为云的安全性和云中的安全性：

- 云安全 — Amazon 负责保护在 Amazon 云中运行 Amazon 服务的基础架构。 Amazon 还为您提供可以安全使用的服务。作为的一部分，第三方审计师定期测试和验证我们安全的有效性。要了解适用的合规计划 Amazon Health，请参阅按合规计划划分的划分的范围内的服务。
- 云端安全-您的责任由您使用的 Amazon 服务决定。您还需要对其它因素负责，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。

本文档可帮助您了解在使用时如何应用分担责任模型 Amazon Health。以下主题向您介绍如何进行配置 Amazon Health 以满足您的安全和合规性目标。您还将学习如何使用其他 Amazon 服务来帮助您监控和保护您的 Amazon Health 资源。

主题

中的数据保护 Amazon Health

分 Amazon 分担责任模型适用于中的数据保护 Amazon Health。如本模型所述 Amazon ，负责保护运行所有内容的全球基础架构 Amazon Web Services 云。您负责维护对托管在此基础结构上的内容的控制。您还负责您所使用的 Amazon Web Services 服务 的安全配置和管理任务。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 Web Services 账户 凭证并使用 Amazon IAM Identity Center 或 Amazon Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证（MFA）。
- 使用 SSL/TLS 与资源通信。 Amazon 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 Amazon CloudTrail。有关使用 CloudTrail 跟踪捕获 Amazon 活动的信息，请参阅《Amazon CloudTrail 用户指南》中的使用跟 CloudTrail 踪。
- 使用 Amazon 加密解决方案以及其中的所有默认安全控件 Amazon Web Services 服务。
- 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 中的敏感数据。
- 如果您在 Amazon 通过命令行界面或 API 进行访问时需要经过 FIPS 140-3 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-3 版》。

强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括您使用控制台、API Amazon Health 或以其他 Amazon Web Services 服务 方式使用控制台 Amazon CLI、API 或时 Amazon SDKs。在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供网址，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

数据加密

请参阅以下有关如何 Amazon Health 加密数据的信息。

数据加密是指保护传输中的数据（当数据从服务传输到您的 Amazon 账户时）和静态数据（存储在 Amazon 服务中时）。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 不会在活动中记录个人识别信息 (PII)，例如电子邮件地址或客户姓名。

静态加密

存储的所有数据都是静态加密 Amazon Health 的。

传输中加密

发送和发送的所有数据在传输过程中 Amazon Health 都经过加密。

密钥管理

Amazon Health 不支持为在 Amazon 云端加密的数据提供客户管理的加密密钥。

对 Amazon Health进行身份和访问管理

Amazon Identity and Access Management (IAM) Amazon Web Services 服务 可帮助管理员安全地控制对 Amazon 资源的访问权限。IAM 管理员控制谁可以进行身份验证（登录）和授权（拥有权限）使用 Amazon Health 资源。您可以使用 IAM Amazon Web Services 服务 ，无需支付额外费用。

主题

受众

您的使用方式 Amazon Identity and Access Management (IAM) 会有所不同，具体取决于您所做的工作 Amazon Health。

服务用户-如果您使用 Amazon Health 服务完成工作，则管理员会为您提供所需的凭证和权限。当你使用更多 Amazon Health 功能来完成工作时，你可能需要额外的权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问 Amazon Health中的特征，请参阅 对 Amazon Health 身份和访问进行故障排除。

服务管理员-如果您负责公司的 Amazon Health 资源，则可能拥有完全访问权限 Amazon Health。您的工作是确定您的服务用户应访问哪些 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。要详细了解您的公司如何将 IAM 与配合使用 Amazon Health，请参阅如何 Amazon Health 与 IAM 配合使用。

IAM 管理员：如果您是 IAM 管理员，您可能希望了解如何编写策略以管理对 Amazon Health的访问权限的详细信息。要查看您可以在 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

使用身份进行身份验证

身份验证是您 Amazon 使用身份凭证登录的方式。您必须以 IAM 用户身份或通过担 Amazon Web Services 账户根用户任 IAM 角色进行身份验证（登录 Amazon）。

如果您 Amazon 以编程方式访问，则会 Amazon 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 Amazon 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅《IAM 用户指南》中的用于签署 API 请求的Amazon 签名版本 4。

无论使用何种身份验证方法，您都可能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《IAM 用户指南》中的 IAM 中的Amazon 多重身份验证。

Amazon 账户 root 用户

创建时 Amazon Web Services 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 Amazon Web Services 服务 和资源。此身份被称为 Amazon Web Services 账户 root 用户，使用您创建账户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关需要您以根用户身份登录的任务的完整列表，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

IAM 用户和群组

I AM 用户是您 Amazon Web Services 账户 内部对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的用例，应在需要时更新访问密钥。

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，您可以拥有一个名为的群组，IAMAdmins并向该群组授予管理 IAM 资源的权限。

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《IAM 用户指南》中的 IAM 用户的使用案例。

IAM 角色

I AM 角色是您内部具有特定权限 Amazon Web Services 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。要在中临时担任 IAM 角色 Amazon Web Services Management Console，您可以从用户切换到 IAM 角色（控制台）。您可以通过调用 Amazon CLI 或 Amazon API 操作或使用自定义 URL 来代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的代入角色的方法。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 联合用户访问：要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关用于联合身份验证的角色的信息，请参阅《IAM 用户指南》中的针对第三方身份提供商创建角色（联合身份验证）。
- 临时 IAM 用户权限：IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取：您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）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，对于某些资源 Amazon Web Services 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 用户指南中的 IAM 中的跨账户资源访问。
- 跨服务访问 — 有些 Amazon Web Services 服务 使用其他 Amazon Web Services 服务服务中的功能。例如，当您在服务中拨打电话时，该服务通常会在 Amazon 中运行应用程序 EC2 或在 Amazon S3 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 Amazon，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 Amazon Web Services 服务 向下游服务发出请求的请求。 Amazon Web Services 服务只有当服务收到需要与其他 Amazon Web Services 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两项操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。
  - 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 IAM 角色。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《IAM 用户指南》中的创建向 Amazon Web Services 服务委派权限的角色。
  - 服务相关角色-服务相关角色是一种链接到的服务角色。 Amazon Web Services 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 Amazon Web Services 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 A@@ mazon 上运行的应用程序 EC2 — 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 Amazon CLI 或 Amazon API 请求的应用程序的临时证书。这比在 EC2 实例中存储访问密钥更可取。要为 EC2 实例分配 Amazon 角色并使其可供其所有应用程序使用，您需要创建一个附加到该实

例的实例配置文件。实例配置文件包含该角色，并允许在 EC2 实例上运行的程序获得临时证书。有关更多信息，请参阅 IAM 用户指南中的使用 IAM 角色向在 A mazon EC2 实例上运行的应用程序授予权限。

使用策略管理访问

您可以 Amazon 通过创建策略并将其附加到 Amazon 身份或资源来控制中的访问权限。策略是其中的一个对象 Amazon ，当与身份或资源关联时，它会定义其权限。 Amazon 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以 JSON 文档的 Amazon 形式存储在中。有关 JSON 策略文档的结构和内容的更多信息，请参阅 IAM 用户指南中的 JSON 策略概览。

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

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。拥有该策略的用户可以从 Amazon Web Services Management Console Amazon CLI、或 Amazon API 获取角色信息。

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《IAM 用户指南》中的使用客户托管策略定义自定义 IAM 权限。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 Amazon Web Services 账户。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和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管策略与内联策略之间进行选择。

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，策略定义指定主体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主体。委托人可以包括账户、用户、角色、联合用户或 Amazon Web Services 服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用 IAM 中的 Amazon 托管策略。

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，您可以创建一个仅允许 IAM 用户访问中的特定 Amazon EC2 事件的策略 Amazon Health Dashboard。

有关更多信息，请参阅 资源。

访问控制列表

访问控制列表 (ACLs) 控制哪些委托人（账户成员、用户或角色）有权访问资源。 ACLs 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 S3 和 Amazon VPC 就是支持的服务示例 ACLs。 Amazon WAF要了解更多信息 ACLs，请参阅《亚马逊简单存储服务开发者指南》中的访问控制列表 (ACL) 概述。

Amazon Health 不支持 ACLs。

其他策略类型

Amazon 支持其他不太常见的策略类型。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特征，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 用户指南中的 IAM 实体的权限边界。
- 服务控制策略 (SCPs)- SCPs 是指定组织或组织单位 (OU) 的最大权限的 JSON 策略 Amazon Organizations。 Amazon Organizations 是一项用于对您的企业拥有的多 Amazon Web Services 账户 项进行分组和集中管理的服务。如果您启用组织中的所有功能，则可以将服务控制策略 (SCPs) 应用于您的任何或所有帐户。SCP 限制成员账户中的实体（包括每个 Amazon Web Services 账户根用户实体）的权限。有关 Organization SCPs s 和的更多信息，请参阅《Amazon Organizations 用户指南》中的服务控制策略。
- 资源控制策略 (RCPs) — RCPs 是 JSON 策略，您可以使用它来设置账户中资源的最大可用权限，而无需更新附加到您拥有的每个资源的 IAM 策略。RCP 限制成员账户中资源的权限，并可能影响身份（包括身份）的有效权限 Amazon Web Services 账户根用户，无论这些身份是否属于您的组织。

有关 Organizations 的更多信息 RCPs，包括 Amazon Web Services 服务 该支持的列表 RCPs，请参阅《Amazon Organizations 用户指南》中的资源控制策略 (RCPs)。

- 会话策略：会话策略是当您以编程方式为角色或联合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 IAM 用户指南中的会话策略。

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。要了解在涉及多种策略类型时如何 Amazon 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

如何 Amazon Health 与 IAM 配合使用

在使用 IAM 管理访问权限之前 Amazon Health，您应该了解哪些可用的 IAM 功能 Amazon Health。要全面了解如何 Amazon Health 和其他 Amazon 服务与 IAM 配合使用，请参阅 IAM 用户指南中的与 IAM 配合使用的Amazon 服务。

主题

- Amazon Health 基于身份的策略
- Amazon Health 基于资源的策略
- 基于 Amazon Health 标签的授权
- Amazon Health IAM 角色

Amazon Health 基于身份的策略

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，以及指定在什么条件下允许或拒绝操作。 Amazon Health 支持特定操作、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 用户指南》 中的 IAM JSON 策略元素参考。

操作

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

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。还有一些操作需要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关联操作的权限。

正在执行的策略操作在操作前 Amazon Health 使用以下前缀:`health:`. 例如，要授予某人DescribeEventDetails通过 API 操作查看有关指定事件的详细信息的权限，您需要在策略中包含该`heath:DescribeEventDetails`操作。

策略声明必须包含`Action`或`NotAction`元素。 Amazon Health 定义了它自己的一组操作，这些操作描述了您可以使用此服务执行的任务。

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 Amazon Health 操作列表，请参阅 IAM 用户指南 Amazon Health中的定义操作。

资源

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

`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 事件的格式如下 Amazon 资源名称 (ARN)。

```
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"
```

要为 Amazon 指定 EC2 属于特定账户的所有 Amazon Health 事件，请使用通配符 (*)。

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

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

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

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

Amazon Health API 操作可能涉及多个资源。例如，该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 ARNs 用逗号分隔。

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

Amazon Health 仅支持运行状况事件的资源级权限，且仅支持DescribeAffectedEntities和DescribeEventDetailsAPI 操作。有关更多信息，请参阅 基于资源和基于操作的条件。

要查看 Amazon Health 资源类型及其列表 ARNs，请参阅 IAM 用户指南 Amazon Health中的由定义的资源。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 Amazon JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

