使用者指南

AWS Health

AWS Health: 使用者指南

Table of Contents

什麼是 AWS Health？

AWS Health讓您持續掌握資源效能以及您AWS 服務和帳戶的可用性。您可以使用AWS Health事件來瞭解服務和資源變更如何影響執行的應用程式AWS。 AWS Health提供相關且即時的資訊，協助您管理進行中的活動。 AWS Health還可以幫助您了解並為計劃的活動做準備。此服務會提供由 AWS 資源運作狀態變更觸發的提醒和通知，讓您獲得近乎即時的事件可見性和引導，有助於加速故障診斷。

所有客戶都可以使用AWS Health由 AWS Health API 提供支援的 Dashboard。儀表板不需要設置，並且可供經過身份驗證的用AWS戶使用。有關更多服務重點，請參閱AWS Health儀表板詳細信息頁面 AWS Health

若要瞭解的基本知識以AWS Health及如何使用服務，請參閱您是第一次使用 AWS Health 的新手嗎？。

如需使用時會看到的術語清單AWS Health，請參閱概念 AWS Health。

> **備註**
>
> - AWS Health儀表板適用於所有AWS客戶，無需額外費用。
> - 所有AWS客戶都可以通過亞馬遜接收AWS Health事件 EventBridge ，無需額外費用。
> - 如果您擁有商業、企業級加速或企業 Support 方案，您可以使用 AWS Health API 與內部和第三方系統整合。如需詳細資訊，請參閱 AWS Health API 參考。
> - 如需可用AWS Support計劃的詳細資訊，請參閱AWS Support。

您是第一次使用 AWS Health 的新手嗎？

如果您是第一次使用 AWS Health，可從閱讀以下章節開始：

- 什麼是 AWS Health？— 本節說明基礎資料模型、其支援的作業，以及可用來與服務互動的 AWS SDK。
- 概念 AWS Health— 了解有關使用服務時會遇到的基本知識AWS Health和條款。
- 開始使用AWS Health儀表板 — 您的帳戶健康狀態— 瞭解如何檢視事件和受影響的實體，以及如何執行進階篩選。此控制面板包含您帳戶和組織的特定事件。
- AWS Health 儀表板 — 服務健康狀— 如果您沒有AWS 帳戶，則可以查看有關每個健康和狀態AWS 服務的信息AWS 區域。
- 使用 Amazon 監控 AWS Health 事件 EventBridge— 您可以使用亞馬遜從 EventBridge 接收推送通知AWS Health.
- 存取 AWS Health API— AWS Health API 區段說明擷取事件和實體相關資訊的作業。

AWS Health為所有客戶提供稱為「AWS Health儀表板」的主控台。您不需要編寫程式碼或執行任何動作來設定儀表板。

您可以設定 EventBridge 規則來接收 Amazon 上的AWS Health事件 EventBridge。這提供了一種使用推送通知自動化AWS Health事件管理的方法，方法是建立 Amazon EventBridge 規則以採取行動。

如果您有「商務」、「企業登入」或「企業 Support」方案，您可以透過程式設計方式存取儀表板上顯示的資訊。您可以使用 AWS Command Line Interface (AWS CLI) 或撰寫程式碼來提出要求，方法是直接使用 REST API 或 AWS SDK。

如需在 Amazon 上使用AWS Health事件的詳細資訊 EventBridge，請參閱使用 Amazon 監控 AWS Health 事件 EventBridge。如需在 AWS CLI 使用 AWS Health 的詳細資訊，請參閱 AWS Health 的 AWS CLI 參考。如需安裝 AWS CLI 的指示，請參閱安裝 AWS Command Line Interface。

概念 AWS Health

瞭解 AWS Health 概念，並瞭解如何使用服務來維護您的應用程式、服務和資源的健全狀況 AWS 帳戶。

主題

AWS Health 事件

AWS Health 事件 (也稱為 Health 事件) 是代表其他 AWS 服務 AWS Health 傳送的通知。您可以使用這些事件來瞭解可能會影響您帳戶的即將發生或排定的變更。例如， AWS Health 如果 AWS Identity and Access Management (IAM) 計劃棄用受管政策或計劃棄用受管 AWS Config 規則，則可以傳送事件。 AWS Health 也會在中發生服務可用性問題時傳送事件 AWS 區域。您可以檢閱事件說明以瞭解問題、識別任何受影響的資源，並採取任何建議的動作。

Health 事件有兩種類型：

內容

帳戶特定事件

帳戶特定事件是您 AWS 帳戶 或組織中帳戶的本機活動 AWS 。例如，如果您使用的區域中的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體類型發生問題，請 AWS Health 提供有關該事件的資訊以及受影響資源的名稱。

您可以從AWS Health 儀表板、AWS Health API 尋找帳戶特定事件，或使用 Amazon CloudWatch 事件接收通知。

公眾活動

公開事件是報告的服務事件並非特定於某個帳戶。例如，如果在美國東部 (俄亥俄) 區域發生 Amazon 簡單儲存服務 (Amazon S3) 的服務問題，即使您未使用該服務或該區域中有 S3 儲存貯體，也會 AWS Health 提供事件的相關資訊。我們建議您先檢閱公開通知，然後再對其採取行動。

您可以從 AWS Health 儀表板和儀表板 — 服務健康狀態找到公開事件。 AWS Health

如果您有帳戶，請參閱開始使用AWS Health儀表板 — 您的帳戶健康狀態。

如果您沒有帳戶，請參閱AWS Health 儀表板 — 服務健康狀。

AWS Health 儀表板

如果您有 AWS 帳戶，則 AWS Health 儀表板會同時顯示公開事件和帳戶特定事件。

我們建議您使用 AWS Health 儀表板來了解提供一般認知的事件，例如某個區域中某項服務即將發生的維護問題。您也可以使用 AWS Health 儀表板來瞭解可能直接影響您的事件，例如帳戶中已淘汰的資源。

您可以登入以檢視您的 AWS Health 儀表板， AWS Management Console 請至 https://health.aws.amazon.com/health/home。

如需詳細資訊，請參閱 開始使用AWS Health儀表板 — 您的帳戶健康狀態。

AWS Health 儀表板 — 服務健康狀

如果您沒有帳戶，可以使用 https://health.aws.amazon.com/health/status 的 AWS Health 儀表板 — 服務健康狀態來檢視公開活動。公開事件會回報服務問題 AWS ，提供有關服務可用性的資訊。該網站僅顯示公共事件，這些活動並不特定於任何帳戶。您無需登錄或擁有帳戶即可查看此頁面。

如需詳細資訊，請參閱 AWS Health 儀表板 — 服務健康狀。

事件類型代碼

Health 全狀況事件中顯示的事件類型代碼包括受影響的服務和事件類型。例如，如果您收到具有事件類型代碼的 Health 全狀況AWS_EC2_SYSTEM_MAINTENANCE_EVENT事件，這表示服務正在排程可能會影響您的維護事件。使用此資訊來提前計劃或為您的帳戶採取行動。

事件類別

所有 Health 事件都有相關聯的事件類型類別。對於某些事件，事件類型類別可能會出現在事件類型代碼中，例如程AWS_RDS_MAINTENANCE_SCHEDULED式碼。在此範例中，類別已排程。您可以使用此資訊來瞭解高層級的事件類別。

我們建議您監視所有事件類型類別。請注意，每個類別會針對不同類型的事件顯示。您也可以使用類DescribeEvent型 API 作業來尋找事件類型類別。

帳戶通知

這些事件提供有關您帳戶和服務的管理或安全性的資訊。這些事件可能會提供資訊豐富，或者可能需要您採取緊急行動。我們建議您注意這些類型的事件，並檢閱所有建議的動作。

以下是帳戶通知的事件類型代碼範例：

- AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION— 您擁有可能允許公開存取的 Amazon S3 儲存貯體。
- AWS_BILLING_SUSPENSION_NOTICE— 您的帳戶有未付費並已被暫停，或您停用了帳戶。
- AWS_WORKSPACES_OPERATIONAL_NOTIFICATION— Amazon 有一個服務問題 WorkSpaces。

問題

這些事件是會影響 AWS 服務或資源的未預期事件。此類別中的常見事件包括有關導致服務降級的操作問題的通訊，或是您感知的當地語系化資源層級問題。

以下是問題的事件類型代碼範例：

- AWS_EC2_OPERATIONAL_ISSUE— 服務的操作問題，例如服務使用延遲。
- AWS_EC2_API_ISSUE— 服務 API 的操作問題，例如 API 操作延遲增加。
- AWS_EBS_VOLUME_ATTACHMENT_ISSUE— 可能會影響您的 Amazon Elastic Block Store (Amazon EBS) 資源的本地化資源層級問題。
- AWS_ABUSE_PII_CONTENT_REMOVAL_REPORT— 此事件意味著如果您不採取行動，您的帳戶可能會被暫停。

排程變更

這些活動提供有關您的服務和資源即將發生變更的資訊。這些事件包括規劃的生命週期事件，例如不同版本的 end-of-support 通知和自動升級。某些事件可能會建議您採取行動以避免服務中斷，而其他事件則會自動發生，而您不會採取任何動作。在已排定變更活動期間，您的資源可能暫時無法使用。此類別中的所有事件都是帳戶特定事件。

以下是排程變更的事件類型代碼範例：

- `AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED`— Amazon EC2 實例需要重新啟動。
- `AWS_SAGEMAKER_SCHEDULED_MAINTENANCE`— SageMaker 需要維護事件，例如修復服務問題。
- `AWS_RDS_PLANNED_LIFECYCLE_EVENT`— Amazon RDS 正在排程規劃的生命週期事件，例如其中一個版本的 end-of-support 事件，需要客戶採取行動。

> **Tip**
>
> 如果您使用 AWS Health API 或 AWS Command Line Interface (AWS CLI) 傳回事件詳細資訊，則`Event`物件會包含具有`ACCOUNT_SPECIFIC`值的`eventScopeCode`欄位。如需詳細資訊，請參閱 AWS Health API 參考。

事件狀態

事件狀態會告訴您「Health」事件是開啟、關閉或即將進行的。您可以在 AWS Health 儀表板或 AWS Health API 中檢視最多 90 天的 Health 事件。

受影響的實體

受影響的實體是可能受到事件影響的 AWS 資源。例如，如果您收到針對帳戶中使用的特定執行個體類型的 Amazon EC2 維護排程事件，則可以使用運作 Health 態事件來判斷受影響執行個體的 ID。使用此資訊來解決任何潛在的服務問題，例如建立或淘汰資源。

AWS Health Amazon 上的事件 EventBridge

您可以為帳戶設定 Amazon EventBridge 規則，以便在帳戶收到適當的 AWS Health 事件後自動執行動作。這些動作可以是一般動作，例如將所有規劃的生命週期事件訊息傳送至聊天介面。或者，它們可以是特定動作，例如在 IT 服務管理工具中觸發工作流程。

如需詳細資訊，請參閱 使用 Amazon 監控 AWS Health 事件 EventBridge。

AWS Health API

您可以使用 AWS Health API 以程式設計方式存取顯示在AWS Health 儀表板中的資訊，如下所示：

- 取得可能影響您 AWS 服務和資源之事件的相關資訊
- 啟用或停用組織的 AWS 組織檢視功能
- 依特定服務、事件類型類別和事件類型代碼篩選您的事件

如需詳細資訊，請參閱 AWS Health API 參考。

> **Note**
>
> AWS Support若要使用 AWS Health API，您必須擁有商業、企業級支援或企業支援方案。如果您從沒有商務、企業版升級或企業 Support 方案的帳戶呼叫 AWS Health API，您會收到`SubscriptionRequiredException`錯誤訊息。

組織檢視

您可以使用此功能，將您 AWS 帳戶的所有健全狀況事件彙總 AWS Organizations 到 AWS Health 儀表板中的單一檢視中。然後，您可以登入組織的管理帳戶，或使用 AWS Health API 來檢視可能會影響不同帳戶和資源的所有事件。您可以從 AWS Health 主控台或 API 啟用此功能。如需更多詳細資訊，請參閱 使用組織檢視跨帳戶彙總 AWS Health 事件。

AWS Health 儀表板 — 服務健康狀

您可以使用 AWS Health 儀表板 — 服務健康狀態來檢視所有的健全狀況 AWS 服務。此頁面顯示所有服務的報告服務事件 AWS 區域。您不需要登入或存取 [AWS Health 儀表板 — 服務健康狀態] 頁面。AWS 帳戶

> **Tip**
>
> 本網站僅顯示公共事件，這些活動並不特定於 AWS 帳戶. 如果您已經有帳戶，我們建議您登入以檢視 AWS Health 控制面板，並隨時瞭解可能會影響您帳戶和服務的事件。如需詳細資訊，請參閱 開始使用AWS Health儀表板 — 您的帳戶健康狀態。

若要檢視 AWS Health 儀表板 — 服務健康狀態

1. 導航到 https://health.aws.amazon.com/health/status 頁面。

   > **Note**
   >
   > 如果您已經登錄到您的頁面 AWS 帳戶，您將被重定向到AWS Health 儀表板-您的帳戶健康狀態頁面。

2. 在 [服務健全狀況] 下，選擇 [開啟和最近的問題] 以檢視最近報告的 您可以檢視有關事件的下列資訊：

   - 事件名稱和受影響的地區。例如，操作問題 — Amazon 彈性運算雲端 (維吉尼亞北部)
   - 服務名稱
   - 事件的嚴重性，例如資訊或降級
   - 活動最近更新的時間表
   - 也受此事件影響的清單 AWS 服務

   > **Note**
   >
   > 您可以在當地時區或 UTC 中檢視事件。如需詳細資訊，請參閱時區設定。

3. (選擇性) 在事件旁邊，選擇 RSS 以訂閱此事件的 RSS 摘要。您將在指定的中收到有關此特定服務的通知 AWS 區域。

4. 選擇服務歷史記錄以檢視「服務歷史記錄」表格 此表格顯示過去 12 個月的所有 AWS 服務 中斷。

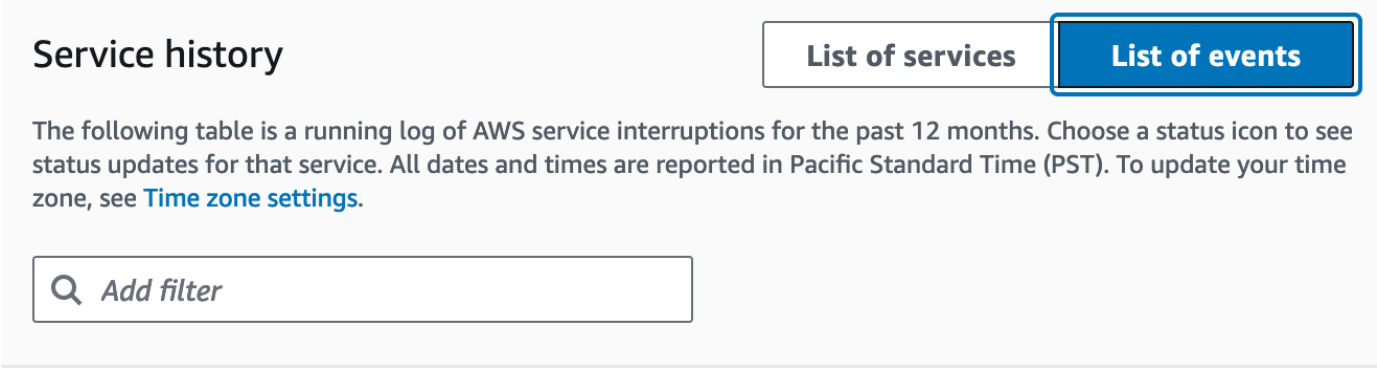
> **Tip**
>
> 您可以依「服務」AWS 區域、和「日期」進行篩選。

5. 在進行中的服務事件旁，選擇狀態圖示

( )

以檢視有關該事件的詳細資訊。

6. (選擇性) 若要將其檢視為歷史事件清單，請選擇事件清單按鈕。選擇事件欄中的任何事件，即可在彈出式側邊面板中檢視該特定事件的詳細資訊。



> **Note**
>
> 選取 2023 年 9 月之後的任何公開活動，瀏覽器中會以該公開 AWS Health 事件的連結填入 URL。選取此連結之後，您可以瀏覽至具有該事件快顯視窗的事件清單檢視。

7. (選擇性) 選擇 RSS 來訂閱 RSS 摘要。您將在指定的中收到有關此特定服務的通知 AWS 區域。
8. (選擇性) 您可以檢視當地時區或 UTC 的事件。如需詳細資訊，請參閱 時區設定。
9. (選擇性) 如果您有帳戶，請選擇 [開啟帳戶健康狀況] 以登入。登入後，您可以檢視您帳戶的特定事件。如需更多詳細資訊，請參閱 開始使用AWS Health儀表板 — 您的帳戶健康狀態。

計劃的生命週期事件 AWS Health

瞭解的規劃生命週期事件 AWS Health。

主題

什麼是計劃的生命週期事件？

AWS Health 傳達可能會影響應用程式可用性的重要變更。在 AWS 共同的責任模型中， AWS 採取行動，將支援資源的基礎硬體和基礎結構保持在最新狀態且安全。但是，某些變更需要客戶採取行動或協調，才能避免對應用程式造成影響。 AWS Health 提前通知您重要更改，例如：

- 開放原始碼軟體終止支援-有些 AWS 服務 執行軟體的開放原始碼版本。如果開放原始碼社群終止對軟體版本的支援，請在需要採取行動升級時通 AWS 知您，並避免對應用程式造成影響。
  - Amazon RDS for MySQL 適用於 MySQL 的引擎版本終止支持
  - Amazon EKS 版本終止支持
- 影響可能需要執行動作的 AWS擁有資源的變更。
  - Amazon RDS 證書頒發機構證書到期。
  - Amazon WorkDocs 伴侶已經到了生命的盡頭，不再可用。

  > **Note**
  >
  > 符合此條件的所有通知都會報告 AWS Health 為「計劃的生命週期事件」。

- 動態資源燃盡和改進的中繼資料：從您收到通知到事件生命週期開始，受影響的資源就會與 AWS Health 事件相關聯，作為具有特定實體狀 AWS Health 態的受影響實體。受影響的資源會在適用的情況下以 ARN 格式指定。如果您受影響的資源需要客戶動作，則會以「待處理」狀態列出。如果受影響的資源執行了必要的動作或已刪除資源，則狀態會更新為「已解決」。

> **Note**
>
> - 資源狀態更新會以非同步且定期的方式執行，在極少數情況下，最多可延遲 72 小時。
> - 在未提供動態更新 (而非具有「擱置中」或「已解決」狀態的資源) 的例外狀況中，資源將不會指定任何狀態。
> - AWS GovCloud (US) 和中國區域不支援資源狀態更新。

