aws

用户指南

AWS Health

AWS Health: 用户指南

Table of Contents

什么是 AWS Health？

AWS Health 持续监控资源性能以及 AWS 服务 和账户可用性。您可以通过 AWS Health 事件 了解服务和资源更改可能会对 AWS 上运行的应用程序产生的影响。AWS Health 会及时提供相关信息，帮助您管理正在进行的事件。另外，AWS Health 还可以帮助您了解和准备已计划活动。该服务会提供由 AWS 资源运行状况变化触发的报警和通知，因此您可以近乎即时地了解事件和获得指导，以帮助加快故障排除。

所有客户都可以使用由 AWS Health API 提供支持的 AWS Health 控制面板。控制面板无需设置，可随时供经过身份验证的 AWS 用户使用。有关服务重要功能的更多信息，请参阅 AWS Health 控制面板详细信息页面。

要了解 AWS Health 的基础知识和服务使用方法，请参阅 您是 AWS Health 新用户吗？。

有关使用 AWS Health 时需参考的术语列表，请参阅 AWS Health 的概念。

> **备注**
>
> - AWS Health 控制面板可供所有 AWS 客户使用，无需额外付费。
> - 所有 AWS 客户均可通过 Amazon EventBridge 免费接收 AWS Health 事件。
> - 如果拥有商业、Enterprise On-Ramp 或企业 Support 计划，您可以使用 AWS Health API 集成内部和第三方系统。有关详细信息，请参阅 AWS Health API 参考。
> - 有关可用 AWS Support 计划的更多信息，请参阅 AWS Support。

您是 AWS Health 新用户吗？

如果您是第一次使用 AWS Health 的用户，请从阅读以下部分开始：

- 什么是 AWS Health？ – 此部分介绍底层数据模型、它支持的操作，以及您可以用来与该服务交互的 AWS 开发工具包。
- AWS Health 的概念 – 了解有关 AWS Health 的基础知识和在您使用服务时会遇到的术语。
- 开始使用您的 AWS Health 控制面板 – 您的账户运行状况 – 学习如何查看事件和受影响的实体以及如何执行高级筛选。此控制面板包含特定于您的账户和组织的事件。
- AWS Health 控制面板-服务运行状况 – 如果您没有 AWS 账户，则可以查看与每个 AWS 区域 的 AWS 服务 运行状况和状态相关的信息。
- 使用 Amazon 监控 AWS Health 事件 EventBridge – 您可以使用 Amazon EventBridge 接收来自 AWS Health 的推送通知。
- 访问 AWS Health API – AWS Health API 部分介绍检索事件和实体相关信息的操作。

AWS Health 为所有客户提供名为 AWS Health 控制面板的控制台。您无需写入代码或执行任何操作，即可设置控制面板。

您可以设置 EventBridge 规则，以便在 Amazon EventBridge 上接收 AWS Health 事件。通过创建要执行操作的 Amazon EventBridge 规则，这提供了一种使用推送通知自动执行 AWS Health 事件管理的方法。

如果您拥有商业、Enterprise On-Ramp 或企业支持计划，则可以编程方式访问显示在控制面板上的信息。通过直接使用 REST API 或使用 AWS 开发工具包，您可以使用 AWS Command Line Interface (AWS CLI) 或写入代码来发出请求。

有关使用 Amazon EventBridge 上 AWS Health 事件的更多信息，请参阅 使用 Amazon 监控 AWS Health 事件 EventBridge。有关通过 AWS CLI 使用 AWS Health 的更多信息，请参阅 AWS Health 的 AWS CLI 参考。有关安装 AWS CLI 的说明，请参阅安装 AWS Command Line Interface。

AWS Health 的概念

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

主题

AWS Health 事件

AWS Health 事件，也称为运行状况事件，是 AWS Health 代表其他 AWS 服务发送的通知。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 AWS Identity and Access Management (IAM)计划弃用托管策略或 AWS Config 计划弃用托管规则，则 AWS Health 可以发送事件。AWS 区域 中存在服务可用性问题时，AWS Health 也可发送事件。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

特定于账户的事件是您的 AWS 账户 或 AWS 组织中某个账户的本地事件。例如，如果您使用的区域中存在与 Amazon Elastic Compute Cloud (Amazon EC2) 实例类型有关的问题，则 AWS Health 提供有关该事件和受影响资源名称的信息。

您可以从 AWS Health控制面板、AWS HealthAPI 中查找特定于账户的事件，也可以使用 Amazon CloudWatch Events 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，AWS 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 AWS Health 控制面板和 AWS Health 控制面板 – 服务运行状况中找到公有事件。

如果您拥有这一账户，请参阅开始使用您的 AWS Health 控制面板 – 您的账户运行状况。

如果您没有这一账户，请参阅AWS Health 控制面板-服务运行状况。

AWS Health 控制面板

如果您拥有 AWS 账户，您的 AWS Health 控制面板会同时显示 公有 事件和 特定于账户 的事件。

我们建议您使用 AWS Health 控制面板来了解可提供总体认识的事件，例如某个地区即将出现的服务维护问题。您还可以使用 AWS 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 AWS Management Console 来查看 AWS Health 控制面板，网址为 https://health.aws.amazon.com/health/home。

有关更多信息，请参阅 开始使用您的 AWS Health 控制面板 – 您的账户运行状况。

AWS Health 控制面板 – 服务运行状况

如果您没有账户，可以使用 https://health.aws.amazon.com/health/status 上的 AWS Health 控制面板 – 服务运行状况来查看公有事件。公有事件是报告的 AWS 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 AWS Health 控制面板-服务运行状况。

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。

我们建议您监控所有事件类型的类别。请注意，每个类别针对不同类型的事件显示。您也可以使用 DescribeEventTypes API 操作来查找事件类型的类别。

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 WorkSpaces 存在服务问题。

问题

这些事件是影响 AWS 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。这些事件包括计划生命周期事件，例如不同版本的支持结束通知和自动升级。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_SYSTEM_REBOOT_MAINTENANCE_SCHEDULED` – Amazon EC2 实例需要重启。
- `AWS_SAGEMAKER_SCHEDULED_MAINTENANCE` – SageMaker 需要维护事件，例如修复服务问题。
- `AWS_RDS_PLANNED_LIFECYCLE_EVENT` – Amazon RDS 正在安排计划生命周期事件，例如其中一个版本的支持结束事件，该事件需要客户采取措施。

> **Tip**
>
> 如果您使用 AWS Health API 或 AWS Command Line Interface (AWS 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。有关详细信息，请参阅 AWS 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AWS Health控制面板或 AWS Health API 中查看最长 90 天的运行状况事件。

受影响的实体

受影响的实体是受事件影响的 AWS 资源。例如，如果您收到账户中使用的特定实例类型的 Amazon EC2 维护的计划事件，则可以使用运行状况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 EventBridge 上的 AWS Health 事件

您可以为自己的账户设置 Amazon EventBridge 规则，以便在账户收到相应的 AWS 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 使用 Amazon 监控 AWS Health 事件 EventBridge。

AWS Health API

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

- 获取有关可能影响您 AWS 服务和资源的事件的信息
- 启用或禁用 AWS 组织的组织视图功能。
- 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

有关详细信息，请参阅 AWS Health API 参考。

> **Note**
>
> 您必须拥有 AWS Support 的商业、Enterprise On-Ramp 或企业 Support 计划才能使用 AWS Health API。如果您使用没有商业、Enterprise On-Ramp 或企业 Support 计划的账户调用 AWS Health API，则会收到 `SubscriptionRequiredException` 错误。

组织视图

您可以使用此功能将您 AWS Organizations 中 AWS 账户的所有运行状况事件汇总到 AWS 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 AWS Health API 查看可能影响不同账户和资源的所有事件。您可以从 AWS Health 控制台或 API 启用此功能。有关更多信息，请参阅 使用组织视图跨账户聚合 AWS Health 事件。

AWS Health 控制面板-服务运行状况

您可以使用 AWS Health 控制面板-服务运行状况来查看所有人的运行状况 AWS 服务。此页面显示了 AWS 区域 中各服务报告的服务事件。您无需登录或拥有即可 AWS 账户 访问 AWS 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 AWS 账户. 如果您已经有一个帐户，我们建议您登录以查看 AWS 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，请参阅开始使用您的 AWS Health 控制面板 – 您的账户运行状况。

查看 AWS Health 控制面板-服务运行状况

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

   > **Note**
   >
   > 如果您已经登录到您的页面 AWS 账户，您将被重定向到AWS 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，例如信息或降级
   - 最近更新的事件时间表
   - 也受 AWS 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。

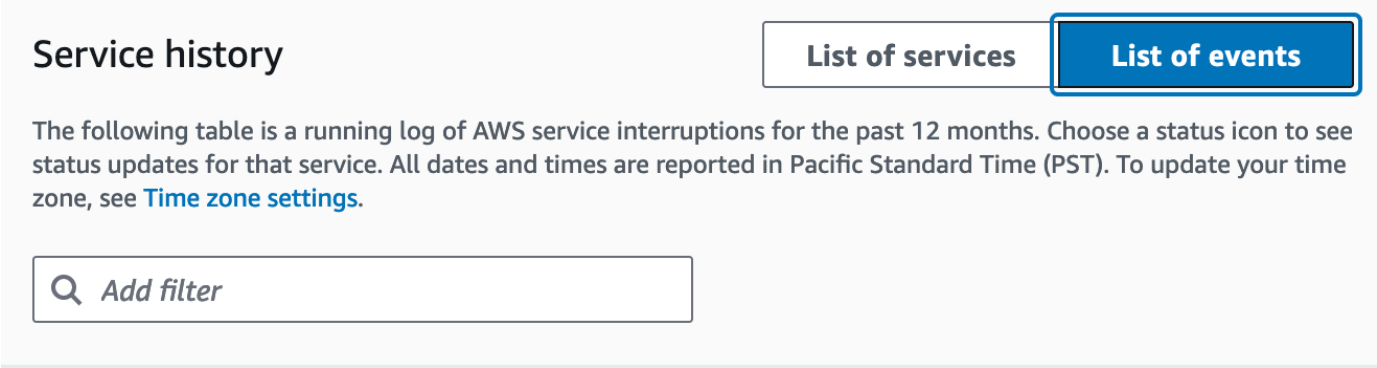
3. （可选）在事件旁边，选择 RSS 以订阅该事件的 RSS 源。您将在指定中收到有关此特定服务的通知 AWS 区域。

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 AWS 服务 中断情况。

> **Tip**
>
> 您可以按服务、AWS 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列表，请选择事件列表按钮。在事件列中选择任何事件，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**
>
> 选择 2023 年 9 月之后的任何公共活动都将在浏览器的 URL 中填充指向该公共 AWS Health 活动的链接。选择此链接后，您将导航到带有该事件弹出窗口的事件列表视图。

7. （可选）选择 RSS 源，以订阅 RSS 源。您将收到指定 AWS 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 开始使用您的 AWS Health 控制面板 – 您的账户运行状况。

计划的生命周期事件 AWS Health

了解计划的生命周期事件 AWS Health。

主题

什么是已计划的生命周期事件？

AWS Health 传达可能影响应用程序可用性的重要更改。在 AWS 分担责任模式中， AWS 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。 AWS 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 AWS 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 AWS 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 AWS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 AWS 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 AWS 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 AWS 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，而不是处于 “待处理” 或 “已解决” 状态的资源的情况下，不会为资源分配任何状态。
> - AWS 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 AWS 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： AWS_{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。

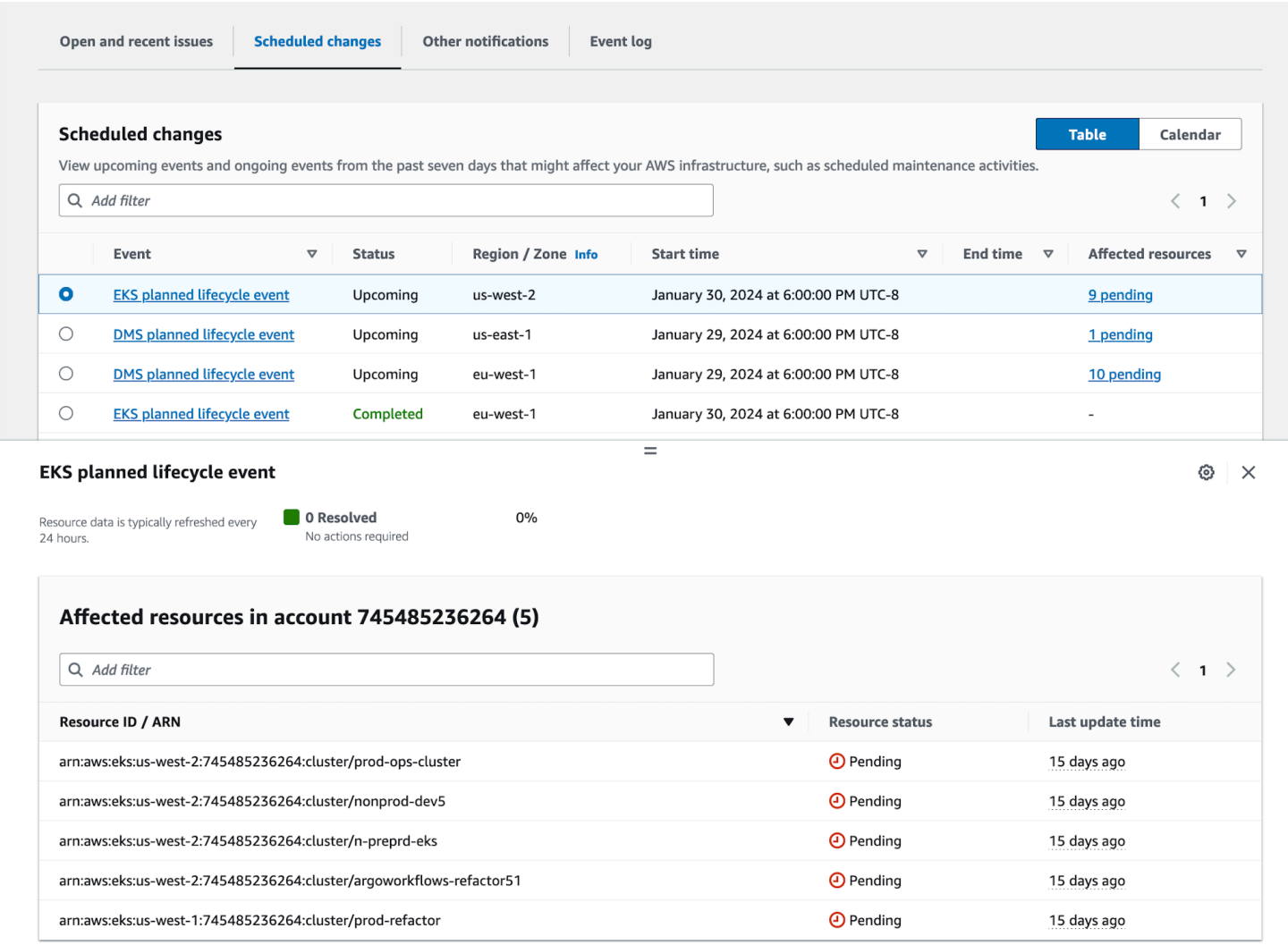
活动结束时间：事件结束时间是指所有 AWS 资源完成更改的日期。请注意，并不总是指定结束时间。将开始时间视为更改日期非常重要。

> **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，如果组织有大量受影响 AWS 账户 或资源，他们可能会收到多个 ARN。

提前了解计划生命周期事件：如果可能，将计划生命周期事件设计为主要版本/更改的最短准备时间为 180 天，次要版本/更改的最短准备时间为 90 天。

动态资源消耗和改进的元数据：从您收到通知到 AWS 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 AWS 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**
>
> - AWS Health 通知会尽可能提供一段时间内的状态更新，但 AWS 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。