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，则使用逻辑OR运算来 Amazon 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 用户指南》中的 IAM 策略元素：变量和标签。

Amazon 支持全局条件密钥和特定于服务的条件密钥。要查看所有 Amazon 全局条件键，请参阅 IAM 用户指南中的Amazon 全局条件上下文密钥。

Amazon Health 定义自己的条件键集，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 IAM 用户指南中的Amazon 全局条件上下文密钥。

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

要查看 Amazon Health 条件键列表，请参阅 IAM 用户指南 Amazon Health中的条件密钥。要了解可以使用条件键的操作和资源，请参阅操作定义者 Amazon Health。

示例

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

Amazon Health 基于资源的策略

基于资源的策略是 JSON 策略文档，用于指定委托人可以在哪些条件下对 Amazon Health 资源执行哪些操作。 Amazon Health 支持针对运行状况事件的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来允许 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。将跨账户主体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，您还必须向委托人实体授予访问资源的权限。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主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅《IAM 用户指南》 中的 IAM 角色与基于资源的策略有何不同。

Amazon Health 仅支持针对DescribeAffectedEntities和 DescribeEventDetailsAPI 操作的基于资源的策略。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。

示例

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。

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权限。

Amazon Health IAM 角色

I AM 角色是您的 Amazon 账户中具有特定权限的实体。

将临时证书与 Amazon Health

可以使用临时凭证进行联合身份验证登录，分派 IAM 角色或分派跨账户角色。您可以通过调用AssumeRole或之类的 Amazon STS API 操作来获取临时安全证书GetFederationToken。

Amazon Health 支持使用临时证书。

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 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 支持与服务相关的角色进行集成。 Amazon Organizations服务相关角色命名为 `AWSServiceRoleForHealth_Organizations`。该角色附带的是 Health_OrganizationsServiceRolePolicy Amazon 托管策略。 Amazon 托管策略 Amazon Health 允许从组织中的其他 Amazon 账户访问健康事件。

您可以使用该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，则必须先调用该DisableHealthServiceAccessForOrganization操作。然后，您可以通过 IAM 控制台、IAM API 或 Amazon Command Line Interface (Amazon CLI) 删除该角色。有关更多信息，请参阅《 IAM 用户指南》中的使用服务相关角色。

有关更多信息，请参阅 跨账号聚合 Amazon Health 事件。

服务角色

此功能允许服务代表您担任服务角色。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 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 Amazon Health 资源的权限。他们也无法使用 Amazon Web Services Management Console Amazon CLI、或 Amazon API 执行任务。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 IAM 基于身份的策略，请参阅《IAM 用户指南》中的 在 JSON 选项卡上创建策略。

主题

策略最佳实践

基于身份的策略决定了某人是否可以在您的账户中创建、访问或删除 Amazon Health 资源。这些操作可能会使 Amazon Web Services 账户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- 开始使用 Amazon 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的Amazon 托管策略。它们在你的版本中可用 Amazon Web Services 账户。我们建议您通过定义针对您的用例的 Amazon 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 Amazon 托管式策略或工作职能的Amazon 托管式策略。
- 应用最低权限：在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM 策略中的条件进一步限制访问权限：您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 Amazon Web Services 服务，例如 Amazon CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。

- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言（JSON）和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM Access Analyzer 验证策略。
- 需要多重身份验证 (MFA)-如果 Amazon Web Services 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的使用 MFA 保护 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅 IAM 用户指南中的 IAM 中的安全最佳实操。

使用 Amazon Health 控制台

要访问 Amazon Health 控制台，您必须拥有一组最低权限。这些权限必须允许您列出和查看有关您 Amazon 账户中 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.

`AWSHealthFullAccess` 策略授予实体对以下内容的完全访问权限：

- 为 Amazon Health 组织中的所有账户启用或禁用 Amazon 组织视图功能
- Amazon Health 控制台 Amazon Health Dashboard 中的
- Amazon Health API 操作和通知
- 查看有关属于您的 Amazon 组织的账户的信息
- 查看管理账户的组织单位 (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Health_OrganizationsServiceRolePolicy Amazon 托管策略，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。

对于仅调用 Amazon CLI 或 Amazon API 的用户，您无需为其设置最低控制台权限。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《IAM 用户指南》中的为用户添加权限。

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式策略。此策略包括在控制台上或使用 Amazon CLI 或 Amazon API 以编程方式完成此操作的权限。

```
{
    "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 Health Dashboard 和 Amazon Health API

Amazon Health Dashboard 适用于所有 Amazon 账户。该 Amazon Health API 仅适用于拥有商业、企业入口或企业 Support 计划的账户。有关更多信息，请参阅 Amazon Web Services 支持。

您可以使用 IAM 创建实体（用户、群组或角色），然后向这些实体授予访问 Amazon Health Dashboard 和 Amazon Health API 的权限。

默认情况下，IAM 用户无权访问 Amazon Health Dashboard 或 Amazon Health API。您可以通过将 IAM 策略附加到单个用户、一组用户或一个角色来授予用户访问您账户 Amazon Health 信息的权限。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，他们可以使用账户特定的登录页面登录您的账户并查看 Amazon Health 信息。有关更多信息，请参阅用户如何登录您的账户。

> **Note**
>
> Amazon Health Dashboard 具有查看权限的 IAM 用户对账户中所有 Amazon 服务的运行状况信息具有只读访问权限，这些信息可能包括但不限于 IDs 诸如 Amazon EC2 实例 IDs、实 EC2 例 IP 地址和一般安全通知之类的 Amazon 资源。
> 例如，如果 IAM 策略仅授予对 Amazon Health API 的访问权限，则该策略适用的用户或角色可以访问发布的有关 Amazon 服务和相关资源的所有信息，即使其他 IAM 策略不允许该访问也是如此。 Amazon Health Dashboard

- 个人账户 — 您可以使用诸如DescribeEvents和之类的操作DescribeEventDetails来获取有关您账户 Amazon Health 的事件的信息。
- 组织帐户-您可以使用DescribeEventsForOrganization和之类的操作DescribeEventDetailsForOrganization来获取有关属于您组织的帐户 Amazon Health 的事件的信息。

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

单个操作

描述访问权限

本政策声明授予访问 Amazon Health Dashboard 和任何 `Describe*` Amazon Health API 操作的权限。例如，具有此策略的 IAM 用户可以访问 Amazon 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

此政策声明拒绝访问 Amazon Health Dashboard 和 Amazon Health API。拥有此策略的 IAM 用户无法 Amazon Health Dashboard 在中查看， Amazon Web Services Management Console 也无法调用任何 Amazon Health API 操作。

Example ：拒绝访问

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

组织视图

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

IAM 策略的 `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

要了解每个操作所需的确切权限 APIs，请参阅 IAM 用户指南中的定义操作 Amazon Health APIs 和通知。

> **Note**
>
> 您必须使用组织管理账户中的凭据才能访问 Amazon Health APIs 的 Amazon Organizations。有关更多信息，请参阅 跨账号聚合 Amazon Health 事件。

允许访问 Amazon Health 组织视图

本政策声明授予您访问组织视图功能所需的所有内容 Amazon Health 和 Amazon Organizations 操作的权限。

Example：允许访问 Amazon Health 组织视图

```
{
    "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*"
        }
    ]
}
```

拒绝访问 Amazon Health 组织视图

此政策声明拒绝访问 Amazon Organizations 操作，但允许个人账户访问 Amazon Health 这些操作。

Example : 拒绝访问 Amazon Health 组织视图

```
{
    "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**
>
> 如果您要向其授予权限的用户或群组已有 IAM 策略，则可以在该策略中添加 Amazon Health特定于该策略的策略声明。

基于资源和基于操作的条件

Amazon Health 支持 DescribeAffectedEntities和 DescribeEventDetailsAPI 操作的 I AM 条件。您可以使用基于资源和操作的条件来限制 Amazon Health API 向用户、群组或角色发送的事件。

为此，请更新 IAM policy 的 `Condition` 数据块或设置 `Resource` 元素。您可以使用字符串条件来限制基于特定 Amazon Health 事件字段的访问权限。

在策略中指定 Amazon Health 事件时，可以使用以下字段：

- `eventTypeCode`
- `service`

备注

- DescribeAffectedEntities和 DescribeEventDetailsAPI 操作支持资源级权限。例如，您可以创建策略，允许或拒绝特定 Amazon Health 事件。
- DescribeAffectedEntitiesForOrganization和 DescribeEventDetailsForOrganizationAPI 操作不支持资源级权限。
- 有关更多信息，请参阅《服务授权参考》中的 “Amazon Health APIs 和通知” 中的操作、资源和条件密钥。

Example ：基于操作的条件

本政策声明允许访问 Amazon Health Dashboard 和 Amazon Health `Describe*` API 操作，但拒绝访问任何与 Amazon 相关 Amazon Health 的事件 EC2。

```
{
    "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 状况

此政策声明授予访问 Amazon Health Dashboard 和 Amazon Health Describe* API 操作的权限，但拒绝访问任何与之匹配 Amazon Health eventTypeCode的事件AWS_EC2_*。

```
{
    "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**
>
> 如果您调用DescribeAffectedEntities和DescribeEventDetails操作但无权访问该 Amazon Health 事件，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。

对 Amazon Health 身份和访问进行故障排除

使用以下信息来诊断和修复您在使用 Amazon Health 和 IAM 时可能遇到的常见问题。

主题

- 我无权在以下位置执行操作 Amazon Health
- 我无权执行 iam：PassRole
- 我想要查看我的访问密钥
- 我是一名管理员，想允许其他人访问 Amazon Health
- 我想允许 Amazon 账户之外的人访问我的 Amazon Health 资源

我无权在以下位置执行操作 Amazon Health

如果 Amazon Web Services Management Console 告诉您您无权执行某项操作，则必须联系管理员寻求帮助。管理员是指提供用户名和密码的人员。

当用户无权使用 Amazon Health Dashboard 或 Amazon Health API 操作时，就会出现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 需要来自Amazon Web Services 支持的商业、企业入口或企业支持计划。如果您通过没有商业、Enterprise On-Ramp 或 Enterprise Support 计划的账户调用 Amazon Health API，则返回以下错误代码：SubscriptionRequiredException。

我无权执行 iam：PassRole

如果您收到一个错误，表明您无权执行 iam:PassRole 操作，则必须更新策略以允许您将角色传递给 Amazon Health。

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

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此操作。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，必须更新 Mary 的策略以允许她执行 iam:PassRole 操作。

如果您需要帮助，请联系您的 Amazon 管理员。您的管理员是提供登录凭证的人。

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，即便是为了帮助找到您的规范用户 ID 也不行。通过这样做，您可以授予他人永久访问您的权限 Amazon Web Services 账户。

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 IAM 用户指南中的管理访问密钥。

我是一名管理员，想允许其他人访问 Amazon Health

要允许其他人访问 Amazon Health，您必须向需要访问的人员或应用程序授予权限。如果使用 Amazon IAM Identity Center 管理人员和应用程序，则可以向用户或组分配权限集来定义其访问权限级别。权限集会自动创建 IAM 策略并将其分配给与人员或应用程序关联的 IAM 角色。有关更多信息，请参阅《Amazon IAM Identity Center 用户指南》中的权限集。

如果未使用 IAM Identity Center，则必须为需要访问的人员或应用程序创建 IAM 实体（用户或角色）。然后，您必须将策略附加到实体，以便在 Amazon Health中向其授予正确的权限。授予权限后，向用户或应用程序开发人员提供凭证。他们将使用这些凭证访问 Amazon。要了解有关创建 IAM 用户、组、策略和权限的更多信息，请参阅《IAM 用户指南》中的 IAM 身份和 IAM 中的策略和权限。