當我收到規劃的生命週期事件通知時，我應該期待什麼？

規劃生命週期活動的 AWS Health 體驗可協助您的團隊瞭解即將到來的生命週期變更，並追蹤動作完成

類型分類:預定變更

事件類型代碼： AWS_ {服務} _ 計劃生命週期 _ 事件

事件開始時間：事件開始時間是指資源受到變更影響的最快日期。

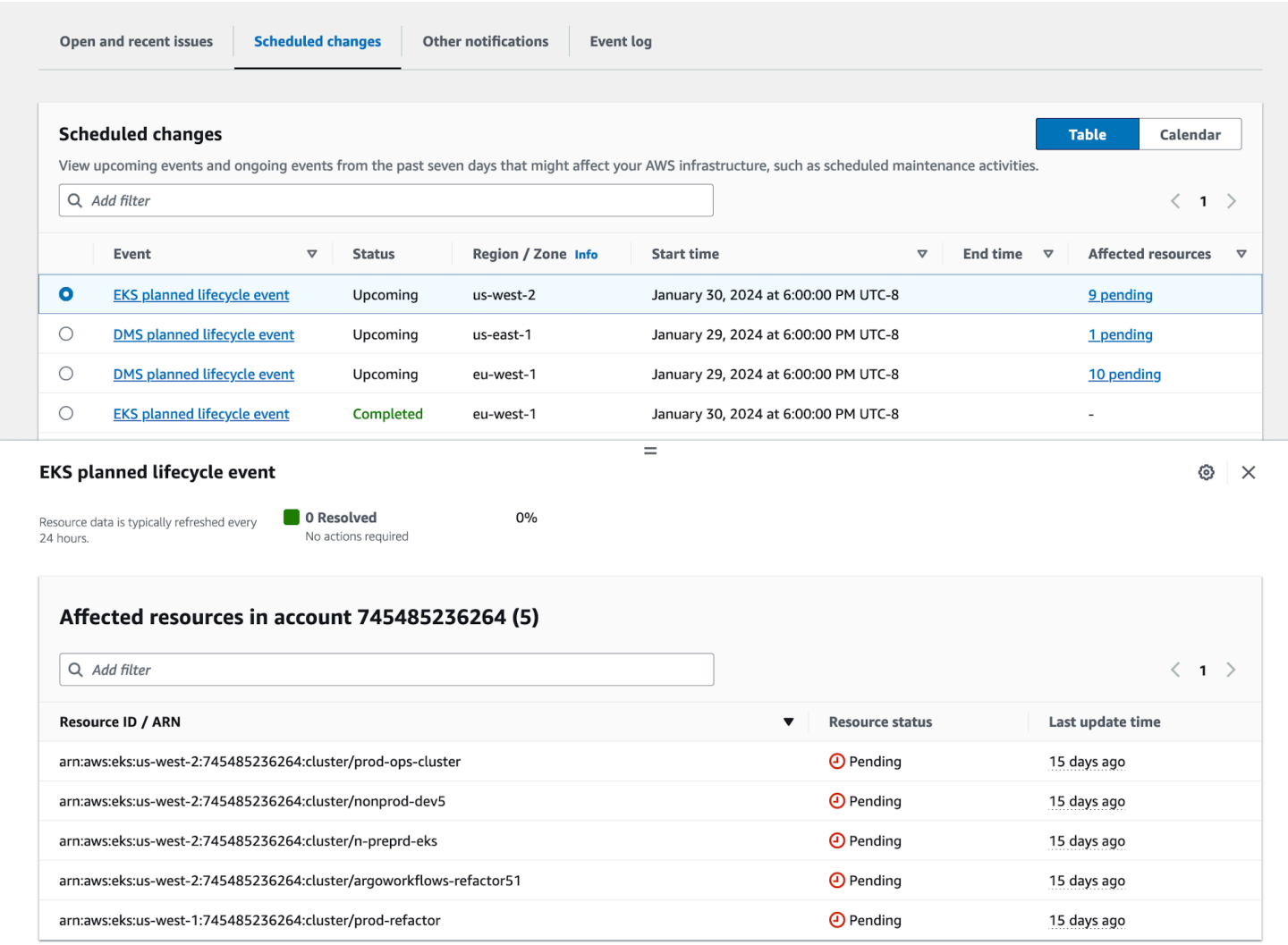
事件結束時間：事件結束時間是指在所有 AWS 資源中完成變更的日期。請注意，並不總是指定結束時間。將開始時間視為變更日期非常重要。

> **Note**
>
> 組 Organizations 可以預期會針對每個受影響資源的區域分組的計劃生命週期事件，收到單一事件 ARN。但是，如果組織有大量受影響 AWS 帳戶 或資源，他們可能會收到多個 ARN。

提早掌握已規劃的生命週期事件：規劃的生命週期事件設計為主要版本/變更的最短前置時間為 180 天，在可能的情況下，次要版本/變更的前置時間至少為 90 天。

動態資源燃盡和改進的中繼資料：從您收到通知到事件生命週期開始，受影響的資源就會與 AWS Health 事件相關聯，作為具有特定實體狀 AWS Health 態的受影響實體。受影響的資源會在適用的情況下以 ARN 格式指定。如果您受影響的資源需要客戶動作，則會以「待處理」狀態列出。如果受影響的資源執行了必要的動作或已刪除資源，則狀態會更新為「已解決」。

> **Note**
>
> - AWS Health 通知會在可能的情況下提供一段時間內的狀態更新， AWS GovCloud (US) 和中國地區除外。
> - 資源狀態更新會以非同步且定期的方式執行，在極少數情況下，最多可延遲 72 小時。

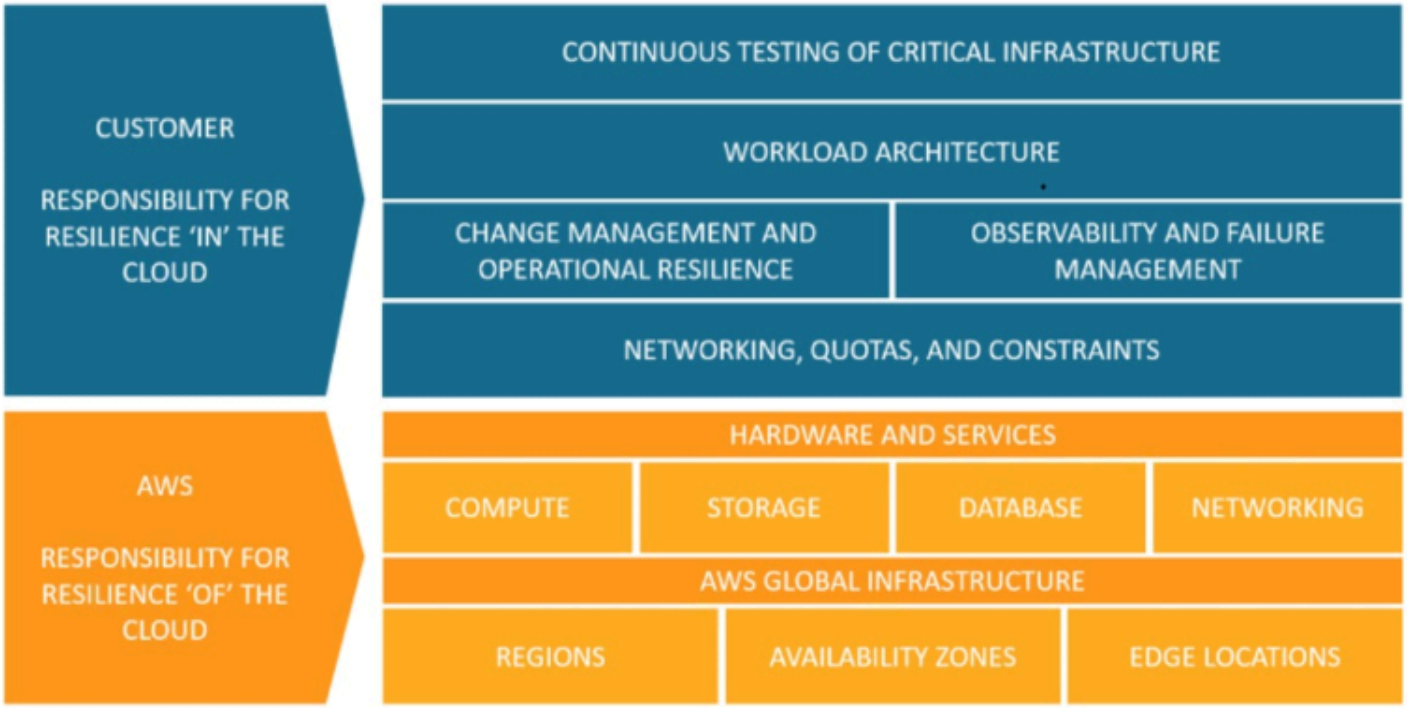


在計劃的活動日期過後：

1. 如果適用，服務可能會在事件開始日期之後的任何時間對您的資源實施所描述的變更。
2. 如果您在支援日期結束之前解決所有資源，則您的 AWS Health 事件狀態會變更為「已關閉」。
3. 如果您在尚未解決的日期之後有未完成的資源，則 AWS Health 事件會在開始或結束日期後 90 天內保持開啟狀態。然後該事件被刪除。

復原力的共同責任模式

安全性和合規性是與客戶之間 AWS 的共同責任。視部署的服務而定，此共用模型可協助減輕客戶的營運負擔。這是因為 AWS 操作、管理和控制元件，從主機作業系統和虛擬化層到服務運作所在設施的實體安全性。除了 AWS提供之安全性群組防火牆的設定外，客戶還需負責管理客體作業系統 (包括更新和安全性修補程式) 及其他相關應用程式軟體。如需詳細資訊，請參閱共同責任模式。



存取規劃的生命週期

規劃的生命週期事件可以使用多個通道存取和監視：

- 使用 Amazon EventBridge
- 使用 AWS Health 儀表板
  - 行事曆檢視
  - 受影響資源檢視
- 使用 AWS Health API

開始使用AWS Health儀表板 — 您的帳戶健康狀態

您可以使用AWS Health儀表板瞭解AWS Health事件。這些事件可能會影響您的AWS 服務或AWS 帳戶. 登入帳戶後，AWS Health儀表板會以下列方式顯示資訊：

- 您的帳戶事件 — 此頁面顯示您帳戶的特定事件。您可以檢視開啟、最近變更和排程的變更。您也可以檢視通知以及顯示過去 90 天內所有事件的事件記錄。
- 您的組織事件 — 此頁面顯示中組織特定的事件AWS Organizations。您可以檢視組織的開啟、最近和排定的變更。您也可以檢視通知，以及顯示過去 90 天內所有組織事件的事件日誌。

> **Note**
>
> 如果您沒有AWS 帳戶，可以使用AWS Health 儀表板 — 服務健康狀來瞭解一般服務可用性。如果您有帳戶，建議您登入AWS Health儀表板，以深入瞭解可能會影響您的服務和資源的事件和即將發生的變更。

內容

在AWS Health儀表板中查看您的帳戶事件

您可以登錄到您的帳戶以獲取個性化的活動和推薦。

在AWS Health儀表板中檢視帳戶事件

1. 在以下位置打開您的AWS Health儀表板。 https://health.aws.amazon.com/health/home
2. 在功能窗格中，針對 [您的帳戶健全狀況]，您可以選擇下列選項：
   a. 未決和最近的問題 — 檢視最近開啟和關閉的事件。
   b. 排程變更 — 檢視可能會影響您服務和資源的即將發生的事件。
   c. 其他通知 — 查看過去七天內可能影響您帳戶的所有其他通知和進行中事件。
   d. 事件記錄 — 檢視過去 90 天的所有事件。

開放和最近的問題

使用 [開啟和最近的問題] 索引標籤，檢視過去 7 天內可能會影響您帳戶的所有進行中事件。

當您從儀表板中選擇事件時，「詳細資料」窗格會出現，其中包含有關該事件的資訊以及受影響資源的清單。如需詳細資訊，請參閱事件詳細資訊。

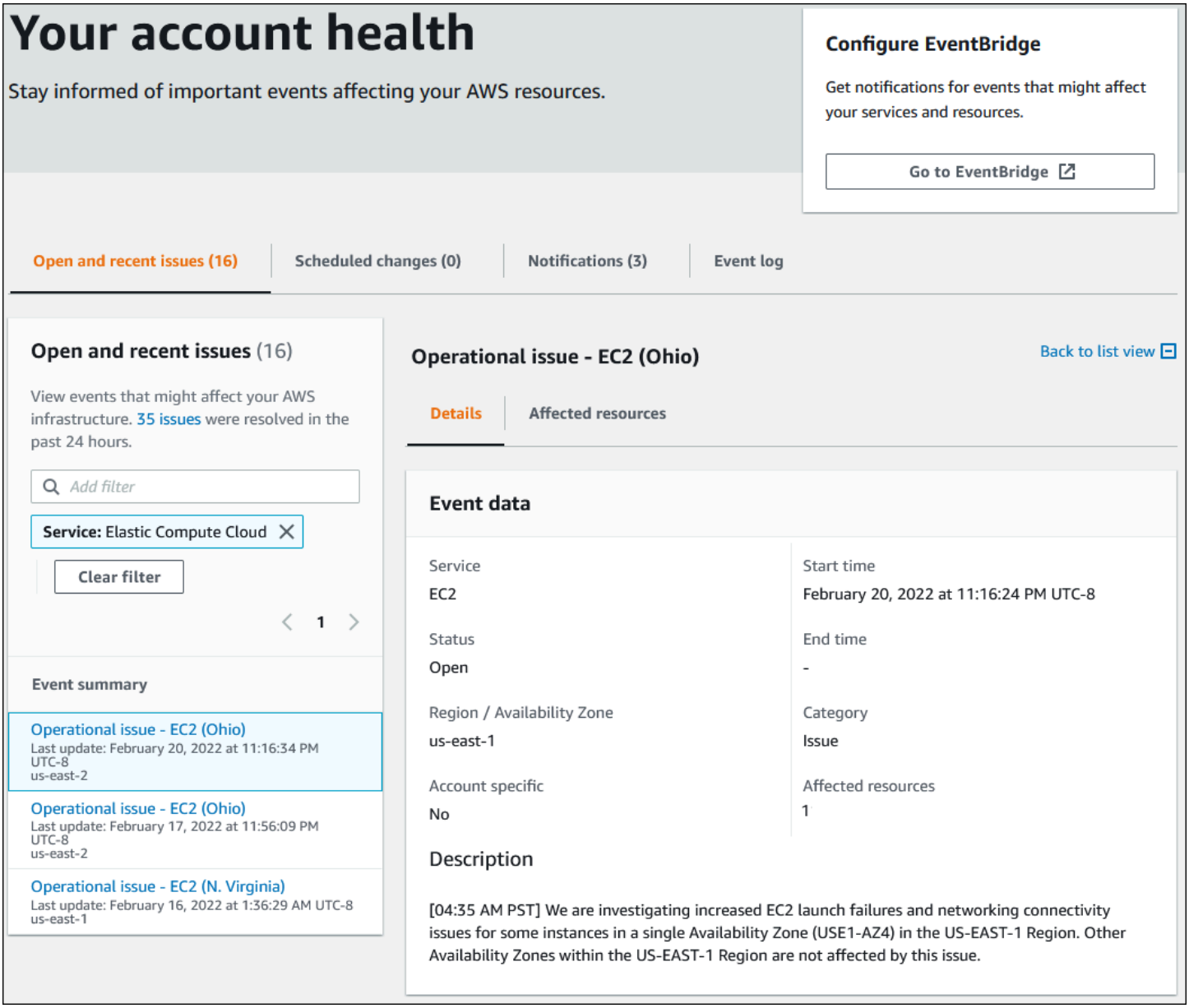
您可以從篩選清單中選擇選項，來篩選出現在任何索引標籤中的事件。例如，您可以依可用區域、區域、事件結束時間或上次更新時間等AWS 服務來縮小結果範圍。

若要查看所有事件，而不是顯示在儀表板中的最近事件，請選擇事件日誌索引標籤。

> **Note**
>
> 目前，您無法刪除AWS Health控制面板中顯示之事件的通知。AWS 服務解決事件後，通知便會從儀表板檢視中移除。

Example ：亞馬遜彈性運算雲端 (Amazon EC2) 的操作問題事件

下圖顯示 Amazon EC2 執行個體的啟動失敗和連線問題的事件。



排程變更

使用 [排程變更] 索引標籤來檢視可能會影響您帳戶的即將發生的事件 這些事件可以包括服務的排程維護活動，以及需要採取行動才能解決的計劃生命週期事件 為了協助您規劃這些活動，系統會提供行事曆檢視，讓您可以將這些排定的變更對應至每月行事曆。過濾器可用。如需計劃生命週期事件的詳細資訊，請參閱計劃的生命週期事件 AWS Health。

其他通知

使用 [通知] 索引標籤可檢視過去七天內可能影響您帳戶的所有其他通知和進行中事件。這可能包括事件，例如憑證輪換、帳單通知和安全性弱點。

事件日誌

使用 [事件記錄] 索引標籤可檢視所有AWS Health事件。記錄表格包含其他欄，因此您可以依「狀態」和「開始時間」進行篩選。

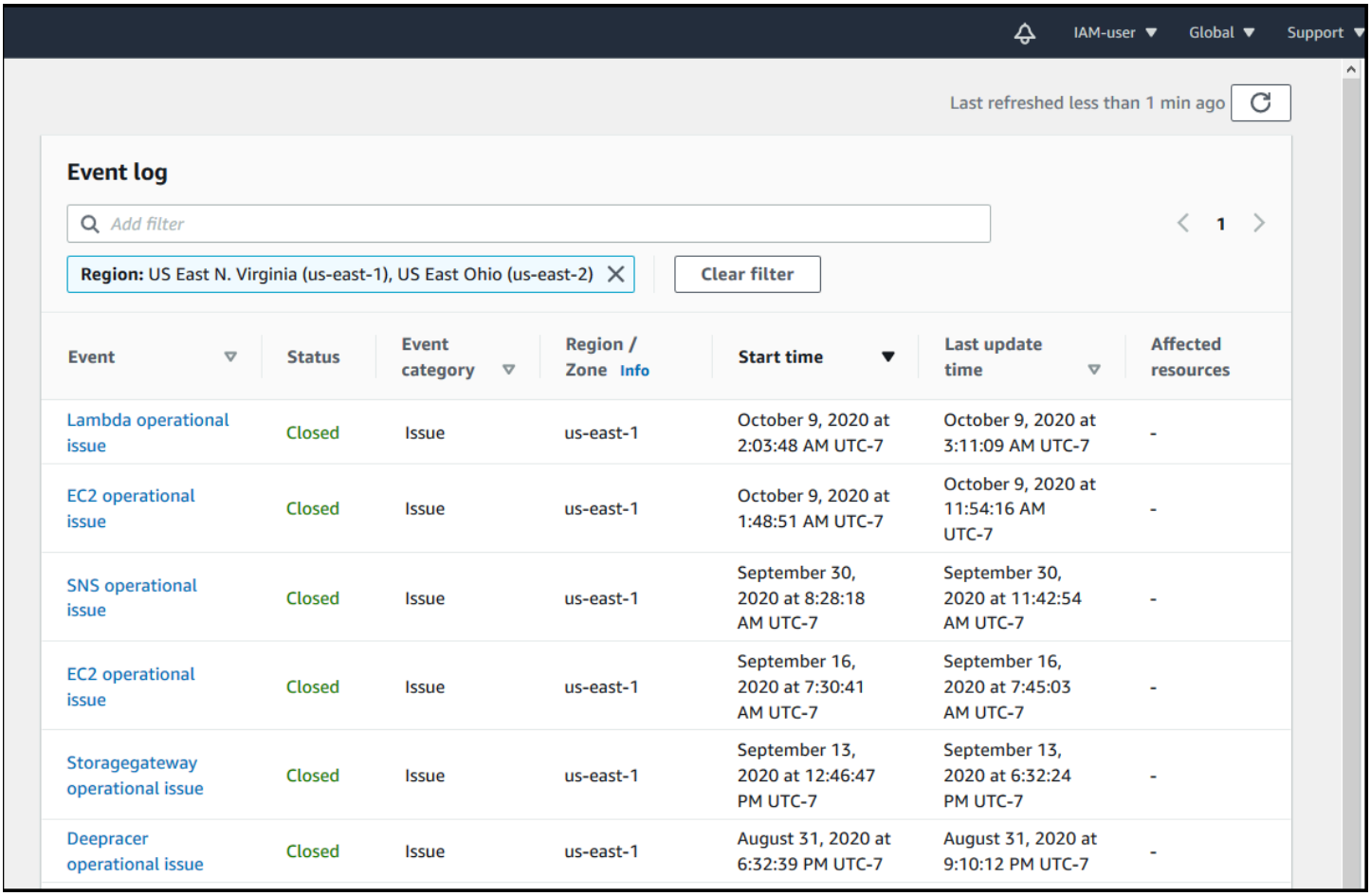
當您在 [事件記錄] 表格中選擇事件時，[詳細資料] 窗格隨即出現，其中包含事件的相關資訊以及受影響的資源清單。如需詳細資訊，請參閱事件詳細資訊。