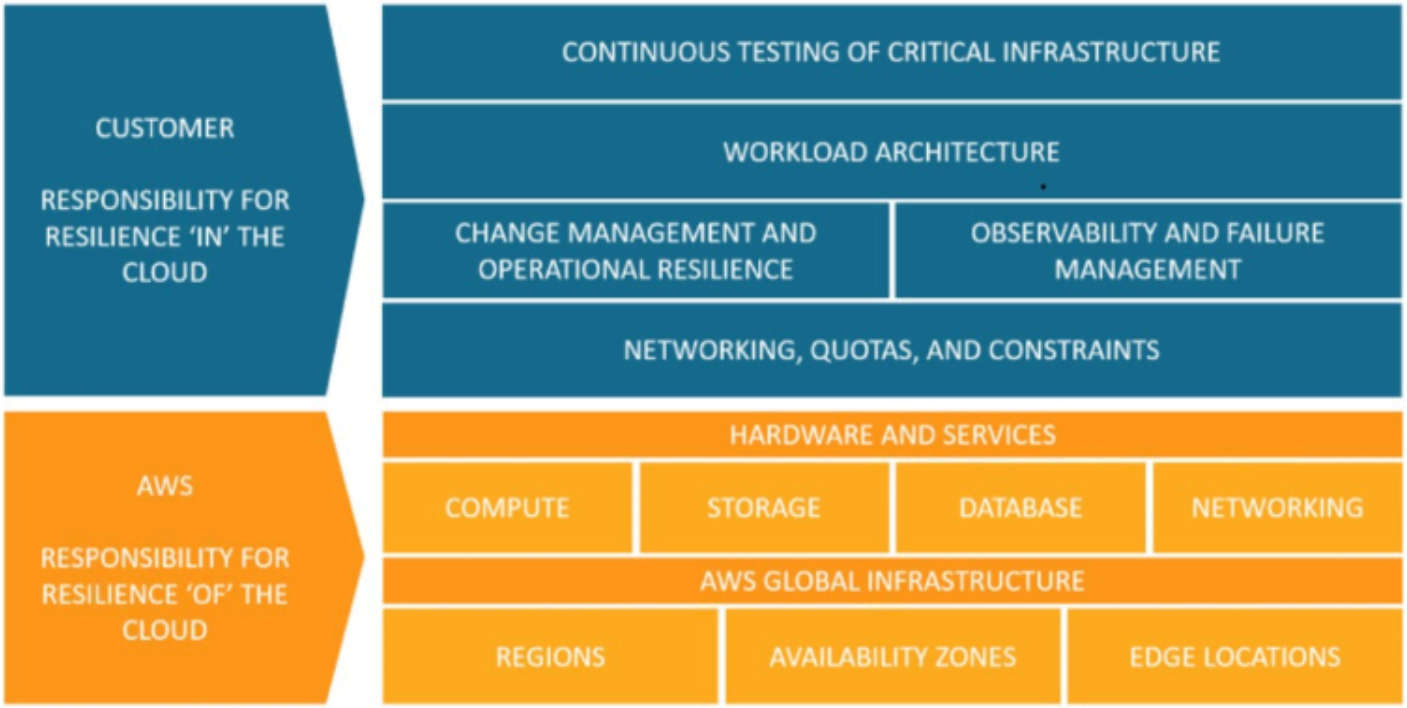


超出计划事件日期：

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. 如果在支持日期结束前解析所有资源，则 AWS Health 事件状态将更改为“Closed”（已关闭）。
3. 如果在该日期结束后仍存在未完成资源未得到解析，则 AWS 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 AWS 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 AWS 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 AWS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 AWS Health 控制面板
  - 日历视图
  - 受影响的资源视图
- 使用 AWS Health API

开始使用您的 AWS Health 控制面板 – 您的账户运行状况

您可以使用 AWS Health 控制面板来了解 AWS Health 事件。这些事件可能会影响您的 AWS 服务 或 AWS 账户。登录账户后，AWS 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 AWS 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 AWS 账户，则可以使用 AWS Health 控制面板-服务运行状况 来了解一般服务的可用性。
> 如果您有账户，我们建议您登录 AWS Health 控制面板，以更深入地了解可能影响您服务和资源的事件和即将发生的变化。

目录

- AWS Health 事件的报警

在 AWS 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。

要在 AWS Health 控制面板中查看账户事件

1. 打开您的 AWS Health 控制面板，网址为 https://health.aws.amazon.com/health/home。
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. 未解决的问题和最近的问题 – 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。

未解决的问题和最近的问题

使用未解决的问题和最近的问题选项卡，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。

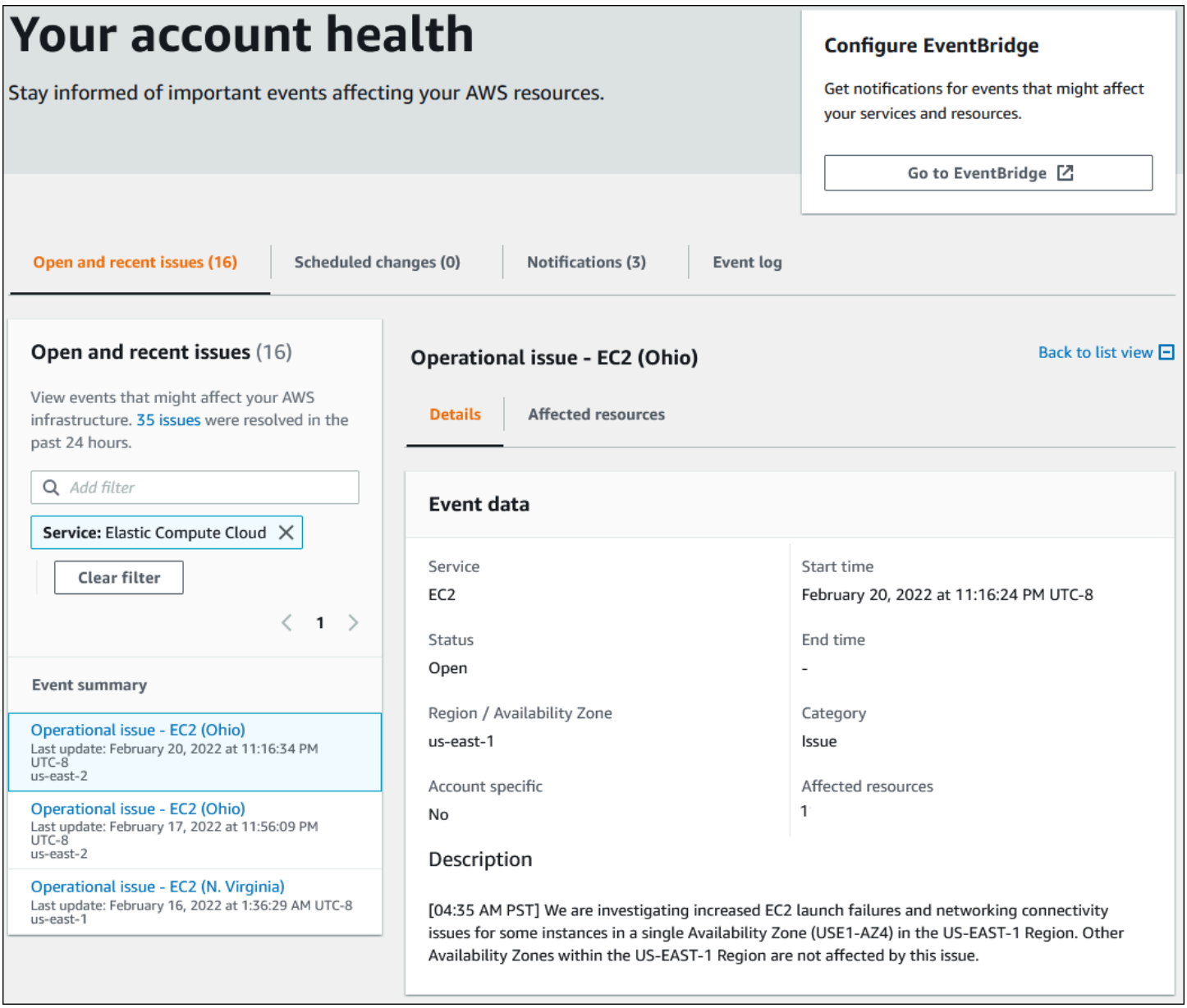
通过从筛选条件列表选择选项，您可以筛选在任何选项卡中显示的事件。例如，您可以按可用区、区域、事件结束时间或上次更新时间、AWS 服务 等条件缩小结果范围。

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 AWS Health 控制面板中显示的事件的通知。待 AWS 服务 解决事件后，通知自会从控制面板视图中删除。

Example : Amazon Elastic Compute Cloud (Amazon EC2) 的操作问题事件

下图显示了 Amazon EC2 实例的启动失败和连接问题事件。



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 计划的生命周期事件 AWS Health。

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 AWS 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。

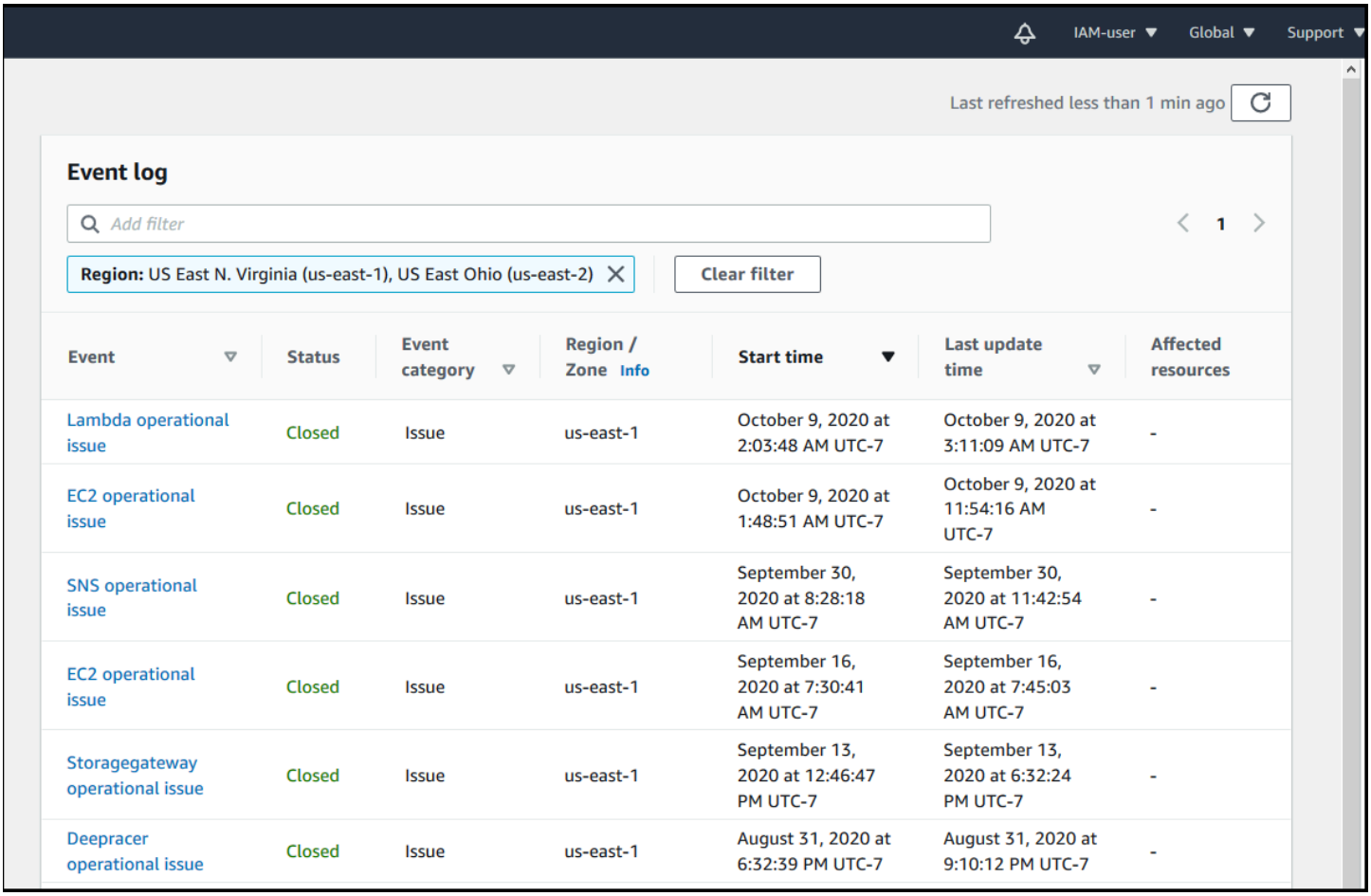
在事件日志表中选择事件时，系统会显示详细信息窗格，其中包含事件和受影响资源列表的相关信息。有关更多信息，请参阅 事件详细信息。

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

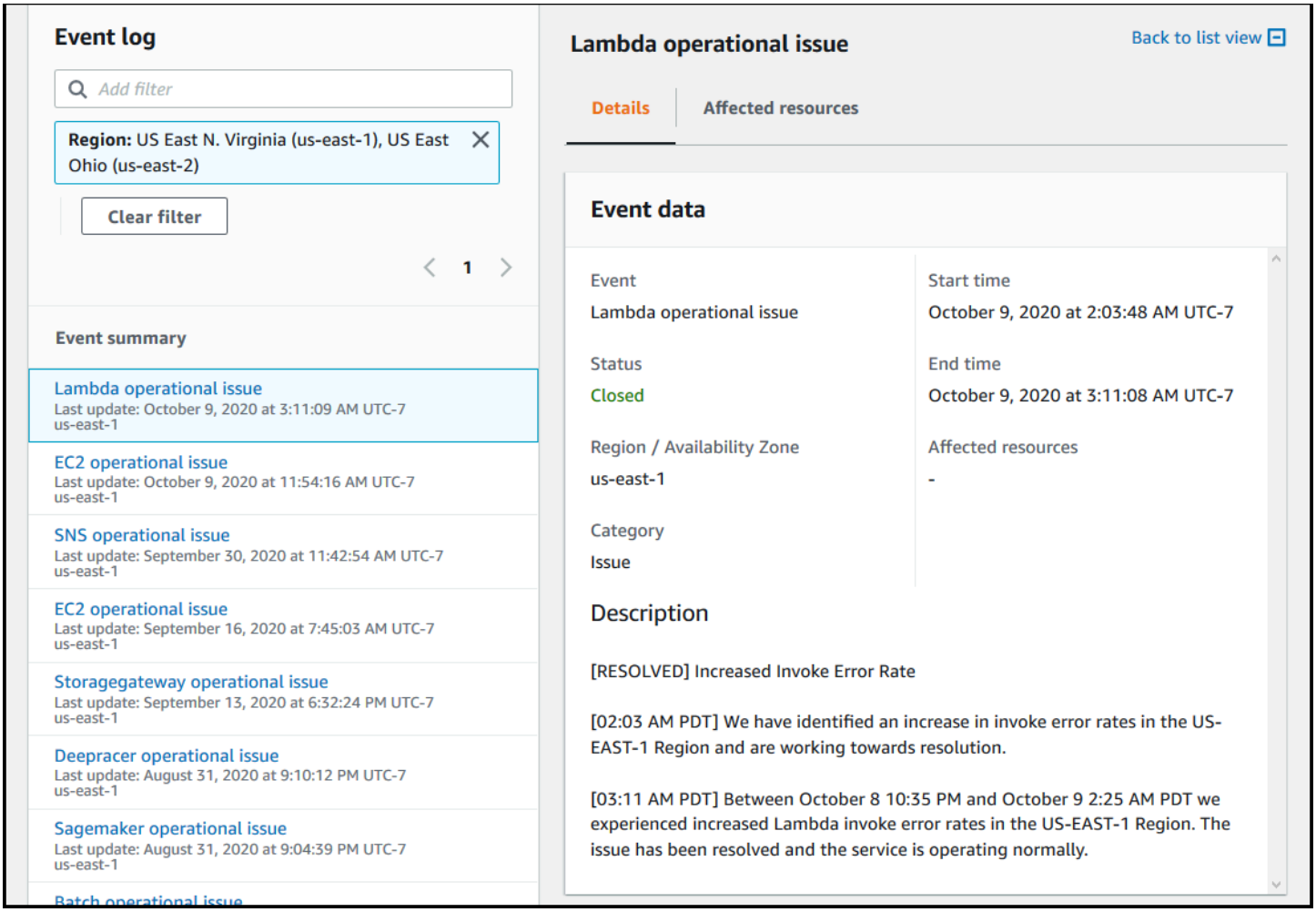
受影响的资源选项卡会显示受事件影响的任何 AWS 资源的相关信息：

- 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：用于 AWS Lambda 的 AWS Health 事件

以下屏幕截图显示 Lambda 的一个示例事件。



事件类型

有两种 AWS Health 事件类型：

- 公有事件是不特定于账户的服务事件。例如，如果某 AWS 区域 中存在与 Amazon EC2 有关的问题，则 AWS Health 提供有关事件的信息，即使您不使用该区域中的服务或资源也是如此。
- 特定于账户的事件特定于您的账户或您组织中的账户。例如，如果您使用的区域中存在与 Amazon EC2 实例有关的问题，则 AWS Health 提供有关该事件和受影响 Amazon EC2 实例列表的信息。