我想允许 Amazon 账户之外的人访问我的 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 (ACLs) 的服务，您可以使用这些策略向人们授予访问您的资源的权限。

要了解更多信息，请参阅以下内容：

- 要了解是否 Amazon Health 支持这些功能，请参阅如何 Amazon Health 与 IAM 配合使用。
- 要了解如何提供对您拥有的资源的访问权限 Amazon Web Services 账户 ，请参阅 IAM 用户指南中的向您拥有 Amazon Web Services 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 Amazon Web Services 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 Amazon Web Services 账户
- 要了解如何通过身份联合验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（身份联合验证）提供访问权限。
- 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 用户指南》中的 IAM 中的跨账户资源访问。

将服务相关角色用于 Amazon Health

Amazon Health 使用 Amazon Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种与之直接关联的 IAM 角色的独特类型。 Amazon Health服务相关角色由 Amazon Health 预定义，并包含相关服务为您调用其他 Amazon Web Services 服务 所需的所有权限。

您可以使用服务相关角色进行设置， Amazon Health 以避免手动添加必要的权限。 Amazon Health 定义其服务相关角色的权限，除非另有定义，否则 Amazon Health 只能担任其角色。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 有两个与服务相关的角色：

- AWSServiceRoleForHealth_Organizations— 此角色信任 Amazon Health (`health.amazonaws.com`) 代替您访问 Amazon Web Services 服务 的角色。附属于此角色的是`Health_OrganizationsServiceRolePolicy` Amazon 托管策略。
- AWSServiceRoleForHealth_EventProcessor— 此角色信任 Amazon Health 服务主体 (`event-processor.health.amazonaws.com`) 代您担任该角色。附属于此角色的是`AWSHealth_EventProcessorServiceRolePolicy` Amazon 托管策略。服务主体使用该角色为 Amazon 事件检测和响应创建 Amazon EventBridge 托管规则。此规则是将警报状态变更信息从您的账户传送 Amazon Web Services 账户 到您的账户所需的基础架构 Amazon Health。

有关 Amazon 托管策略的更多信息，请参阅Amazon 的托管策略 Amazon Health。

为 Amazon Health创建服务相关角色

你不需要创建 AWSServiceRoleForHealth_Organizations 服务相关角色。当您调用EnableHealthServiceAccessForOrganization操作时， Amazon Health 会在账户中为您创建此服务相关角色。

您必须手动创建 AWSServiceRoleForHealth_EventProcessor 在您的账户中扮演与服务相关的角色。有关更多信息，请参阅 IAM 用户指南 中的创建服务相关角色。

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《IAM 用户指南》中的编辑服务相关角色。

删除 Amazon Health的服务相关角色

要删除 AWSServiceRoleForHealth_Organizations 角色，必须先调用该DisableHealthServiceAccessForOrganization操作。然后，您可以通过 IAM 控制台、IAM API 或 Amazon Command Line Interface (Amazon CLI) 删除该角色。

要删除 AWSServiceRoleForHealth_EventProcessor 角色、联系 Amazon Web Services 支持 并要求他们将你的工作负载从 Amazon 事件检测和响应中移开。完成此过程后，您可以通过 IAM 控制台、IAM API 或其他 Amazon CLI删除任一角色。

相关信息

有关更多信息，请参阅《 IAM 用户指南》中的使用服务相关角色。

Amazon 的托管策略 Amazon Health

Amazon 托管策略是由创建和管理的独立策略 Amazon。 Amazon 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住， Amazon 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 Amazon 客户使用。我们建议通过定义特定于您的使用场景的客户管理型策略来进一步减少权限。

您无法更改 Amazon 托管策略中定义的权限。如果 Amazon 更新 Amazon 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。 Amazon 最有可能在启动新的 API 或现有服务可以使用新 Amazon Web Services 服务 的 API 操作时更新 Amazon 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 Amazon 托管策略。

Amazon Health 具有以下托管策略。

目录

Amazon 托管策略：AWSHealth_EventProcessorServiceRolePolicy

Amazon Health 使用 AWSHealth_EventProcessorServiceRolePolicy Amazon 托管策略。此托管策略附加到 `AWSServiceRoleForHealth_EventProcessor` 服务相关角色。该策略允许服务相关角色为您完成操作。您不能将此策略附加到您的 IAM 实体。有关更多信息，请参阅 将服务相关角色用于 Amazon Health。

托管策略具有以下权限， Amazon Health 允许访问 Amazon 事件检测和响应的 Amazon EventBridge 规则。

权限详细信息

该策略包含以下权限。

- `events`— 描述和删除 EventBridge 规则，并描述和更新这些规则的目标。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Condition": {
                "StringEquals": {"events:ManagedBy": "event-
processor.health.amazonaws.com"}
            },
            "Action": [
                "events:DeleteRule",
                "events:RemoveTargets",
                "events:PutTargets",
                "events:PutRule"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "events:ListTargetsByRule",
                "events:DescribeRule"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

有关对策略的更改列表，请参阅 Amazon HealthAmazon 托管策略的更新。

Amazon 托管策略：Health_OrganizationsServiceRolePolicy

Amazon Health 使用 Health_OrganizationsServiceRolePolicy Amazon 托管策略。此托管策略附加到 `AWSServiceRoleForHealth_Organizations` 服务相关角色。该策略允许服务相关角色为您完成操作。您不能将此策略附加到您的 IAM 实体。有关更多信息，请参阅 将服务相关角色用于 Amazon Health。

此策略授予的权限 Amazon Health 允许访问 Health Organization 视图所需的 Amazon Organizations 详细信息。

权限详细信息

该策略包含以下权限。

- `organizations`— 描述中的帐户 Amazon Organizations 以及可以与 Organ Amazon Web Services 服务 izations 一起使用的帐户。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListDelegatedAdministrators",
                "organizations:DescribeOrganization",
                "organizations:DescribeAccount"
            ],
            "Resource": "*"
        }
    ]
}
```

有关对策略的更改列表，请参阅 Amazon HealthAmazon 托管策略的更新。

Amazon 托管策略：AWSHealthFullAccess

Amazon Health 使用 AWSHealthFullAccess Amazon 托管策略。该策略授予实体（IAM 用户或角色）访问 Amazon Health 控制台的权限。有关更多信息，请参阅 使用 Amazon Health 控制台。

权限详细信息

该策略包含以下权限。

- organizations— 启用或禁用 Amazon Health 组织中所有账户的 Amazon 组织视图功能，并查看管理账户的组织单位 (OU)
- health— 访问 Amazon Health API 操作和通知
- iam – 创建链接到 Amazon Health 服务的 IAM 角色

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

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

有关对策略的更改列表，请参阅 Amazon HealthAmazon 托管策略的更新。

Amazon HealthAmazon 托管策略的更新

查看 Amazon Health 自该服务开始跟踪这些更改以来 Amazon 托管策略更新的详细信息。要获得有关此页面更改的自动提示，请订阅 的文档历史记录 Amazon Health 页面上的 RSS 源。

下表描述了自 2022 年 1 月 13 日以来 Amazon Health 托管策略的重要更新。

Amazon Health

更改	描述	日期
Amazon 托管策略：AWSHealthFullAccess – 对现有策略的更新	Amazon Health 已将该 AWSHealthFullAccess 政策扩展到 Amazon GovCloud (US) Regions 和中国地区。	2023 年 10 月 16 日
Amazon 托管策略：Health_OrganizationsServiceRolePolicy – 对现有策略的更新	Amazon Health 添加了新的 Amazon Organizations 操作，允许服务相关角色描述可以与之配合 Amazon Organizations 使用的账户和 Amazon 服务。	2023 年 7 月 19 日
已发布的更改日志	Amazon Health 托管策略的更改日志。	2023 年 1 月 13 日

登录和监控 Amazon Health

监控是维护和其他 Amazon 解决方案的可靠性、可用性和性能的重要组成部分。 Amazon Health Amazon 提供以下监控工具 Amazon Health，供您监视、报告问题并在适当时采取措施：

- Amazon 会实时 CloudWatch监控您的 Amazon 资源和您运行 Amazon 的应用程序。您可以收集和跟踪指标，创建自定义的控制平面，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 CloudWatch 跟踪亚马逊弹性计算云 (Amazon EC2) 实例的 CPU 使用率或其他指标，并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 EventBridge 提供了一 near-real-time系列描述 Amazon 资源变化的系统事件。EventBridge 支持事件驱动的自动计算。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 通过 Amaz Amazon Health on 监控事件 EventBridge。
- Amazon CloudTrail捕获由您的账户或代表您的 Amazon 账户进行的 API 调用和相关事件，并将日志文件传输到您指定的亚马逊简单存储服务 (Amazon S3) Service 存储桶。您可以识别哪些用户和帐户拨打了电话 Amazon、发出呼叫的源 IP 地址以及呼叫发生的时间。有关更多信息，请参阅 用户指南。Amazon CloudTrail

有关更多信息，请参阅 监控 Amazon Health。

合规性验证 Amazon Health

要了解是否属于特定合规计划的范围，请参阅Amazon Web Services 服务 “” Amazon Web Services 服务 中的 “按合规计划划分的范围”，然后选择您感兴趣的合规计划。 Amazon Web Services 服务 有关一般信息，请参阅合规计划。

您可以使用下载第三方审计报告 Amazon Artifact。有关更多信息，请参阅中的 “下载报告” Amazon Artifact。

您在使用 Amazon Web Services 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。 Amazon 提供了以下资源来帮助实现合规性：

- Security & Compliance：这些解决方案实施指南讨论了架构考虑因素，并提供了部署安全性和合规性功能的步骤。
- 合规资源 — 此工作簿和指南集可能适用于您的行业和所在地区。
- 使用Amazon Config 开发人员指南中的规则评估资源 — 该 Amazon Config 服务评估您的资源配置在多大程度上符合内部实践、行业指导方针和法规。

- Amazon Security Hub— 这 Amazon Web Services 服务 提供了您内部安全状态的全面视图 Amazon。Security Hub 通过安全控制措施评估您的 Amazon 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控制措施的列表，请参阅 Security Hub 控制措施参考。
- Amazon GuardDuty — 它通过监控您的 Amazon Web Services 账户环境中是否存在可疑和恶意活动，来 Amazon Web Services 服务 检测您的工作负载、容器和数据面临的潜在威胁。 GuardDuty 通过满足某些合规性框架规定的入侵检测要求，可以帮助您满足各种合规性要求，例如 PCI DSS。

韧性在 Amazon Health

Amazon 全球基础设施是围绕 Amazon 区域和可用区构建的。 Amazon 区域提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络相连。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失效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结构相比，可用区具有更高的可用性、容错性和可扩展性。

Amazon Health 事件在多个可用区中存储和复制。这种方法可确保您可以通过 Amazon Health Dashboard 或 Amazon Health API 操作访问它们。您可以在 Amazon Health 事件发生后的 90 天内查看事件。

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中的基础结构安全性

作为一项托管服务， Amazon Health 受到《Amazon Web Services：安全流程概述》白皮书中描述的 Amazon 全球网络安全程序的保护。

您可以使用 Amazon 已发布的 API 调用 Amazon Health 通过网络进行访问。客户端必须支持传输层安全性协议 (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 主体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。

中的配置和漏洞分析 Amazon Health

配置和 IT 控制由您（我们的客户）共同 Amazon 负责。有关更多信息，请参阅责任 Amazon 共担模型。

Amazon Health的安全最佳实践

请参阅以下使用的最佳实践 Amazon Health。

向 Amazon Health 用户授予尽可能少的权限

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，您可以允许 Amazon Identity and Access Management (IAM) 用户访问 Amazon 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。

查看 Amazon Health Dashboard

Amazon Health Dashboard 经常检查您的账号或应用程序，以确定可能影响您的账户或应用程序的事件。例如，您可能会收到有关您的资源的事件通知，例如需要更新的亚马逊弹性计算云 (Amazon EC2) 实例。

有关更多信息，请参阅 Amazon Health Dashboard 入门。

Amazon Health 与 Amazon Chime 或 Slack 集成

您可以 Amazon Health 与聊天工具集成。这种集成可让您和您的团队实时收到有关 Amazon Health 事件的通知。有关更多信息，请参阅中的Amazon Health 工具 GitHub。

监视 Amazon Health 事件

您可以 Amazon Health 与 Amazon E CloudWatch vents 集成，以便为特定事件创建规则。当 Events 检测到与您的规则匹配 CloudWatch 的事件时，您会收到通知，然后可以采取措施。 CloudWatch 事件事件是特定于区域的，因此您必须在您的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，事件将在美国东部（弗吉尼亚州北部）地区出现。您可以在此区域中设置 CloudWatch 事件，以确保监控这些事件。

有关更多信息，请参阅 通过 Amaz Amazon Health on 监控事件 EventBridge。

跨账号聚合 Amazon Health 事件

默认情况下，您可以使用 Amazon Health 查看单个 Amazon 账户 Amazon Health 的事件。如果您使用 Amazon Organizations，您还可以在整个组织中集中查看 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。您可以使用筛选器来查看特定 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。您然后可以使用该信息，在组织内主动管理和自动化资源维护事件。使用此功能可以随时了解 Amazon 服务即将发生的变更，这些变更可能需要更新或代码更改。

最佳做法是使用 “委派管理员” 功能将 Amazon Health 组织视图的访问权限委托给成员账户。这使运营团队可以更轻松地访问组织中的 Amazon Health 事件。您可以使用委派管理员功能限制管理账户，同时为团队提供他们对 Amazon Health 事件采取行动所需的可见性。

> **Important**
>
> - Amazon Health 不会记录在您启用组织视图之前组织中发生的事件。例如，如果您组织中的一个成员账户 (111122223333) 在您启用亚马逊弹性计算云 (Amazon EC2) 之前收到了该活动，则该事件将不会出现在您的组织视图中。
> - Amazon Health 只要活动可用，为组织中的账户发送的事件将显示在组织视图中，最长可达 90 天，即使其中一个或多个账户离开您的组织也是如此。
> - 组织事件在 90 天内可用，然后会被删除。这个配额不能提高。

先决条件

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 Amazon Identity and Access Management (IAM) 用户身份登录管理账户或担任 IAM 角色。

  您也可以用组织管理账户中的根用户身份登录（不推荐）。有关更多信息，请参阅 IAM 用户指南中的锁定 Amazon 账户根用户访问密钥。
- 如果您以 IAM 用户身份登录，请使用授予访问 Amazon Health 和 Organizations 操作的 IAM 策略，例如 AWSHealthFullAccess政策。有关更多信息，请参阅 Amazon Health 基于身份的策略示例。

主题

启用组织视图

您可以使用 Amazon Health 控制台集中查看 Amazon 组织中的健康事件。

所有 Amazon Web Services 支持 套餐均可在 Amazon Health 控制台中查看组织视图，无需支付额外费用。

> **Note**
>
> 如果您想允许用户使用管理账户中的此功能，则他们必须拥有诸如 AWSHealthFullAccess政策。有关更多信息，请参阅 Amazon Health 基于身份的策略示例。

Enabling organizational view (Console)

您可以从 Amazon Health 控制台启用组织视图。您必须登录您所在 Amazon 组织的管理帐户。

查看您组织的 Amazon Health 控制面板

1. 在https://health.aws.amazon.com/health/家中打开 Amazon Health 控制面板。
2. 在导航窗格的您的组织运行状况下，选择配置。
3. 在启用组织视图页面上，选择启用组织视图。
4. （可选）如果要对 Amazon 组织进行更改，例如创建组织单位（OUs），请选择管理 Amazon Organizations。

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

> **备注**
>
> - 启用此功能是一个异步过程，需要花点时间才能完成。根据您组织中的账户数量，加载账户可能需要几分钟。您可以稍后离开并查看 Amazon Health 控制台。
> - 如果您有 Business、Enterprise On-Ramp 或 Enterprise Support 计划，则可以调用 DescribeHealthServiceStatusForOrganizationAPI 操作来检查流程的状态。
> - 启用此功能后，具有`Health_OrganizationsServiceRolePolicy` Amazon 托管策略的`AWSServiceRoleForHealth_Organizations`服务相关角色将应用于组织中的管理账户。有关更多信息，请参阅 将服务相关角色用于 Amazon Health。

Enabling organizational view (CLI)

您可以使用 EnableHealthServiceAccessForOrganizationAPI 操作启用组织视图。

你可以使用 Amazon Command Line Interface (Amazon CLI) 或你自己的代码来调用这个操作。

> **Note**
>
> - 您必须有商业、企业入口或企业支持计划才能调用 Amazon Health API。
> - 您必须使用美国东部（弗吉尼亚州北部）区域端点。

Example

以下 Amazon CLI 命令可在您的 Amazon 账户中启用此功能。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

您可以将适用于 Java 2.0 版本的 Amazon 软件开发工具包用于以下示例。