您可以選擇下列篩選選項來縮小結果範圍：

- 可用區域
- 結束時間
- 事件
- 活動 ARN
- 事件類別
- 上次更新時間
- 區域
- 資源識別碼
- 服務
- 開始時間
- 狀態

Example ：事件記錄

下圖顯示美國東部 (維吉尼亞北部) 和美國東部 (俄亥俄) 區域近期的事件。



事件詳細資訊

當您選擇事件時，會出現兩個有關該事件的索引標籤。「詳細資訊」標籤會顯示下列資訊：

- 服務
- 狀態
- 區域/可用區域
- 活動是否為帳戶特定
- 開始和結束時間
- 類別
- 受影響資源的數量
- 描述和有關事件的更新時間表

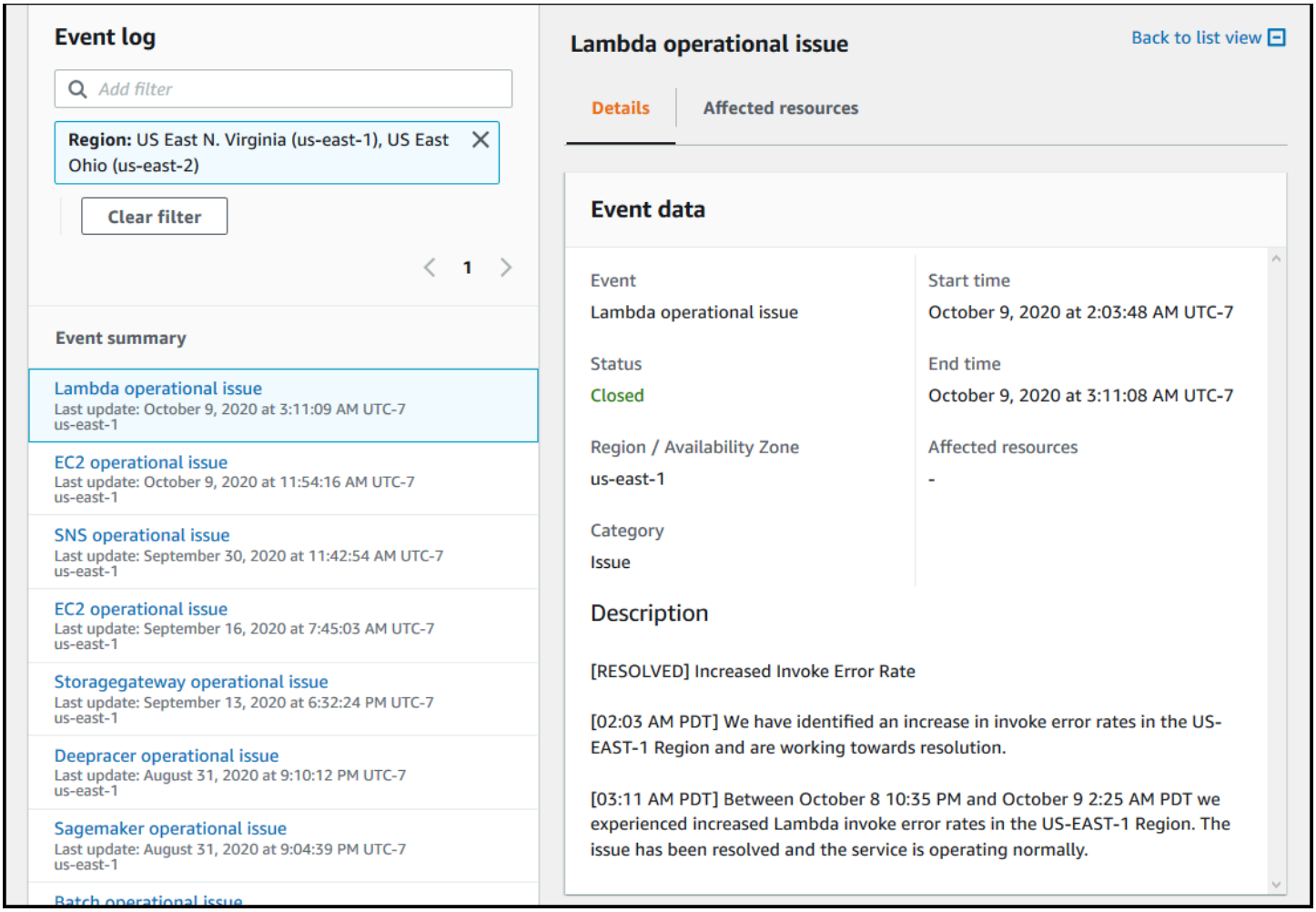
[受影響的資源] 索引標籤會顯示有關受事件影響之任何AWS資源的下列資訊：

- 資源識別碼 (例如，Amazon EBS 磁碟區識別碼，例如`vol-a1b2c34f`) 或亞馬遜資源名稱 (ARN) (如果可用或相關)。
- 對於規劃的生命週期事件，此受影響的資源清單也包含資源的最新狀態 (「擱置中」、「未知」或「已解決」。此清單通常每 24 小時重新整理一次。

您可以篩選出現在資源中的項目。您可以依資源 ID 或 ARN 來縮小結果範圍。

Example : AWS Health 事件 AWS Lambda

下列螢幕擷取畫面顯示 Lambda 的範例事件。



事件類型

AWS Health 事件有兩種類型：

- 公開事件是不特定於帳戶的服務事件。例如，如果中的 Amazon EC2 發生問題AWS 區域，即使您未使用該區域的服務或資源，也會AWS Health提供有關該事件的資訊。
- 帳戶特定事件專屬於您的帳戶或組織中的帳戶。例如，如果您使用的區域中的 Amazon EC2 執行個體發生問題，請AWS Health提供有關該事件的資訊以及受影響的 Amazon EC2 執行個體清單。

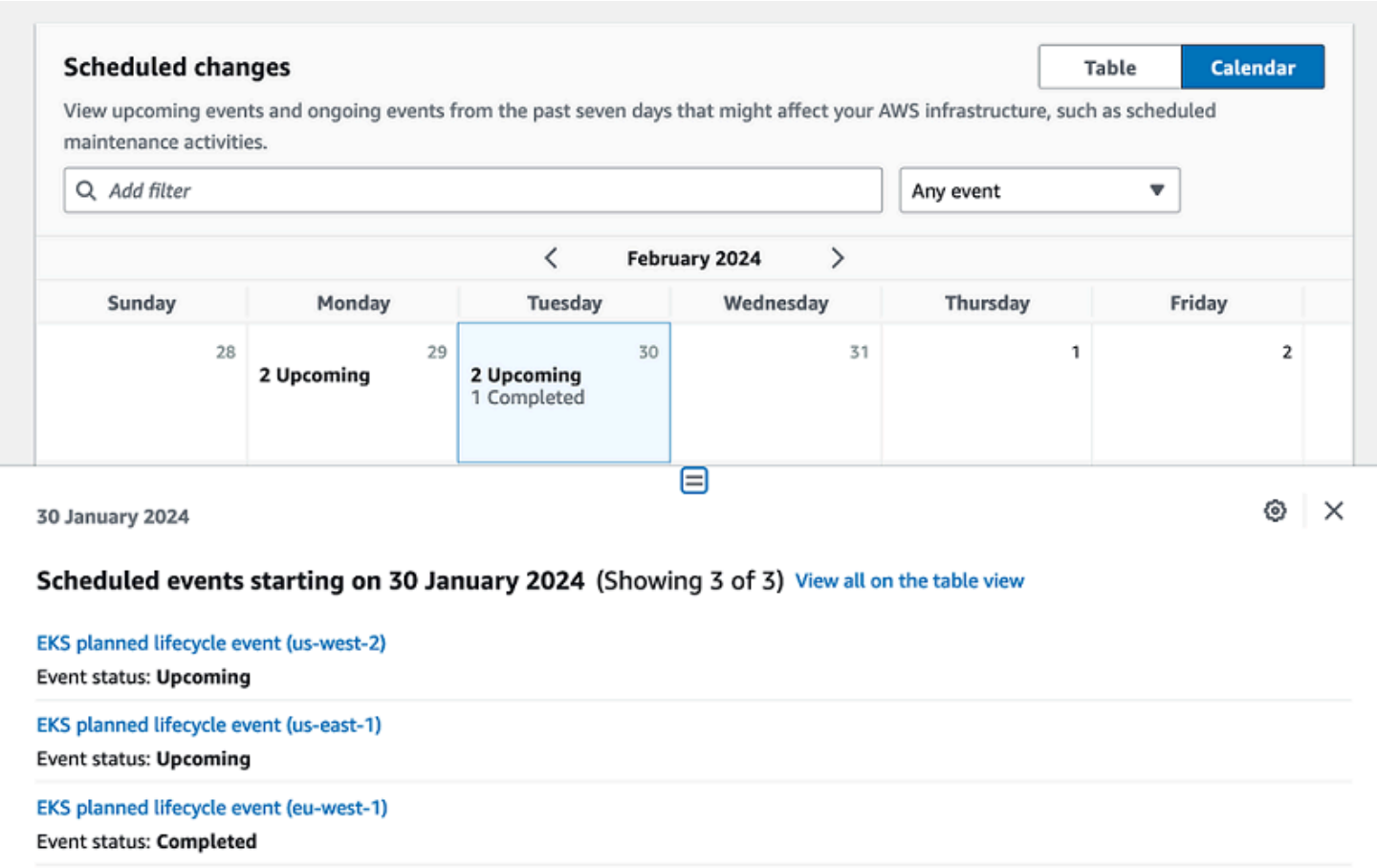
您可以使用下列選項來識別事件是公開事件還是帳戶特定：

- 在 [AWS Health儀表板] 中，選擇事件的 [受影響的資源] 索引標籤。具備資源的事件係專屬於您的帳戶。不具資源的事件為公開的，並非專屬於您的帳戶。如需詳細資訊，請參閱開始使用AWS Health儀表板 — 您的帳戶健康狀態。
- 使用 AWS Health API 傳回 `eventScopeCode` 參數。事件可具備 `PUBLIC`、`ACCOUNT_SPECIFIC` 或 `NONE` 值。如需詳細資訊，請參閱 AWS HealthAPI 參考中的DescribeEventDetails作業。

行事曆檢視

[行事曆] 檢視可在 [排程變更] 索引標籤中使用，以將AWS Health事件專案至月行事曆。此檢視可讓您查看過去 3 個月以及 future 一年的排程變更。

AWS Health事件按日期顯示。選取日期以顯示包含AWS Health事件詳細資訊的側邊面板。即將發生和正在進行的事件以黑色顯示。已完成的事件會以灰色顯示。如果一個日期中有兩個以上的事件，則只會顯示黑色和灰色事件的數量。選取日期以在側邊面板中顯示AWS Health事件清單。您可以在側邊面板中選擇一個事件，以顯示有關該事件的信息。側面板具有導航到早期視圖的麵包屑。

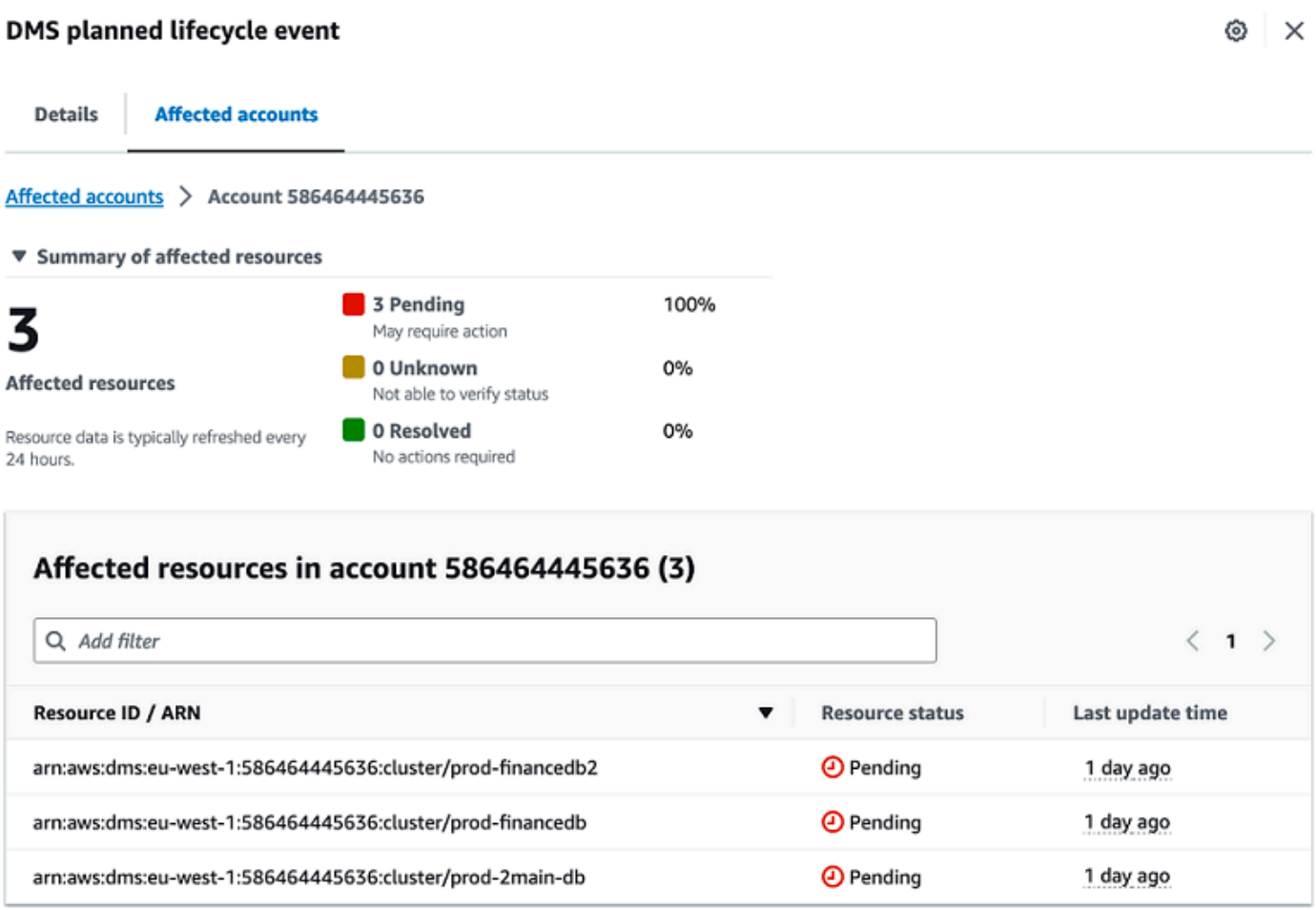


受影響資源檢視

對於規劃的生命週期事AWS Health件，事件通常會提供受影響資源狀態的每日更新。若要檢視狀態，請選取AWS Health事件。狀態會顯示在側邊面板的受影響資源標籤中。

帳號層級AWS Health事件會在 [受影響的資源] 索引標籤頂端顯示受影響資源狀態的摘要。受影響資源的清單會顯示在表格中，以及對應的狀態。規劃的生命週期事件是使用資源狀態欄位的事件類型範例。若要深入瞭解已規劃的生命週期事件，請參閱計劃的生命週期事件 AWS Health。

如果存取組織檢視，AWS Health事件會顯示所有包含帳號之所有受影響資源的狀態摘要。摘要之後是受影響帳號的清單，以及該帳號的擱置資源數目。選取要顯示帳號檢視彙總的帳號或暫緩資源數目。帳戶檢視摘要包含可導覽回受影響帳戶的組織清單。分割面板頂端會顯示受影響資源狀態的摘要。



時區設定

您可以在AWS Health儀表板中以當地時區或 UTC 檢視事件。如果您變更儀表板中的時區，AWS Health儀表板和公開事件中的所有時間戳記都會更新為您指定的時區。

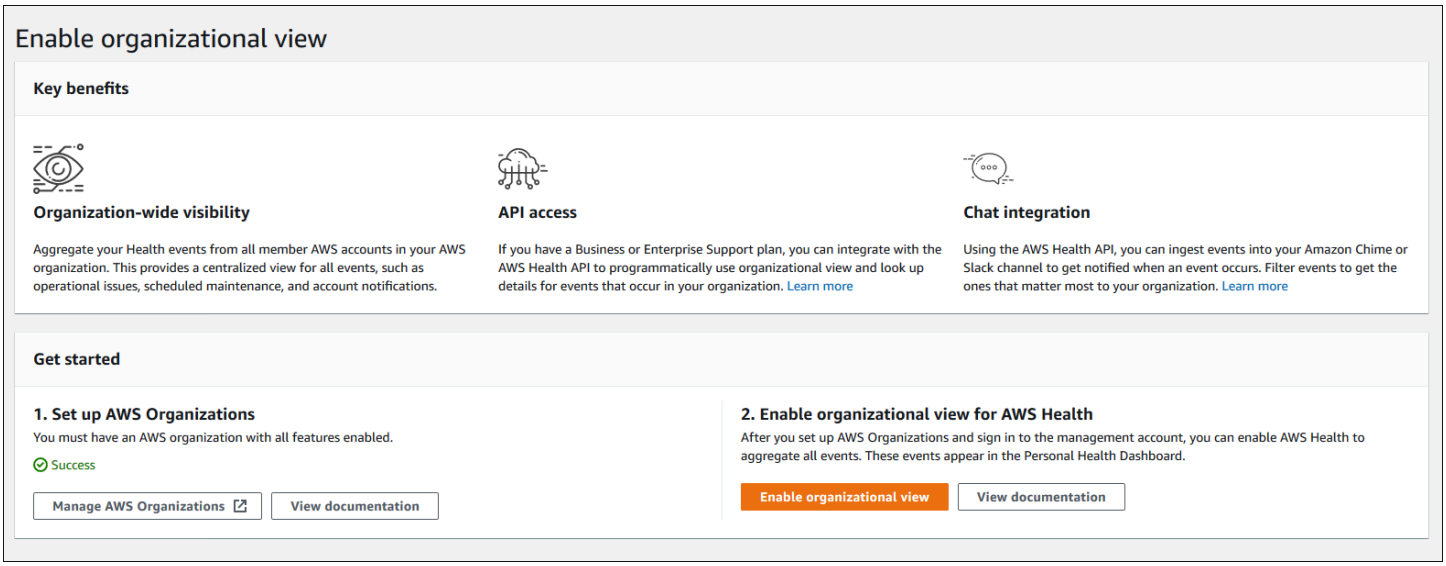
更新您的時區設定

1. 在以下位置打開您的AWS Health儀表板。 https://health.aws.amazon.com/health/home
2. 在頁面底部，選擇 Cookie 偏好設定。
3. 對於功能性餅乾選擇允許。然後選擇儲存偏好設定。
4. 在AWS Health儀表板的導覽窗格中，選擇 [時區設定]。
5. 選取AWS Health儀表板工作階段的時區。接著選擇 Save changes (儲存變更)。