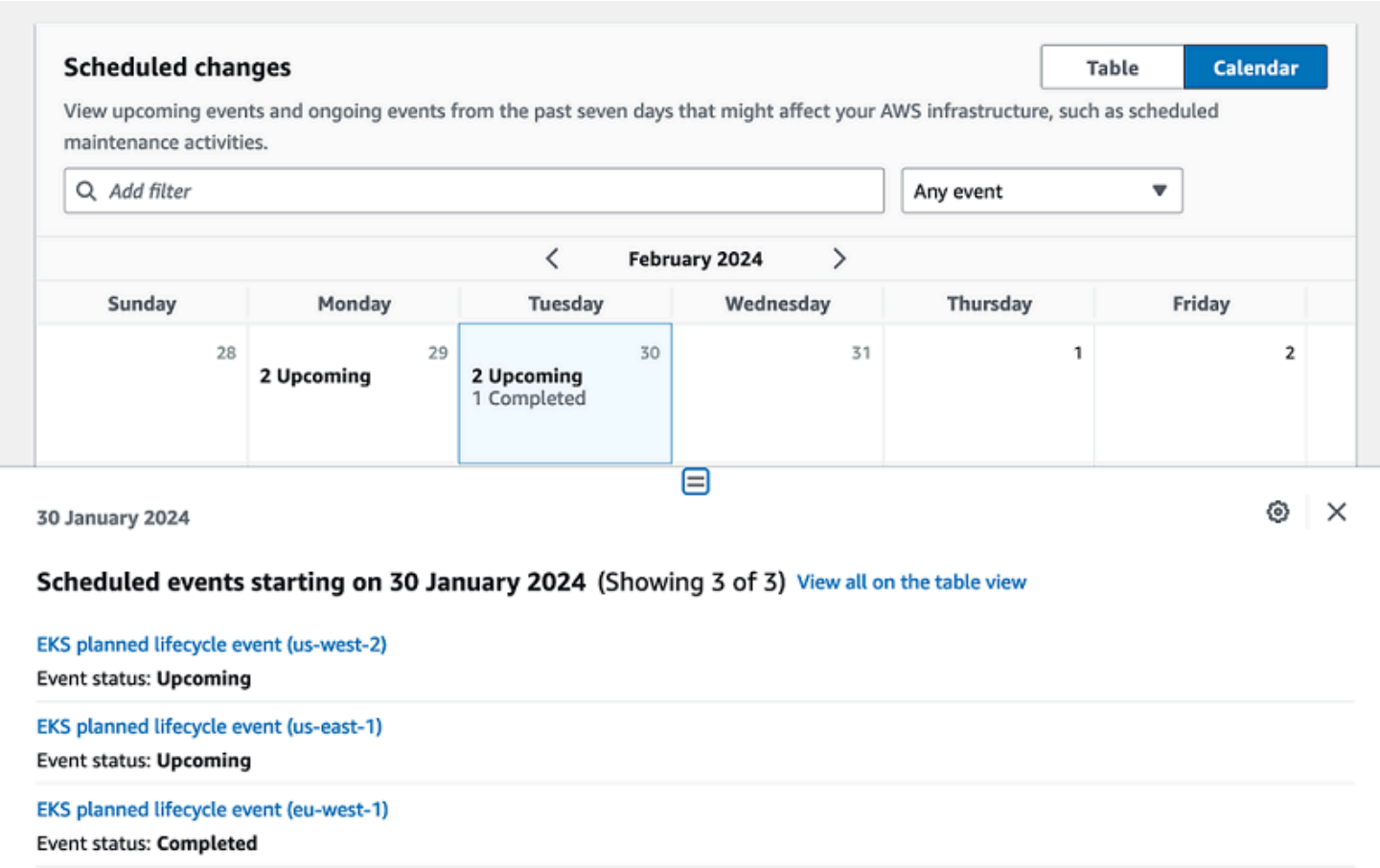
使用以下选项确定事件是公有事件还是特定于账户的事件：

- 在 AWS Health 控制面板中，选择事件的受影响资源选项卡。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 开始使用您的 AWS Health 控制面板 – 您的账户运行状况。
- 使用 AWS 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 AWS HealthAPI 参考中的 DescribeEventDetails 操作。

日历视图

日历视图在已计划的更改选项卡中可用，用于将 AWS 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。

AWS Health 事件按日期显示。选择一个日期以显示侧面板，其中包含 AWS Health 事件的更多详细信息。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 AWS 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。

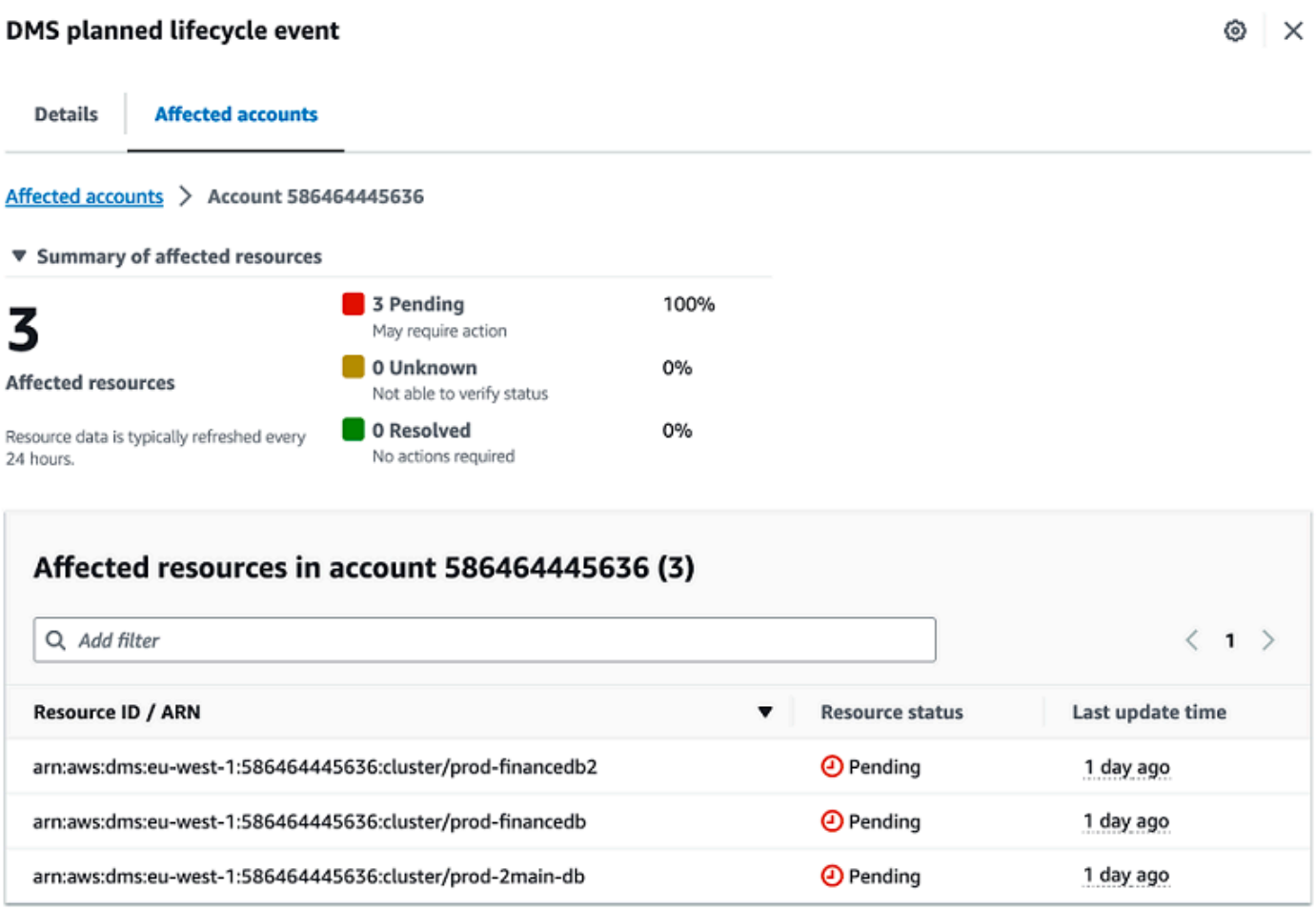


受影响的资源视图

对于已计划的生命周期事件，AWS Health 事件通常提供受影响资源状态的每日更新。要查看状态，请选择 AWS Health 事件。状态显示在侧面板的受影响资源选项卡中。

账户级别 AWS 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 计划的生命周期事件 AWS Health。

如果访问组织视图，则 AWS 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。



时区设置

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

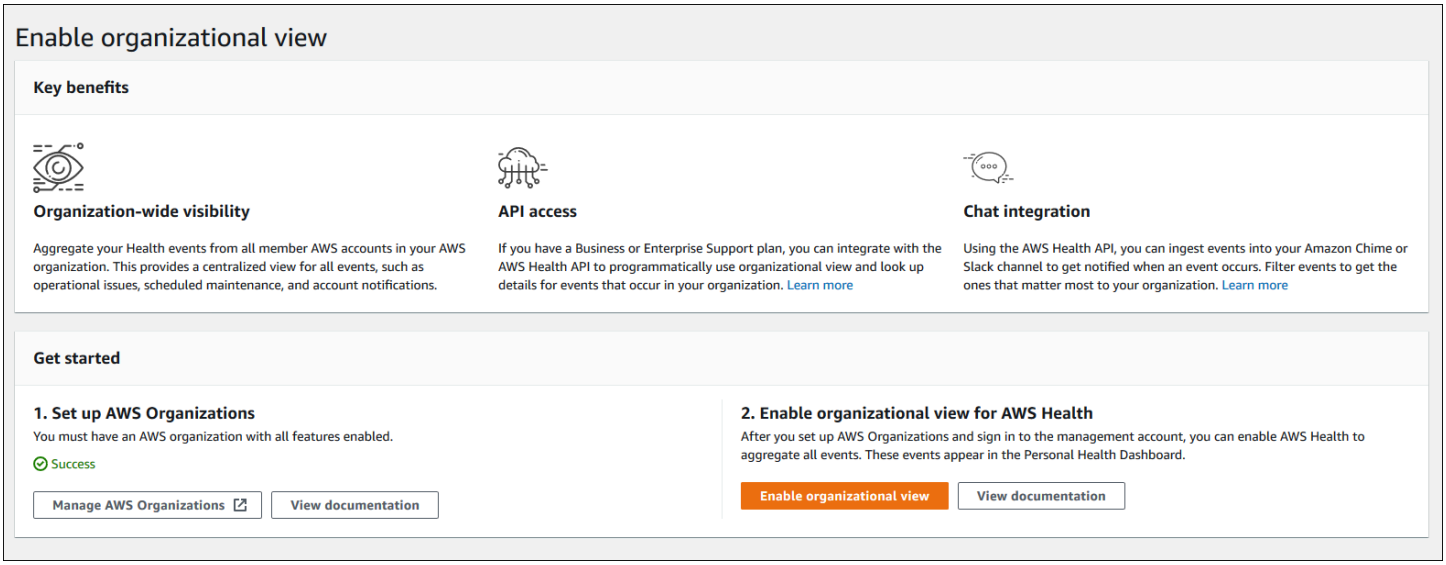
要更新您的时区设置

1. 打开您的 AWS Health 控制面板，网址为 https://health.aws.amazon.com/health/home。
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 AWS Health 控制面板的导航窗格中，选择时区设置。
5. 为您的 AWS 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

AWS Health 与 AWS Organizations 集成，因此您可以查看属于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 使用组织视图跨账户聚合 AWS Health 事件。



配置 Amazon EventBridge

使用 EventBridge 检测和响应 AWS Health 事件的更改。您可以监控账户中发生的特定 AWS Health 事件，然后设置规则，以便在事件发生变化时收到 AWS Health 通知或采取措施。

将 EventBridge 与 AWS Health 结合使用

1. 打开您的 AWS Health 控制面板，网址为 https://health.aws.amazon.com/health/home。
2. 要导航到 EventBridge 控制台创建规则，请执行以下操作之一：
   - 在导航窗格的运行状况集成下，选择 Amazon EventBridge。
   - 在配置 EventBridge 下，选择转到 EventBridge。
3. 按照该步骤为事件创建规则和监控。请参阅使用 Amazon 监控 AWS Health 事件 EventBridge。

AWS Health Aware

您可以开始使用 AWS Health API，借助 AWS Health Aware 这一低成本的应用程序，可向 Slack、JIRA、ServiceNow 等发送运行状况事件。网络研讨会直播现已免费提供。

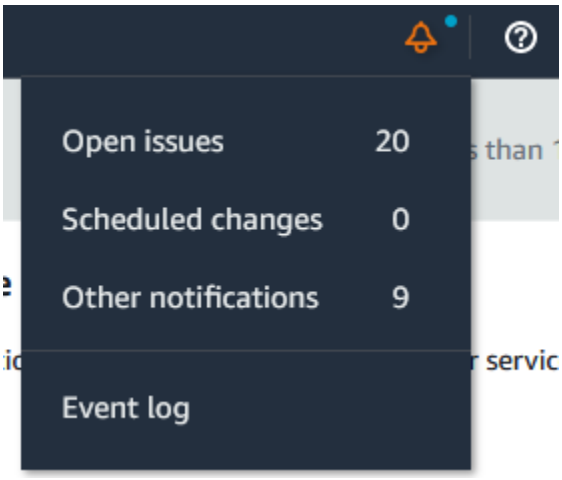
AWS Health 事件的报警

AWS Health 控制面板在控制台导航栏中有一个带报警菜单的铃铛图标。此功能显示控制面板上每个类别中出现的最近 AWS Health 事件的数量。此铃铛图标在多个 AWS 控制面板上出现，例如 Amazon EC2、Amazon Relational Database Service (Amazon RDS)、AWS Identity and Access Management (IAM) 和 AWS Trusted Advisor。

选择铃铛图标，以查看最近的事件是否影响您的账户。然后，您可以选择要导航到 AWS Health 控制面板的事件以了解更多信息。

Example : 未决事件

下图显示了账户的打开和通知事件。



为 AWS Health 配置 AWS 用户通知

AWS Health 提供有关服务运营的信息，例如操作问题、计划维护和计划软件生命周期事件。为了全面了解 AWS Health 事件详情，例如受影响的资源 ID、当前状态（打开或关闭）和资源状态，最佳做法是使用 AWS Health 端点，例如 AWS Health API、Amazon EventBridge 中的 aws.health 源和 AWS Health 控制面板。这些端点提供有关可能影响工作负载的持续事件和变化的最详细的实时信息。

AWS用户通知通过其他 UX 通道（电子邮件、聊天或向 AWS Console Mobile Application 推送通知）通知您。AWS Health 事件通知包含的详细数据没有上面列出的端点那么多；但是，它们提供了一种简单而有效的方式，来通知利益相关者所出现的问题和发生的变化。当事件与规则中指定的值匹配时，用户通知会根据您创建的规则，来创建和发送用户通知。您可以选择发送通知的 UX 传递通道，并设置聚合以减少针对特定事件生成的通知数量。您还可以在控制台通知中心中查看通知。例如，如果您的 AWS 账户中有计划更新的资源，例如 Amazon Elastic Compute Cloud（Amazon EC2）实例，则可以接收聊天通知。

要了解有关设置 AWS 用户通知的更多信息，请参阅AWS 用户通知入门。

访问 AWS Health API

AWS Health 是一种 RESTful Web 服务，它使用 HTTPS 进行传输，并采用 JSON 作为消息序列化格式。您的应用程序代码可以直接向 AWS 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 AWS Health 操作和参数的更多信息，请参阅 AWS Health API 参考。

> **Note**
>
> 您必须拥有 AWS Support 的商业、Enterprise On-Ramp 或企业 Support 计划才能使用 AWS Health API。如果您使用没有商业、Enterprise On-Ramp 或企业 Support 计划的 AWS 账户调用 AWS Health API，则会收到 `SubscriptionRequiredException` 错误。

您可以使用 AWS SDK 封装 AWS Health REST API 调用，从而简化应用程序开发。您指定 AWS 证书后，这些库会处理您的身份验证和请求登录事宜。

AWS Health 还可以在 AWS Management Console 中提供 AWS Health 控制面板，您可以用来查看并搜索事件和受影响的实体。请参阅 开始使用您的 AWS Health 控制面板 – 您的账户运行状况。

端点

AWS HealthAPI 遵循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，AWS Health 提供了一个全局端点。您可以在全局端点上执行 DNS 查找，以确定主动端点和相应的签名 AWS 区域。这可以帮助您了解要在代码中使用哪个端点，以便您可以从 AWS Health 中获取最新信息。

当您向全局端点发出请求时，必须指定您对目标区域端点的 AWS 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 签署 AWS Health API 请求。

下表列出了默认配置。

描述	签名区域	端点	协议
Active	us-east-1	health.us-east-1.amazonaws.com	HTTPS

描述	签名区域	端点	协议
Passive	us-east-2	health.us-east-2.amazonaws.com	HTTPS
Global	us-east-1 **Note** 这是当前主动端点的签名区域。	global.health.amazonaws.com	HTTPS

要确定端点是否为主动端点，请在全局端点 CNAME 上进行 DNS 查找，然后从解析的名称中提取 AWS 区域。

Example : 在全局端点上查找 DNS

以下命令在 global.health.amazonaws.com 端点上完成 DNS 查找。然后，该命令返回 us-east-1 区域端点。此输出告诉您应该使用哪个 AWS Health 端点。

```
dig global.health.amazonaws.com | grep CNAME
global.health.amazonaws.com. 10 IN CNAME health.us-east-1.amazonaws.com
```

Tip

主动端点和被动端点都返回 AWS Health 数据。但是，最新 AWS 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。

使用高可用性端点演示

在以下代码示例中，AWS Health 使用针对全局端点的 DNS 查找来确定主动区域端点和签名区域。然后，如果主动端点发生变化，代码将重新启动工作流程。

主题

- 使用 Java 演示
- 使用 Python 演示

使用 Java 演示

先决条件

您必须安装 Gradle。

要使用 Java 示例

1. 从 GitHub 下载 AWS Health 高可用性端点演示。
2. 导航到演示项目 `high-availability-endpoint/java` 目录。
3. 在命令行窗口中，输入以下命令。

```
gradle build
```

4. 输入以下命令，以指定您的 AWS 凭证。

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

5. 输入以下命令，以运行演示。

```
gradle run
```

Example : AWS Health 事件输出

该代码示例返回您 AWS 账户中最近七天内的最新 AWS Health 事件。在以下示例中，输出包括 AWS Config 服务的 AWS Health 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,
AWS 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 AWS 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, AWS 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 AWS 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 AWS
 Support [1]. Additional sample queries to retrieve the relationship information
 for the resources listed above is provided in [2].