```
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.EnableHealthServiceAccessForOrganizationReques
import
 software.amazon.awssdk.services.health.model.EnableHealthServiceAccessForOrganizationRespon
import
 software.amazon.awssdk.services.health.model.DescribeHealthServiceStatusForOrganizationRequ
import
 software.amazon.awssdk.services.health.model.DescribeHealthServiceStatusForOrganizationResp

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，具有Health_OrganizationsServiceRolePolicy Amazon 托管策略的AWSServiceRoleForHealth_Organizations服务相关角色将应用于组织中的管理账户。

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

查看组织视图

您可以使用 Amazon Health 控制台集中查看 Amazon 组织中的健康事件。

所有 Amazon Web Services 支持 套餐均可在 Amazon Health 控制台中查看组织视图，无需支付额外费用。

> **Note**
>
> 如果您想允许用户使用管理账户中的此功能，则他们必须拥有诸如 AWSHealthFullAccess政策。有关更多信息，请参阅 Amazon Health 基于身份的策略示例。

Viewing organizational view events (Console)

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

当一个帐户加入您的组织时，Amazon Health 会自动将该帐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 控制台可以显示控制Amazon Health 面板中的公共事件 — 过去 7 天的服务运行状况。这些公有事件不是特定于您组织中的账户。 Amazon Health 控制面板中的事件 — 服务运行状况提供有关 Amazon 服务区域可用性的公共信息。

您可以在以下页面中查看组织视图事件：

未决问题和近期问题

您可以使用 “未解决的问题和最近的问题” 选项卡来查看可能影响您的 Amazon 基础架构的事件，例如影响您的组织的更改 Amazon Web Services 服务 和资源。

要查看组织视图事件

1. 在https://health.aws.amazon.com/health/家中打开 Amazon Health 控制面板。
2. 在导航窗格的您的组织运行状况下，选择未决问题和近期问题以查看最近报告的事件。
3. 选择一个事件。在详细信息选项卡中，您可以查看有关事件的以下信息：
   - 事件名称
   - 状态
   - 区域/可用区
   - 受影响的账户
   - 开始时间
   - 结束时间
   - 类别
   - 描述

已计划的更改

使用计划更改选项卡，查看可能影响您组织的即将发生的事件。这些事件可能包括服务的计划维护活动。

其他通知

使用通知选项卡，查看过去七天内可能影响您组织的所有其他通知和持续进行中的事件。这可能包括证书轮换、账单通知和安全漏洞等事件。

Event Log (事件日志)

您也可以使用事件日志选项卡查看组织视图的 Amazon Health 事件。列布局和行为与未决问题和近期问题选项卡类似，不同之处在于事件日志选项卡包含其他列和筛选条件选项，例如事件类别、状态和开始时间。

要在事件日志选项卡中查看组织视图事件

1. 在https://health.aws.amazon.com/health/家中打开 Amazon Health 控制面板。
2. 在导航窗格的您的组织运行状况下，选择事件日志。
3. 在事件日志下，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
   - 区域/可用区
   - 受影响的账户
   - 开始时间
   - 结束时间
   - 类别
   - 描述

Viewing affected accounts and resources (Console)

在您的组织运行状况下，您可以查看组织中受该事件影响的账户以及任何相关资源。例如，如果即将举行亚马逊弹性计算云 (Amazon EC2) 实例维护活动，则您的组织中拥有亚马逊 EC2 实例的账户可以显示在详细信息选项卡中。您可以确定具体的资源，然后联系账户所有者。

要查看受影响的账户和资源

1. 在https://health.aws.amazon.com/health/家中打开 Amazon Health 控制面板。

2. 在导航窗格的您的组织运行状况下，选择其中一个选项卡。
3. 选择一个具有受影响账户值的事件。
4. 选择受影响帐户选项卡。
5. 选择显示账户详细信息查看账户的以下信息：

   - 帐户 ID
   - 帐户名称
   - 主电子邮件
   - 组织部门（OU）
6. 展开账户以查看受影响的资源。
7. 如果资源超过 10 个，请选择查看所有资源进行查看。
8. 要按账户 ID 筛选此特定事件，请执行以下操作：

   a. 在受影响账户选项卡上，依次选择添加筛选条件、账户 ID，然后输入账户 ID。一次只能输入一个账户 ID。
   b. 选择应用。您输入的账户在列表中显示。

Viewing organizational view events (CLI)

启用此功能后，将 Amazon Health 开始记录影响组织中帐户的事件。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。

> **Note**
>
> Amazon Health 不会记录在您启用组织视图之前组织中发生的事件。

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。

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 Amazon CLI 命令返回组织中 Amazon 账户的运行状况事件。

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

禁用组织视图

如果您不想为组织聚合事件，可以从管理账户中关闭此功能，也可以使用 DisableHealthServiceAccessForOrganizationAPI 操作禁用组织视图。

Disabling organizational view events (Console)

Amazon Health 停止汇总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，直到这些事件被删除。

要禁用组织视图

1. 在https://health.aws.amazon.com/health/家中打开 Amazon Health 控制面板。
2. 在导航窗格的您的组织运行状况下，选择配置。
3. 在启用组织视图页面上，选择禁用组织视图。

关闭此功能后，将 Amazon Health 不再聚合组织中的事件。但是，在您通过 Amazon Identity and Access Management (IAM) 控制台、IAM API 或 Amazon Command Line Interface (Amazon CLI) 将其删除之前，服务相关角色仍保留在管理账户中。有关更多信息，请参阅《IAM 用户指南》中的删除服务相关角色。

Disabling organizational view events (CLI)

Example

以下 Amazon CLI 命令会从您的账户中禁用此功能。

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

> **Note**
>
> 您也可以使用 Organizations Disable Access API 操作AWSService禁用组织功能。调用此操作后， Amazon Health 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， Amazon Health 则会返回错误。 Amazon Health 继续汇总您 Amazon 账户的健康事件。

禁用此功能后，将 Amazon Health 不再聚合组织中的事件。但是，服务相关角色仍保留在管理账户中，直到您通过 Amazon Identity and Access Management (IAM) 控制台、IAM API 或 Amazon CLI将其删除。有关更多信息，请参阅 IAM 用户指南中的删除服务相关角色。