您的組織健康

AWS Health與整合，以AWS Organizations便您可以檢視屬於組織中所有帳戶的事件。這可讓您集中檢視出現在組織中的事件。您可以使用這些事件來監控資源、服務和應用程式的變更。

如需詳細資訊，請參閱使用組織檢視跨帳戶彙總 AWS Health 事件。



配置亞馬遜 EventBridge

用 EventBridge 於偵測AWS Health事件的變更並做出反應。您可以監控帳戶中發生的特定AWS Health事件，然後設定規則，以便在事件變更時AWS Health通知您或採取行動。

EventBridge 搭配使用 AWS Health

1. 在以下位置打開您的AWS Health儀表板。 https://health.aws.amazon.com/health/home
2. 若要導覽至主 EventBridge 控台以建立規則，請執行下列其中一個動作：
   - 從導覽窗格的 Health 整合下，選擇 Amazon EventBridge。
   - 在「設定」下 EventBridge，選擇「移至」 EventBridge。
3. 請遵循此程序來建立規則並監視事件。請參閱 使用 Amazon 監控 AWS Health 事件 EventBridge。

AWS Health知道

您可以使用 A AWS Healthware 開始使用 AWS Health API，這是一種低成本的應用程式，可用來將健康事件傳送至 Slack、JIRA ServiceNow 等。免費直播網絡研討會現已提供。

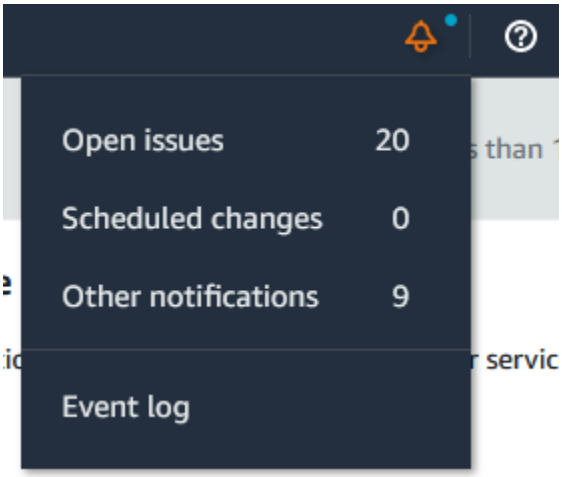
AWS Health 事件的警示

您的AWS Health儀表板在控制台導航欄中有一個帶有警報菜單的鈴鐺圖標。此功能會顯示每個類別中顯示在儀表板上的最近 AWS Health 事件數目。此鈴鐺圖示會出現在多個AWS主控台上，例如 Amazon EC2、Amazon Relational Database Service 服務 AWS Identity and Access Management (Amazon RDS)、(IAM) 和AWS Trusted Advisor。

選擇鈴鐺圖示，查看最近發生的事件是否會影響您的帳戶。然後，您可以選擇一個事件以導航到AWS Health儀表板以獲取更多信息。

Example : 開放活動

下圖顯示帳戶的開啟和通知事件。



配置AWS的使用者通知AWS Health

AWS Health提供服務作業的相關資訊，例如作業問題、計劃維護，以及規劃好的軟體生命週期事件。對於全面的可見性AWS Health事件詳細資料，例如受影響的資源 ID、目前狀態 (開啟或關閉) 以及資源狀態，最佳作法是使用AWS Health端點，例如AWS HealthAPI，亞馬遜的健康來源 EventBridge，以及AWS Health儀表板。這些端點提供有關可能影響工作負載的進行中事件和變更的最詳細且即時的資訊。

AWS使用者通知通過其他 UX 渠道（電子郵件，聊天或推送通知AWS控制台移動應用程序）。AWS Health事件通知包含的詳細資料不如上面列出的端點；但是，它們提供了一種簡單有效的方法來通知利益相關者問題和變更。根據您建立的規則，「使用者通知」會在事件符合您在規則中指定的值時建立並傳送通知。您可以選擇將通知發送到哪些 UX 交付渠道，並設置聚合以減少針對特定事件生成的通知數量。通知也會顯示在「主控台通知中心」中。例如，如果您有資源，您可以接收聊天通知AWS排程進行更新的帳戶，例如亞馬遜彈性運算雲端 (Amazon EC2) 執行個體。

進一步了解設定AWS使用者通知，請參閱開始使用AWS使用者通知。

存取 AWS Health API

AWS Health是使用 HTTPS 作為傳輸和 JSON 作為消息序列化格式的 RESTful Web 服務。您的應用程式程式碼能夠直接向 AWS Health API 發出請求。直接使用 REST API 時，您必須編寫必要的程式碼，以簽署和驗證您的請求。如需AWS Health作業和參數的詳細資訊，請參閱《AWS HealthAPI 參考》。

> **Note**
>
> 您必須訂閱商業、Enterprise On-Ramp 或企業 Support 計劃AWS Support才能使用AWS Health API。如果您從沒有商業、Enterprise On-Ramp 或企業 Support 計劃的AWS帳戶呼叫 AWS Health API，您會收到`SubscriptionRequiredException`錯誤。

您可以使用AWS SDK 來包裝AWS Health REST API 呼叫，以簡化應用程式開發作業。您可以指定您的AWS憑據，這些庫會為您處理身份驗證和請求簽名。

AWS Health也會在中提供AWS Health儀表板AWS Management Console，讓您用來檢視和搜尋事件和受影響的實體。請參閱 開始使用AWS Health儀表板 — 您的帳戶健康狀態。

端點

AWS HealthAPI 遵循多區域應用程式架構，並在主動-被動組態中具有兩個地區端點。若要支援主動-被動 DNS 容錯移轉，請AWS Health提供單一的全域端點。您可以在全域端點上執行 DNS 查閱，以判斷作用中端點和對應的簽署AWS區域。這有助於您知道程式碼中要使用哪個端點，以便從AWS Health.

向全域端點提出要求時，您必須指定對目標的地區端點的AWS存取認證，並為您的區域設定簽署。否則，您的驗證可能會失敗。如需詳細資訊，請參閱簽署 AWS Health API 請求。

下表代表預設組態。

描述	簽署區域	端點	通訊協定
作用中	us-east-1	健康 .1. amazonaws .com	HTTPS
被動	us-east-2	健康 .1.	HTTPS

描述	簽署區域	端點	通訊協定
全球服務	us-east-1 **Note** 這是目前作用中端點的簽署區域。	全球健康. 亞馬遜	HTTPS

若要判斷端點是否為作用中端點，請在全域端點 CNAME 上執行 DNS 查閱，然後從解析的名稱擷取該AWS區域。

Example ：全域端點上的 DNS 查詢

下列命令會完成在然後，命令會傳回 US-東-1 區域端點。此輸出告訴您應該使用哪個端點AWS Health。

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

Tip

主動端點和被動端點都會傳回AWS Health資料。不過，最新AWS Health資料只能從作用中端點取得。來自被動端點的資料最終會與主動端點一致。建議您在作用中端點變更時重新啟動任何工作流程。

使用高可用性端點示範

在下列程式碼範例中，AWS Health使用 DNS 查閱對全域端點來判斷作用中的地區端點和簽署區域。然後，如果作用中端點變更，程式碼會重新啟動工作流程。

主題

- 使用
- 使用 Python

使用

先決條件

您必須安裝搖籃。

若要使用 Java 範例

1. 從下載AWS Health高可用性端點示範 GitHub。
2. 導覽至示範專案high-availability-endpoint/java目錄。
3. 在命令行視窗中，請輸入下列命令。

```
gradle build
```

4. 輸入下列命令以指定您的AWS憑證。

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

5. 輸入下列命令來執行示範。

```
gradle run
```

Example ：AWS Health事件輸出

程式碼範例會傳回您AWS帳戶中過去七天內最近發生的AWS Health事件。在下列範例中，輸出包含AWS Config服務的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 資源

- 有關更多信息，請參閱 AWS SDK for JavaAPI 參考 HealthClient中的接口和源代碼。
- 如需此示範中針對 DNS 查閱所使用之程式庫的詳細資訊，請參閱中的 dnsjava GitHub。

使用 Python

先決條件

您必須安裝蟒 3。

若要使用 Python 範例

1. 從下載AWS Health高可用性端點示範 GitHub。
2. 導覽至示範專案high-availability-endpoint/python目錄。
3. 在命令行視窗中，請輸入下列命令。

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

> **Note**
>
> 對於 Python 3.3 及更高版本，您可以使用內置venv模塊創建虛擬環境，而不是安裝virtualenv。如需詳細資訊，請參閱 venv-在 Python 網站上建立虛擬環境。
>
> ```
> python3 -m venv v-aws-health-env
> ```

4. 輸入下列命令以啟動虛擬環境。

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

5. 輸入下列命令以安裝相依性。

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

6. 輸入下列命令以指定您的AWS憑證。

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

7. 輸入下列命令來執行示範。

```
python3 main.py
```

Example ：AWS Health事件輸出

程式碼範例會傳回您AWS帳戶中過去七天內最近發生的AWS Health事件。下列輸出會傳回安AWS全性通知的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. 完成後，請輸入下列命令以停用虛擬機器。

```
deactivate
```

Python 資源

- 如需詳細資訊Health. Client，請參閱AWS SDK for Python (Boto3)
- 如需有關此示範中用於 DNS 查閱的程式庫的詳細資訊，請參閱 dnspython 工具組和上的原始程式碼 GitHub。

簽署 AWS Health API 請求

在使用AWS軟體開發套件或AWS Command Line Interface (AWS CLI) 對提出請求時AWS，這些工具會自動使用您設定工具時指定的存取金鑰，替您簽署請求。例如，如果您使用先前AWS SDK for Java的高可用性端點示範例，您不必自行簽署請求。

Java 程式碼範例

如需有關如何搭配使用AWS Health API 的更多範例AWS SDK for Java，請參閱此範例程式碼。

在提出請求時，我們強烈建議您不要使用AWS根帳戶憑證來定期存取AWS Health。您可以使用 IAM 使用者的登入資料。如需詳細資訊，請參閱 IAM 使用者指南中的鎖定AWS帳戶根使用者存取金鑰。

如果您未使用AWS軟體開發套件或AWS CLI，您必須自行簽署請求。我們建議您使用AWS簽章第 4 版。如需詳細資訊，請參閱《AWS 一般參考》AWS中的簽署 API 請求。

AWS Health 中支援的操作

AWS Health 支援使用下列操作來取得會影響 AWS 帳戶的事件相關資訊：

- AWS Health 支援的事件類型。
- 符合指定篩選條件的一或多個事件的相關資訊。
- 受到一或多個事件影響的實體相關資訊。
- 符合指定篩選條件的事件或實體的分類計數。

所有操作都是非變化操作。也就是說，它們會擷取資料但不會修改資料。以下章節總結 AWS Health 操作：

Event types (事件類型)

所以此DescribeEventTypes操作會擷取符合選擇性指定篩選器的事件類型。事件類型是事件的模板定義AWS服務、事件類型代碼和類別。事件類型和事件類似於物件導向程式設計中的類別和物件。AWS Health 支援的事件類型數目會隨著時間增長。

事件

所以此DescribeEvents作業會擷取有關事件的摘要資訊AWS帳戶。事件可能與 AWS 操作問題、AWS 基礎設施的排定變更，或安全和帳單通知相關。所以此DescribeEventDetails作業擷取一或多個事件的詳細資訊，例如AWS服務、區域、可用區域、事件開始和結束時間，以及文字說明。

受影響的實體

所以此DescribeAffectedEntities作業會擷取受一或多個事件影響之實體的相關資訊。您可以透過其他條件篩選結果，例如可能指派給 AWS 資源的狀態。

聚合

所以此DescribeEventAggregates操作會擷取每個事件類別中的事件計數，並以其他條件選擇性地篩選。所以此DescribeEntityAggregates作業會擷取受一或多個指定事件影響的實體 (資源) 計數。

AWS Organizations 和組織檢視

DescribeEventsForOrganization

DescribeEventsForOrganization返回有關事件的摘要信息AWS Organizations，符合特定的篩選標準。

DescribeAffectedAccountsForOrganization

DescribeAffectedAccountsForOrganization傳回一個清單AWS中的帳戶AWS Organizations受提供的事件影響。

DescribeEventDetailsForOrganization

DescribeEventDetailsForOrganization針對中的一或多個帳戶，傳回一或多個指定事件的詳細資訊。AWS Organizations。

DescribeAffectedEntitiesForOrganization

DescribeAffectedEntitiesForOrganization根據篩選標準，針對組織中的一或多個帳戶，傳回一或多個事件所影響的實體清單。

EnableHealthServiceAccessForOrganization

EnableHealthServiceAccessForOrganization操作授予AWS Health與之互動的服務權限AWS Organizations代表客戶，並將服務連結角色套用至組織中的管理帳戶。

DisableHealthServiceAccessForOrganization

DisableHealthServiceAccessForOrganization作業撤銷的權限AWS Health與之互動的服務AWS Organizations代表客戶。

DescribeHealthServiceStatusForOrganization

DescribeHealthServiceStatusForOrganization作業提供啟用或停用的狀態資訊AWS Health與您的組織合作

如需這些操作的詳細資訊，請參閱AWS HealthAPI 參考。

適用於 AWS Health API 的範本 Java 程式碼

以下 Java 程式碼範例示範如何初始化 AWS Health 用戶端並擷取事件和實體的相關資訊。

步驟 1：初始化憑據

需有有效的登入資料才能與 AWS Health API 通訊。您 key pair 以使用與AWS帳戶。

建立和初始化 AWSCredentials 執行個體：

```
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);
}
```