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

Java 资源

- 有关更多信息，请参阅 AWS SDK for Java API 参考中的 Interface HealthClient 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 GitHub 中的 dnsjava。

使用 Python 演示

先决条件

您必须安装 Python 3。

要使用 Python 示例

1. 从 GitHub 下载 AWS Health 高可用性端点演示。
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，以指定您的 AWS 凭证。

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

7. 输入以下命令，以运行演示。

```
python3 main.py
```

Example : AWS Health 事件输出

该代码示例返回您 AWS 账户中最近七天内的最新 AWS Health 事件。以下输出返回 AWS 安全通知的 AWS Health 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 AWS Federal Information Processing Standard
 (FIPS) endpoints across all AWS 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 AWS 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 AWS 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 AWS 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 AWS Security Blog, with a ‘TLS’ tag [1].
 If you need further guidance or assistance, please contact AWS Support [2] or your
 Technical Account Manager (TAM).
Additional information is below.\n\nHow can I identify clients that are connecting
 with TLS
1.0/1.1?\nFor customers using S3 [3], Cloudfront [4] or Application Load Balancer
 [5] you can use
your access logs to view the TLS connection information for these services, and
 identify client
connections that are not at TLS 1.2. If you are using the AWS 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 AWS [7] or our associated AWS 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 AWS FIPS endpoints? \nAll AWS services offer Transport Layer
 Security (TLS) 1.2 encrypted endpoints that can be used for all API calls. Some
 AWS 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 AWS 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 GitHub 上的源代码。

签署 AWS Health API 请求

当您使用 AWS SDK 或 AWS Command Line Interface (AWS CLI) 来向 AWS 发出请求时，这些工具会自动使用您在配置工具时指定的访问密钥为您签署请求。例如，如果您使用前面用于高可用性端点演示的 AWS SDK for Java，则无需亲自签署这些请求。

Java 代码示例

有关如何将 AWS Health API 与 AWS SDK for Java 一起使用的更多示例，请参阅此示例代码。

当您进行请求时，我们强烈建议您不要使用 AWS 根账户凭证定期访问 AWS Health。您可以使用 IAM 用户的凭证。有关更多信息，请参阅 IAM 用户指南中的隐藏您的 AWS 账户根用户访问密钥。

如果您不使用 AWS SDK 或 AWS CLI，则必须自行对请求签名。我们建议您使用 AWS Signature 版本 4。有关更多信息，请参阅 AWS 一般参考 中的签署 AWS API 请求。

AWS Health 中支持的操作

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

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

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

事件类型

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

事件

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

受影响的实体

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

聚合

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

AWS Organizations 和组织视图

DescribeEventsForOrganization

DescribeEventsForOrganization 返回有关满足指定筛选条件的整个 AWS Organizations 中的事件的摘要信息。

DescribeAffectedAccountsForOrganization

DescribeAffectedAccountsForOrganization 返回 AWS Organizations 中受提供事件影响的 AWS 账户的列表。

DescribeEventDetailsForOrganization

DescribeEventDetailsForOrganization 返回有关 AWS Organizations 中一个或多个账户的一个或多个指定事件的详细信息。

DescribeAffectedEntitiesForOrganization

DescribeAffectedEntitiesForOrganization 根据筛选条件返回组织中一个或多个账户受到一个或多个事件影响的实体列表。

EnableHealthServiceAccessForOrganization

EnableHealthServiceAccessFor 操作授予 AWS Health 服务代表客户与 AWS Organizations 进行交互的权限，并将服务相关角色应用于组织中的管理账户。

DisableHealthServiceAccessForOrganization

DisableHealthServiceAccessForOrganization 操作撤销 AWS Health 服务代表客户与 AWS Organizations 进行交互的权限。

DescribeHealthServiceStatusForOrganization

DescribeHealthServiceStatusForOrganization 操作提供有关允许或禁止 AWS Health 与您的组织一起工作的状态信息

有关使用这些操作的更多信息，请参阅 AWS Health API 参考。

适用于 AWS Health API 的 Java 代码示例

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

步骤 1：初始化凭证

需要有效凭证，才可以与 AWS Health API 进行通信。您可以使用与 AWS 账户关联的任何 IAM 用户的密钥对。

创建并初始化 AWSCredentials 实例：

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

步骤 2：初始化 AWS Health API 客户端

使用上一步中的初始化凭证对象来创建 AWS Health 客户端：

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

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

步骤 3：使用 AWS 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 AWS Health EventFilter model.
// Here is an example for Region us-east-1 events from the EC2 service.
filter.setServices(singletonList("EC2"));
filter.setRegions(singletonList("us-east-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("us-east-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:us-
east-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:us-
east-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:us-
east-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 AWS Health

云安全 AWS 是重中之重。作为 AWS 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 AWS 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 — AWS 负责保护在 AWS 云中运行 AWS 服务的基础架构。 AWS 还为您提供可以安全使用的服务。作为AWS 合规计划合规计划合规计划合的一部分，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 AWS Health，请参阅按合规计划划分的范围内的AWSAWS 服务按合规计划。
- 云端安全-您的责任由您使用的 AWS 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 AWS Health。以下主题向您介绍如何进行配置 AWS 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 AWS 服务来帮助您监控和保护您的 AWS Health 资源。

主题

- 中的数据保护 AWS Health
- 适用于 AWS Health的身份和访问管理
- 登录和监控 AWS Health
- 合规性验证 AWS Health
- 韧性在 AWS Health
- AWS Health中的基础设施安全性
- 中的配置和漏洞分析 AWS Health
- AWS Health的安全最佳实践

中的数据保护 AWS Health

分 AWS 担责任模型适用于中的数据保护 AWS Health。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础设施上的内容的控制。您还负责您所使用的 AWS 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。有关欧洲数据保护的信息，请参阅 AWS 安全性博客 上的 AWS 责任共担模式和 GDPR 博客文章。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS IAM Identity Center 或 AWS 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。我们还建议您通过以下方式保护数据：

- 对每个账户使用 multi-factor authentication（MFA）。
- 使用 SSL/TLS 与资源通信。 AWS 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 AWS CloudTrail。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 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 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-2 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 140-2 版》。

我们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 AWS Health 或 SDK 或以其他 AWS 服务 方式使用控制台 AWS CLI、API 或 AWS SDK 的情况。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 AWS 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 AWS 账户时）和静态数据（存储在 AWS 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。

AWS 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 AWS Health 的。

传输中加密

发送和发送的所有数据在传输过程中 AWS Health 都经过加密。

密钥管理

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

适用于 AWS Health的身份和访问管理

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 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 AWS Health 资源。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题

受众

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

服务用户-如果您使用 AWS 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 AWS 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 AWS Health中的特征，请参阅 对 AWS 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 AWS Health 资源，则可能拥有完全访问权限 AWS Health。您的工作是确定您的服务用户应访问哪些 AWS 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 AWS Health，请参阅如何 AWS 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 AWS Health的访问权限的详细信息。要查看您可以在 IAM 中使用的 AWS Health 基于身份的策略示例，请参阅。AWS 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 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份或通过担 AWS 账户根用户任 IAM 角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 AWS IAM Identity Center （IAM Identity Center）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。当您以联合身份登录时，您的管理员以前使用 IAM 角色设置了身份联合验证。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》中的如何登录到您 AWS 账户的。

如果您 AWS 以编程方式访问，则会 AWS 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 AWS 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 用户指南中的签署 AWS API 请求。

无论使用何种身份验证方法，您可能需要提供其他安全信息。例如， AWS 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《AWS IAM Identity Center 用户指南》中的 多重身份验证 和《IAM 用户指南》中的 在 AWS中使用多重身份验证（MFA）。

AWS 账户 root 用户

创建时 AWS 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 AWS 服务 和资源。此身份被称为 AWS 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 AWS 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，我们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使用场景定期轮换访问密钥。

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，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

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

IAM 角色

I AM 角色是您内部具有特定权限 AWS 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。您可以 AWS Management Console 通过切换角色在中临时担任 IAM 角色。您可以通过调用 AWS CLI 或 AWS 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 使用 IAM 角色。

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。有关联合身份验证的角色的信息，请参阅《IAM 用户指南》中的 为第三方身份提供商创建角色。如果您使用 IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的权限集。
- 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 AWS 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 角色与基于资源的策略有何不同。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 Amazon S3 中存储对象。服务可能会使用发出调用的主体的权限、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 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 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个操作的权限。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 AWS 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。 AWS 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 AWS 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 EC2 上运行的应用程序 — 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时证书。这优先于在 EC2 实例中存储访问密钥。要向 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建附加到该实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅《IAM 用户指南》中的 使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限。

要了解是使用 IAM 角色还是 IAM 用户，请参阅 IAM 用户指南中的何时创建 IAM 角色（而不是用户）。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。 AWS 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 AWS 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 AWS 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。然后，管理员可以向角色添加 IAM 策略，并且用户可以代入角色。

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 AWS Management Console AWS CLI、或 AWS 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》中的创建 IAM 策略。

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 AWS 账户。托管策略包括

AWS 托管策略和客户托管策略。要了解如何在托管式策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管式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 Simple Storage Service（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 AWS 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 AWS 托管策略。

AWS Health 支持基于资源的条件。您可以指定用户可以查看的 AWS Health 事件。例如，您可以创建一个策略，仅允许 IAM 用户访问 AWS Health Dashboard中的特定 Amazon EC2 事件。

有关更多信息，请参阅 资源。

访问控制列表

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

Amazon S3 和 Amazon VPC 就是支持 ACL 的服务示例。 AWS WAF要了解有关 ACL 的更多信息，请参阅 Amazon Simple Storage Service 开发人员指南 中的访问控制列表（ACL）概览。

AWS Health 不支持 ACL。

其它策略类型

AWS 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 (SCP)-SCP 是 JSON 策略，用于指定组织或组织单位 (OU) 的最大权限。 AWS Organizations AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果在组织内启用了所有特征，则可对任意或全部账户应用服务控制策略 (SCP)。SCP

限制成员账户中的实体（包括每个 AWS 账户根用户实体）的权限。有关 Organizations 和 SCP 的更多信息，请参阅 AWS Organizations 用户指南中的 SCP 的工作原理。

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

在使用 IAM 管理访问权限之前 AWS Health，您应该了解哪些可用的 IAM 功能 AWS Health。要全面了解如何 AWS Health 和其他 AWS 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AWS 服务。

主题

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

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

资源

管理员可以使用 AWS 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": "*"
```

AWS 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"
```