管理组织的委派管理员视图

使用 Amazon Health，您可以利用中的委托管理员功能 Amazon Organizations ，该功能允许管理账户以外的账户在Amazon Health 控制面板上或通过 Amazon Health API 以编程方式查看聚合 Amazon Health 事件。委托管理员功能使不同团队能够灵活查看和管理整个组织的运行状况事件。在可能的情况下，将责任委派到管理账户之外是一种最佳 Amazon 安全实践。

目录

为您的组织视图注册委派管理员

为组织启用组织视图后，最多可以在组织中注册五个成员账户作为委托管理员。为此，请调用RegisterDelegatedAdministratorAPI 操作。在您注册成员账户后，他们将被委派为管理员账户，可以从 Amazon Health 控制面板访问 Amazon Health 组织视图。如果该账户有商业、企业入口或企业支持计划，则授权的管理员可以使用 Amazon Health API 访问 Amazon Health 组织视图。

要通过组织中的管理账户建立委托管理员，请调用以下 Amazon Command Line Interface (Amazon CLI) 命令。您可以从管理账户或能够以所需 Amazon Identity and Access Management 权限代入该角色的账户使用此命令。在以下示例命令中，将 ACCOUNT_ID 替换为您要注册的成员账户 ID 以及 Amazon Health 服务主体 “health.amazonaws.com”。

```
aws organizations register-delegated-administrator --account-id ACCOUNT_ID --service-
principal  health.amazonaws.com
```

注册委托管理员后，您可以查看影响全组织账户的所有 Amazon Health 事件。您可以查看过去 90 天或自首次启用组织视图功能以来的历史事件（以较近者为准）。请注意，启用委托管理员功能是异步过程，需要长达一分钟完成。

从组织视图中移除委派管理员

要删除委派管理员的访问权限，请调用 DeregisterDelegatedAdministratorAPI 操作。

在贵组织的管理账户中，调用以下 Amazon CLI 命令以移除委派管理员的成员账户。在以下示例命令中，将 ACCOUNT_ID 替换为要移除的成员账户 ID。

```
aws organizations deregister-delegated-administrator --account-id ACCOUNT_ID --service-principal  health.amazonaws.com
```

通过 Amaz Amazon Health on 监控事件 EventBridge

您可以使用 Amazon EventBridge 来检测事件并对 Amazon Health 事件做出反应。然后，根据您创建的规则，当事件与您在规则中指定的值匹配时， EventBridge 调用一个或多个目标操作。根据事件的类型，您可以捕获事件信息、启动其他事件、发送通知、采取纠正措施或执行其他操作。例如，如果您的 Amazon Amazon Web Services 账户 资源计划更新，例如亚马逊弹性计算云 (Amazon EC2) 实例，则可以使用 Amazon Health 接收电子邮件通知。

> **备注**
>
> - Amazon Health 尽最大努力举办活动。不一定能保证活动一定会送到 EventBridge.
> - 您创建的任何 EventBridge 规则都只能接收您的通知 Amazon Web Services 账户。要接收您内部其他账户的组织活动 Amazon Organizations，请参阅使用组织视图和委派的管理员访问权限聚合 Amazon Health 事件。

EventBridge 作为 Amazon Health 工作流程的一部分，您可以在多种目标类型之间进行选择，包括：

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

例如，您可以使用 Lambda 函数，以在发生 Amazon Health 事件时将通知传递至 Slack 通道。或者，您可以使用 Lambda 和 EventBridge 在事件发生时 Amazon Health 通过 Amazon SNS 发送自定义文本或短信通知。

主题

- 为 Amazon Web Services 区域 覆盖范围创建 EventBridge 规则
- 监控 Amazon Health的账户特定事件和公共事件
- 安装服务相关角色以使用 Amazon 事件检测及响应服务
- 查看分页显示 Amazon Health 的事件列表 EventBridge

- 使用组织视图和委派的管理员访问权限聚合 Amazon Health 事件
- 将 Amazon Health 事件监控和通知与 JIRA 相集成 ServiceNow
- 配置 EventBridge 规则以发送有关事件的通知 Amazon Health
- 在聊天应用程序中配置 Amazon Q Developer 以发送有关事件的通知 Amazon Health
- 自动对 EC2 实例运行操作以响应中的事件 Amazon Health
- 参考： Amazon Health 事件 Amazon EventBridge 架构

为 Amazon Web Services 区域 覆盖范围创建 EventBridge 规则

您必须为要接收 Amazon Health 事件通知的每个区域创建 EventBridge 规则。如未创建规则，则无法接收事件。例如，如果要接收来自中国（北京）区域的事件，则必须为该区域创建规则。

有些 Amazon Health 活动不是特定于地区的。非特定于某个区域的事件称为全局事件。其中包括为 Amazon Identity and Access Management (IAM) 发送的事件。要接收全局事件，必须为中国（宁夏）区域创建规则。

监控 Amazon Health的账户特定事件和公共事件

当您创建用于监控事件的 EventBridge 规则时 Amazon Health，该规则会同时传送特定于账户的事件和公共事件：

- 特定于账户的事件会影响您的账户和资源，例如告知您有关亚马逊 EC2 实例所需更新的事件或其他计划更改事件的事件。
- 公共事件显示在Amazon Health 控制面板 — 服务运行状况上。公共事件并非特定于 Amazon Web Services 账户 ，而是提供有关服务的区域可用性的公共信息。

> **Important**
>
> 要接收两种事件类型，则规则必须使用 `"source": [ "aws.health"]` 值。通配符（如 `"source": [ "aws.health*"]`）与希望监控的任何事件的模式均不相符。

如果您正在监视来自的公共事件 Amazon Web Services 区域，我们建议您创建备份规则。的 Amazon Health 公共事件同时发送到受影响的区域和备用区域。建议您使用 eventArn 和 CommunicationID 删除重复 Amazon Health 事件，因为对于发送到备份区域的 Amazon Health 消息，这些事件保持一致。

您可以使用参数在中识别事件是公共事件还是特定于 EventBridge账户的事件。 eventScopeCode 事件可以是 PUBLIC 事件，也可以是 ACCOUNT_SPECIFIC 事件。您也可以根据此参数筛选规则。

示例：Amazon Elastic Compute Cloud 的公共事件

以下事件显示了亚马逊 EC2 在美国东部（弗吉尼亚北部）地区的运营问题。

```
{
    "version": "0",
    "id": "fd9d4512-1eb0-50f6-0491-d016ae56aef0",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-02-15T10:07:10Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "eventArn": "arn:aws:health:us-east-1::event/EC2/AWS_EC2_OPERATIONAL_ISSUE",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_OPERATIONAL_ISSUE",
        "eventTypeCategory": "issue",
        "eventScopeCode": "PUBLIC",
        "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
        "startTime": "Wed, 15 Feb 2023 22:07:07 GMT",
        "lastUpdatedTime": "Wed, 15 Feb 2023 22:07:07 GMT",
        "statusCode": "open",
        "eventRegion": "us-east-1",
        "eventDescription": [{
            "latestDescription": "We are investigating increased API Error rates and
 Latencies for Amazon Elastic Compute Cloud in the US-EAST-1 Region.",
            "language": "en_US"
        }],
        "page": "1",
        "totalPages": "1",
        "affectedAccount": "123456789012"

    }
}
```

安装服务相关角色以使用 Amazon 事件检测及响应服务

如果您的账户使用 Amazon 事件检测和响应，则必须在您的账户中安装AWSServiceRoleForHealth_EventProcessor服务相关角色。

此角色信任 event-processor.health.amazonaws.com 服务主体担任角色。附属于此角色的是AWSHealth_EventProcessorServiceRolePolicy Amazon 托管策略。此策略列出了该角色可以执行的权限，例如 Amazon Web Services 服务 为您调用其他权限。

然后，此角色会在您的账户中创建一个 Amazon EventBridge 托管规则。该规则被命名为 AWSHealthEventProcessor-DO-NOT-DELETE。此规则是您的账户所需的基础架构，因此 EventBridge 可以将警报状态变更信息从您的账户传送到 Amazon Health。

相关信息

要了解更多信息，请参阅以下主题：

- 将服务相关角色用于 Amazon Health
- Amazon 托管策略：AWSHealth_EventProcessorServiceRolePolicy

查看分页显示 Amazon Health 的事件列表 EventBridge

Amazon Health 当resources或列表affectedEntities导致消息大小超过 EventBridge 256KB 的邮件大小限制时，支持对 Amazon Health 事件进行分页。

Amazon Health 包括消息中的所有resources和detail.affectedEntities字段。如果此列表resources和detail.affectedEntities值超过 256KB，则会将运行状况事件 Amazon Health 拆分为多个页面，并将这些页面作为单独的消息发布到中。 EventBridge每个页面均保留相同的 eventARN 和 communicationId 值，以便在收到所有页面后重新合并 resources 或 detail.affectedEntities 列表。

这些额外的消息可能会导致不必要的消息，例如，当 EventBridge 规则被定向到人类可读的界面（例如电子邮件或聊天）时。收到人类可读通知的客户可以为 detail.page 字段添加筛选条件，从而仅处理第一个页面，这将消除利用后续页面创建的不必要消息。

在此架构中，每个 communicationId 均会在 communicationId 后包含用连字符连接的页码，即使只有 1 页也不例外。字段detail.page和detail.totalPages描述了 Amazon Health 活动的当前页码和总页数。除 detail.affectedEntities 或 resources 列表以外，每个分页消息中包含的信息完全相同。收到所有页面后，可以重新构造这些列表。受影响资源和实体页面不会排序。

使用组织视图和委派的管理员访问权限聚合 Amazon Health 事件

Amazon Health 支持对在 Amazon 上发布 Amazon Health 的事件进行组织视图和委派管理员访问权限 EventBridge。开启组织视图后 Amazon Health，管理账户或委托管理员账户将收到来自组织内所有账户的单个 Amazon Health 事件提要 Amazon Organizations。

此功能旨在提供集中视图，以帮助管理整个组织中的 Amazon Health 事件。在管理账户中设置组织视图和 EventBridge 规则不会停用组织中其他账户的 EventBridge 规则。

有关在上启用组织视图和委派管理员访问权限的更多信息 Amazon Health，请参阅聚合 Amazon Health 事件。

将 Amazon Health 事件监控和通知与 JIRA 相集成 ServiceNow

您可以使用服务管理连接器 (SMC) 将 Amazon Health 事件与 JIRA 集成，接收操作和账户信息，为计划的更改做好准备，以及管理 Health 事件。 ServiceNow 与的 SMC 集成 Amazon Health 可以使用发送的 Health 事件 EventBridge 来自动创建、映射和更新 JIRA 工单和 ServiceNow事件。

您可以使用组织视图和委托管理员访问权限在 JIRA 中轻松管理整个组织的 Health 事件 ServiceNow，并将 Amazon Health 信息直接整合到团队的工作流程中。

有关使用 SMC 进行 ServiceNow 集成的更多信息，请参阅集成 Amazon Health 。 ServiceNow

有关使用 SMC 集成 JIRA Management Cloud 的更多信息，请参阅 Amazon Health in JIRA。

配置 EventBridge 规则以发送有关事件的通知 Amazon Health

您可以创建一条 EventBridge 规则，以便收到有关您账户中 Amazon Health 发生的事件的通知。在为创建事件规则之前 Amazon Health，请执行以下操作：

- 熟悉中的事件、规则和目标。 EventBridge有关更多信息，请参阅什么是亚马逊 EventBridge？ 在 Amazon EventBridge 用户指南和新增内容中 EventBridge — 跟踪和响应您的 Amazon 资源更改。
- 创建要在您的事件规则中使用的目标。