步驟 2：初始化AWS HealthAPI 用户端

使用之前步驟初始化的登入資料物件來建立 AWS Health 用戶端：

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

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

步驟 3：使用AWS HealthAPI 操作取得事件資訊

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());
 }
```

中的安全性 AWS Health

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，這些架構是為了滿足對安全性最敏感的組織的需求而建置的。

安全是 AWS 與您之間共同承擔的責任。共同責任模型將其描述為雲端的安全性和雲端中的安全性：

- 雲端的安全性 — AWS 負責保護在 AWS 雲端中執行 AWS 服務的基礎架構。 AWS 還為您提供可以安全使用的服務。若要深入瞭解適用於的規範遵循計劃 AWS Health，請參閱合規計劃的AWS 服務範圍範圍)。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您瞭解如何在使用時套用共同責任模型 AWS Health。下列主題說明如何設定 AWS Health 以符合安全性與合規性目標。您還將學習如何使用其他 AWS 服務來幫助您監控和保護您的 AWS Health 資源。

主題

- 資料保護 AWS Health
- 適用於 AWS Health的 Identity and Access Management
- 登錄和監控 AWS Health
- 符合性驗證 AWS Health
- 韌性 AWS Health
- AWS Health中的基礎設施安全
- 中的配置和漏洞分析 AWS Health
- AWS Health的安全最佳實務

資料保護 AWS Health

AWS 共用責任模型適用於中的資料保護 AWS Health。如此模型中所述， AWS 負責保護執行所有 AWS 雲端. 您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 AWS 共同的責任模型和 GDPR 部落格文章。

基於資料保護目的，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 登入資料並設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源進行通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用設定 API 和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案以及其中的所有默認安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2 概觀。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用主控台、API AWS Health 或 AWS SDK 時 AWS 服務 使用或其他使用時。 AWS CLI您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

資料加密

請參閱下列有關如何 AWS Health 加密資料的資訊。

數據加密是指在傳輸中（從服務傳輸到您的 AWS 帳戶時）以及靜態（存儲在服 AWS 務中時）保護數據。您可以使用 Transport Layer Security (TLS) 保護傳輸中的資料，或使用用戶端加密保護靜態資料。

AWS Health 不會在活動中記錄個人識別資訊 (PII)，例如電子郵件地址或客戶名稱。

靜態加密

儲存的所有資料都會在靜態時加密。 AWS Health

傳輸中加密

傳送至和傳出的所有資料都會 AWS Health 在傳輸過程中加密。

金鑰管理

AWS Health 對於在 AWS 雲端中加密的資料，不支援客戶管理的加密金鑰。

適用於 AWS Health的 Identity and Access Management

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM 管理員控制哪些人可以驗證 (登入) 和授權 (具有權限) 以使用 AWS Health 資源。IAM 是您可以使用的 AWS 服務 ，無需額外付費。

主題

物件

您使用 AWS Identity and Access Management (IAM) 的方式會有所不同，具體取決於您在進行的工作 AWS Health。

服務使用者 — 如果您使用 AWS Health 服務執行工作，則管理員會為您提供所需的認證和權限。當您使用更多 AWS Health 功能來完成工作時，您可能需要其他權限。了解存取的管理方式可協助您向管理員請求正確的許可。若您無法存取 AWS Health中的某項功能，請參閱 疑難排解 AWS Health 身分和存取。

服務管理員 — 如果您負責公司的 AWS Health 資源，您可能擁有完整的存取權 AWS Health。決定您的服務使用者應該存取哪些 AWS Health 功能和資源是您的工作。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步瞭解貴公司如何搭配使用 IAM AWS Health，請參閱如何與 IAM AWS Health 搭配使用。

IAM 管理員：如果您是 IAM 管理員，建議您掌握如何撰寫政策以管理 AWS Health存取權的詳細資訊。若要檢視可在 IAM 中使用的 AWS Health 基於身分的政策範例，請參閱。AWS Health 以識別為基礎的原則範例

使用身分驗證

驗證是您 AWS 使用身分認證登入的方式。您必須以 IAM 使用者身分或假設 IAM 角色進行驗證 (登入 AWS)。 AWS 帳戶根使用者

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。 AWS IAM Identity Center (IAM 身分中心) 使用者、貴公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料都是聯合身分識別的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使 AWS 用同盟存取時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需有關登入的詳細資訊 AWS，請參閱《AWS 登入 使用指南》 AWS 帳戶中的如何登入您的。

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以加密方式簽署要求。如果您不使用 AWS 工具，則必須自行簽署要求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱 IAM 使用者指南中的簽署 AWS API 請求。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如， AWS 建議您使用多重要素驗證 (MFA) 來增加帳戶的安全性。如需更多資訊，請參閱 AWS IAM Identity Center 使用者指南中的多重要素驗證和 IAM 使用者指南中的在 AWS中使用多重要素驗證 (MFA)。

AWS 帳號根使用者

當您建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取該帳戶中的所有資源 AWS 服務和資源。此身分稱為 AWS 帳戶 root 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需這些任務的完整清單，了解需以根使用者登入的任務，請參閱《IAM 使用者指南》中的需要根使用者憑證的任務。

IAM 使用者和群組

IAM 使用者是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定許可。建議您盡可能依賴暫時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 IAM 使用者指南中的為需要長期憑證的使用案例定期輪換存取金鑰。

IAM 群組是一種指定 IAM 使用者集合的身分。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。如需進一步了解，請參閱 IAM 使用者指南中的建立 IAM 使用者 (而非角色) 的時機。

IAM 角色

IAM 角色是您 AWS 帳戶 內部具有特定許可的身分。它類似 IAM 使用者，但不與特定的人員相關聯。您可以切換角色，在中暫時擔任 IAM 角色。 AWS Management Console 您可以透過呼叫 AWS CLI 或 AWS API 作業或使用自訂 URL 來擔任角色。如需使用角色的方法更多相關資訊，請參閱 IAM 使用者指南中的使用 IAM 角色。

使用暫時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 – 若要向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱 IAM 使用者指南中的為第三方身分提供者建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權 – 您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的委託人) 存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。若要了解跨帳戶存取權角色和資源型政策間的差異，請參閱 IAM 使用者指南中的 IAM 角色與資源類型政策的差異。
- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉寄存取工作階段 (FAS) — 當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。
  - 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需更多資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務。
  - 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

- 在 Amazon EC2 上執行的應用程式 — 您可以使用 IAM 角色來管理在 EC2 執行個體上執行的應用程式以及發出 AWS CLI 或 AWS API 請求的臨時登入資料。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並提供給其所有應用程式，請建立連接至執行個體的執行個體設定檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得暫時憑證。如需更多資訊，請參閱 IAM 使用者指南中的利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式。

若要了解是否要使用 IAM 角色或 IAM 使用者，請參閱 IAM 使用者指南中的建立 IAM 角色 (而非使用者) 的時機。

使用政策管理存取權

您可以透 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS ，當與身分識別或資源相關聯時，會定義其權限。 AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以 JSON 文件的形式儲存在中。如需 JSON 政策文件結構和內容的更多相關資訊，請參閱 IAM 使用者指南中的 JSON 政策概觀。

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

預設情況下，使用者和角色沒有許可。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該原則的使用者可以從 AWS Management Console AWS CLI、或 AWS API 取得角色資訊。

身分型政策

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分類型政策，請參閱 IAM 使用者指南中的建立 IAM 政策。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶. 受管政策包括 AWS 受管政策和客戶管理的策略。若要了解如何在受管政策及內嵌政策間選擇，請參閱 IAM 使用者指南中的在受管政策和內嵌政策間選擇。

資源型政策

資源型政策是連接到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的政策中使用 IAM 的 AWS 受管政策。

AWS Health 支持基於資源的條件。您可以指定使用者可檢視哪一個 AWS Health 事件。例如，您可以建立一個政策，該政策只允許 IAM 使用者存取中的特定 Amazon EC2 事件 AWS Health Dashboard。

如需詳細資訊，請參閱 資源。

存取控制清單

存取控制清單 (ACL) 可控制哪些委託人 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

Amazon S3 和 Amazon VPC 是支援 ACL 的服務範例。 AWS WAF若要進一步了解 ACL，請參閱 Amazon Simple Storage Service 開發人員指南中的存取控制清單 (ACL) 概觀。

AWS Health 不支援 ACL。

其他政策類型

AWS 支援其他較不常見的原則類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 許可界限 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可範圍的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 實體許可範圍。
- 服務控制策略（SCP）— SCP 是 JSON 策略，用於指定中組織或組織單位（OU）的最大權限。AWS Organizations AWS Organizations 是一種用於分組和集中管理您企業擁 AWS 帳戶 有的多個服務。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 限制成員帳戶中實體的權限，包括每個 AWS 帳戶根使用者帳戶。如需組織和 SCP 的更多相關資訊，請參閱 AWS Organizations 使用者指南中的 SCP 運作方式。

- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需更多資訊，請參閱 IAM 使用者指南中的工作階段政策。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。要了解如何在涉及多個政策類型時 AWS 確定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

如何與 IAM AWS Health 搭配使用

在您使用 IAM 管理存取權限之前 AWS Health，您應該瞭解哪些 IAM 功能可搭配使用 AWS Health。若要深入瞭解如何 AWS Health 和其他 AWS 服務如何使用 IAM，請參閱 IAM 使用者指南中的與 IAM 搭配使用的AWS 服務。

主題

- AWS Health 身分型政策
- AWS Health 資源型政策
- 以 AWS Health 標籤為基礎的授權
- AWS Health IAM 角色

AWS Health 身分型政策

使用 IAM 身分類型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下會允許或拒絕動作。 AWS Health 支援特定動作、資源及條件索引鍵。若要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 JSON 政策元素參考。

動作

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼条件下可以對什麼資源執行哪些動作。

JSON 政策的 `Action` 元素描述您可以用來允許或拒絕政策中存取的動作。原則動作通常與關聯的 AWS API 作業具有相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

中的策略動作在動作之前 AWS Health 使用下列前置詞：health:。例如，若要授與某人使用 DescribeEventDetails API 作業來檢視有關指定事件之詳細資訊的權限，您可以將heath:DescribeEventDetails動作納入原則中。

原則陳述式必須包含Action或NotAction元素。 AWS Health 定義了它自己的一組動作，描述您可以使用此服務執行的任務。

若要在單一陳述式中指定多個 動作，請用逗號分隔，如下所示。

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

您也可以使用萬用字元 (*) 來指定多個動作。例如，如需指定開頭是 Describe 文字的所有動作，請包含以下動作：

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

若要查看 AWS Health 動作清單，請參閱《IAM 使用者指南》 AWS Health中的 「定義的動作」。

資源

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Resource JSON 政策元素可指定要套用動作的物件。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

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

AWS Health 事件具有以下 Amazon 資源名稱（ARN）格式。

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

例如，若要在陳述式中指定 EC2_INSTANCE_RETIREMENT_SCHEDULED_ABC123-DEF456 事件，請使用以下 ARN。

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

若要為屬於特定帳戶的 Amazon EC2 指定所有 AWS Health 事件，請使用萬用字元 (*)。

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

如需 ARN 格式的詳細資訊，請參閱 Amazon 資源名稱 (ARN) 和 AWS 服務命名空間。

某些 AWS Health 動作無法在特定資源上執行。在這些情況下，您必須使用萬用字元 (*)。

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

AWS Health API 操作可能涉及多個資源。例如，DescribeEvents作業會傳回符合指定篩選準則之事件的相關資訊。這表示 IAM 使用者必須擁有檢視此事件的權限。

若要在單一陳述式中指定多項資源，請使用逗號分隔 ARN。

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

AWS Health 僅支援健全狀況事件的資源層級權限，而且僅支援「DescribeAffected實體」和「詳DescribeEvent細資料」API 作業。如需詳細資訊，請參閱 根據資源與根據動作的條件。

若要查看 AWS Health 資源類型及其 ARN 的清單，請參閱《IAM 使用者指南》 AWS Health中的「定義資源」。若要了解您可以使用哪些動作指定每個資源的 ARN，請參閱 AWS Health定義的動作。

條件索引鍵

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，請使用邏輯OR運算來 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需更多資訊，請參閱 IAM 使用者指南中的 IAM 政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 AWS 全域條件金鑰，請參閱《IAM 使用者指南》中的AWS 全域條件內容金鑰。

AWS Health 定義了它自己的一組條件鍵，並且還支持使用一些全局條件鍵。若要查看所有 AWS 全域條件金鑰，請參閱 IAM 使用者指南中的AWS 全域條件內容金鑰。

DescribeAffected實體和DescribeEvent詳細資料 API 作業支援`health:eventTypeCode`和`health:service`條件金鑰。

若要查看 AWS Health 條件金鑰清單，請參閱《IAM 使用者指南》 AWS Health中的條件金鑰。若要瞭解您可以使用條件索引鍵的動作和資源，請參閱動作定義者 AWS Health。

範例

若要檢視以 AWS Health 身分為基礎的原則範例，請參閱。AWS Health 以識別為基礎的原則範例

AWS Health 資源型政策

以資源為基礎的策略是 JSON 政策文件，指定指定的主體可以在 AWS Health 資源上以及在何種情況下執行的動作。 AWS Health 支援健康事件的以資源為基礎的權限原則。資源型政策可讓您依資源將使用許可授予至其他帳戶。您也可以使用以資源為基礎的政策來允許 AWS 服務存取您的 AWS Health 事件。

若要啟用跨帳戶存取，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，作為資源型政策的委託人。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主參與者和資源位於不同的 AWS 帳號中時，您也必須授與主參與者實體存取資源的權限。透過將身分型政策連接到實體來授予許可。不過，如果資源型政策會為相同帳戶中的委託人授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 角色與以資源為基礎的原則有何差異。

AWS Health 僅支援「DescribeAffected實體」和「詳細資DescribeEvent料 API」作業的資源型政策。您可以在策略中指定這些動作，以定義哪些主參與者實體 (帳戶、使用者、角色和同盟使用者) 可以對 AWS Health 事件執行動作。

範例

若要檢視 AWS Health 以資源為基礎的政策範例，請參閱根據資源與根據動作的條件。

以 AWS Health 標籤為基礎的授權

AWS Health 不支持標記資源或基於標籤控制訪問。

AWS Health IAM 角色

IAM 角色是您 AWS 帳戶中具有特定許可的實體。

使用臨時登入資料 AWS Health

您可以搭配聯合使用暫時憑證、擔任 IAM 角色，或是擔任跨帳戶角色。您可以透過呼叫AssumeRole或GetFederation權杖等 AWS STS API 作業來取得臨時安全登入資料。

AWS Health 支援使用臨時認證。

服務連結角色

服務連結角色可讓 AWS 服務存取其他服務中的資源，以代表您完成動作。服務連結角色會顯示在您的 IAM 帳戶中，並由該服務所擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

AWS Health 支援要整合的 AWS Organizations服務連結角色。服務連結角色名為 `AWSServiceRoleForHealth_Organizations`。附加至角色的是健全 OrganizationsServiceRolePolicy AWS 受管理的原則。受 AWS 管理的策略 AWS Health 允許從組織中的其他 AWS 帳戶存取健全狀況事件。

您可以使用此EnableHealthServiceAccessForOrganization作業在帳戶中建立服務連結角色。但是，如果要禁用此功能，則必須首先調用該DisableHealthServiceAccessForOrganization操作。然後，您可以透過 IAM 主控台、IAM API 或 AWS Command Line Interface (AWS CLI) 刪除該角色。如需詳細資訊，請參閱《 IAM 使用者指南》中的使用服務連結角色。

如需詳細資訊，請參閱 使用組織檢視跨帳戶彙總 AWS Health 事件。

服務角色

此功能可讓服務代表您擔任服務角色。此角色可讓服務存取其他服務中的資源，以代表您完成動作。服務角色會出現在您的 IAM 帳戶中，且由該帳戶所擁有。這表示 IAM 管理員可以變更此角色的許可。不過，這樣可能會破壞此服務的功能。

AWS Health 不支援服務角色。

AWS Health 以識別為基礎的原則範例

根據預設，IAM 使用者和角色不具備建立或修改 AWS Health 資源的許可。他們也無法使用 AWS Management Console AWS CLI、或 AWS API 執行工作。IAM 管理員必須建立 IAM 政策，授予使用者和角色在指定資源上執行特定 API 作業的所需許可。管理員接著必須將這些政策連接至需要這些許可的 IAM 使用者或群組。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的在 JSON 標籤上建立政策。

主題

政策最佳實務

以身分識別為基礎的政策會決定某人是否可以建立、存取或刪除您帳戶中的 AWS Health 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始授與使用者和工作負載的權限，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們可用在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低許可許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的權限。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需更多資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access

Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。

- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫 API 作業時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。

使用 AWS Health 主控台

若要存取 AWS Health 主控台，您必須擁有最少一組權限。這些權限必須允許您列出並檢視您 AWS 帳戶中 AWS Health 資源的詳細資料。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (IAM 使用者或角色) 而言，主控台就無法如預期運作。

若要確保這些實體仍可使用主 AWS Health 控台，您可以附加下列 AWS 受管理的原則AWSHealthFullAccess。

此原AWSHealthFullAccess則會授與實體對下列項目的完整存取權：

- 啟用或停用 AWS Health 組織中所有帳戶的 AWS 組織檢視功能
- AWS Health 主控台 AWS Health Dashboard 中的
- AWS Health API 操作和通知
- 檢視屬於您 AWS 組織之帳戶的相關資訊
- 檢視管理帳戶的組織單位 (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**
>
> 您也可以使用受Health_OrganizationsServiceRolePolicy AWS 管理的策略， AWS Health 以便檢視組織中其他帳戶的事件。如需詳細資訊，請參閱 使用 AWS Health的服務連結角色。

您不需要為僅對 AWS CLI 或 AWS API 進行呼叫的使用者允許最低主控台權限。反之，只需允許存取符合您嘗試執行之 API 作業的動作就可以了。

如需詳細資訊，請參閱《IAM 使用者指南》中的新增許可到使用者。

允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加到他們使用者身分的內嵌及受管政策。此原則包含在主控台上或以程式設計方式使用 AWS CLI 或 AWS API 完成此動作的權限。

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

存取 AWS Health Dashboard 和 AWS Health API

適用 AWS Health Dashboard 於所有 AWS 帳戶。此 AWS Health API 僅適用於具有商業、企業版升級或企業 Support 方案的帳戶。如需詳細資訊，請參閱 AWS Support。

您可以使用 IAM 建立實體 (使用者、群組或角色)，然後授與這些實體存取 AWS Health Dashboard 和 AWS Health API 的權限。

依預設，IAM 使用者無法存取 AWS Health Dashboard 或 AWS Health API。您可以將 IAM 政策附加到單一使用者、使用者群組或角色，讓使用者存取您帳戶的 AWS Health 資訊。如需詳細資訊，請參閱身分 (使用者、群組和角色) 和 IAM 政策概觀。

在您建立 IAM 使用者之後，您可以為這些使用者提供個別的密碼。然後，他們可以使用帳戶特定的登錄頁面登錄到您的帳戶並查看 AWS Health 信息。如需詳細資訊，請參閱使用者如何登入您的帳戶。

> **Note**
>
> AWS Health Dashboard 具有檢視許可的 IAM 使用者可以唯讀存取帳戶上所有 AWS 服務的健康資訊，其中包括但不限於 AWS 資源 ID，例如 Amazon EC2 執行個體 ID、EC2 執行個體 IP 地址和一般安全通知。
> 例如，如果 IAM 政策僅授予 AWS Health Dashboard 和 AWS Health API 的存取權，則套用該政策的使用者或角色可以存取張貼的所有有關 AWS 服務和相關資源的資訊，即使其他 IAM 政策不允許該存取權。

您可以將兩個 API 群組用於 AWS Health.

- 個人帳戶 — 您可以使用DescribeEvents和 [DescribeEvent詳細資料] 等操作來取得帳戶 AWS Health 事件的相關資訊。
- 組織帳戶 — 您可以使用DescribeEventsForOrganization和 [DescribeEventDetailsFor組織] 等作業來取得屬於組織一部分之帳戶的 AWS Health 事件相關資訊。

如需有關可用 API 作業的詳細資訊，請參閱 AWS Health API 參考資料。

個別動作

您可以將 IAM 政策的`Action`元素設定為`health:Describe*`。這允許存取 AWS Health Dashboard 和 AWS Health。 AWS Health 支援根據`eventTypeCode`和服務對事件的存取控制。

描述存取權

本政策聲明授予對 API 操作的訪問權限 AWS Health Dashboard 和任何 `Describe*` AWS Health API 操作。例如，具有此政策的 IAM 使用者可以存取 AWS Health Dashboard 中的， AWS Management Console 並呼叫 AWS Health `DescribeEvents` API 作業。

Example ：描述存取權

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

拒絕存取

本政策聲明拒絕訪問 AWS Health Dashboard 和 AWS Health API。具有此政策的 IAM 使用者無法在 AWS Health Dashboard 中檢視 AWS Management Console ，也無法呼叫任何 AWS Health API 作業。

Example ：拒絕存取

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

組織檢視

如果您要啟用的組織檢視 AWS Health，您必須允許存取 AWS Health 和 AWS Organizations 動作。

IAM 政策的`Action`元素必須包含下列許可：

- `iam:CreateServiceLinkedRole`
- `organizations:EnableAWSServiceAccess`

- organizations:DescribeAccount
- organizations:DisableAWSServiceAccess
- organizations:ListAccounts
- organizations:ListDelegatedAdministrators
- organizations:ListParents

若要瞭解每個 API 所需的確切許可，請參閱 IAM 使用者指南中的 AWS Health API 和通知定義的動作。

> **Note**
>
> 您必須使用組織的管理帳戶中的認證才能存取的 AWS Health API AWS Organizations。如需詳細資訊，請參閱 使用組織檢視跨帳戶彙總 AWS Health 事件。

允許存取 AWS Health 組織檢視

此政策聲明會授予您對組織檢視功能所需的所有 AWS Health 和 AWS Organizations 動作的存取權。

Example：允許 AWS Health 組織檢視存取

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

拒絕存取 AWS Health 組織檢視

此政策聲明拒絕存取 AWS Organizations 動作，但允許存取個別帳號的 AWS Health 動作。

Example ：拒絕 AWS Health 組織檢視存取

```
{
    "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**
>
> 如果您要授予權限的使用者或群組已有 IAM 政策，您可以將 AWS Health特定政策聲明新增至該政策。

根據資源與根據動作的條件

AWS Health 支援 DescribeAffectedEntities和DescribeEvent詳細資料 API 作業的 IAM 條件。您可以使用資源型和動作型條件來限制 AWS Health API 傳送給使用者、群組或角色的事件。

若要這麼做，請更新 IAM 政策的`Condition`區塊或設定`Resource`元素。您可以使用字串條件，根據特定 AWS Health 事件欄位限制存取。

當您在策略中指定 AWS Health 事件時，您可以使用下列欄位：

- `eventTypeCode`
- `service`

備註

- DescribeAffectedEntities和DescribeEvent詳細資料 API 作業支援資源層級權限。例如，您可以建立策略來允許或拒絕特定 AWS Health 事件。
- DescribeAffectedEntitiesForOrganization和組DescribeEventDetailsFor織 API 作業不支援資源層級權限。
- 如需詳細資訊，請參閱服務授權參考中 AWS Health API 和通知的動作、資源和條件金鑰。

Example ：以動作為基礎的條件

本政策聲明授予存取權限 AWS Health Dashboard 和 AWS Health `Describe*` API 操作，但拒絕存取任何與 Amazon EC2 相關的 AWS Health 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 ：以資源為基礎的條件