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

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

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

某些 AWS 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": "*"
```

AWS 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，请使用逗号分隔 ARN。

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

AWS 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 AWS Health 资源类型及其 ARN 的列表，请参阅 IAM 用户指南 AWS 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 AWS Health定义的操作。

条件键

管理员可以使用 AWS 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 AWS 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 AWS 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。

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

AWS 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 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 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 AWS Health 条件键列表，请参阅 IAM 用户指南 AWS 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 AWS Health。

示例

要查看 AWS Health 基于身份的策略的示例，请参阅。AWS Health 基于身份的策略示例

AWS 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 AWS Health 资源执行哪些操作。 AWS 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 AWS 服务访问您的 AWS 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 AWS 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。

AWS 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 AWS Health 事件执行操作。

示例

要查看 AWS 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 AWS Health 标签的授权

AWS Health 不支持标记资源或基于标签控制访问权限。

AWS Health IAM 角色

I AM 角色是您的 AWS 账户中具有特定权限的实体。

将临时证书与 AWS 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 AWS STS API 操作来获取临时安全证书GetFederationToken。

AWS Health 支持使用临时证书。

服务相关角色

服务相关角色允许 AWS 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。

AWS Health 支持与服务相关的角色进行集成。 AWS Organizations服务相关角色命名为 `AWSServiceRoleForHealth_Organizations`。该角色附带的是 Health_OrganizationsServiceRolePolicy AWS 托管策略。 AWS 托管策略 AWS Health 允许从组织中的其他 AWS 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 AWS Command Line Interface (AWS 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 使用组织视图跨账户聚合 AWS 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。

AWS Health 不支持服务角色。

AWS 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 AWS Health 资源的权限。他们也无法使用 AWS Management Console AWS CLI、或 AWS 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 AWS Health 资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下准则和建议：

- 开始使用 AWS 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AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 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 AWS 托管策略或工作职能的AWS 托管策略。
- 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 AWS 服务，例如 AWS 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 IAM Acess Analyzer 策略验证。

- 需要多重身份验证 (MFA)-如果 AWS 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 配置受 MFA 保护的 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 AWS Health 控制台

要访问 AWS 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 AWS 账户中 AWS 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 AWS Health 控制台，您可以附加以下 AWS 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 AWS Health 组织中的所有账户启用或禁用 AWS 组织视图功能
- AWS Health 控制台 AWS Health Dashboard 中的
- AWS Health API 操作和通知
- 查看有关属于您的 AWS 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 AWS 托管策略，以便 AWS 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 AWS Health。

对于仅调用 AWS CLI 或 AWS 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 AWS CLI 或 AWS 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 AWS Health Dashboard 和 AWS Health API

AWS Health Dashboard 适用于所有 AWS 账户。该 AWS 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 AWS Support。

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 AWS Health Dashboard 和 AWS Health API 的权限。

默认情况下，IAM 用户无权访问 AWS Health Dashboard 或 AWS 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 AWS 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 AWS Health 信息。有关更多信息，请参阅用户如何登录您的账户。

> **Note**
>
> AWS Health Dashboard 具有查看权限的 IAM 用户对账户中所有 AWS 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 AWS 资源 ID，例如 Amazon EC2 实例 ID、EC2 实例 IP 地址和一般安全通知。
> 例如，如果 IAM 策略仅授予对 AWS 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 AWS 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。 AWS Health Dashboard

您可以将两组 API 用于 AWS Health。

- 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 AWS 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 AWS Health 的事件的信息。

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

单个操作

您可以将 IAM policy 的 `Action` 元素设置为 `health:Describe*`。这允许访问 AWS Health Dashboard 和 AWS Health。 AWS Health 支持基于`eventTypeCode`和服务对事件的访问控制。

描述访问权限

本政策声明授予访问 AWS Health Dashboard 和任何 `Describe*` AWS Health API 操作的权限。例如，具有此策略的 IAM 用户可以访问 AWS Health Dashboard 中的 AWS Management Console 并调用 AWS 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 AWS Health Dashboard 和 AWS Health API。拥有此策略的 IAM 用户无法 AWS Health Dashboard 在中查看 ， AWS Management Console 也无法调用任何 AWS 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 AWS Health，则必须允许访问 AWS Health 和 AWS 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 API 所需的确切权限，请参阅 IAM 用户指南中的由 AWS Health API 定义的操作和通知。

> **Note**
>
> 您必须使用管理账户中的凭证才能访问组织的 AWS Health API AWS Organizations。有关更多信息，请参阅 使用组织视图跨账户聚合 AWS Health 事件。

允许访问 AWS 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 AWS Health 和 AWS Organizations 操作的权限。

Example：允许访问 AWS 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 AWS Health 组织视图

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

Example : 拒绝访问 AWS 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 AWS Health特定于该策略的策略声明。

基于资源和基于操作的条件

AWS 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 AWS 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 AWS Health 事件字段的访问权限。

在策略中指定 AWS Health 事件时，可以使用以下字段：

- `eventTypeCode`
- `service`

注意事项

- 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 AWS 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 AWS Health API 和通知的操作、资源和条件密钥。

Example ：基于操作的条件

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

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

Example ：基于资源的条件

以下策略具有相同的效果，但使用 Resource 元素。

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

Example : eventTypeCode 状况

此政策声明授予访问 AWS Health Dashboard 和 AWS Health Describe* API 操作的权限，但拒绝访问任何与之匹配 AWS 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 AWS Health 事件，则会出现AccessDeniedException错误。有关更多信息，请参阅 对 AWS Health 身份和访问进行故障排除。

对 AWS 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 AWS Health 和 IAM 时可能遇到的常见问题。

主题

- 我无权在中执行操作 AWS 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 AWS Health
- 我想允许 AWS 账户之外的人访问我的 AWS Health 资源

我无权在中执行操作 AWS Health

如果 AWS 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 AWS Health Dashboard 或 AWS 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。

AWS Health API 需要来自AWS Support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 AWS 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 AWS Health。

有些 AWS 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 AWS 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 AWS 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 AWS 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 AWS Health

要允许其他人访问 AWS Health，您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）。它们将使用该实体的凭证访问 AWS。然后，您必须将策略附加到实体，以便在 AWS Health中向其授予正确的权限。

要立即开始使用，请参阅《IAM 用户指南》中的创建您的第一个 IAM 委派用户和组。

我想允许 AWS 账户之外的人访问我的 AWS 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，可以担任角色。对于支持基于资源的策略或访问控制列表（ACL）的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解是否 AWS Health 支持这些功能，请参阅如何 AWS 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 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 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 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户
- 要了解如何通过联合身份验证提供访问权限，请参阅 IAM 用户指南中的为经过外部身份验证的用户（联合身份验证）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存取之间的差别，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。

将服务相关角色用于 AWS Health

AWS Health 使用 AWS 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。 AWS Health服务相关角色由 AWS Health 预定义，并包含相关服务为您调用其他 AWS 服务 所需的所有权限。

您可以使用服务相关角色进行设置， AWS Health 以避免手动添加必要的权限。 AWS Health 定义其服务相关角色的权限，除非另有定义，否则 AWS 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。

AWS Health的服务相关角色权限

AWS Health 有两个与服务相关的角色：

- AWSServiceRoleForHealth_Organizations— 此角色信任 AWS Health (health.amazonaws.com) 代替您访问 AWS 服务 的角色。附属于此角色的是Health_OrganizationsServiceRolePolicy AWS 托管策略。
- AWSServiceRoleForHealth_EventProcessor— 此角色信任 AWS 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 AWS 托管策略。服务主体使用该角色为 AWS 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 AWS 账户 到您的账户所需的基础架构 AWS Health。

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

为 AWS Health创建服务相关角色

您无需创建 AWSServiceRoleForHealth_Organizations 服务相关角色。当您调用EnableHealthServiceAccessForOrganization操作时， AWS Health 会在账户中为您创建此服务相关角色。

您必须在账户中手动创建 AWSServiceRoleForHealth_EventProcessor 服务相关角色。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 AWS Health编辑服务相关角色

AWS 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 AWS Health的服务相关角色

要删除该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 AWS Command Line Interface (AWS CLI) 删除该角色。

要删除该AWSServiceRoleForHealth_EventProcessor角色，请联系 AWS Support 并要求他们将您的工作负载从 AWS 事件检测和响应中移除。完成此过程后，您可以通过 IAM 控制台、IAM API 或其他 AWS 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。

AWS 的托管策略 AWS Health

AWS 托管策略是由创建和管理的独立策略 AWS。 AWS 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， AWS 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 AWS 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 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 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）。 AWS 最有可能在启动新的 API 或现有服务可以使用新 AWS 服务 的 API 操作时更新 AWS 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略。

AWS Health 具有以下托管策略。

目录

AWS 托管式策略：AWSHealth_EventProcessorServiceRolePolicy

AWS Health 使用AWSHealth_EventProcessorServiceRolePolicy AWS 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 AWS Health。

托管策略具有以下权限， AWS Health 允许访问 AWS 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 AWS HealthAWS 托管策略的更新。

AWS 托管式策略：Health_OrganizationsServiceRolePolicy

AWS Health 使用Health_OrganizationsServiceRolePolicy AWS 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 AWS Health。

此策略授予的权限 AWS Health 允许访问 Health Organization 视图所需的 AWS 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 AWS Organizations 以及可以与 Organ AWS 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 AWS HealthAWS 托管策略的更新。

AWS 托管式策略：AWSHealthFullAccess

AWS Health 使用AWSHealthFullAccess AWS 托管策略。该策略授予实体（IAM 用户或角色）访问 AWS Health 控制台的权限。有关更多信息，请参阅 使用 AWS 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 AWS Health 组织中所有账户的 AWS 组织视图功能，并查看管理账户的组织单位 (OU)
- `health`— 访问 AWS Health API 操作和通知
- `iam`— 创建与 AWS Health 服务关联的 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 AWS HealthAWS 托管策略的更新。

AWS HealthAWS 托管策略的更新

查看 AWS Health 自该服务开始跟踪这些更改以来 AWS 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 AWS Health 页面上的 RSS 源。

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

AWS Health

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

登录和监控 AWS Health

监控是维护和其他 AWS 解决方案的可靠性、可用性和性能的重要组成部分。 AWS Health AWS 提供以下监控工具 AWS 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 AWS 资源和您运行 AWS 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 AWS 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，监视某些事件，并在这些事件发生时在其他 AWS 服务中触发自动操作。有关更多信息，请参阅 使用 Amazon 监控 AWS Health 事件 EventBridge。
- AWS CloudTrail捕获由您的账户或代表您的 AWS 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账户拨打了电话 AWS、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《AWS CloudTrail 用户指南》。

有关更多信息，请参阅 监控 AWS Health。

合规性验证 AWS Health

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

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

您在使用 AWS 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。 AWS 提供了以下资源来帮助实现合规性：

- 安全与合规性快速入门指南 — 这些部署指南讨论了架构注意事项，并提供了在这些基础上 AWS 部署以安全性和合规性为重点的基准环境的步骤。
- 在 A@@ mazon Web Services 上构建 HIPAA 安全与合规架构 — 本白皮书描述了各公司如何使用 AWS 来创建符合 HIPAA 资格的应用程序。

> **Note**
>
> 并非所有 AWS 服务 人都符合 HIPAA 资格。有关更多信息，请参阅符合 HIPAA 要求的服务参考。

- AWS 合规资源AWS — 此工作簿和指南集可能适用于您所在的行业和所在地区。
- AWS 客户合规指南 — 从合规角度了解责任共担模式。这些指南总结了保护的最佳实践， AWS 服务并将指南映射到跨多个框架（包括美国国家标准与技术研究院 (NIST)、支付卡行业安全标准委员会 (PCI) 和国际标准化组织 (ISO)）的安全控制。
- 使用AWS Config 开发人员指南中的规则评估资源 — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- AWS Security Hub— 这 AWS 服务 可以全面了解您的安全状态 AWS。Security Hub 通过安全控件评估您的 AWS 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件的列表，请参阅 Security Hub 控件参考。
- AWS Audit Manager— 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

韧性在 AWS Health

AWS 全球基础设施是围绕 AWS 区域和可用区构建的。 AWS 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设施相比，可用区具有更高的可用性、容错性和可扩展性。

AWS 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 AWS Health Dashboard 或 AWS Health API 操作访问它们。您可以在 AWS Health 事件发生后的 90 天内查看事件。

有关 AWS 区域和可用区的更多信息，请参阅AWS 全球基础设施。

AWS Health中的基础设施安全性

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

您可以使用 AWS 已发布的 API 调用 AWS 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 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service（AWS 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 AWS Health

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

AWS Health的安全最佳实践

请参阅以下使用的最佳实践 AWS Health。

向 AWS 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 AWS Identity and Access Management (IAM) 用户访问 AWS Health Dashboard。但是，您可能不允许同一用户启用或禁用对 AWS Organizations的访问。

有关更多信息，请参阅 AWS Health 基于身份的策略示例。

查看 AWS Health Dashboard

AWS 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，您可能会收到有关资源的事件通知，如需要更新的 Amazon Elastic Compute Cloud (Amazon EC2) 实例。

有关更多信息，请参阅 开始使用您的 AWS Health 控制面板 – 您的账户运行状况。

AWS Health 与 Amazon Chime 或 Slack 集成

您可以 AWS 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 AWS Health 事件的通知。有关更多信息，请参阅中的AWS Health 工具 GitHub。

监控 AWS Health 事件

您可以 AWS 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 AWS 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 使用 Amazon 监控 AWS Health 事件 EventBridge。

使用组织视图跨账户聚合 AWS Health 事件

默认情况下，您可以使用 AWS Health 查看单个 AWS 账户的 AWS Health 事件。如果您使用 AWS Organizations，也可以在组织中集中查看 AWS Health 事件。使用此功能可以访问与单个账户操作相同的信息。您可以使用筛选条件查看特定 AWS 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。使用此功能可随时了解即将发生的 AWS 服务更改，这些更改可能需要您更新或更改代码。

最佳做法是使用委派管理员功能，将对 AWS Health 组织视图的访问权限委派给成员账户。这样，运营团队便可更轻松地访问组织中的 AWS 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 AWS Health 事件采取行动所需的可见性。

Important

- AWS Health 不会记录您启用组织视图之前组织中发生的事件。例如，如果您组织中的一个成员账户 (111122223333) 在您启用该功能之前收到了 Amazon Elastic Compute Cloud (Amazon EC2) 的事件，则该事件将不会在您的组织视图中出现。
- 一旦事件可用，为组织中的账户发送的 AWS Health 事件就会在组织视图中显示，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，然后会将其删除。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 AWS 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 用户指南中的隐藏您的 AWS 账户根用户访问密钥。
- 如果您以 IAM 用户身份登录，请使用将访问权限授予 AWS Health 和 Organizations 操作的 IAM policy，例如 AWSHealthFullAccess 策略。有关更多信息，请参阅 AWS Health 基于身份的策略示例。

主题

组织视图（控制台）

您可以使用 AWS Health 控制台集中查看您 AWS 组织中的运行状况事件。

所有 AWS Support 计划的组织视图均可在 AWS Health 控制台中进行查看，无需支付额外费用。

> **Note**
>
> 如果允许用户访问管理账户中的此功能，则他们必须拥有诸如 AWSHealthFullAccess 策略之类的权限。有关更多信息，请参阅 AWS Health 基于身份的策略示例。

目录

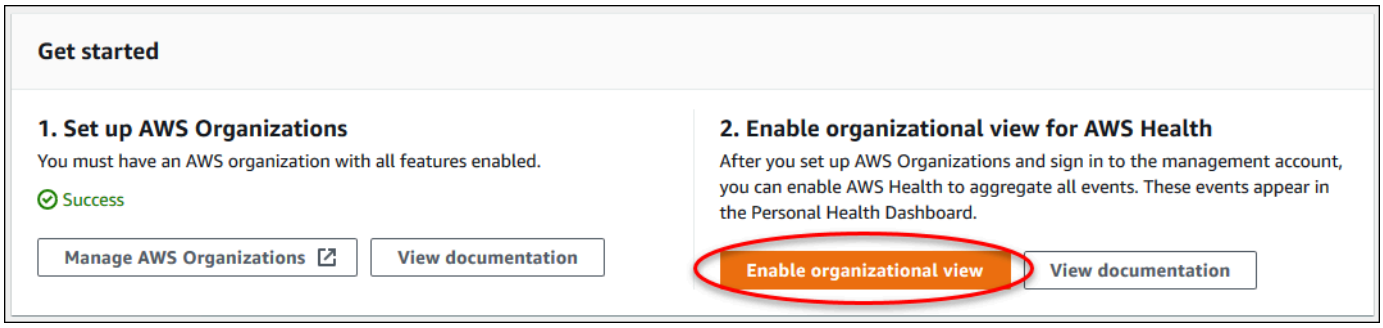
启用组织视图（控制台）

您可以从 AWS Health 控制台启用组织视图。您必须登录 AWS 组织的管理账户。

要查看您组织的 AWS Health 控制面板

1. 打开您的 AWS Health 控制面板，网址为 https://health.aws.amazon.com/health/home。
2. 在导航窗格的您的组织运行状况下，选择Configurations（配置）。

3. 在启用组织视图页面上，选择Enable organizational view（启用组织视图）。



4. （可选）如果要对 AWS 组织进行更改，例如创建组织单位 (OU)，请选择管理AWS Organizations。

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

> **注意**
>
> - 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。您可以离开，并在稍后检查 AWS Health 控制台。
> - 如果您拥有商业、Enterprise On-Ramp 或企业 Support 计划，则可以调用 DescribeHealthServiceStatusForOrganization API 操作来检查流程的状态。
> - 启用此功能时，`AWSServiceRoleForHealth_Organizations`服务相关角色和`Health_OrganizationsServiceRolePolicy` AWS 托管策略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 AWS Health。

查看组织视图事件（控制台）

禁用组织视图功能后，AWS Health 会显示您组织中所有账户的运行状况事件。

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

AWS 将在管理员账户关闭生效之日起 90 天内保留该账户的策略数据。在 90 天期限结束时，AWS 会永久删除该账户的所有策略数据。

- 要将结果保留 90 天以上，您可以将策略存档。您还可以使用采用 Eventbridge 规则的自定义操作将结果存储到 S3 存储桶中。

- 只要 AWS 保留策略数据，当您重新打开关闭的账户时，AWS 就会将该账户重新分配为服务管理员并恢复该账户的服务策略数据。
- 有关更多信息，请参阅关闭账户。

> **Important**
>
> 对于 AWS GovCloud (US) 区域的客户：
>
> - 在关闭账户前，备份并删除账户资源。关闭账户后，您将不再拥有其访问权限。

> **Note**
>
> 启用此功能后，AWS Health 控制台可以显示过去 7 天 AWS Health 控制面板 – 服务运行状况中的公有事件。这些公有事件不是特定于您组织中的账户。AWS Health控制面板 – 服务运行状况事件会提供有关 AWS 服务的区域可用性的公有信息。

您可以在以下页面中查看组织视图事件：

主题

- 未解决的问题和最近的问题
- 已计划的更改
- 其他通知
- 事件日志

未解决的问题和最近的问题

您可以使用未决问题和近期问题选项卡，查看可能影响您 AWS 基础架构的事件，例如影响您组织的 AWS 服务 和资源更改。

要查看组织视图事件

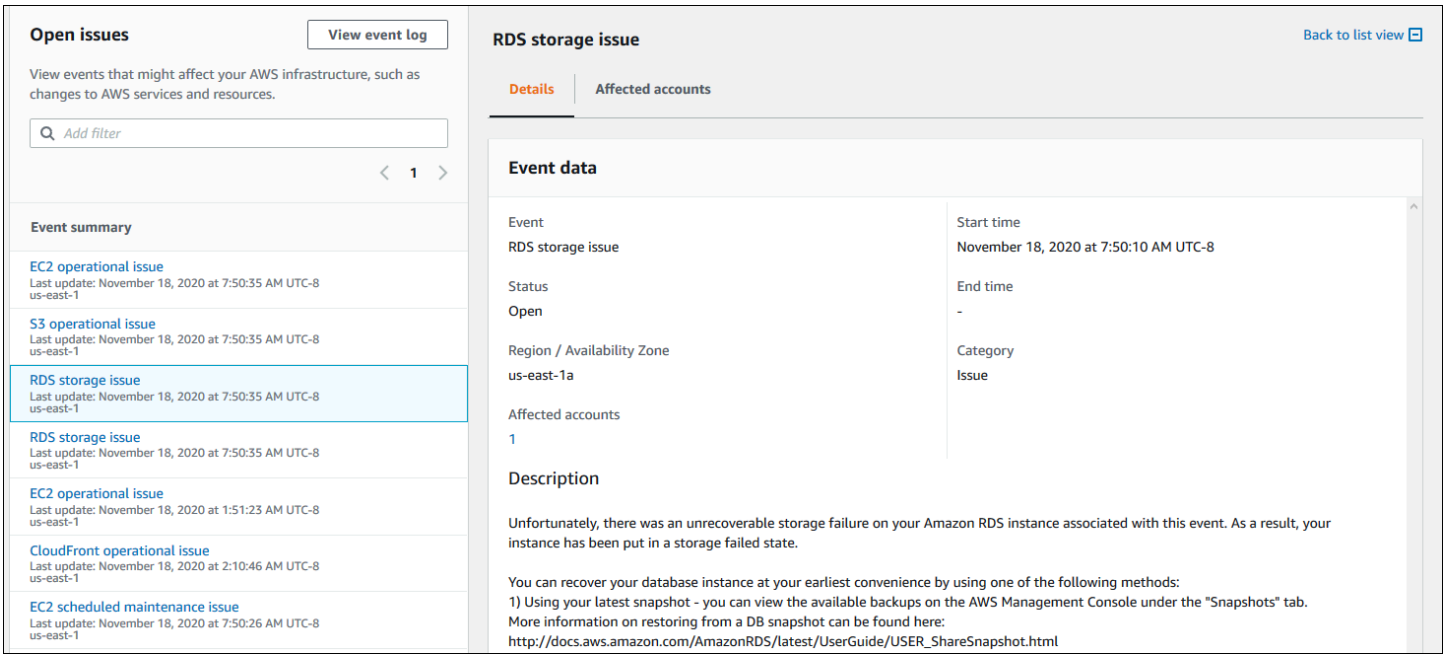
1. 打开您的 AWS Health 控制面板，网址为 https://health.aws.amazon.com/health/home。
2. 在导航窗格的您的组织运行状况下，选择未决问题和近期问题以查看最近报告的事件。

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

Example：组织视图的未决问题

以下 Amazon Relational Database Service (Amazon RDS) 事件出现在组织视图的未决问题和近期问题选项卡中，该事件会影响组织中的一个账户。



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

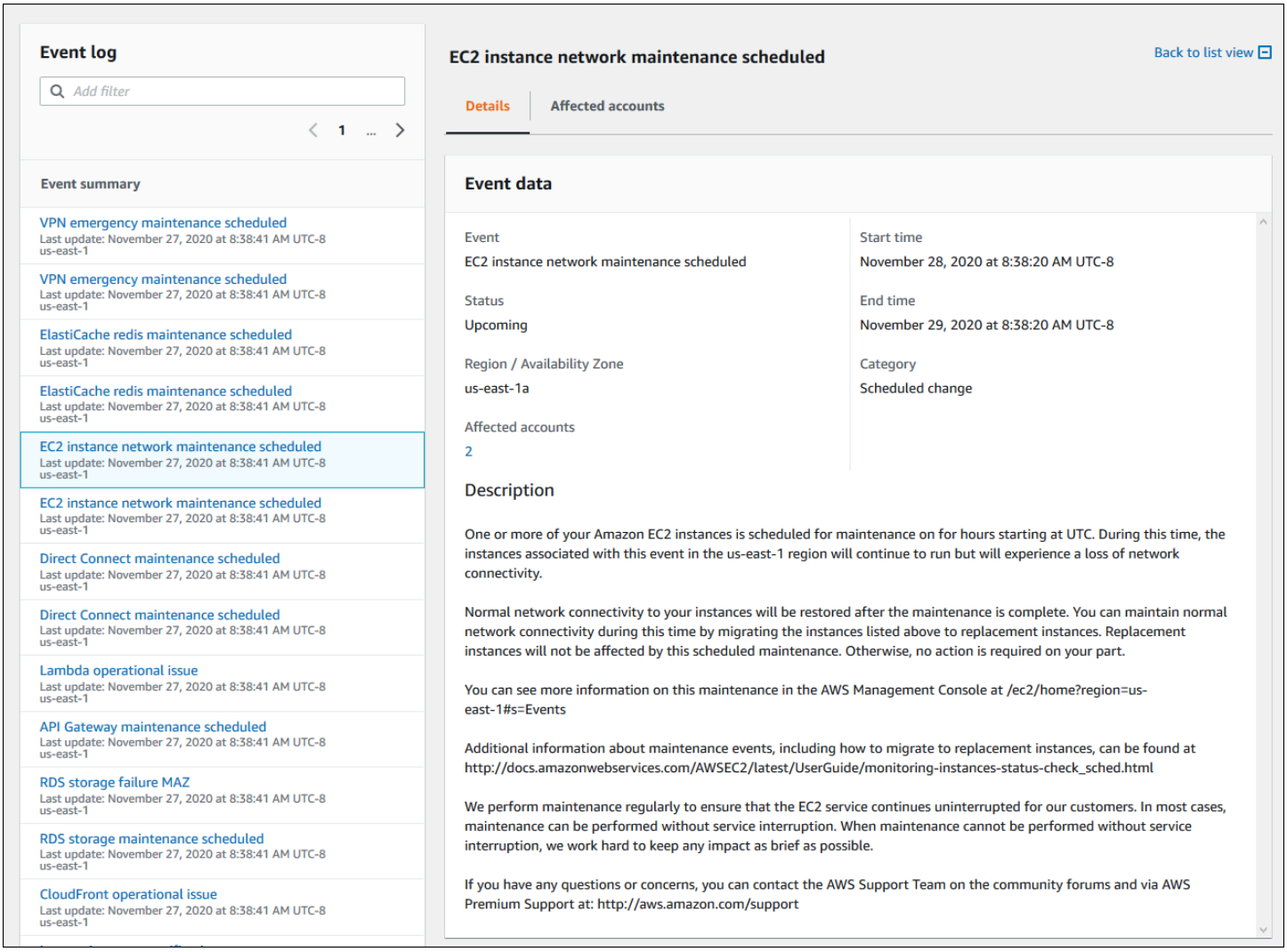
您也可以使用事件日志选项卡查看组织视图的 AWS Health 事件。列布局和行为与未决问题和近期问题选项卡类似，不同之处在于事件日志选项卡包含其他列和筛选条件选项，例如事件类别、状态和开始时间。

要在事件日志选项卡中查看组织视图的事件

1. 打开您的 AWS Health 控制面板，网址为 https://health.aws.amazon.com/health/home。
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

Example : 组织视图的事件日志选项卡

以下示例 Amazon DynamoDB (DynamoDB) 事件显示在事件日志选项卡中，它会影响组织中的两个账户。



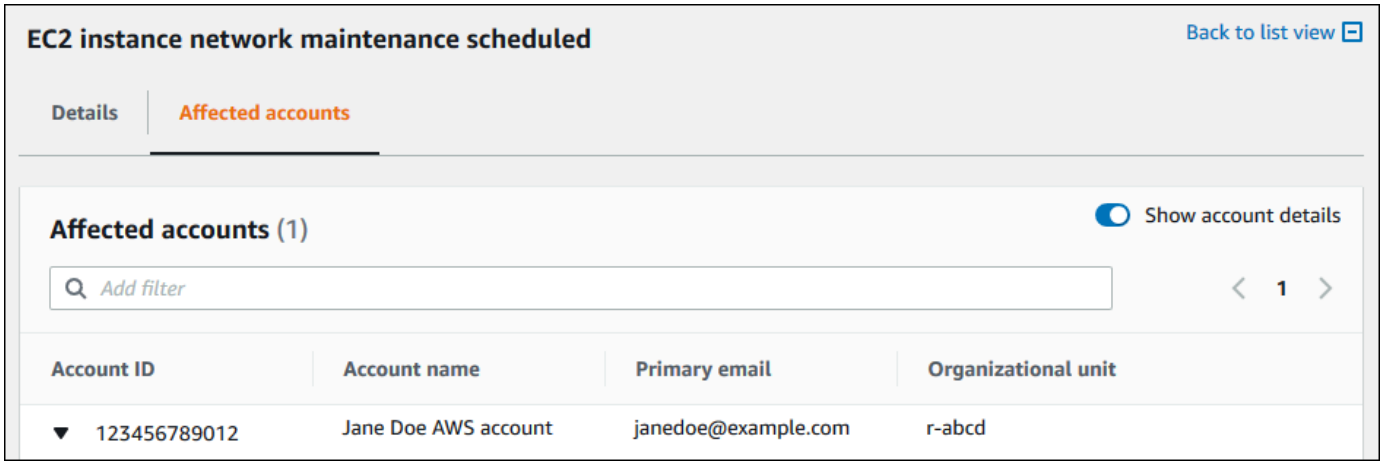
查看受影响的账户和资源（控制台）

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，如果有即将发生的 Amazon Elastic Compute Cloud (Amazon EC2) 实例维护事件，则您组织中拥有 Amazon EC2 实例的账户会在详细信息选项卡中显示。您可以确定具体的资源，然后联系账户所有者。

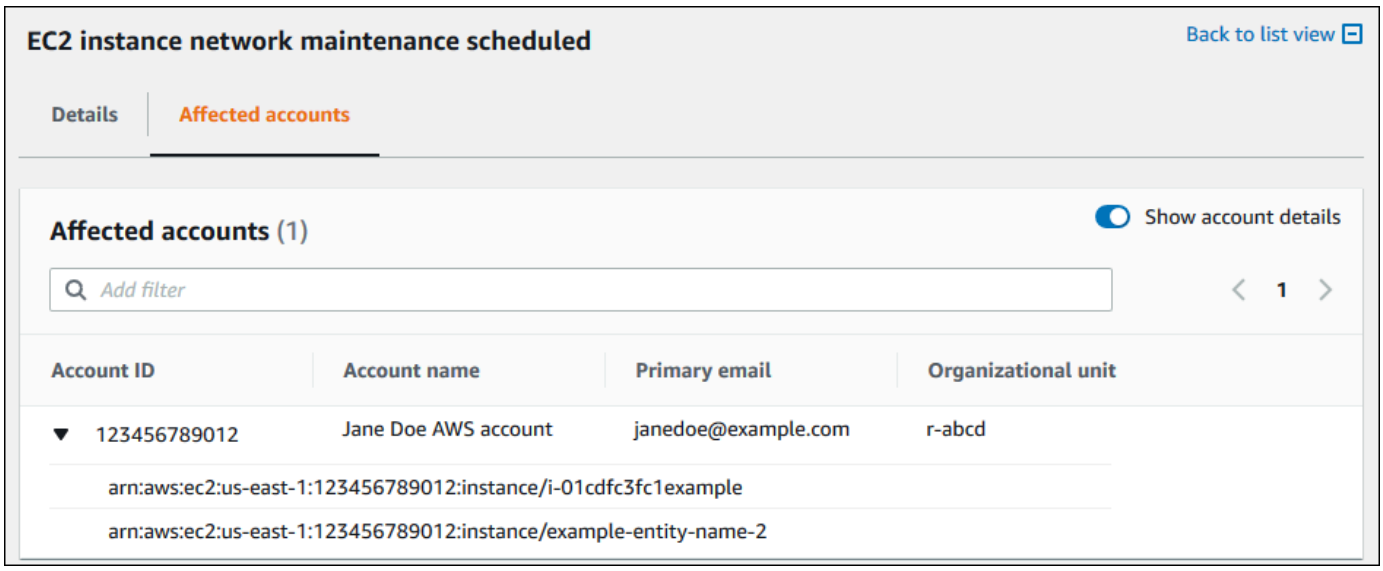
要查看受影响的账户和资源

1. 打开您的 AWS Health 控制面板，网址为 https://health.aws.amazon.com/health/home。
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可查看账户的以下信息：

- 账户 ID
- 账户名称
- 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以进行查看。
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。

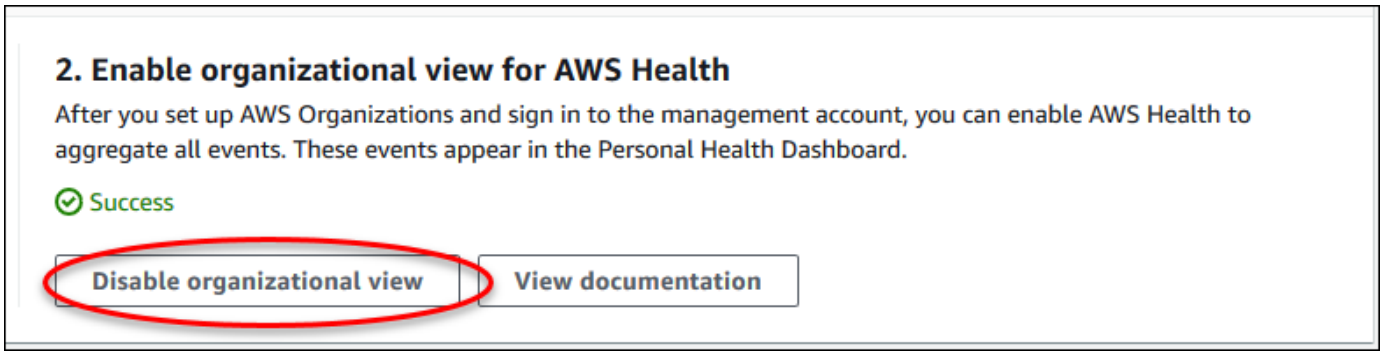
禁用组织视图（控制台）

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。

AWS Health 会停止聚合组织中所有其他账户的事件。您可以继续查看组织中以前的事件，直到这些事件被删除。

要禁用组织视图

1. 打开您的 AWS Health 控制面板，网址为 https://health.aws.amazon.com/health/home。
2. 在导航窗格的您的组织运行状况下，选择Configurations（配置）。
3. 在启用组织视图页面上，选择Disable organizational view（禁用组织视图）。



关闭此功能后，AWS Health 不再聚合来自组织的事件。但是，服务相关角色保留在管理账户上，直到您通过 AWS Identity and Access Management (IAM) 控制台、IAM API 或 AWS Command Line Interface (AWS CLI) 将其删除为止。有关更多信息，请参阅 IAM 用户指南中的删除服务相关角色。

组织视图 (CLI)

您也可以通过 AWS Command Line Interface (AWS CLI) 而不是 AWS Health 控制台启用组织视图功能。要使用控制台，请参阅 启用组织视图（控制台）。

> **Note**
>
> 如果允许用户访问管理账户以使用组织视图功能，则他们必须拥有诸如 AWSHealthFullAccess 策略之类的权限。有关更多信息，请参阅 AWS Health 基于身份的策略示例。

目录

- 查看组织视图事件 (CLI)
- 禁用组织视图 (CLI)
- AWS Health 组织视图 API 操作

启用组织视图 (CLI)

只能通过使用 EnableHealthServiceAccessForOrganization API 操作来启用组织视图。

您可以使用 AWS Command Line Interface (AWS CLI) 或自己的代码来调用此操作。

> **Note**
>
> - 您必须拥有商业、Enterprise On-Ramp 或企业 Support 计划才能调用 AWS 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 AWS CLI 命令从 AWS 账户启用此功能。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 EnableHealthServiceAccessForOrganization API 操作。

Python