要为创建 EventBridge 规则 Amazon Health

1. 打开 Amazon EventBridge 控制台，网址为https://console.aws.amazon.com/events/。
2. 要更改 Amazon Web Services 区域，请使用页面右上角的区域选择器。选择要在其中跟踪 Amazon Health 事件的区域。

3. 在导航窗格中，选择规则。
4. 选择 创建规则。
5. 在 Define rule detail（定义规则详细信息）页面上，输入规则名称和描述。
6. 对于 事件总线和 规则类型，保留默认值，然后选择下一步。
7. 在构建事件模式页面上，为事件源选择Amazon 事件和 EventBridge 合作伙伴事件。
8. 在 事件模式下，对于 E事件源，选择 Amazon Web Services 服务。
9. 在 事件模式下，对于 Amazon Web Services 服务，选择运行状况。
10. 对于 事件类型，选择以下选项之一：
    - 特定运行状况滥用事件 — 为事件类型名称中包含单词 Abuse 的 Amazon Health 事件创建一个规则。
    - 特定的 Health 事件 — 为特定 Amazon Web Services 服务事件（例如 Amazon）创建规则 EC2。
11. 您可以选择 任何服务 或 特定服务。如果已选择特定服务，请选择以下选项之一：
    - 选择 任何事件类型类别可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，如 issue、accountNotification 或 scheduledChange。

    > **Tip**
    >
    > - 要监控特定服务的所有 Amazon Health 事件，我们建议您选择 “任意事件类型” 类别和 “任何资源”。这样可以确保规则监控您指定服务的所有 Amazon Health 事件，包括任何新的事件类型代码。有关规则示例，请查看所有 Amazon EC2 事件。
    > - 您可以创建一条规则监控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。

12. 如果选择特定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 任何事件类型类别，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。将创建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**，则规则仅适用于您的账户中发生的此类事件。
13. 为受影响资源选择以下选项之一：
    - 选择 任何资源以创建适用于所有资源的规则。

- 选择 “特定资源”，然后输入一个或多个资源中的。 IDs 例如，您可以指定一个 Amazon EC2 实例 ID（例如*i-EXAMPLEa1b2c3de4*）来监控仅影响此资源的事件。

14. 审查您的规则设置以使其符合您的事件监控要求。
15. 选择下一步。
16. 在 选择目标页面上，选择您为此规则创建的目标类型，然后配置该类型所需的任何其他选项。例如，您可以将事件发送到 Amazon SQS 队列或 Amazon SNS 主题。
17. 选择下一步。
18. （可选）在 配置标签页面上，添加任意标签，然后选择 下一步。
    - 注意：标签目前不是由 aws.health 来源发送的。 EventBridge
19. 在 Review and create（审查并创建）页面上，审查您的规则设置并确保其符合您的事件监控要求。
20. 选择 创建规则。

Example：特定 Amazon EC2 活动的规则

以下示例创建了一个用于 EventBridge 监控以下内容的规则：

- Amazon EC2 服务
- scheduledChange 事件类型类别
- `AWS_EC2_INSTANCE_TERMINATION_SCHEDULED` 和 `AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED` 的事件类型代码
- ID 为 `i-EXAMPLEa1b2c3de4` 的实例

为多个服务和类别创建规则

上述步骤中的示例向您展示如何为单个服务和事件类型类别创建规则。您也可以为多个服务和事件类型类别创建规则。这意味着您不必为希望监控的每个服务和类别单独创建规则。为此，您必须编辑事件模式，然后手动输入更改。

您可以使用以下任一选项。

为现有规则添加服务和类别

1. 在 EventBridge 控制台的 “规则” 页面上，选择规则名称。
2. 在右上角，选择 编辑。

3. 选择下一步。
4. 对于 事件模式,选择编辑模式，然后在文本字段中输入您的更改。
5. 选择 下一步，直到进入 审查并更新页面。
6. 单击 更新规则以保存您的更改。

为新规则添加服务和类别

1. 请按照 配置 EventBridge 规则以发送有关事件的通知 Amazon Health 到 步骤 9 中的过程操作。
2. 对于 事件模式，选择 编辑模式，而不是从列表中选择单个服务或类别。
3. 在文本字段中输入您的更改。请将以下示例模式作为自行创建事件模式的模型。
4. 审查您的事件模式，然后按照 配置 EventBridge 规则以发送有关事件的通知 Amazon Health 中的剩余过程创建规则。

使用 API 或 Amazon Command Line Interface (Amazon CLI)

对于新的或现有的规则，请使用 PutRuleAPI 操作或`aws events put-rule`命令更新事件模式。有关 Amazon CLI 命令示例，请参阅《命令参考》中的 put-Amazon CLI r ule。

Example 示例：多个服务和事件类型类别

以下事件模式创建了一条规则，用于监控三种 Amazon 服务的`issue`、和`scheduledChange`事件类型类别的事件：亚马逊`accountNotification` EC2、Amazon A EC2 uto Scaling 和 Amazon VPC。

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

```
  ],
  "source": [
    "aws.health"
  ]
}
```

在聊天应用程序中配置 Amazon Q Developer 以发送有关事件的通知 Amazon Health

你可以直接在聊天客户端（例如 Slack 和 Amazon Chime）中接收 Amazon Health 事件。您可以使用此事件来识别最近可能影响您的 Amazon 应用程序和基础架构的 Amazon 服务问题。然后，您可以登录 Amazon Health 控制面板了解有关更新的更多信息。例如，如果您正在监控 Amazon 账户中的AWS_EC2_INSTANCE_STOP_SCHEDULED事件类型，则该 Amazon Health 事件可以直接显示在您的 Slack 频道中。

先决条件

在开始之前，您必须满足以下条件：

- 在聊天应用程序中使用 Amazon Q Developer 配置的聊天客户端。您可以配置 Amazon Chime 和 Slack。有关更多信息，请参阅 Amazon Q 开发者聊天应用程序管理员指南中的聊天应用程序中的 Amazon Q 开发者入门。
- 您创建并订阅的 Amazon SNS 主题。如果已具有 SNS 主题，则可以使用现有主题。有关更多信息，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门。

在聊天应用程序中与 Amazon Q 开发者一起接收 Amazon Health 活动

1. 按照 配置 EventBridge 规则以发送有关事件的通知 Amazon Health 到步骤 13 中的过程操作。

   a. 在步骤 13 中完成事件模式的设置后，在模式的最后一行添加逗号，然后添加以下行以从分页 Amazon Health 事件中删除不必要的聊天消息。请参阅 查看分页显示 Amazon Health 的事件列表 EventBridge。

      ```
      "detail.page": ["1"]
      ```

   b. 在步骤 14 中选择目标时，请选择 SNS 主题。您将在聊天应用程序的 Amazon Q 开发者控制台中使用相同的 SNS 主题。

   c. 完成剩余步骤，以创建规则。

2. 在聊天应用程序控制台中导航到 Amazon Q 开发者。
3. 选择聊天客户端，如 Slack 通道名称，然后选择 Edit（编辑）。
4. 在 Notifications - optional（通知 - 可选）部分，在 Topics（主题）中选择与步骤 1 指定的相同的 SNS 主题。
5. 选择保存。

   当 Amazon Health 向其 EventBridge 发送符合您规则的事件时，该 Amazon Health 事件将显示在您的聊天客户端中。
6. 选择活动名称可在 Amazon Health 控制面板中查看更多信息。

自动对 EC2 实例运行操作以响应中的事件 Amazon Health

您可以自动执行操作，以响应 Amazon EC2 实例的计划事件。当 Amazon Health 向您的 Amazon 账户发送事件时，您的 EventBridge 规则可以调用目标（例如 Automati Amazon Systems Manager on 文档）来代表您自动执行操作。

例如，当为亚马逊 EC2 弹性区块存储 (Amazon EBS) Store EC2 支持的实例安排亚马逊实例停用事件时 Amazon Health ，会将事件类型发送到您的控制AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED面板。 Amazon Health 当规则检测到此事件类型后，您可以自动停止和启动实例。这样，将不必手动执行这些操作。

> **Note**
>
> 要自动对您的亚马逊 EC2 实例执行操作，这些实例必须由 Systems Manager 管理。

有关更多信息，请参阅《亚马逊 EC2 EC2 用户指南》 EventBridge中的 “实现亚马逊自动化”。

先决条件

在创建规则之前，您必须创建 Amazon Identity and Access Management (IAM) 策略、创建 IAM 角色并更新该角色的信任策略。

创建 IAM policy

按照此步骤为您的角色创建客户管理型策略。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 policy

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

```
{
  "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/AutomationEVRole"
    }
  ]
}
```

a. 在Resource参数中，在亚马逊资源名称 (ARN) 中，输入您的 Amazon 账户 ID。

b. 您也可以替换角色名称或使用默认名称。此示例使用 *AutomationEVRole*。

6. 选择下一步：标签。
7. （可选）您可以使用标签作为键值对将元数据添加到策略。
8. 选择 下一步: 审核。
9. 在 “查看策略” 页面上，输入名称（例如）*AutomationEVRolePolicy*和可选的描述。
10. 查看 Summary（摘要）页面，以查看策略允许的权限。如果您对策略感到满意，请选择 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《IAM 用户指南》中的创建 IAM policy（控制台）。

创建 IAM 角色

创建策略后，您必须创建 IAM 角色，并将策略附加到此角色。

为 Amazon 服务创建角色

1. 登录 Amazon Web Services Management Console 并打开 IAM 控制台，网址为https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择角色，然后选择创建角色。
3. 对于Select type of trusted entity（选择受信任实体的类型），选择 Amazon service（服务）。
4. EC2为要允许担任此角色的服务进行选择。
5. 选择下一步: 权限。
6. 输入您创建的策略名称，例如*AutomationEVRolePolicy*，然后选中策略旁边的复选框。
7. 选择下一步：标签。

8. （可选）您可以使用标签作为键值对将元数据添加到角色。
9. 选择 下一步: 审核。
10. 对于 Role name（角色名称），输入 *AutomationEVRole*。此名称必须与您创建的 IAM policy 的 ARN 中显示的名称相同。
11. （可选）对于 Role description(角色描述)，输入角色的描述。
12. 检查角色，然后选择创建角色。

有关更多信息，请参阅 IAM 用户指南中的为 Amazon 服务创建角色。

更新信任策略

最后，您可以更新所创建角色的信任策略。您必须完成此过程，才能在 EventBridge 控制台中选择此角色。

要更新该角色的信任策略

1. 登录 Amazon Web Services Management Console 并打开 IAM 控制台，网址为https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择角色。
3. 在您 Amazon 账户中的角色列表中，选择您创建的角色的名称，例如*AutomationEVRole*。
4. 选择 信任关系 选项卡，然后选择 编辑信任关系。
5. 对于 Policy Document，复制以下 JSON，删除默认策略，然后将复制的 JSON 粘贴到所在位置。