以下政策有相同的效果，但是改用 `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 條件

此政策聲明授予存取權限 AWS Health Dashboard 和 AWS Health `Describe*` API 作業，但拒絕存取符合`AWS_EC2_*`的任何 AWS Health 事件。`eventTypeCode`

```
{
    "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**
>
> 如果您呼叫 [DescribeAffected實體] 和 [DescribeEvent詳細資料] 作業，但沒有存取 AWS Health 事件的權限，則會出現`AccessDeniedException`錯誤。如需詳細資訊，請參閱 疑難排解 AWS Health 身分和存取。

疑難排解 AWS Health 身分和存取

使用下列資訊來診斷和修正使用和 IAM 時可能會遇到的 AWS Health 常見問題。

主題

- 我沒有執行動作的授權 AWS Health
- 我沒有授權執行 iam：PassRole
- 我想要檢視我的存取金鑰
- 我是系統管理員，想要允許其他人存取 AWS Health
- 我想允許 AWS 帳戶以外的人員存取我的 AWS Health 資源

我沒有執行動作的授權 AWS Health

如果 AWS Management Console 告訴您您沒有執行動作的授權，則您必須聯絡管理員以尋求協助。您的管理員是提供您使用者名稱和密碼的人員。

`AccessDeniedException`當用戶沒有使用權限 AWS Health Dashboard 或 AWS Health API 操作時，會出現錯誤。

在此情況下，使用者的管理員必須將政策更新為允許使用者存取。

AWS Health API 需要來AWS Support自的商業、企業級支援或企業 Support 計劃。如果您從沒有商務、企業版升級或企業 Support 方案的帳戶呼叫 AWS Health API，則會傳回下列錯誤碼:`SubscriptionRequiredException`.

我沒有授權執行 iam：PassRole

如果您收到錯誤，告知您未獲授權執行 `iam:PassRole` 動作，您的政策必須更新，允許您將角色傳遞給 AWS Health。

有些 AWS 服務 允許您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

名為 `marymajor` 的 IAM 使用者嘗試使用主控台在 AWS Health中執行動作時，發生下列範例錯誤。但是，動作要求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

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

在這種情況下，Mary 的政策必須更新，允許她執行 `iam:PassRole` 動作。

如果您需要協助，請聯絡您的 AWS 系統管理員。您的管理員提供您的登入憑證。

我想要檢視我的存取金鑰

在您建立 IAM 使用者存取金鑰後，您可以隨時檢視您的存取金鑰 ID。但是，您無法再次檢視您的私密存取金鑰。若您遺失了密碼金鑰，您必須建立新的存取金鑰對。

存取金鑰包含兩個部分：存取金鑰 ID (例如 `AKIAIOSFODNN7EXAMPLE`) 和私密存取金鑰 (例如 `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`)。如同使用者名稱和密碼，您必須一起使用存取金鑰 ID 和私密存取金鑰來驗證您的請求。就如對您的使用者名稱和密碼一樣，安全地管理您的存取金鑰。

> **Important**
>
> 請勿將您的存取金鑰提供給第三方，甚至是協助尋找您的標準使用者 ID。通過這樣做，您可能會讓某人永久訪問您的 AWS 帳戶.

建立存取金鑰對時，您會收到提示，要求您將存取金鑰 ID 和私密存取金鑰儲存在安全位置。私密存取金鑰只會在您建立它的時候顯示一次。若您遺失了私密存取金鑰，您必須將新的存取金鑰新增到您的 IAM 使用者。您最多可以擁有兩個存取金鑰。若您已有兩個存取金鑰，您必須先刪除其中一個金鑰對，才能建立新的金鑰對。若要檢視說明，請參閱《IAM 使用者指南》中的管理存取金鑰。

我是系統管理員，想要允許其他人存取 AWS Health

若要允許其他人存取 AWS Health，您必須為需要存取的人員或應用程式建立 IAM 實體 (使用者或角色)。他們將使用該實體的憑證來存取 AWS。您接著必須將政策連接到實體，在 AWS Health中授予他們正確的許可。

若要立即開始使用，請參閱《IAM 使用者指南》中的建立您的第一個 IAM 委派使用者及群組。

我想允許 AWS 帳戶以外的人員存取我的 AWS Health 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要瞭解是否 AWS Health 支援這些功能，請參閱如何與 IAM AWS Health 搭配使用。
- 若要了解如何提供對您所擁有資源 AWS 帳戶 的存取權，請參閱 IAM 使用者指南中您擁有的另一 AWS 帳戶 個 IAM 使用者提供存取權限。
- 若要了解如何將資源存取權提供給第三方 AWS 帳戶，請參閱 IAM 使用者指南中的提供第三方 AWS 帳戶 擁有的存取權。
- 若要了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱 IAM 使用者指南中的 IAM 角色與資源型政策的差異。

使用 AWS Health的服務連結角色

AWS Health 使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結到 AWS Health的唯一 IAM 角色類型。服務連結角色由預先定義， AWS Health 並包含服務 AWS 服務 為您呼叫其他人所需的所有權限。

您可以使用服務連結角色進行設定，以 AWS Health 避免手動新增必要的權限。 AWS Health 定義其服務連結角色的權限，除非另有定義，否則只 AWS Health 能擔任其角色。定義的許可包括信任政策和許可政策，並且該許可政策不能連接到任何其他 IAM 實體。

AWS Health的服務連結角色許可

AWS Health 有兩個服務連結角色：

- AWSServiceRoleForHealth_Organizations— 此角色信任 AWS Health (health.amazonaws.com) 擔任您存取 AWS 服務 的角色。附加到此角色的是受Health_OrganizationsServiceRolePolicy AWS 管理的策略。
- AWSServiceRoleForHealth_EventProcessor— 此角色信任 AWS Health 服務主體 (event-processor.health.amazonaws.com) 擔任您的角色。附加到此角色的是受AWSHealth_EventProcessorServiceRolePolicy AWS 管理的策略。服務主體使用此角色為 AWS 事件偵測和回應建立 Amazon EventBridge 受管規則。此規則是您 AWS 帳戶 將警報狀態變更資訊從您的帳戶傳送至所需的基礎結構 AWS Health。

如需有關 AWS 受管理原則的詳細資訊，請參閱AWS 受管理的政策 AWS Health。

為 AWS Health建立服務連結角色

您不需要建立AWSServiceRoleForHealth_Organizations服務連結角色。當您呼叫EnableHealthServiceAccessForOrganization作業時， AWS Health 會在帳戶中為您建立此服務連結角色。

您必須在帳戶中手動建立AWSServiceRoleForHealth_EventProcessor服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的「建立服務連結角色」。

為 AWS Health編輯服務連結角色

AWS Health 不允許您編輯服務連結角色。因為可能有各種實體會參考服務連結角色，所以您無法在建立角色之後變更其名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱《IAM 使用者指南》中的編輯服務連結角色。

為 AWS Health刪除服務連結角色

若要刪除AWSServiceRoleForHealth_Organizations角色，您必須先呼叫DisableHealthServiceAccessForOrganization作業。然後，您可以透過 IAM 主控台、IAM API 或 AWS Command Line Interface (AWS CLI) 刪除該角色。

若要刪除AWSServiceRoleForHealth_EventProcessor角色，請聯絡 AWS Support 並要求他們從 AWS 事件偵測與回應離開您的工作負載。完成此程序後，您可以透過 IAM 主控台、IAM API 或刪除任一角色 AWS CLI。

相關資訊

如需詳細資訊，請參閱《 IAM 使用者指南》中的使用服務連結角色。

AWS 受管理的政策 AWS Health

受 AWS 管理的策略是由建立和管理的獨立策略 AWS。 AWS 受管理的策略旨在為許多常見使用案例提供權限，以便您可以開始將權限指派給使用者、群組和角色。

請記住， AWS 受管理的政策可能不會為您的特定使用案例授與最低權限權限，因為這些權限可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的客戶管理政策，以便進一步減少許可。

您無法變更受 AWS 管理策略中定義的權限。如果 AWS 更新 AWS 受管理原則中定義的權限，則此更新會影響附加原則的所有主體識別 (使用者、群組和角色)。 AWS 當新的啟動或新 AWS 服務 的 API 操作可用於現有服務時，最有可能更新 AWS 受管理策略。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

AWS Health 具有下列受管理的策略。

內容

- AWS 受管政策：AWSHealth_EventProcessorServiceRolePolicy
- AWS 受管政策：Health_OrganizationsServiceRolePolicy
- AWS 受管政策：AWSHealthFullAccess
- AWS HealthAWS 受管理策略的更新

AWS 受管政策：AWSHealth_EventProcessorServiceRolePolicy

AWS Health 使用受AWSHealth_EventProcessorServiceRolePolicy AWS 管理的策略。此受管政策連接至 `AWSServiceRoleForHealth_EventProcessor` 服務連結角色。此原則可讓服務連結角色為您完成動作。您無法將此政策連接至 IAM 實體。如需詳細資訊，請參閱 使用 AWS Health的服務連結角色。

受管政策具有下列許可，可存 AWS Health 取 Amazon AWS 事件偵測和回應 EventBridge 規則。

許可詳細資訊

此政策包含以下許可。

- `events`— 描述和刪除 EventBridge 規則，以及描述和更新這些規則的目標。

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

如需策略變更的清單，請參閱AWS HealthAWS 受管理策略的更新。

AWS 受管政策：Health_OrganizationsServiceRolePolicy

AWS Health 使用受Health_OrganizationsServiceRolePolicy AWS 管理的策略。此受管政策連接至 AWSServiceRoleForHealth_Organizations 服務連結角色。此原則可讓服務連結角色為您完成動作。您無法將此政策連接至 IAM 實體。如需詳細資訊，請參閱 使用 AWS Health的服務連結角色。

此原則授與允 AWS Health 許存取 [Health 組織] 檢視之必要 AWS Organizations 詳細資料的權限。

許可詳細資訊

此政策包含以下許可。

- `organizations`— 描述中的帳號以 AWS Organizations 及 AWS 服務 可與 Organizations 搭配使用的帳號。

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

如需策略變更的清單，請參閱AWS HealthAWS 受管理策略的更新。

AWS 受管政策：AWSHealthFullAccess

AWS Health 使用受AWSHealthFullAccess AWS 管理的策略。該政策授予實體（IAM 使用者或角色）對 AWS Health 主控台的存取權。如需詳細資訊，請參閱 使用 AWS Health 主控台。

許可詳細資訊

此政策包含以下許可。

- `organizations`— 啟用或停用 AWS Health 組織中所有帳戶的 AWS 組織檢視功能，並檢視管理帳戶的組織單位 (OU)
- `health`— 訪問 AWS Health API 操作和通知
- `iam`— 建立連結 AWS Health 服務的 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"
                    }
                }
            }
        ]
}
```

如需策略變更的清單，請參閱AWS HealthAWS 受管理策略的更新。

AWS HealthAWS 受管理策略的更新

檢視 AWS Health 自此服務開始追蹤這些變更以來的 AWS 受管理策略更新詳細資料。如需有關此頁面變更的自動提醒，請訂閱 的文件歷史記錄 AWS Health 頁面的 RSS 摘要。

下表說明自 2022 年 1 月 13 日起對 AWS Health 受管理策略的重要更新。

AWS Health

變更	描述	日期
AWS 受管政策：AWSHealthFullAccess - 更新現有政策	AWS Health 已將 AWSHealthFullAccess 政策擴展到 AWS GovCloud (US) Regions 中國地區。	2023 年 10 月 16 日
AWS 受管政策：Health_OrganizationsServiceRolePolicy - 更新現有政策	AWS Health 已新增 AWS Organizations 動作，允許服務連結角色描述可搭配 AWS Organizations使用的帳戶和 AWS 服務。	2023 年 7 月 19 日
變更發佈的日誌	變更 AWS Health 受管理策略的記錄檔。	2023 年 1 月 13 日

登錄和監控 AWS Health

監控是維持其他 AWS 解決方案的可靠性、可用性和效能的 AWS Health 重要組成部分。 AWS 提供下列監控工具來監視 AWS Health、回報錯誤，並在適當時採取行動：

- Amazon 會即時 CloudWatch監控您的 AWS 資源和執行 AWS 的應用程式。您可以收集和追蹤指標、建立自訂儀板表，以及設定警示，在特定指標達到您指定的閾值時通知您或採取動作。例如，您可以 CloudWatch 追蹤 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 CPU 使用率或其他指標，並在需要時自動啟動新執行個體。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。

- Amazon EventBridge 提供描述 AWS 資源變更的系統事件 near-real-time 串流。 EventBridge 實現自動化事件驅動計算。您可以編寫規則來監視某些事件，並在這些事件發生時觸發其他 AWS 服務中的自動化操作。如需詳細資訊，請參閱 使用 Amazon 監控 AWS Health 事件 EventBridge。
- AWS CloudTrail擷取您帳戶或代表您 AWS 帳戶發出的 API 呼叫和相關事件，並將日誌檔交付到您指定的 Amazon Simple Storage Service (Amazon S3) 儲存貯體。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。如需詳細資訊，請參閱 AWS CloudTrail 使用者指南。

如需詳細資訊，請參閱 監控 AWS Health。

符合性驗證 AWS Health

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用時的合規責任取決 AWS 服務 於資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- 在 Amazon Web Services 上架構 HIPAA 安全性與合規性 — 本白皮書說明公司如何使用建立符合 HIPAA 資格的應 AWS 用程式。

> **Note**
>
> 並非所有人 AWS 服務 都符合 HIPAA 資格。如需詳細資訊，請參閱 HIPAA 資格服務參照。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)) 中，保 AWS 服務 護指引並對應至安全控制的最佳實務。
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。

- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。
- Amazon GuardDuty — 透過監控環境中的 AWS 帳戶可疑和惡意活動，藉此 AWS 服務 偵測您的工作負載、容器和資料的潛在威脅。 GuardDuty 可協助您滿足特定合規性架構所要求的入侵偵測需求，如 PCI DSS 等各種合規性需求。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

韌性 AWS Health

AWS 全球基礎架構是圍繞區 AWS 域和可用區域建立的。 AWS 區域提供多個實體分離和隔離的可用區域，這些區域透過低延遲、高輸送量和高度備援的網路連線。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

AWS Health 事件會跨多個可用區域儲存和複寫。這種方法可確保您可以從 AWS Health Dashboard 或 AWS Health API 操作訪問它們。您最多可以檢視 AWS Health 事件發生後 90 天內的事件。

如需區域和可用區域的相關 AWS 資訊，請參閱AWS 全域基礎結構。

AWS Health中的基礎設施安全

作為受管服務， AWS Health 受 Amazon Web Services：安 AWS 全流程概觀白皮書中所述的全球網路安全程序保護。

您可以使用 AWS 已發佈的 API 呼叫透 AWS Health 過網路存取。用戶端必須支援 Transport Layer Security (TLS) 1.0 或更新版本。建議使用 TLS 1.2 或更新版本。用戶端也必須支援具備完美轉送私密 (PFS) 的密碼套件，例如臨時 Diffie-Hellman (DHE) 或橢圓曲線臨時 Diffie-Hellman (ECDHE)。現代系統 (如 Java 7 和更新版本) 大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與 IAM 主體相關聯的私密存取金鑰來簽署。或者，您可以透過 AWS Security Token Service (AWS STS) 來產生暫時安全憑證來簽署請求。

中的配置和漏洞分析 AWS Health

配置和 IT 控制是我們的客戶 AWS 之間的共同責任。如需詳細資訊，請參閱 AWS 共用的責任模型。

AWS Health的安全最佳實務

請參閱下列使用的最佳作法 AWS Health。

授予 AWS Health 使用者可能的最低權

使用 使用者和群組的最低存取原則許可集，以遵循最低權限的原則。例如，您可能允許 AWS Identity and Access Management (IAM) 使用者存取 AWS Health Dashboard. 但是，您可能不允許同一位使用者啟用或停用存取 AWS Organizations。

如需詳細資訊，請參閱 AWS Health 以識別為基礎的原則範例。

檢視 AWS Health Dashboard

請 AWS Health Dashboard 經常檢查您的資訊，找出可能會影響您帳戶或應用程式的事件。例如，您可能會收到有關資源的事件通知，例如需要更新的 Amazon 彈性運算雲端 (Amazon EC2) 執行個體。

如需詳細資訊，請參閱 開始使用AWS Health儀表板 — 您的帳戶健康狀態。

AWS Health 與 Amazon Chime 聲或鬆弛整合

您可以 AWS Health 與聊天工具集成。這項整合可讓您和您的團隊即時收到有關 AWS Health 事件的通知。如需詳細資訊，請參閱中的AWS Health 工具 GitHub。

監控事 AWS Health 件

您可以 AWS Health 與 Amazon CloudWatch 活動整合，以便為特定事件建立規則。當 CloudWatch 事件偵測到符合規則的事件時，系統會通知您，然後可以採取行動。 CloudWatch 事件事件是區域特定的，因此您必須在應用程式或基礎結構所在的區域中設定此服務。

在某些情況下，無法確定 AWS Health 活動的地區。如果發生這種情況，預設會在美國東部 (維吉尼亞北部) 區域中顯示事件。您可以在此區域中設定 CloudWatch 事件，以確保監控這些事件。

如需詳細資訊，請參閱 使用 Amazon 監控 AWS Health 事件 EventBridge。

使用組織檢視跨帳戶彙總 AWS Health 事件

默認情況下，您可以使用AWS Health以檢視AWS Health單個事件AWS帳戶。如果您使用 AWS Organizations，您也可以集中檢視整個組織中的 AWS Health 事件。此功能可讓您存取與單一帳戶操作相同的資訊。您可以使用篩選條件來檢視特定 AWS 區域、帳戶和服務中的事件。

您可以彙總事件，以識別組織中受操作事件影響的帳戶，或者接收安全性弱點通知的帳戶。然後，您可以使用此資訊來主動管理和自動化整個組織的資源維護事件。使用此功能可以隨時掌握可能需要更新或變更程式碼的即將發生 AWS 服務變更。

這是一個最佳實踐使用委派管理員可委派存取權的功能AWS Health對成員帳戶的組織視圖。這使得運營團隊更容易訪問AWS Health組織中的事件。「委派管理員」功能可讓您管理帳戶受到限制，同時為團隊提供他們需要採取行動的能見度AWS Health事件。

Important

- AWS Health 不會記錄在您啟用組織檢視之前組織中發生的事件。例如，如果您組織中的某個成員帳戶 (111122223333) 在您啟用此功能之前收到 Amazon 彈性運算雲端 (Amazon EC2) 的事件，則此事件將不會出現在您的組織檢視中。
- AWS Health只要活動可用，針對組織中的帳號傳送的事件，就會顯示在組織檢視中，即使這些帳戶中有一或多個離開您的組織，最長可達 90 天。
- 組織活動在刪除前可使用 90 天。此配額無法增加。

先決條件

使用組織檢視之前，您必須：

- 成為已啟用所有功能之組織的一員。
- 使用者身分登入管理帳戶AWS Identity and Access Management(IAM) 使用者或擔任 IAM 角色。

  您也可以在組織的管理帳戶中以 root 使用者身分登入 (不建議使用)。如需詳細資訊，請參閱鎖定你的AWS帳號根使用者存取金鑰在IAM 使用者指南。
- 如果您以 IAM 使用者身分登入，請使用授予存取權的 IAM 政策AWS Health與組織動作，例如AWSHealthFullAccess政策。如需更多詳細資訊，請參閱 AWS Health 以識別為基礎的原則範例。

主題

組織檢視 (主控台)