```
import boto3

client = boto3.client('health')

response = client.enable_health_service_access_for_organization()

print(response)
```

Java

您可以在以下示例中使用适用于 Java 2.0 版的 AWS 开发工具包。

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

import software.amazon.awssdk.services.health.model.ConcurrentModificationException;
import
 software.amazon.awssdk.services.health.model.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 AWS 开发工具包开发人员指南。

启用此功能时，AWSServiceRoleForHealth_Organizations 服务相关角色和 Health_OrganizationsServiceRolePolicy AWS 托管式策略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 DescribeHealthServiceStatusForOrganization 操作以检查该过程的状态。

查看组织视图事件 (CLI)

启用此功能后，AWS Health 会开始记录影响组织中账户的事件。当某个账户加入您的组织时，AWS Health 会自动将该账户添加到组织视图中。

> **Note**
>
> AWS Health 不会记录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。

AWS 将在管理员账户关闭生效之日起 90 天内保留该账户的策略数据。在 90 天期限结束时，AWS 会永久删除该账户的所有策略数据。

- 要将结果保留 90 天以上，您可以将策略存档。您还可以使用采用 Eventbridge 规则的自定义操作将结果存储到 S3 存储桶中。
- 只要 AWS 保留策略数据，当您重新打开关闭的账户时，AWS 就会将该账户重新分配为服务管理员并恢复该账户的服务策略数据。
- 有关更多信息，请参阅关闭账户。

> **Important**
>
> 对于 AWS GovCloud (US) 区域的客户：
>
> - 在关闭账户前，备份并删除账户资源。关闭账户后，您将不再拥有其访问权限。

您可以使用 AWS Health API 操作从组织视图返回事件。

Example ：描述组织视图事件

以下 AWS CLI 命令返回组织中 AWS 账户的运行状况事件。

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

有关其他 AWS Health API 操作，请参阅以下部分。

禁用组织视图 (CLI)

您可以通过使用 DisableHealthServiceAccessForOrganization API 操作来禁用组织视图。

Example

以下 AWS CLI 命令从您的账户禁用此功能。

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

> **Note**
>
> 您也可以通过使用 Organizations DisableAWSServiceAccess API 操作来禁用组织功能。调用此操作后，AWS Health 会停止聚合组织中所有其他账户的事件。如果您为组织视图调用 AWS

Health API 操作，则 AWS Health 会返回错误。AWS Health 会继续为 AWS 账户聚合运行状况事件。

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

AWS Health 组织视图 API 操作

您可以将以下 AWS Health API 操作用于组织视图：

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

可使用以下操作来允许或禁止 AWS Health 与组织结合使用：

- EnableHealthServiceAccessForOrganization – 授予 AWS Health 与组织互动的权限，并将 SLR 应用于组织中的管理账户。
- DisableHealthServiceAccessForOrganization – 撤消 AWS Health 与组织互动的权限。
- DescribeHealthServiceStatusForOrganization – 返回有关是否为组织启用 AWS Health 的状态信息。

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

Example 示例：组织包含具有商业和开发人员支持计划的账户

- 您的组织中有三个账户。管理账户具有商业支持计划，而另两个账户具有开发人员支持计划。
- 您可以从管理账户或从可使用所需权限担任角色的账户调用 `DescribeEventForOrganization` API 操作。

- AWS Health 返回所有三个账户的信息。

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

Example 示例：组织具有包含企业、商业和开发人员支持计划的账户

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

委托管理员组织视图

在 AWS Health 中，您可以利用 AWS Organizations 的委托管理员功能，该功能允许管理账户以外的账户在 AWS Health 控制面板上或通过 AWS HealthAPI 以编程方式查看聚合 AWS 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。将责任委派到管理账户之外是一种 AWS 安全最佳实践（如果可能）。

目录

为您的组织视图注册委托管理员

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 RegisterDelegatedAdministrator API 操作。注册成员账户后，成员账户将成为委托管理员账户，并可从 AWS Health 控制面板访问 AWS Health 组织视图。如果账户具有商业、Enterprise On-Ramp 或企业 Support 计划，则委托管理员可以使用 AWS Health API 访问 AWS Health 组织视图。

要建立委托管理员，请从组织的管理账户调用以下 AWS Command Line Interface (AWS CLI) 命令。您可以从管理账户或从可担任具有所需 AWS Identity and Access Management 权限的角色的账户使用此命令。在以下命令示例中，将 ACCOUNT_ID 替换为要与 AWS Health 服务主体 "health.amazonaws.com" 一起注册的成员账户 ID。

```
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 AWS 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。

从您的组织视图中移除委托管理员

要移除委托管理员的访问权限，请调用 DeregisterDelegatedAdministrator API 操作。

从组织的管理账户中，调用以下 AWS CLI 命令，从而以委托管理员的身份移除成员账户。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
```

使用 Amazon 监控 AWS Health 事件 EventBridge

您可以使用 Amazon EventBridge 来检测 AWS Health 事件并做出反应。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，如果您有计划 AWS Health 进行更新的 AWS 资源，例如亚马逊弹性计算云 (Amazon EC2) 实例，则可以使用接收电子邮件通知。 AWS 账户

> **注意事项**
>
> - AWS 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 AWS 账户。要接收您内部其他账户的组织活动 AWS Organizations，请参阅使用组织视图和委派的管理员访问权限聚合 AWS Health 事件。

EventBridge 作为 AWS 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：

- AWS 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 AWS 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 AWS Health 通过 Amazon SNS 发送自定义文本或短信通知。

有关您可以为响应 AWS Health 事件而创建的自动化和自定义警报的示例，请参阅中的AWS Health 工具 GitHub。

主题

- 的事件处理器 AWS Health
- 为创建 EventBridge 规则 AWS Health
- AWS Health 事件 Amazon EventBridge 架构
- 对 AWS Health 事件进行分页 EventBridge
- 使用组织视图和委派的管理员访问权限聚合 AWS Health 事件
- 使用接收 AWS Health 事件 AWS Chatbot
- 针对 Amazon EC2 实例实现自动化操作
- 配置 SMC 连接器 AWS Health

差不 AWS 区域 多是 AWS Health

您必须为要接收其 AWS Health 事件的每个区域创建 EventBridge 规则。如未创建规则，则无法接收事件。例如，要接收来自美国西部（俄勒冈州）区域的事件，您必须为此区域创建规则。

如果主规则受到持续事件的影响，则在备份区域中设置其他规则可额外增加工作流程的恢复能力。的 AWS Health 公共事件同时发送到受影响的区域和备用区域。有关更多信息，请参阅关于 AWS Health 的公共事件。您可以在美国西部（俄勒冈州）针对标准 AWS 分区中的所有区域设置规则作为备份，即使主区域受到持续问题的影响，也可以继续接收事件。美国西部（俄勒冈州）区域的备份区域是美国东部（弗吉尼亚州北部）区域。

例如，如果您正在监控欧洲（法兰克福）地区的事件，而该区域暂时不可用，那么该事件 AWS Health 也会传送到美国西部（俄勒冈）区域。接下来，您的备份 EventBridge 规则将事件发送到您指定的目标。要创建备份规则，请按 为创建 EventBridge 规则 AWS Health 的以下过程操作并使用美国西部（俄勒冈州）区域。

有些 AWS 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。其中包括针对 AWS Identity and Access Management 发送的事件。要接收全局事件，必须创建规则，将美国东部（弗吉尼亚州北部）作为主区域，将美国西部（俄勒冈州）区域作为备份区域。

要在中接收全球事件 AWS GovCloud (US)，您必须在 AWS GovCloud （美国西部）地区创建规则。

关于的公共活动 AWS Health

当您创建用于监控事件的 EventBridge规则时 AWS 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，例如说明必要 Amazon EC2 实例更新的事件或其他计划更改事件。
- 公共事件显示在AWS Health 控制面板 — 服务运行状况上。公共事件并非特定于 AWS 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 AWS 区域，我们建议您创建备份规则。的 AWS 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 AWS Health 的事件，因为对于发送到备份区域的 AWS 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或ACCOUNT_SPECIFIC。您也可以根据此参数筛选规则。

示例：Amazon Elastic Compute Cloud 的公共事件

以下事件显示美国东部（弗吉尼亚州北部）区域的一个 Amazon EC2 操作问题。