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

6. 选择更新信任策略。

有关更多信息，请参阅 IAM 用户指南中的修改角色信任策略（控制台）。

为以下各项创建规则 EventBridge

按照此过程在 EventBridge 控制台中创建规则，以便您可以自动停止和启动计划停用的 EC2 实例。

为 Systems EventBridge Manager 自动操作创建规则

1. 打开 Amazon EventBridge 控制台，网址为https://console.aws.amazon.com/events/。
2. 在导航窗格中的 Events（事件）下，选择 Rules（规则）。
3. 在 创建规则页面上，输入规则的 名称 和 描述。
4. 在 Define pattern（定义模式）下，选择 Event pattern（事件模式），然后选择 Pre-defined pattern by service（按服务预定义的模式）。
5. 对于 Service provider（服务提供商），选择 Amazon。
6. 对于 服务名称，选择 运行状况。
7. 对于 事件类型，选择 特定运行状况事件。
8. 选择 “特定服务”，然后选择EC2。
9. 选择 特定事件类型类别，然后选择 scheduledChange。
10. 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，选择。**AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED**对于 Amazon EC2 实例存储支持的实例，请选择。**AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED**
11. 选择 Any resource（任何资源）。

    您的 事件模式类似于以下示例。

    Example

```
{
  "source": [
    "aws.health"
  ],
  "detail-type": [
```

```
    "AWS Health Event"
  ],
  "detail": {
    "service": [
      "EC2"
    ],
    "eventTypeCategory": [
      "scheduledChange"
    ],
    "eventTypeCode": [
      "AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED"
    ]
  }
}
```

12. 添加 Systems Manager Automation 文档目标。在 选择目标下，对于 目标，选择 SSM Automation。
13. 对于 Document（文档），选择 `Amazon-RestartEC2Instance`。
14. 展开 配置自动化参数，然后选择 输入转换器。
15. 在 输入路径字段中输入 **`{"Instances":"$.resources"}`**。
16. 对于第二个字段，输入 **`{"InstanceId": <Instances>}`**。
17. 选择使用现有角色，然后选择您创建的 IAM 角色，例如*`AutomationEVRole`*。

> **Note**
>
> 如果您没有具有必需权限和 Systems Manager 权限 EC2 以及可信关系的现有 IAM 角色，则您的角色将不会出现在列表中。有关更多信息，请参阅 先决条件。

18. 选择创建。

如果您的账户中发生了符合您规则的事件，则 EventBridge 会将该事件发送给您的指定目标。

参考： Amazon Health 事件 Amazon EventBridge 架构

以下是 Amazon Health 事件的架构。详细信息参数的内容详见第二个表。该架构表后提供了示例有效载荷。

Amazon Health 事件架构

Amazon Health 事件架构

参数	描述	必填
版本	EventBridge 版本，当前为“0”。	是
id	EventBridge 事件的唯一标识符。	是
detail-type	详细信息的类型。对于 Amazon Health 事件，支持的值为&Amazon Health Event和 Amazon Health Abuse Event	是
source	事件总线源。对于 Amazon Health 事件，支持的值为 aws.health	是
account	向其发送 Amazon Health 事件的账户 ID。	是

参数	描述	必填
	Note 对于组织视图，如果通过管理账户或委派管理员账户接收，则将是与受影响账户不同的账户。	
time	通知发送到的时间 EventBridge。格式：yyyy-mm-ddThh:mm:ssZ 。	是

参数	描述	必填
region	Amazon Web Services 区域通知已发送到的。 Note 此字段未指明此 Amazon Health 事件的受影响区域。该信息已在 detail.eventRegion 中报告。	是
resources	描述账户中受影响资源的列表（如有）。 如未提及任何资源，则此字段为空。	否

参数	描述	必填
detail	包含 Amazon Health 事件详细信息的部分，如本次活动之后的表格中所述。	是

“detail”参数的架构内容

下表记录了 Amazon Health 事件架构中 det a il 参数的内容。

Amazon Health 事件架构：详细参数内容

“detail”参数的内容	描述	必填
eventArn	特定区域 Amazon Health 的事件的唯一标识符，包括区域和事件 ID。 **Note** 事件 ARN 不是特定 Amazon Web Services 账户 或地区所独有的。	是
service	Amazon Web Services 服务 受 Amazon Health 事件影响的。例如，亚马逊 EC2、亚马逊简单存储服务、亚马逊 Redshift 或亚马逊关系数据库服务。	是
eventTypeCode	事件类型的唯一标识符。例如：AWS_EC2_INSTANCE_NETWORK_MA	是

“detail”参数的内容	描述	必填
	INTENANCE_SCHEDULED 和 AWS_EC2_INSTANCE_REBOOT_MAINTENANCE_SCHEDULED 。包含 MAINTENANCE_SCHEDULED 的事件通常在开始时间之前约两周推送。 **Note** 所有新的计划生命周期事件都具有事件类型 AWS_{SERVICE}_PLANNED_LIFECYCLE_EVENT 。	
eventTypeCategory	事件的类别代码。支持的值包括 issue、accountNotification 、investigation 和 scheduledChange 。	是
eventScopeCode	指明该 Amazon Health 事件是针对特定账户的还是公开的。支持的值为 ACCOUNT_SPECIFIC 或 PUBLIC。	是

“detail”参数的内容	描述	必填
communicationId	此次 Amazon Health 活动通信的唯一标识符。 具有相同通信 ID 的消息可能是单个 Amazon Health 事件的备份消息或页面。此标识符可以与账户 ID 结合使用，有助于消除重复的消息。 在支持 Amazon Health 事件分页的情况下，通信 ID 包括页码，以保持通信 ID 在各个页面上的唯一性，例如 123456789 10-1。有关更多信息，请参阅查看分页显示 Amazon Health 的事件列表 EventBridge。	是
startTime	Amazon Health 事件的开始时间，格式为DoW, DD, MMM, YYYY, HH:MM:SS TZ。 计划事件的开始时间可以是未来。	是
endTime	Amazon Health 事件的结束时间，格式为：DoW, DD MMM YYYY HH:MM:SS TZ。 无法为计划某个未来时间进行的事件提供结束时间。	否
lastUpdatedTime	Amazon Health 事件的上次更新时间，格式为DoW, DD MMM YYYY HH:MM:SS TZ。	是

“detail”参数的内容	描述	必填
statusCode	Amazon Health 事件的状态。 支持的值包括 `open`、`closed` 和 `upcoming`。	是
eventRegion	此 Amazon Health 事件描述的受影响区域。	是
eventDescription	描述 Amazon Health 事件的部分。包括用于描述事件的语言和文本字段。 • 语言- Amazon Health 事件中使用的语言的代码。通常由事件发布区域决定。例如，在 `us-east-1` 区域通常为 `en_US`。 • LatestDescription — 描述从 Amazon Health API 呈现 Amazon Health 的事件，通常显示在仪表板上 Amazon Health 。 **Note** 对于公共事件，其中仅包含最新更新，而非事件的完整历史记录。	是

“detail”参数的内容	描述	必填
eventMetadata	可以为 Amazon Health 事件提供的其他事件元数据。 • <metadata key 1> – 元数据键值对字符串："keystring1": "keyvalue1" 事件元数据的键值对由发送事件的服务确定。 Amazon Health	否
affectedEntities	描述 Amazon Health 事件中受影响资源的资源值和状态的数组。 • entityValue – 资源/实体 ID。 • lastUpdatedtime – 此资源/实体状态的上次更新时间，格式为 `DoW, DD MMM YYYY HH:MM:SS TZ`。 • status – 受影响资源/实体的状态。支持的值包括 `IMPAIRED`、`UNIMPAIRED` 、`PENDING`、`RESOLVED` 和 `UNKNOWN`。	否

“detail”参数的内容	描述	必填
page	此消息所表示的页面。有关更多信息，请参阅 查看分页显示 Amazon Health 的事件列表 EventBridge。 **Note** 分页仅在资源上发生。如果由于其他原因超出 256KB 大小限制，则通信会失败。	是
totalPages	此运行状况事件的总页数。有关更多信息，请参阅 查看分页显示 Amazon Health 的事件列表 EventBridge。 您可以通过该值来确定是否收到某个账户多页通信的所有页面。	是
affectedAccount	受影响账户的账户 ID。 如果将此运行状况事件发送到属于的账户， Amazon Organizations 并且在管理账户或委托管理员账户中接收，则该值可能与account字段中的值不同。	是

Public Health Event-亚马逊 EC2 运营问题

```
{
    "version": "0",
    "id": "7bf73129-1428-4cd3-a780-95db273d1602",
```

```
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-01-27T09:01:22Z",
    "region": "af-south-1",
    "resources": [],
    "detail": {
        "eventArn": "arn:aws:health:af-south-1::event/EC2/AWS_EC2_OPERATIONAL_ISSUE/
AWS_EC2_OPERATIONAL_ISSUE_7f35c8ae-af1f-54e6-a526-d0179ed6d68f",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_OPERATIONAL_ISSUE",
        "eventTypeCategory": "issue",
        "eventScopeCode": "PUBLIC",
        "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
        "startTime": "Fri, 27 Jan 2023 06:02:51 GMT",
        "endTime": "Fri, 27 Jan 2023 09:01:22 GMT",
        "lastUpdatedTime": "Fri, 27 Jan 2023 09:01:22 GMT",
        "statusCode": "open",
        "eventRegion": "af-south-1",
        "eventDescription": [{
            "language": "en_US",
            "latestDescription": "Current severity level: Operating normally\n
\n[RESOLVED] \n\n [03:15 PM PST] We continue see recovery \n\nThe following AWS
 services were previously impacted but are now operating normally: APPSYNC, BACKUP,
 EVENTS."
        }],
        "affectedEntities": [],
        "page": "1",
        "totalPages": "1",
        "affectedAccount": "123456789012"
    }
}
```

账户特定 Amazon Health 事件-Elastic Load Balancing API 问题

```
{
    "version": "0",
    "id": "121345678-1234-1234-1234-123456789012",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2022-06-10T06:27:57Z",
    "region": "ap-southeast-2",
```

```
    "resources": [],
    "detail": {
        "eventArn": "arn:aws:health:ap-southeast-2::event/
AWS_ELASTICLOADBALANCING_API_ISSUE_90353408594353980",
        "service": "ELASTICLOADBALANCING",
        "eventTypeCode": "AWS_ELASTICLOADBALANCING_API_ISSUE",
        "eventTypeCategory": "issue",
        "eventScopeCode": "ACCOUNT_SPECIFIC",
        "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
        "startTime": "Fri, 10 Jun 2022 05:01:10 GMT",
        "endTime": "Fri, 10 Jun 2022 05:30:57 GMT",
        "statusCode": "open",
        "eventRegion": "ap-southeast-2",
        "eventDescription": [{
            "language": "en_US",
            "latestDescription": "A description of the event will be provided here"
        }],
        "page": "1",
        "totalPages": "1",
        "affectedAccount": "123456789012"
    }
}
```

账户特定 Amazon Health 事件-Amazon EC2 实例存储驱动器性能下降

```
{
    "version": "0",
    "id": "121345678-1234-1234-1234-123456789012",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2022-06-03T06:27:57Z",
    "region": "us-west-2",
    "resources": [
        "i-abcd1111"
    ],
    "detail": {
        "eventArn": "arn:aws:health:us-west-2::event/
AWS_EC2_INSTANCE_STORE_DRIVE_PERFORMANCE_DEGRADED_90353408594353980",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_INSTANCE_STORE_DRIVE_PERFORMANCE_DEGRADED",
        "eventTypeCategory": "issue",
        "eventScopeCode": "ACCOUNT_SPECIFIC",
```

```
        "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
        "startTime": "Fri, 3 Jun 2022 05:01:10 GMT",
        "endTime": "Fri, 3 Jun 2022 05:30:57 GMT",
        "statusCode": "open",
        "eventRegion": "us-west-2",
        "eventDescription": [{
            "language": "en_US",
            "latestDescription": "A description of the event will be provided here"
        }],
        "affectedEntities": [{
            "entityValue": "i-abcd1111"
        }],
        "page": "1",
        "totalPages": "1",
        "affectedAccount": "123456789012"
    }
}
```