您可以使用主AWS Health控台取得AWS組織中健全狀況事件的集中檢視。

所有AWS Support方案均可在AWS Health主控台中使用組織檢視，無需額外付費。

> **Note**
>
> 如果您想要允許使用者存取管理帳戶中的此功能，他們必須具有諸如AWSHealthFullAccess策略之類的權限。如需詳細資訊，請參閱AWS Health 以識別為基礎的原則範例。

內容

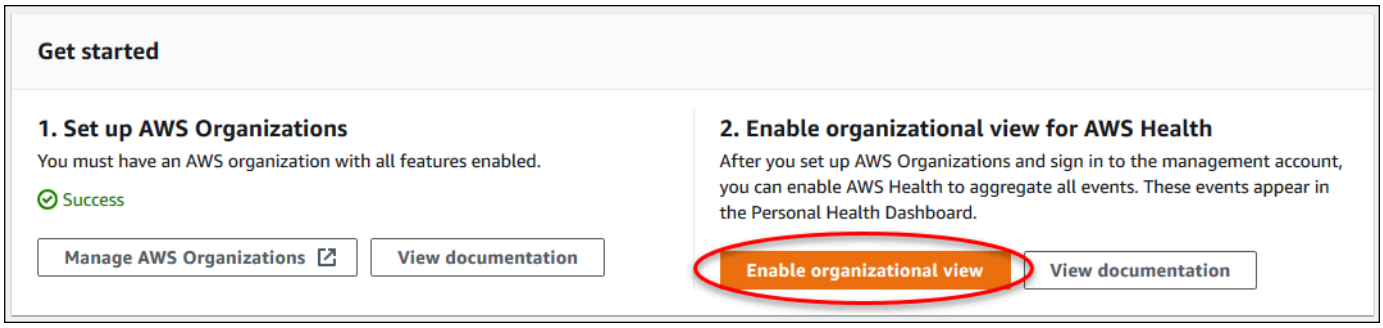
啟用組織檢視 (主控台)

您可以從AWS Health主控台啟用組織檢視。您必須登入AWS組織的管理帳戶。

檢視您的組織的AWS Health儀表板

1. 在以下位置打開您的AWS Health儀表板。 https://health.aws.amazon.com/health/home
2. 在導覽窗格的組織健康情況下，選擇組態。

3. 在 [啟用組織檢視] 頁面上，選擇 [啟用組織檢視]。



4. (選擇性) 如果您要對組AWS織進行變更，例如建立組織單位 (OU)，請選擇管理AWS Organizations。

   如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的 AWS Organizations 入門

> **備註**
>
> - 啟用此功能是非同步程序，因此需要一些時間才能完成。根據您組織中的帳戶數量，它可能需要數分鐘的時間，才能載入帳戶。您可以離開並稍後檢查AWS Health控制台。
> - 如果您有商業、Enterprise On-Ramp 或企業 Support 計劃，可以呼叫 DescribeHealthServiceStatusForOrganizationAPI 作業以檢查程序的狀態。
> - 啟用此功能時，包含`Health_OrganizationsServiceRolePolicy`AWS受管理策略的`AWSServiceRoleForHealth_Organizations`服務連結角色會套用至組織中的管理帳戶。如需詳細資訊，請參閱使用 AWS Health的服務連結角色。

檢視組織檢視事件 (主控台)

啟用組織檢視之後，AWS Health會顯示組織中所有帳戶的健全狀況事件。

當帳戶加入您的組織時，AWS Health 會自動將帳戶新增至組織檢視。當帳戶離開您的組織時，該帳戶的新事件不會再記錄到組織檢視中。但是，現有的事件仍然存在，您仍然可以查詢這些事件最多 90 天。

AWS 會將帳戶的政策資料保留 90 天，自您管理員帳戶關閉生效日起算。在 90 天期結束時，AWS 會永久刪除帳戶的所有政策資料。

- 若要保留問題清單超過 90 天，您可以封存政策。您也可以將自訂動作與 EventBridge 規則搭配使用，將問題清單存放在 S3 儲存貯體中。

- 只要 AWS 會保留政策資料，當您重新開啟已關閉的帳戶時，AWS 會將帳戶重新指派為服務管理員，並復原帳戶的服務政策資料。
- 如需詳細資訊，請參閱關閉帳戶。

> **Important**
>
> 對於 AWS GovCloud (US) 區域的客戶：
>
> - 在關閉帳戶前，請先備份帳戶資源，然後刪除。在您關閉帳戶後，您將沒有存取這些的權限。

> **Note**
>
> 啟用此功能時，AWS Health主控台可以從AWS Health儀表板 — 服務健全狀況顯示過去 7 天的公用事件。這些公開事件並不適用於組織中的帳戶。AWS Health儀表板中的事件 — 服務健康狀態提供有關服AWS務區域可用性的公開資訊。

您可以在下列頁面中檢視組織檢視事件：

主題

- 開放和最近的問題
- 排程變更
- 其他通知
- 事件日誌

開放和最近的問題

您可以使用 [開啟] 和 [最近的問題] 索引標籤來檢視可能會影響AWS基礎結構的事件，例如對組織造成影響的變更AWS 服務和資源。

檢視組織檢視事件

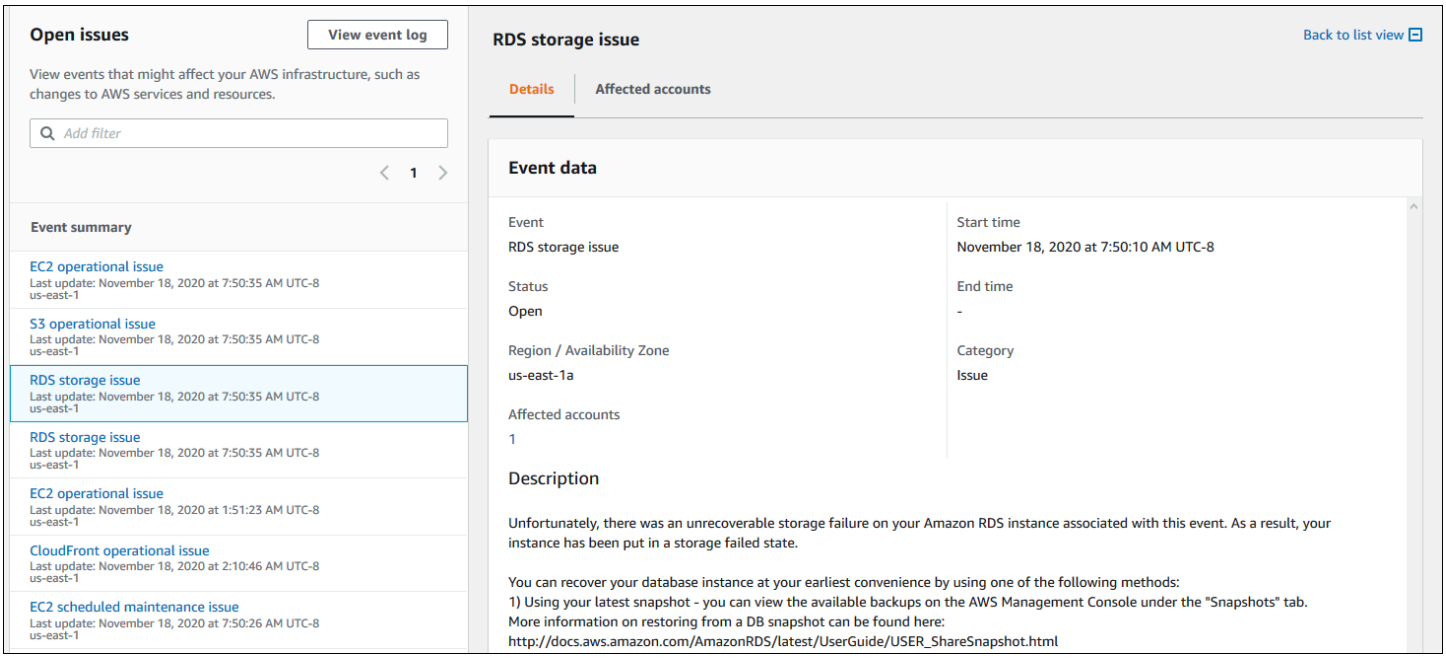
1. 在以下位置打開您的AWS Health儀表板。 https://health.aws.amazon.com/health/home
2. 在功能窗格的 [您的組織健全狀況] 下，選擇 [開啟和最近的問題] 以檢視最近報告的事件。

3. 選擇一個事件。您可以在詳細資訊標籤上檢閱下列有關事件的資訊：

   - 事件名稱
   - 狀態
   - 地區/可用區域
   - 影響的帳戶
   - 開始時間
   - 結束時間
   - 類別
   - 描述

Example ：組織檢視的未決問題

下列 Amazon Relational Database Service (Amazon RDS) 事件會顯示在組織檢視的「開啟中」和「最近的問題」索引標籤中，並影響組織中的一個帳戶。



排程變更

使用 [排程變更] 索引標籤來檢視可能會影響您組織的即將發生的事件 這些事件可能包括服務的排程維護活動。

其他通知

使用 [通知] 索引標籤可檢視過去七天內可能會影響您組織的所有其他通知和進行中事件。這可能包括事件，例如憑證輪換、帳單通知和安全性弱點。

事件日誌

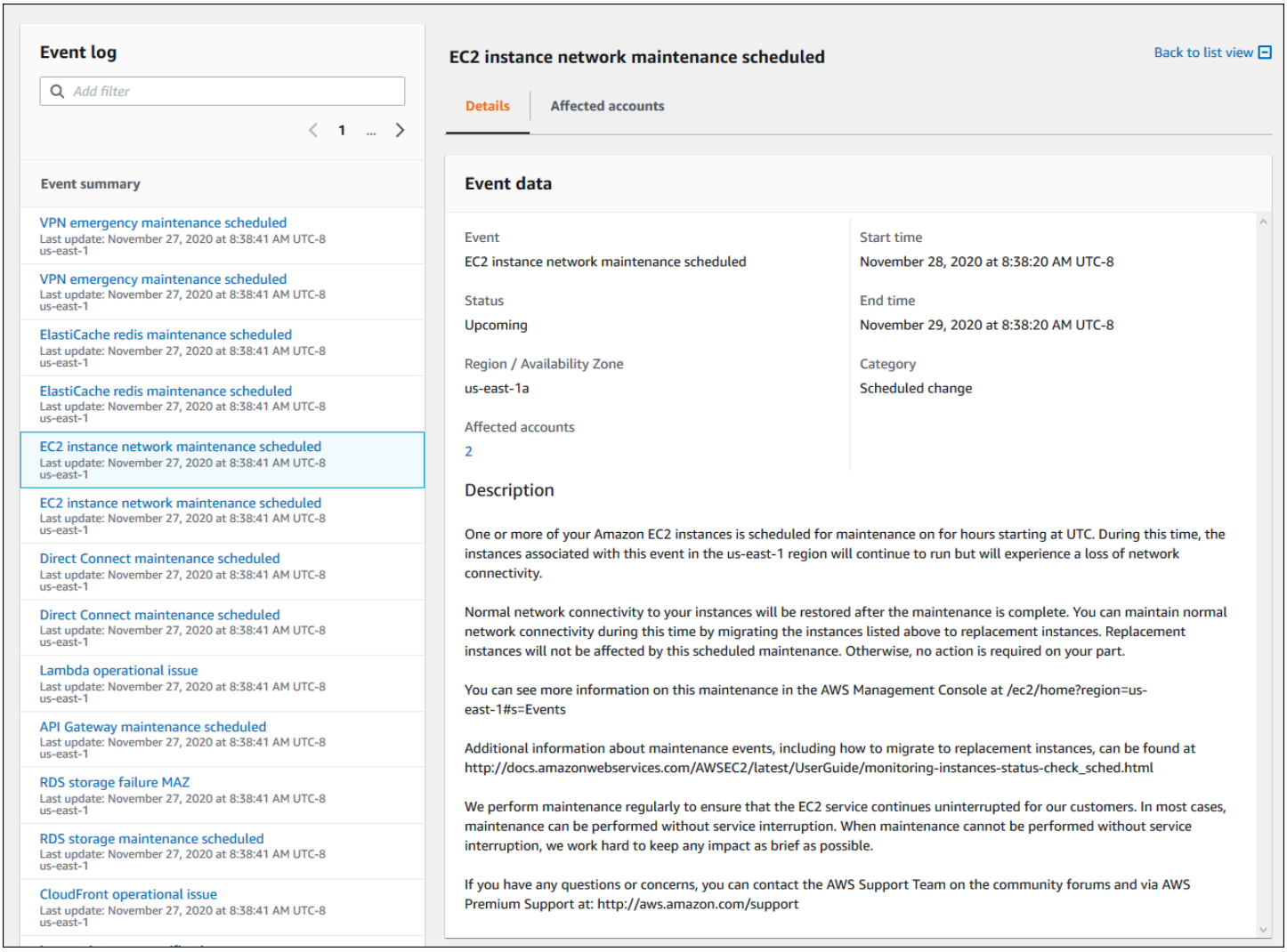
您也可以使用 [事件記錄] 索引標籤來檢視組織檢視的AWS Health事件。欄配置和行為與 [開啟] 和 [最近的問題] 索引標籤類似，不同之處在於 [事件記錄] 索引標籤包含其他欄和篩選選項，例如 [事件] 類別、[狀態] 和 [開始時間]。

在事件日誌標籤中檢視組織檢視事件

1. 在以下位置打開您的AWS Health儀表板。 https://health.aws.amazon.com/health/home
2. 在功能窗格的 [您的組織健全狀況] 下，選擇 [事件記錄]。
3. 在事件記錄下，選擇事件名稱。您可以檢閱下列有關事件的資訊：
   - 事件名稱
   - 狀態
   - 地區/可用區域
   - 影響的帳戶
   - 開始時間
   - 結束時間
   - 類別
   - 描述

Example ：組織檢視的事件記錄檔索引標籤

下列範例 Amazon DynamoDB (DynamoDB) 事件會出現在事件日誌索引標籤中，並影響組織中的兩個帳戶。



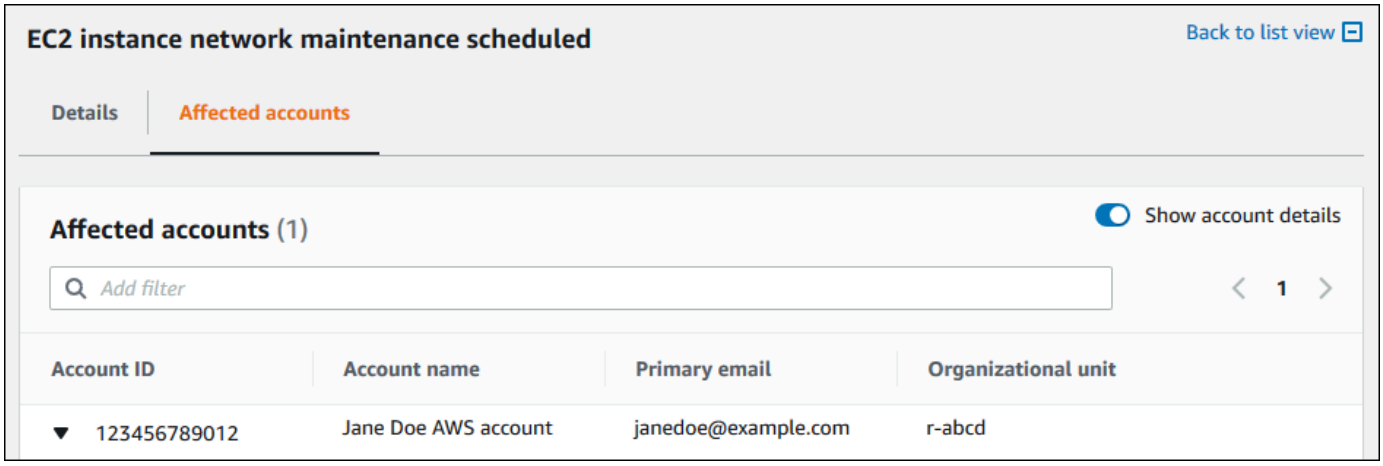
檢視受影響的帳號和資源 (主控台)

在 [您的組織健全狀況] 底下，您可以檢視組織中受事件影響的帳號以及任何相關資源。例如，如果 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的事件，組織中有 Amazon EC2 執行個體的帳戶可以出現在詳細資訊索引標籤中。您可以識別特定資源，然後聯絡帳戶擁有者。

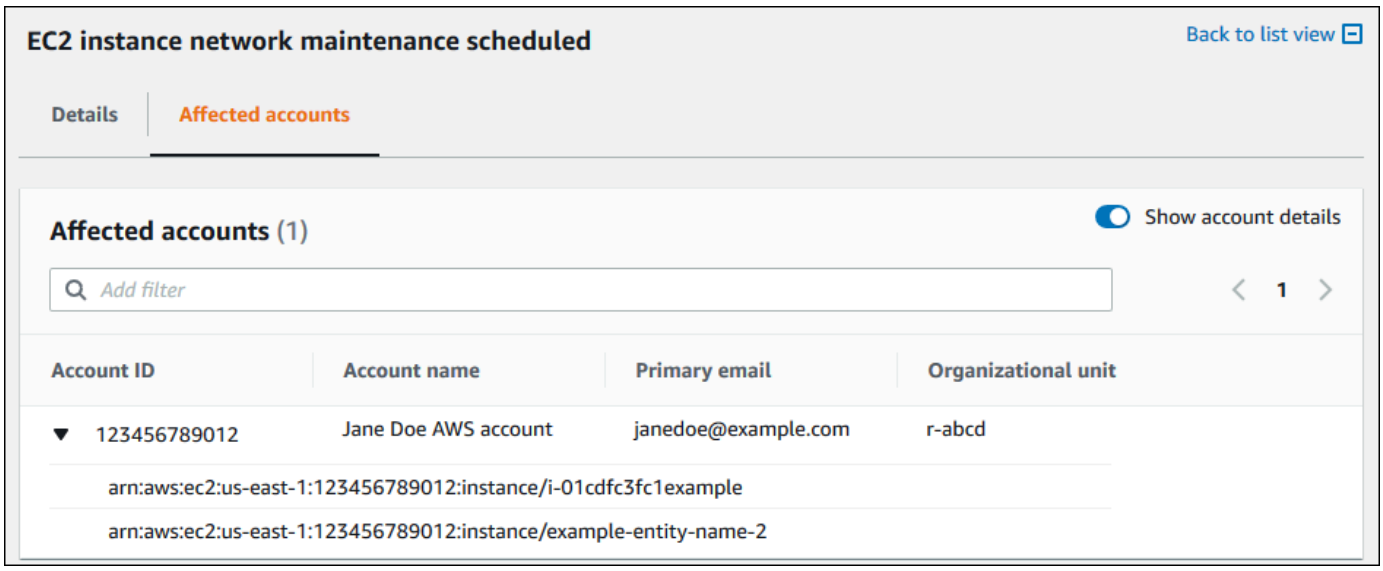
若要檢視受影響的帳號和資源

1. 在以下位置打開您的AWS Health儀表板。 https://health.aws.amazon.com/health/home
2. 在導覽窗格的組織健康情況下，選擇其中一個標籤。
3. 選擇具有「受影響帳戶」值的事件。
4. 選擇「受影響的帳戶」標籤。
5. 選擇「顯示帳戶詳細資訊」以檢視帳號的下列資訊：