```
{
    "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",

    }
}
```

的事件处理器 AWS Health

如果您对自己的账户使用 AWS 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` AWS 托管策略。此策略列出了该角色可以执行的权限，例如 AWS 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 AWS 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 AWS Health](#)
- [AWS 托管式策略：AWSHealth_EventProcessorServiceRolePolicy](#)

为创建 EventBridge 规则 AWS Health

您可以创建一条 EventBridge 规则，以便收到有关您账户中 AWS Health 发生的事件的通知。在为创建事件规则之前 AWS 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 AWS 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 AWS Health

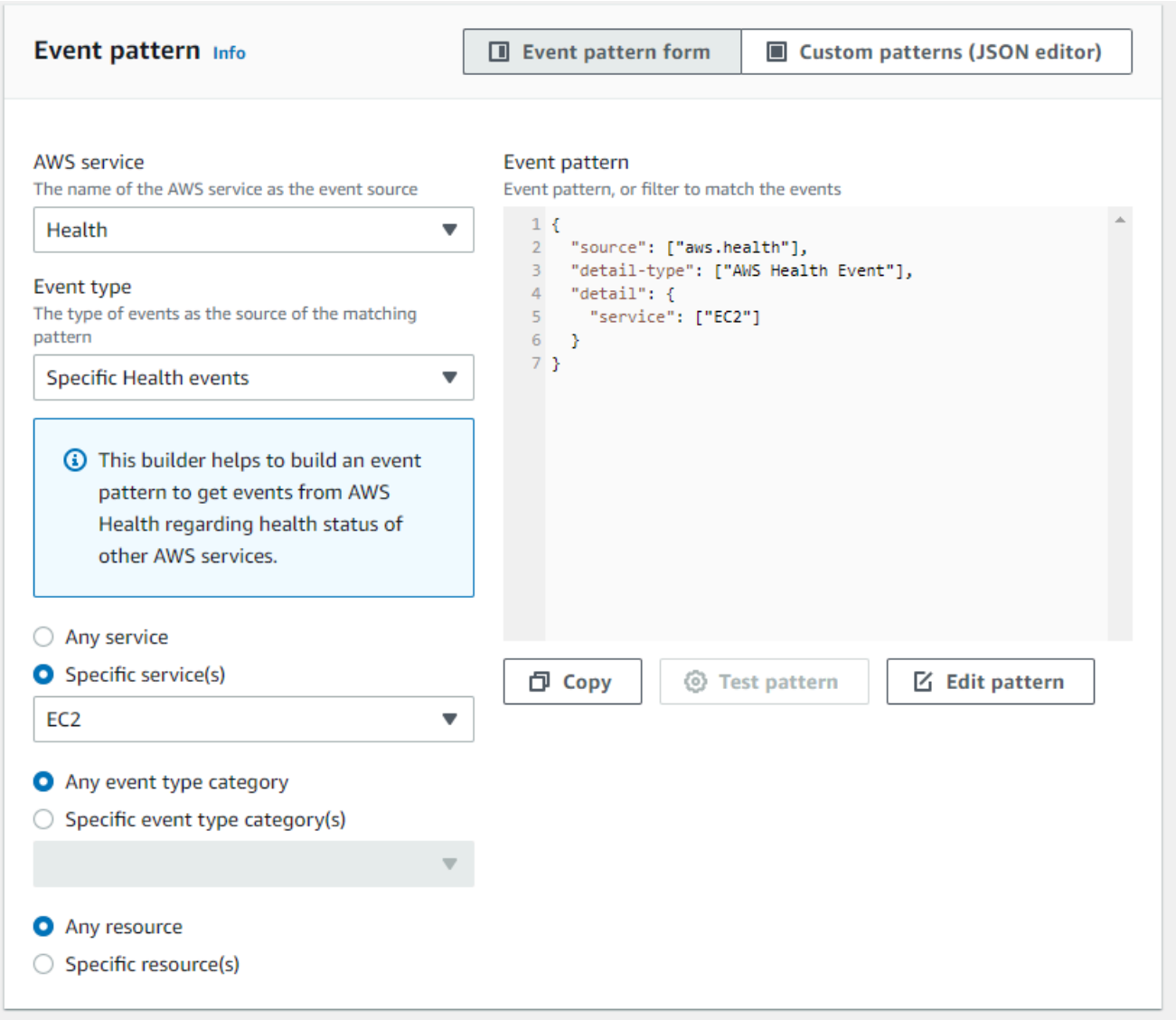
1. 打开亚马逊 EventBridge 控制台，网址为 https://console.aws.amazon.com/events/。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。选择要在其中跟踪 AWS Health 事件的区域。
3. 在导航窗格中，选择规则。
4. 选择 创建规则。
5. 在 Define rule detail（定义规则详细信息）页面上，输入规则名称和描述。
6. 对于 事件总线和 规则类型，保留默认值，然后选择下一步。
7. 在构建事件模式页面上，为事件源选择AWS 事件和 EventBridge 合作伙伴事件。
8. 在 事件模式下，对于 E事件源，选择 AWS 服务。
9. 在 事件模式下，对于 AWS 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 AWS Health 事件创建一个规则。
    - 特定健康事件 — 为特定事件（例如 Amazon EC2）创建规则。 AWS 服务
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 AWS 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 AWS Health 事件，包括任何新的事件类型代码。有关规则示例，请参阅所有 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。
    - 选择特定资源并输入一个或多个资源的 ID。例如，您可以指定一个 Amazon EC2 实例 ID（如 *i-EXAMPLEa1b2c3de4*），以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 ：适用于所有 Amazon EC2 事件的规则

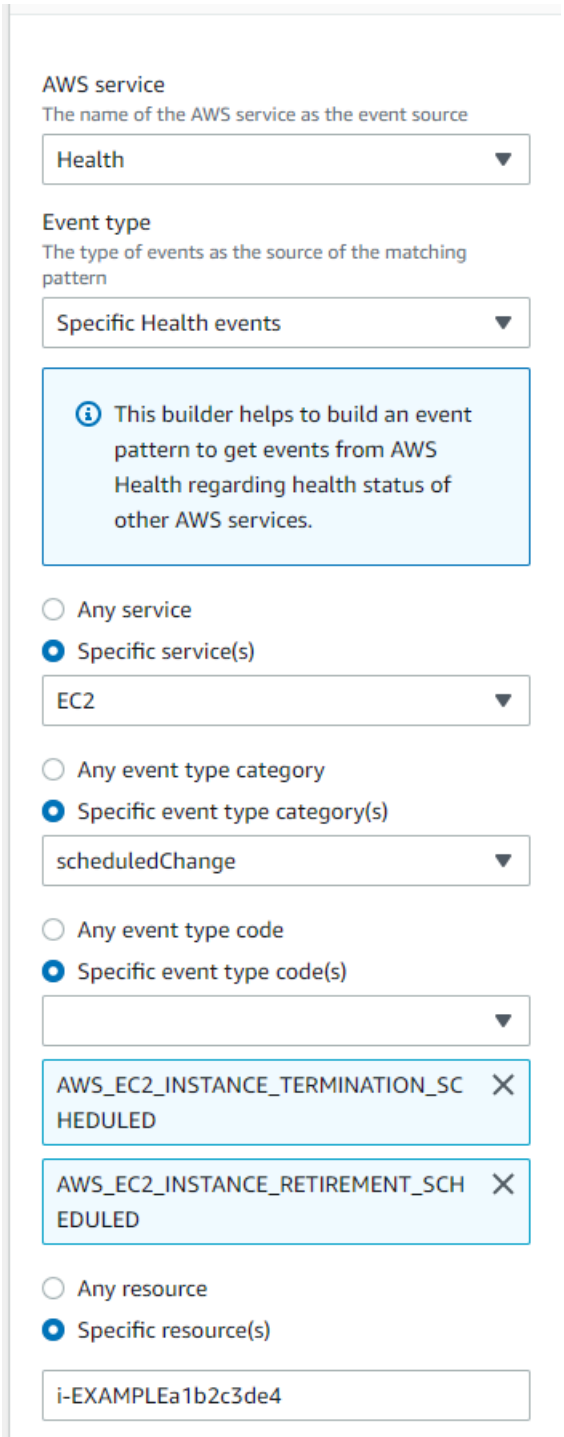
以下示例创建了一个规则，用于 EventBridge 监控所有 Amazon EC2 事件，包括事件类型类别、事件代码和资源。



Example ：适用于特定 Amazon EC2 事件的规则

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 为创建 EventBridge 规则 AWS 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 为创建 EventBridge 规则 AWS Health 中的剩余过程创建规则。

使用 API 或 AWS Command Line Interface (AWS 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 AWS CLI 命令示例，请参阅《命令参考》中的 put-AWS 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 AWS 服务的`issue`、`accountNotification`和`scheduledChange`事件类型类别的事件：Amazon EC2、Amazon EC2 Auto Scaling 和 Amazon VPC。

```
{
  "detail": {
    "eventTypeCategory": [
      "issue",
      "accountNotification",
      "scheduledChange"
    ],
    "service": [
      "AUTOSCALING",
```

```
      "VPC",
      "EC2"
    ]
  },
  "detail-type": [
    "AWS Health Event"
  ],
  "source": [
    "aws.health"
  ]
}
```

AWS Health 事件 Amazon EventBridge 架构

以下是 AWS Health 事件架构。对先前版本架构所做的增改将突出显示为“新”。架构后提供了示例负载。

AWS Health 事件架构

AWS Health 事件架构

参数	描述	必填
版本	EventBridge 版本，当前为“0”	支持
id	事件的 uniqueEventBridge 标识符	支持
detail-type	描述详细信息类型。对于 AWS Health 活动，这将是&AWS Health Event或AWS Health	支持

参数	描述	必填
	`Abuse Event`	
source	事件总线源。对于 AWS Health 活动，这将是 `aws.health`	支持

参数	描述	必填
account	事件发送到 AWS Health 的账户 ID。 Note 对于组织视图，如果通过管理账户或委托管理员账户接收，则与 AffectedAccount 有所不同。	支持

参数	描述	必填
time	通知发送到的时间 EventBridge。格式：`yyyy-mm-ddThh:mm:ssZ` 。	支持
region	标识 AWS 区域 通知已发送到的。 **Note** 此字段未指明此 AWS Health 事件的受影响区域。此信息通过 "detail.eventRegion" 提供。	支持

参数	描述	必填
resources	如果存在受影响的资源，则描述账户中受影响的一系列资源。 Note 如未引用任何资源，此字段可以为空。	不支持
detail	本部分包含 AWS Health 活动的所有细节，如下所示。	支持

参数		描述	必填
	eventArn	特定区域 AWS Health 的事件的唯一标识符，包括区域和事件 ID。 Note eventArn 在特定客户账户或区域并非唯一。	支持
	服务	AWS 服务 受 AWS Health 事件影响的。例如，Amazon EC2、Amazon Simple Storage Service、Amazon Redshift 或 Amazon Relational Database Service。	支持

参数		描述	必填
	eventTypeCode	事件类型的唯一标识符。例如：AWS_EC2_NSTANCE_NETWORK_MAINTENANCE_SCHEDULED 和 AWS_EC2_INSTANCE_REBOOT_MAINTENANCE_SCHEDULED 。包含 MAINTENANCE_SCHEDULED 的事件通常在 startTime 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_{SEI	支持

参数		描述	必填
		ICE}_PLA NED_LIFE YCLE_EVE T 。	
	eventTypeCategory	事件的类别代码。可能的值为 issue、accou tificatio n 、investig tion 和 scheduled Change 。	支持
	eventScopeCode	指明该 AWS Health 事件是特定账户还是公开的。可能的值为 ACCOUNT_S PECIFIC 或 PUBLIC。	支持

参数		描述	必填
	communicationId（新）	此次 AWS Health 活动通信的唯一标识符。 具有相同 CommunicationID 的消息可能是单个 AWS Health 事件的备份消息或页面。此标识符可以与 accountID 一起使用，帮助去除重复的消息。 Note 在分页功能版本中，communicationId 包含页码，以保持 communicationId 在多	支持

参数	描述	必填
	个页面中的唯一性，例如 12345678 10-1。有关更多信息，请参阅 对 AWS Health 事件进行分页 EventBridge。	

参数		描述	必填
	startTime	AWS Health 事件的开始时间，格式为：DoW, DD, MMM, YYYY, HH:MM:SS TZ。 Note 计划事件的开始时间可以是未来。	支持

参数		描述	必填
	endTime	AWS Health 事件的结束时间，格式为：DoW, DD MMM YYYY HH:MM:SS TZ。 Note 可能不会为将来设置的事件提供 endTime。	不支持
	lastUpdatedTime	AWS Health 事件的最后更新时间，格式为:DoW, DD MMM YYYY HH:MM:SS TZ。	支持

参数		描述	必填
	statusCode	AWS Health 事件的状态。类型类别具有不同状态。 `Issue`事件类别的可能值为 `open`、`closed` `scheduledChanges` 事件类别具有不同状态：`Upcoming` 或 `Completed` 。 `AccountNotifications` 事件类别没有状态，被设置为 "-"。	支持
	eventRegion	此 AWS Health 事件描述的受影响区域。	支持
	eventDescription	描述 AWS Health 事件的部分。包括用于描述事件的语言和文本字段。	支持

参数			描述	必填
		language	AWS Health 活动中使用的语言。通常由事件发布区域决定。对于 us-east-1 区域，通常为 "en_US"。	支持

参数			描述	必填
		latestDescription	描述从 AWS Health API 呈现 AWS Health 的事件，通常显示在 AWS Health 仪表板上。 **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。	支持
	eventMetadata		可以为 AWS Health 事件提供的其他事件元数据。	不支持

参数			描述	必填
		<元数据键 1>	元数据键，值字符串 "keystring1": "keyvalue1" Note 事件元数据的键值对由发送事件的服务确定。AWS Health	不支持
	affectedEntities		描述此 AWS Health 事件中受影响资源的资源值和状态的数组。	不支持
		entityValue	资源/实体 ID	不支持
		lastUpdatedtime（新）	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	不支持

参数		描述	必填
	status（新）	受影响资源/实体的状态。可能的值包括：IMPAIRED、D 、PENDING、	不支持 KNOWN
	page（新）	此消息所表示的页面。有关更多信息，请参阅 对 AWS Health 事件进行分页 EventBridge。 Note 分页仅在资源上发生。其他导致超出 256KB 大小限制的原因也会引发通信失败。	支持

参数		描述	必填
	totalPages（新）	此运行状况事件的总页数。有关更多信息，请参阅 对 AWS Health 事件进行分页 EventBridge。 Note 您可以通过它确定是否收到某个账户多页通信的所有页面。	支持

参数		描述	必填
	affectedAccount（新）	这是受影响账户的账户 ID。 Note 如果将此健康事件发送到属于的账户，AWS Organizations 并且在管理或委托管理员账户中接收，则这可能与“账户”字段不同。	支持

公共运行状况事件 - Amazon EC2 操作问题

```
        {
          "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 AWS 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",
          }
        }
```

特定于账户的 AWS 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",
          }
        }
```

对 AWS Health 事件进行分页 EventBridge

AWS Health 当 “资源” 或 “AffectedE EventBridge ntities” 列表导致消息大小超过 256KB 的邮件大小限制时，支持对 AWS Health 事件进行分页。以前 AWS Health ，当资源超过此限制时，不会将完整的资源列表与事件进行通信。

AWS Health 现在，消息中包含所有 “资源” 和 “detail.AffectedEntities”。如果此 “资源” 和 “detail.AffectedEntities” 列表超过 256KB，则会将运行状况事件 AWS 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，以便在收到所有页面后帮助重新组合“resources”和“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。收到用户可读通知的客户可以针对“detail.page”字段添加筛选器，仅处理第一个页面，从而消除后续页面中创建的不必要消息。

纳入多项架构更改，以支持启动分页。现在，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。还有两个新字段，detail.page 和 detail.TotalPages，它们描述了活动的当前页码和总页数。 AWS Health 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 AWS Health 事件

AWS Health 支持对在 Amazon 上发布 AWS 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 AWS 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一 AWS Health 事件提要 AWS Organizations。

此功能旨在提供集中视图，以帮助管理整个组织中的 AWS Health 事件。在管理账户中设置组织视图和 EventBridge 规则并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 AWS Health，请参阅聚合 AWS Health 事件。

使用接收 AWS Health 事件 AWS Chatbot

你可以直接在聊天客户端（例如 Slack 和 Amazon Chime）中接收 AWS Health 事件。您可以使用此事件来识别最近可能影响您的 AWS 应用程序和基础架构的 AWS 服务问题。然后，您可以登录 AWS 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 AWS 账户中的`AWS_EC2_INSTANCE_STOP_SCHEDULED`事件类型，则该 AWS 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：