监控 Amazon Health

监控是维护和其他 Amazon 解决方案的可靠性、可用性和性能的重要组成部分。 Amazon Health Amazon 提供以下监控工具 Amazon Health，供您监视、报告问题并在适当时采取措施：

- Amazon 会实时 CloudWatch 监控您的 Amazon 资源和您运行 Amazon 的应用程序。您可以收集和跟踪指标，创建自定义的控制平面，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， EventBridge 以便收到有关可能影响您的服务和资源 Amazon Health 的事件的通知。例如，如果 Amazon Health 发布了有关您的 Amazon EC2 实例的事件，您可以使用这些通知来采取行动，并根据需要更新或替换您的资源。有关更多信息，请参阅 通过 Amaz Amazon Health on 监控事件 EventBridge。
- Amazon CloudTrail 捕获由您的账户或代表您的 Amazon 账户进行的 API 调用和相关事件，并将日志文件传输到您指定的 Amazon S3 存储桶。您可以识别哪些用户和帐户拨打了电话 Amazon、发出呼叫的源 IP 地址以及呼叫发生的时间。有关更多信息，请参阅 用户指南。Amazon CloudTrail

主题

- 使用记录 Amazon Health API 调用 Amazon CloudTrail

使用记录 Amazon Health API 调用 Amazon CloudTrail

Amazon Health 与 Amazon CloudTrail一项服务集成，该服务提供用户、角色或 Amazon 服务在中执行的操作的记录 Amazon Health。 CloudTrail 将发出的 API 调用捕获 Amazon Health 为事件。捕获的调用包括来自 Amazon Health 控制台的调用和对 Amazon Health API 操作的代码调用。如果您创建了跟踪，则可以允许将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括的事件 Amazon Health。如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的 “事件历史记录” 中查看最新的事件。使用收集到的信息 CloudTrail，您可以确定向哪个请求发出 Amazon Health、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。

要了解更多信息 CloudTrail，包括如何配置和启用它，请参阅Amazon CloudTrail 用户指南。

Amazon Health 信息在 CloudTrail

CloudTrail 在您创建 Amazon 账户时已在您的账户上启用。当支持的事件活动发生在中时 Amazon Health，该活动会与其他 Amazon 服务 CloudTrail 事件一起记录在事件历史记录中。您可以在自己

的 Amazon 账户中查看、搜索和下载最近发生的事件。有关更多信息，请参阅使用事件历史记录查看 CloudTrail 事件。

要持续记录您 Amazon 账户中的事件，包括的事件 Amazon Health，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。默认情况下，当您在控制台中创建跟踪时，该跟踪将应用于所有 Amazon 区域。此跟踪记录在 Amazon 分区中记录所有区域中的事件，并将日志文件传送至您指定的 Simple Storage Service（Amazon S3）存储桶。此外，您可以配置其他 Amazon 服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。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
- 配置 Amazon SNS 通知 CloudTrail
- 接收来自多个账户的 CloudTrail 日志文件

所有 Amazon Health API 操作均由《API 参考》记录 CloudTrail 并记录在《Amazon Health API 参考》中。例如，对`DescribeEventsDescribeEventDetails`、和`DescribeAffectedEntities`操作的调用会在 CloudTrail 日志文件中生成条目。

Amazon Health 支持将以下操作作为事件记录在 CloudTrail 日志文件中：

- 使用根用户凭证还是 IAM 凭证发出请求
- 请求是使用角色还是联合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。

要在日志文件传送时收到通知，您可以配置 CloudTrail 为在传送新日志文件时发布 Amazon SNS 通知。有关更多信息，请参阅为 CloudTrail 配置 Amazon SNS 通知。

您还可以将来自 Amazon 账户的 Amazon Health 日志文件聚合到单个 Amazon S3 存储桶中。

有关更多信息，请参阅从多个账户中接收 CloudTrail 日志文件。

示例： Amazon Health 日志文件条目

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 Amazon S3 存储桶。 CloudTrail 日志文件包含一个或多个日志条目。事件代表来自任何来源的单个请求，包括有关请求的操作、操作的日期和时间、请求参数等的信息。 CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此它们不会按任何特定的顺序出现。

以下示例显示了演示该DescribeEntityAggregates操作的 CloudTrail 日志条目。


```
{
   "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"
   }
   ],
   ...
```

```
}
```

的文档历史记录 Amazon Health

下表描述了此版本的文档 Amazon Health。

- API 版本：2016-08-04

下表描述了自 2020 年 8 月 28 日起对 Amazon Health 文档进行的重要更新。您可以订阅 RSS 源来接收有关更新的通知。

变更	说明	日期
中添加了管理 Amazon Health 通知的常见问题解答 Amazon 用户通知服务	有关更多信息，请参阅Amazon 用户通知服务 常见问题解答中的管理通知。	2025年2月18日
添加了有关向终端节点发 IPv6 出的仅限请求的信息。	有关更多信息，请参阅为 Amazon Health API 请求选择终端节点。	2025 年 1 月 28 日
在中管理 Amazon Health 通知 Amazon 用户通知服务	有关更多信息，请参阅中的管理通知 Amazon 用户通知服务。	2025 年 1 月 16 日
更正了使用 Amazon 监控 Amazon Health 事件中的 JSON EventBridge	有关更多信息，请参阅使用 Amazon 监控 Amazon Health 事件 EventBridge。	2024 年 9 月 3 日
更新了有关下载受影响资源的信息	有关更多信息，请参阅 Affected resources view。	2024 年 7 月 27 日
从 Amazon Health 文档的“安全”部分移除了有关网际流量隐私的内容	有关更多信息，请参阅中的安全性 Amazon Health。	2024 年 3 月 27 日
更新了 Amazon Health 文档的“Amazon Health Dashboard – 服务运行状况”和“计划生命周期事件”部分。	有关更多信息，请参阅 Amazon Health Dashboard – Service health 和 Planned	2024 年 2 月 15 日

	lifecycle events for Amazon Health。	
在 “为以下对象创建 EventBridge 规则” 中删除了重复的要点 Amazon Health	在 “为其创建 EventBridge 规则” 中删除了重复的要点 Amazon Health。	2023 年 12 月 4 日
添加了有关已计划的生命周期事件的文档	有关更多信息，请参阅 Amazon Health的已计划的生命周期事件。	2023 年 10 月 31 日
更新了 AWSHealthFullAccess 的文档	现在，您可以在中国区域使用 AWSHealthFullAccess 。有关信息，请参阅Amazon 托管策略 Amazon Health。	2023 年 10 月 16 日
更新了 AWSHealthFullAccess 的文档	现在，您可以在 Amazon GovCloud (US) Regions使用 AWSHealthFullAccess 托管策略。有关信息，请参阅Amazon 托管策略 Amazon Health。	2023 年 10 月 16 日
在中添加了有关配置 Amazon 用户通知的文档 Amazon Health。	现在，您可以在中配置 Amazon 用户通知 Amazon Health。有关更多信息，请参阅为配置 Amazon 用户通知 Amazon Health。	2023 年 8 月 30 日
在 “聚合 Amazon Health 事件” 部分中添加了有关委派管理员功能的文档。	有关更多信息，请参阅委托管理员组织视图。	2023 年 7 月 27 日
SLR 策略更新	Amazon 托管策略更新：Health_ OrganizationsServiceRolePolicy。有关更多信息，请参阅适用于 Amazon Health的Amazon 托管策略。	2023 年 7 月 19 日

Amazon Health 架构现在支持事件元数据	现在，您可以从事件中接收 Amazon Health 事件元数据。有关更多信息，请参阅使用 Amazon 监控 Amazon Health 事件 EventBridge。	2023 年 6 月 20 日
更新了 Amazon 的文档 EventBridge	现在，您可以使用 Amazon EventBridge 规则来监控账户特定事件和公共事件。有关更多信息，请参阅使用 Amazon 监控 Amazon Health 事件 EventBridge。	2023 年 5 月 2 日
添加了 Amazon 托管策略的文档	添加了用于 Amazon Health 的Amazon 托管策略的文档并为Amazon Health使用与服务相关的角色。	2023 年 1 月 18 日
添加了时区设置文档	使用新的时区功能按当地时区或 UTC 查看 Amazon Health 控制面板。有关更多信息，请参阅Amazon Health 控制面板入门-您的账户健康状况和Amazon Health 控制面板-服务运行状况。	2022 年 9 月 21 日
已更新的文档	为 A Amazon Health ware 添加了文档。有关更多信息，请参阅 Amazon Health Aware。	2022 年 5 月 25 日

已更新的文档	这些区域有：Service Health Dashboard 还有 Amazon Personal Health Dashboard 已更名为 Amazon Health 控制面板。 有关更多信息，请参阅Amazon Health 控制面板入门-您的账户健康状况和Amazon Health 控制面板-服务运行状况。	2022 年 2 月 28 日
更新了 Amazon 的文档 EventBridge	关于使用 Amazon 监控 H EventBridge ealth 事件的新主题。 Amazon Health 有关更多信息，请参阅使用 Amazon 监控 Amazon Health 事件 EventBridge。	2022 年 2 月 3 日
已更新的文档	如果您有 E nterprise On-Ramp S upport 计划，则可以使用 Amazon Health API。	2021 年 11 月 24 日
添加的文档	Amazon Health 概念的新主题。有关更多信息，请参阅 Amazon Health的概念。	2021 年 7 月 29 日
更新了 CloudWatch 活动文档	添加了有关如何为多个服务和事件类型的类别创建规则的部分。有关更多信息，请参阅为多种服务和类别创建规则。	2021 年 5 月 7 日
更新了 CloudWatch 活动文档	更新了本节以自动执行 Amazon Event CloudWatch s 规则的 Amazon Systems Manager 操作。有关更多信息，请参阅自动执行 Amazon EC2 实例的操作。	2021 年 4 月 28 日

更新了 CloudWatch 活动文档	添加了一个用于在聊天客户端中接收 Amazon Health 事件的部分。有关更多信息，请参阅在聊天应用程序中使用 Amazon Q Developer 接收 Amazon Health 事件。	2021 年 3 月 16 日
已更新的文档	更新了以下主题： • 更新了聚合 Amazon Health 事件主题 • 重组并更新了 “使用 Amazon Ev Amazon Health ents 监控 CloudWatch 事件” 主题 • 更新了基于资源和操作的条件部分	2021 年 1 月 29 日
在控制 Amazon Health 台中添加了用于组织视图的 Amazon Health 仪表板	您可以使用 Amazon Health 控制台启用组织视图功能。然后，您可以查看 Amazon 组织中成员账户的运行状况事件。	2020 年 12 月 14 日
高可用性端点演示	您可以使用示例代码来确定其有效的区域终端节点和签名 Amazon 区域 Amazon Health。	2020 年 10 月 22 日
更新了 Amazon Health 用户指南	组织更新并添加了 RSS 提要，以便您可以订阅 Amazon Health 文档的最新更新。	2020 年 8 月 28 日

早期更新

更改	描述	日期
更新了组织视图主题以包含示例。	请参阅 跨账号聚合 Amazon Health 事件。	2020 年 6 月 3 日
安全和 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 安全性 Amazon Health。	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 跨账号聚合 Amazon Health 事件。	2019 年 12 月 18 日
添加了新的 “基于资源和操作的条件” 部分，以解释 API 出售的事件限制。 Amazon Health	请参阅 对 Amazon Health进行身份和访问管理。	2018 年 8 月 2 日
服务发布。	Amazon Health 已发布。	2019 年 12 月 18 日

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。