- 配置为的聊天客户端 AWS Chatbot。您可以配置 Amazon Chime 和 Slack。有关更多信息，请参阅 AWS Chatbot 管理指南中的 AWS Chatbot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。

通过以下方式接收 AWS Health 活动 AWS Chatbot

1. 按照 为创建 EventBridge 规则 AWS 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 AWS Health 事件中删除不必要的聊天消息。请参阅 对 AWS Health 事件进行分页 EventBridge。

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

   b. 在步骤 14 中选择目标时，请选择 SNS 主题。您将在 AWS Chatbot 控制台中使用相同的 SNS 主题。

   c. 完成剩余步骤，以创建规则。

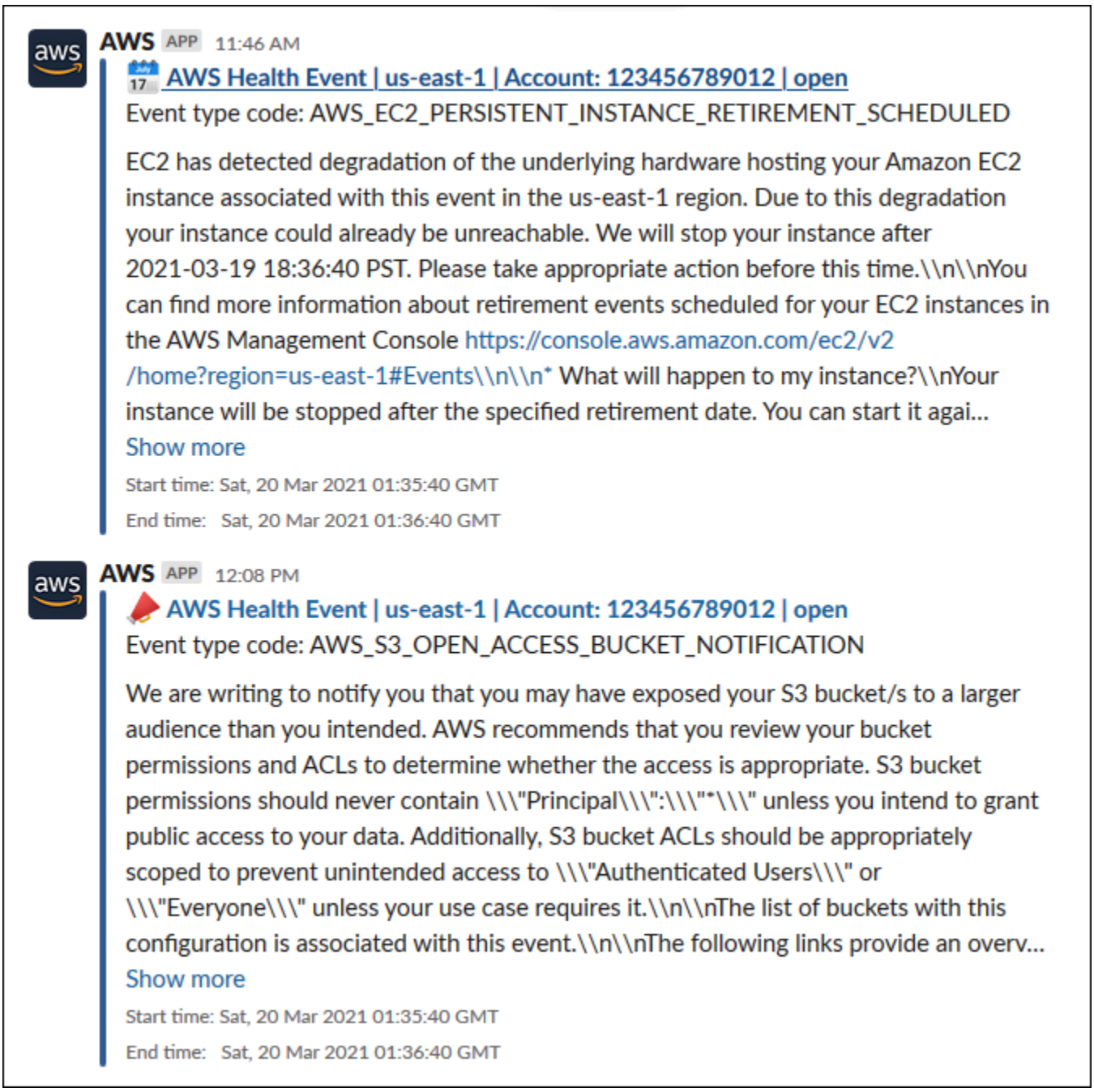
2. 导航到 AWS Chatbot 控制台。
3. 选择聊天客户端，如 Slack 通道名称，然后选择 Edit（编辑）。
4. 在 Notifications - optional（通知 - 可选）部分，在 Topics（主题）中选择与步骤 1 指定的相同的 SNS 主题。
5. 选择保存。

   当 AWS Health 向其 EventBridge 发送符合您规则的事件时，该 AWS Health 事件将显示在您的聊天客户端中。

6. 选择活动名称可在 AWS Health 控制面板中查看更多信息。

Example : 发送到 Slack AWS Health 的事件

以下是美国东部（弗吉尼亚北部）地区的 Amazon EC2 和亚马逊简单存储服务 (Amazon S3) Service 在 Slack 频道中出现的两个 AWS Health 活动示例。



针对 Amazon EC2 实例实现自动化操作

您可以针对 Amazon EC2 实例，通过自动化操作来响应新的计划事件。当 AWS Health 向您的 AWS 账户发送事件时，您的 EventBridge 规则可以调用目标（例如 Automati AWS Systems Manager on 文档）来代表您自动执行操作。

例如，当为亚马逊弹性区块存储 (Amazon EBS) Elastic Block Store 支持的 EC2 实例安排亚马逊EC2实例停用活动时 AWS Health ，会将事件类型发送到您的控

制AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED面板。 AWS 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**
>
> 为自动执行 Amazon EC2 实例操作，必须通过 Systems Manager 管理这些实例。

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

先决条件

在创建规则之前，您必须创建 AWS 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 AWS 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 AWS 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 A ***utomationEV RolePolicy*** 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 AWS 服务创建角色

1. 登录 AWS 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 AWS service（服务）。
4. 对于您希望允许其承担此角色的服务，选择 EC2。
5. 选择下一步：权限。
6. 输入您创建的策略名称，例如 *AutomationEV RolePolicy*，然后选中该策略旁边的复选框。
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. 在 角色名称中，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 AWS 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 AWS 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 AWS 账户中的角色列表中，选择您创建的角色的名称，例如 A *utomat* ionEvRole。

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）。

为创建规则 EventBridge

按照此过程在 EventBridge 控制台中创建规则，这样您就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. 打开亚马逊 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 AWS。
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。

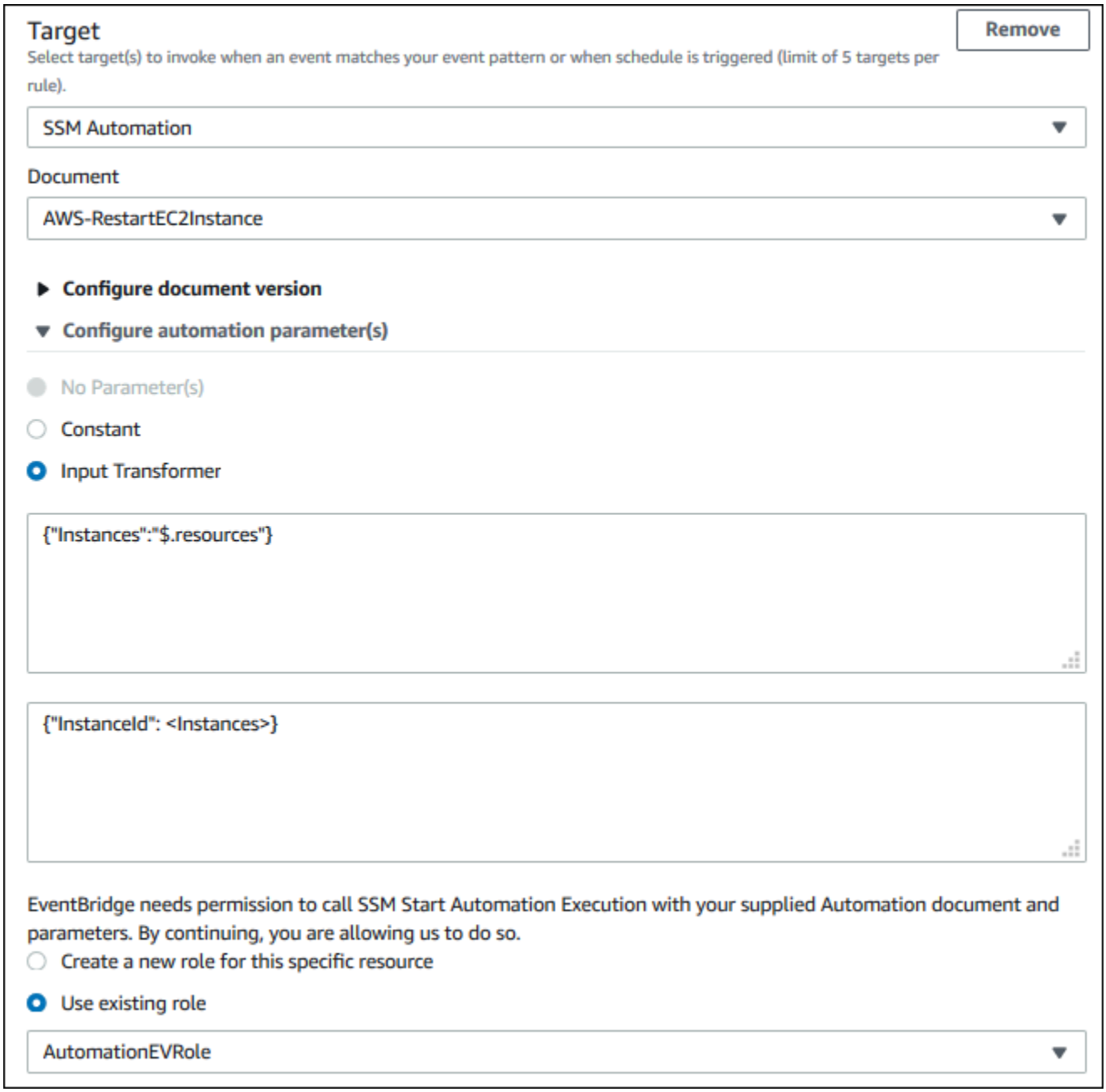
    例如，对于由 Amazon EC2 EBS 支持的实例，选择 **AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED**。对于由 Amazon EC2 实例存储支持的实例，选择 **AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED**。
11. 选择 Any resource（任何资源）。

    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 AWS-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，如 *AutomationEVRole*。

您的目标应类似于以下示例。



> **Note**
>
> 如果没有具备所需 EC2 和 Systems Manager 权限以及信任关系的现有 IAM 角色，则角色将不会显示在列表中。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。

配置 SMC 连接器 AWS Health

您可以使用服务管理连接器 (SMC) 将 AWS 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 AWS 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派的管理员访问权限在 JIRA 和中轻松管理整个组织的 Health 事件 ServiceNow，并将 AWS 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 AWS Health 。 ServiceNow

有关使用 SMC 集成 JIRA 管理云的更多信息，请参阅 JIRA AWS Health 。

监控 AWS Health

监控是维护和其他 AWS 解决方案的可靠性、可用性和性能的重要组成部分。 AWS Health AWS 提供以下监控工具 AWS 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 AWS 资源和您运行 AWS 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 AWS Health 的事件的通知。例如，如果 AWS Health 发布了有关您的 Amazon EC2 实例的事件，则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 使用 Amazon 监控 AWS Health 事件 EventBridge。
- AWS CloudTrail 捕获由您的账户或代表您的 AWS 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账户拨打了电话 AWS、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《AWS CloudTrail 用户指南》。

主题

使用记录 AWS Health API 调用 AWS CloudTrail

AWS Health 与 AWS CloudTrail一项服务集成，该服务提供用户、角色或 AWS 服务在中执行的操作的记录 AWS Health。 CloudTrail 将发出的 API 调用捕获 AWS Health 为事件。捕获的调用包括来自 AWS Health 控制台的调用和对 AWS 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 AWS 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 AWS 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AWS CloudTrail 用户指南。

AWS Health 信息在 CloudTrail

CloudTrail 在您创建 AWS 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 AWS Health，该活动会与其他 AWS 服务 CloudTrail 事件一起记录在事件历史记录中。您可以在自己的 AWS 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 AWS 账户中的事件，包括的事件 AWS 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 AWS 区域。此跟踪记录在 AWS 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 AWS 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
- 接收来自多个区域的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail 日志文件

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

AWS 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 AWS 服务发出

有关更多信息，请参阅CloudTrail 用户身份元素。

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，请参阅为其配置 Amazon SNS 通知。 CloudTrail

您还可以将来自多个 AWS 区域和多个 AWS 账户的 AWS Health 日志文件聚合到单个 Amazon S3 存储桶中。

有关更多信息，请参阅从多个区域接收 CloudTrail 日志文件和从多个账户接收 CloudTrail 日志文件。

示例： AWS 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": "AWS Internal"
    },
   "eventTime": "2016-11-21T07:06:28Z",
   "eventSource": "health.amazonaws.com",
   "eventName": "DescribeEntityAggregates",
   "awsRegion": "us-east-1",
   "sourceIPAddress": "203.0.113.0",
   "userAgent": "AWS Internal",
   "requestParameters": {"eventArns": ["arn:aws:health:us-east-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 AWS Health

下表描述了此版本的文档 AWS Health。

- API 版本：2016-08-04

下表描述了自 2020 年 8 月 28 日起对 AWS 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
从 “安全” 部分 AWS Health 的文档中删除了网际网络流量隐私	有关更多信息，请参阅中的安全性AWS Health	2024 年 3 月 27 日
更新了 AWS Health 文档的 AWS Health 控制面板 — 服务运行状况和计划生命周期事件。	有关更多信息，请参阅AWS Health 控制面板-服务运行状况和计划的生命周期事件 AWS Health。	2024 年 2 月 15 日
在 “为以下对象创建 EventBridge 规则” 中删除了重复的要点 AWS Health	在 “为其创建 EventBridge 规则” 中删除了重复的要点 AWS 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 AWS 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 AWS GovCloud (US) Regions使用 `AWSHealthFullAccess` 托管策略。有关信息，请参阅AWS 托管策略 AWS Health。	2023 年 10 月 16 日
在中添加了有关配置 AWS 用户通知的文档 AWS Health。	现在，您可以在中配置 AWS 用户通知 AWS Health。有关	2023 年 8 月 30 日

	更多信息，请参阅为配置 AWS 用户通知 AWS Health。	
在 “聚合 AWS 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	AWS 托管策略更新：Health_OrganizationsServiceRolePolicy。有关更多信息，请参阅适用于 AWS Health的AWS 托管策略。	2023 年 7 月 19 日
AWS Health 架构现在支持事件元数据	现在，您可以从事件中接收 AWS Health 事件元数据。有关更多信息，请参阅使用 Amazon 监控 AWS 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 AWS Health 事件 EventBridge。	2023 年 5 月 2 日
添加了 AWS 托管策略的文档	添加了用于 AWS Health的AWS 托管策略的文档并为AWS 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 AWS Health 控制面板。有关更多信息，请参阅AWS Health 控制面板入门-您的账户健康状况和AWS 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 AWS Health ware 添加了文档。有关更多信息，请参阅 AWS Health Aware。	2022 年 5 月 25 日
已更新的文档	Service Health Dashboard 和AWS Personal Health Dashboard已更名为 AWS Health 控制面板。 有关更多信息，请参阅AWS Health 控制面板入门-您的账户健康状况和AWS 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	使用亚马逊监控 Heal EventBridge th 事件的新主题。 AWS Health 有关更多信息，请参阅使用 Amazon 监控 AWS 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 AWS Health API。	2021 年 11 月 24 日
添加的文档	AWS Health 概念的新主题。有关更多信息，请参阅 AWS 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 AWS Systems Manager 操作。有关更多信息，请参阅为 Amazon EC2 实例自动执行操作。	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 AWS Health 事件的部分。有关更多信息，请参阅使用接收 AWS Health 事件 AWS Chatbot。	2021 年 3 月 16 日
已更新的文档	更新了以下主题： • 更新了聚合 AWS Health 事件主题 • 重组并更新了 “使用 Amazon Ev AWS 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 AWS Health 台中添加了用于组织视图的 AWS Health 仪表板	您可以使用 AWS Health 控制台启用组织视图功能。然后，您可以查看 AWS 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 AWS 区域 AWS Health。	2020 年 10 月 22 日
更新了 AWS Health 用户指南	组织更新并添加了 RSS 提要，以便您可以订阅 AWS 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 使用组织视图跨账户聚合 AWS Health 事件。	2020 年 6 月 3 日
安全和 AWS Health	添加了有关使用 AWS Health 时的安全注意事项的信息。请参阅 安全性 AWS 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 AWS Organizations中的所有账户聚合事件。	请参阅 使用组织视图跨账户聚合 AWS 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。 AWS Health	请参阅 适用于 AWS Health的身份和访问管理。	2018 年 8 月 2 日
添加了有关 AWS Health 信息可见性的注释。	请参阅 适用于 AWS Health的身份和访问管理。	2017 年 8 月 16 日
服务发布。	AWS Health 已发布。	2016 年 12 月 1 日

AWS 术语表

有关最新的 AWS 术语，请参阅《AWS 词汇表参考》中的 AWS 词汇表。

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。