- 帳戶 ID
- 帳戶名稱
- 主要電郵
- 組織單位 (OU)



6. 展開帳戶以檢視受影響的資源。



7. 如果資源超過 10 個，請選擇 [檢視所有資源] 以檢視資源。
8. 若要依此特定事件的帳號 ID 篩選，請執行下列動作：

   a. 在 [受影響的帳戶] 索引標籤上，選擇 [新增篩選器]，選擇 [帳戶 ID]，然後輸入帳號 ID。您一次只能輸入一個帳戶 ID。

   b. 選擇 Apply (套用)。您輸入的帳戶將出現在清單中。

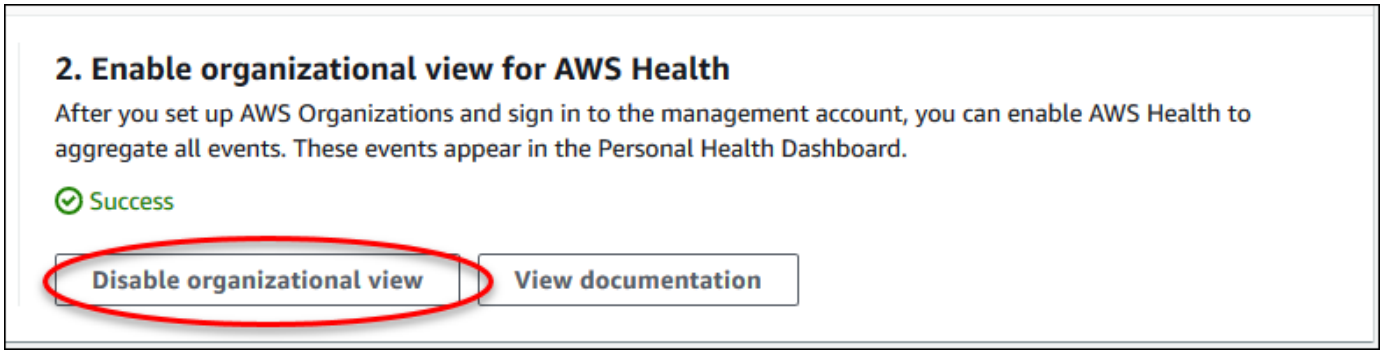
停用組織檢視 (主控台)

如果您不想為組織彙總事件，可以從管理帳戶關閉此功能。

AWS Health停止彙總組織中所有其他帳戶的事件。您可以繼續檢視組織先前的事件，直到它們被刪除為止。

停用組織檢視

1. 在以下位置打開您的AWS Health儀表板。 https://health.aws.amazon.com/health/home
2. 在導覽窗格的組織健康情況下，選擇組態。
3. 在 [啟用組織檢視] 頁面上，選擇 [停用組織檢視]。



關閉此功能之後，就AWS Health不再彙總組織的事件。不過服務連結的角色會留在管理帳戶中，直到您透過AWS Identity and Access Management (IAM) 主控台、IAM API 或AWS Command Line Interface (AWS CLI) 刪除。如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

組織檢視

您也可以啟用組織檢視功能AWS Command Line Interface(AWS CLI) 而不是AWS Health控制台。若要使用主控台，請參閱啟用組織檢視 (主控台)。

> **Note**
>
> 如果您想要允許使用者存取組織檢視功能的管理帳戶，他們必須具有的權限，例如AWSHealthFullAccess政策。如需詳細資訊，請參閱AWS Health 以識別為基礎的原則範例。

內容

- 啟用組織檢視 (CLI)
- 檢視組織檢視事件 (CLI)
- 停用組織檢視 (CLI)
- AWS Health 組織檢視 API 操作

啟用組織檢視 (CLI)

您可以使用啟用組織檢視EnableHealthServiceAccessForOrganizationAPI 操作。

您可以使用 AWS Command Line Interface (AWS CLI) 或您自己的程式碼來呼叫此操作。

> **Note**
>
> - 您必須擁有一個業務,企業斜坡，或企業支援計劃撥打AWS HealthAPI。
> - 您必須使用美國東部 (維吉尼亞北部) 區域端點。

Example

下列 AWS CLI 命令可從您的 AWS 帳戶啟用此功能。您可以從管理帳戶或可以擔任具有必要權限之角色的帳戶中使用此命令。

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

下列程式碼範例會呼叫EnableHealthServiceAccessForOrganizationAPI 操作。

Python

```
import boto3

client = boto3.client('health')

response = client.enable_health_service_access_for_organization()

print(response)
```

Java

您可以在下列範例中使用 Java 2.0 版本的 AWS 開發套件。

```
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);
        }
    }
}
```

如需詳細資訊，請參閱 適用於 Java 的 AWS 開發套件 2.0 開發人員指南。

當您啟用此功能時，AWSServiceRoleForHealth_Organizations 服務連結角色與Health_OrganizationsServiceRolePolicy AWS受管理的策略會套用至組織中的管理帳戶。

> **Note**
>
> 啟用此功能是非同步程序，因此需要一些時間才能完成。您可以呼叫DescribeHealthServiceStatusForOrganization操作來檢查過程的狀態。

檢視組織檢視事件 (CLI)

啟用此功能後，AWS Health 就會開始記錄影響組織中帳戶的事件。當帳戶加入您的組織時，AWS Health 會自動將帳戶新增至組織檢視。

> **Note**
>
> AWS Health 不會記錄在您啟用組織檢視之前組織中發生的事件。

當帳戶離開您的組織時，該帳戶的新事件不會再記錄到組織檢視中。但是，現有的事件仍然存在，您仍然可以查詢這些事件最多 90 天。

AWS 會將帳戶的政策資料保留 90 天，自您管理員帳戶關閉生效日起算。在 90 天期結束時，AWS 會永久刪除帳戶的所有政策資料。

- 若要保留問題清單超過 90 天，您可以封存政策。您也可以將自訂動作與EventBridge規則將發現項目存儲在 S3 存儲桶中。
- 只要 AWS 會保留政策資料，當您重新開啟已關閉的帳戶時，AWS 會將帳戶重新指派為服務管理員，並復原帳戶的服務政策資料。
- 如需詳細資訊，請參閱關閉帳戶。

> **Important**
>
> 對於 AWS GovCloud (US) 區域的客戶：
>
> - 在關閉帳戶之前，請先備份帳號資源，然後刪除帳號資源。在您關閉帳戶後，您將沒有存取這些的權限。

您可以使用 AWS Health API 操作從組織檢視傳回事件。

Example ：描述組織檢視事件

下列 AWS CLI 命令會傳回組織中 AWS 帳戶的運作狀態事件。

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

如需其他 AWS Health API 操作，請參閱下列章節。

停用組織檢視 (CLI)

您可以使用停用組織檢視DisableHealthServiceAccessForOrganizationAPI 操作。

Example

下列 AWS CLI 命令會停用您的帳戶中的此功能。

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

> **Note**
>
> 您也可以使用「組織」來停用組織功能停用AWSServiceAccessAPI 操作。呼叫此操作之後，AWS Health 就會停止彙總組織中所有其他帳戶的事件。如果您呼叫組織檢視的 AWS

Health API 操作，AWS Health 會傳回錯誤。AWS Health 會繼續彙總您 AWS 帳戶的運作狀態事件。

停用此功能之後，AWS Health 就不會再彙總組織中的事件。不過，服務連結的角色會保留在管理帳戶中，直到您透過AWS Identity and Access Management(IAM) 主控台、IAM API 或AWS CLI。如需詳細資訊，請參閱刪除服務連結角色在IAM 使用者指南。

AWS Health 組織檢視 API 操作

您可以針對組織檢視使用下列 AWS Health API 操作：

- DescribeEventsForOrganization— 傳回有關整個組織事件的摘要資訊。
- DescribeAffectedAccountsForOrganization-返回列表AWS組織中受指定事件影響的帳號。
- DescribeEventDetailsForOrganization— 傳回組織中一或多個帳戶之指定事件的詳細資訊。
- DescribeAffectedEntitiesForOrganization— 針對組織中的一或多個帳戶傳回受到一或多個事件影響的實體清單。

您可以使用下列操作來啟用或停用AWS Health從與組織合作：

- EnableHealthServiceAccessForOrganization— 補助金AWS Health與組織互動的權限，並將 SLR 套用至組織中的管理帳戶。
- DisableHealthServiceAccessForOrganization— 撤銷許可AWS Health與組織互動。
- DescribeHealthServiceStatusForOrganization— 傳回有關是否狀態資訊AWS Health已為您的組織啟用。

您必須擁有商業、企業上線或企業支援方案，才能呼叫這些 API 作業。如果您從至少具有商業支援方案的帳戶呼叫 `DescribeEventForOrganization` 和 `DescribeAffectedAccountsForOrganization` 操作，您可以傳回組織中任何帳戶的相關資訊，不論個別帳戶的支援層級為何。請參閱以下範例。

Example 範例：具有企業和開發人員支援方案之帳戶的組織

- 您的組織中有三個帳戶。管理帳戶具有商業支援計劃，另外兩個帳戶則有開發人員支援計劃。
- 你打電話給`DescribeEventForOrganization`從管理帳戶或可承擔角色具有所需權限的帳戶進行 API 操作。

- AWS Health 會傳回所有三個帳戶的資訊。

如果您呼叫`DescribeEventDetailsForOrganization`和`DescribeAffectedEntitiesForOrganization`從至少具有業務支援計劃的帳戶進行 API 作業，您只能傳回有關組織中具有商務、企業版或企業支援方案的帳戶資訊。

Example 範例：具有企業、商業和開發人員支援方案之帳戶的組織

- 您的組織中有五個帳戶。管理帳戶具有企業支援方案、兩個帳戶有一個商務支援方案，而兩個帳戶則有開發人員支援方案。
- 你打電話給`DescribeEventDetailsForOrganization`來自管理帳戶的 API 操作。
- AWS Health 只會傳回具有企業或商業支援方案之帳戶的資訊。具有開發人員支援方案的帳戶會出現在 `failedSet` 回應中。

委派管理員組織檢視

同AWS Health，您可以利用委派的管理員功能AWS Organizations允許管理帳戶以外的帳戶查看彙總AWS Health在上的事件AWS Health儀表板或以編程方式通過AWS HealthAPI。委派的管理員功能可讓不同團隊彈性檢視及管理整個組織的健全狀況事件。這是一個AWS在可能的情況下，將責任委派給管理帳戶之外的安全性最佳做法。

內容

為您的組織檢視註冊委派管理員

啟用組織的組織檢視之後，您最多可以將組織中的五個成員帳戶註冊為委派管理員。若要這麼做，請呼叫RegisterDelegatedAdministratorAPI 操作。註冊會員帳戶後，他們會被委派管理帳戶，並且可以訪問AWS Health從組織檢視AWS Health儀表板。如果帳戶有業務,企業斜坡，或企業支援方案，則委派系統管理員可以使用AWS Health用於存取的 APIAWS Health組織檢視。

若要建立委派的系統管理員，請從組織中的管理帳戶呼叫下列人員AWS Command Line Interface(AWS CLI) 指令。您可以從管理帳戶或可以擔任所需角色的帳戶使用此命令AWS Identity and

Access Management權限。在下面的示例命令中，替換帳戶識別碼使用您要註冊的會員帳戶 ID 以及AWS Health服務主體「健康. 亞馬遜」.

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

委派的管理員註冊後，您就可以看到所有AWS Health影響整個組織帳戶的事件。您可以檢視過去 90 天的歷史事件，或自從首次啟用組織檢視功能後 (以較新的日期為準)。請注意，啟用委派管理員功能是非同步程序，最多需要一分鐘才能完成。

從組織檢視中移除委派的管理員

若要移除委派系統管理員的存取權，請呼叫DeregisterDelegatedAdministratorAPI 操作。

從您組織的管理帳戶中，撥打下列電話AWS CLI以委派管理員身分移除成員帳戶的命令。在下面的示例命令中，替換帳戶識別碼使用您要刪除的會員帳戶 ID。

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

使用 Amazon 監控 AWS Health 事件 EventBridge

您可以使用 Amazon EventBridge 偵測事件並回應 AWS Health 事件。然後，根據您建立的規則，當事件符合您在規則中指定的值時， EventBridge 叫用一或多個目標動作。視事件類型而定，您可以擷取事件資訊、起始其他事件、傳送通知、採取更正動作或執行其他動作。例如，如果您 AWS 帳戶 的資源中有排定進行更新的 AWS 資源，例如 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，則可以使用 AWS Health 來接收電子郵件通知。

> **備註**
>
> - AWS Health 以最大的努力為基礎提供事件。事件並不總是保證交付給 EventBridge.
> - 您建立的任何 EventBridge 規則只能接收您的 AWS 帳戶. 若要接收您內其他帳戶的組織事件 AWS Organizations，請參閱使用組織檢視彙總 AWS Health 事件和委派的管理員存取權限。

您可以在多個目標類型之間進行選擇，作 EventBridge 為 AWS Health 工作流程的一部分，包括：

- AWS Lambda 函數
- Amazon Kinesis Data Streams
- Amazon Simple Queue Service (Amazon SQS) 佇列
- 內建目標 (例如 CloudWatch 警示動作)
- Amazon Simple Notification Service (Amazon SNS) 主題

例如，您可以使用 Lambda 函數在 AWS Health 事件發生時將通知傳遞給 Slack 通道。或者，您也可以使用 Lambda，並 EventBridge 在 AWS Health 事件發生時透過 Amazon SNS 傳送自訂文字或簡訊通知。

如需您可以建立以回應 AWS Health 事件的自動化和自訂警示範例，請參閱中的AWS Health 工具 GitHub。

主題

- 關於 AWS 區域 對於 AWS Health
- 關於公眾活動 AWS Health

- 事件處理器 AWS Health
- 建立 EventBridge 規則 AWS Health
- AWS Health 事件 Amazon EventBridge 架構
- 分頁上的 AWS Health 事件 EventBridge
- 使用組織檢視和委派的管理員存取彙總 AWS Health 事件
- 接收 AWS Health 事件 AWS Chatbot
- 自動執行 Amazon EC2 執行個體的動作
- 設定 SMC 連接器 AWS Health

關於 AWS 區域 對於 AWS Health

您必須為每個要接收 AWS Health 事件的區域建立 EventBridge 規則。如果您未建立規則，就不會收到事件。例如，若要接收來自美國西部 (奧勒岡) 區域的事件，您必須為此區域建立規則。

如果您的主要規則受到進行中的事件影響，則在備份區域中設定其他規則可為您的工作流程增加一層額外的復原能力。的公開事件 AWS Health 會同時傳送至受影響的區域和備份區域。如需詳細資訊，請參閱關於 AWS Health 的公開活動。對於標準 AWS 分區中的所有區域，您可以在美國西部 (奧勒岡) 設定規則作為備份，以繼續接收事件，即使您的主要區域受到持續發生的問題影響也一樣。美國西部 (奧勒岡) 區域的備份區域是美國東部 (維吉尼亞北部) 區域。

例如，如果您正在監視歐洲 (法蘭克福) 區域的事件，而該區域暫時無法使用，則也 AWS Health 會將該事件傳送至美國西部 (奧勒岡) 區域。接下來，您的備份 EventBridge 規則會將事件傳送至您指定的目標。若要建立備份規則，請遵循下列程序建立 EventBridge 規則 AWS Health並使用美國西部 (奧勒岡) 區域。

有些 AWS Health 事件不是特定於區域的。不是特定於某個區域的事件稱為全域事件。其中包括為 AWS Identity and Access Management (IAM) 傳送的事件。若要接收全域事件，您必須為主要區域的美國東部 (維吉尼亞北部) 區域和美國西部 (奧勒岡) 區域建立規則作為備份區域。

若要在中接收全域事件 AWS GovCloud (US)，您必須在 AWS GovCloud (美國西部) 區域中建立規則。

關於公眾活動 AWS Health

當您建立 EventBridge規則來監視事件時 AWS Health，規則會同時傳遞帳戶特定事件和公開事件：

- 帳戶特定事件會影響您的帳戶和資源，例如告訴您 Amazon EC2 執行個體的必要更新或其他排程變更事件的事件。
- 公開事件會顯示在AWS Health 儀表板 — 服務健康狀態。公開活動 AWS 帳戶 並不是特定於提供服務區域可用性的公開資訊。

> **Important**
>
> 若要接收這兩種事件類型，您的規則必須使用該`"source": [ "aws.health"]`值。萬用字元，例如`"source": [ "aws.health*"]`不符合要監視任何事件的模式。

如果您要從監視公開事件 AWS 區域，建議您建立備份規則。的公開事件 AWS Health 會同時傳送至受影響的區域和備份區域。建議您使用 EventARN 和通訊 ID 來刪除重複的 AWS Health 事件，因為這些事件對傳送至備份區域的 AWS Health 郵件會保持一致。

您可以使用參數來識別中 EventBridge的事件是公用事件還是帳戶特定。 eventScopeCode 事件可以具有`PUBLIC`或`ACCOUNT_SPECIFIC`。您也可以在此參數上篩選規則。

範例：Amazon 彈性運算雲端的公開事件

下列事件顯示美國東部 (維吉尼亞北部) 區域 Amazon EC2 的操作問題。

```
{
    "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",

    }
}
```

事件處理器 AWS Health

如果您的帳戶使用 AWS 事件偵測與回應，則必須在帳戶中安裝AWSServiceRoleForHealth_EventProcessor服務連結角色。

此角色會信任event-processor.health.amazonaws.com服務主體擔任該角色。附加到此角色的是受AWSHealth_EventProcessorServiceRolePolicy AWS 管理的策略。此原則會列出角色可執行的權限，例如 AWS 服務 為您呼叫其他人。

然後，此角色會在您的帳戶中建立 Amazon EventBridge 受管規則。規則命名為AWSHealthEventProcessor-DO-NOT-DELETE。此規則是您帳戶所需的基礎結構，因此 EventBridge 可以將警示狀態變更資訊從您的帳戶傳送至 AWS Health。

相關資訊

若要進一步了解，請參閱下列主題：

- 使用 AWS Health的服務連結角色
- AWS 受管政策：AWSHealth_EventProcessorServiceRolePolicy

建立 EventBridge 規則 AWS Health

您可以建立 EventBridge 規則以接收帳戶中 AWS Health 事件的通知。在建立的事件規則之前 AWS Health，請先執行下列動作：

- 熟悉中的事件、規則和目標。 EventBridge如需詳細資訊，請參閱什麼是 Amazon EventBridge？ 在 Amazon EventBridge 使用者指南和新增 EventBridge — 追蹤和回應 AWS 資源的變更。
- 建立要在事件規則中使用的一或多個目標。

若要建立 EventBridge 規則 AWS Health

1. 在以下位置打開 Amazon EventBridge 控制台 https://console.aws.amazon.com/events/。
2. 若要變更 AWS 區域，請使用頁面右上角的「地區」選取器。選擇您要追蹤 AWS Health 事件的地區。
3. 在導覽窗格中，選擇規則。
4. 選擇建立規則。
5. 在 Define rule detail (定義規則詳細資訊) 頁面中，輸入規則名稱和描述。
6. 請保留 Event bus (事件匯流排) 和 Rule type (規則類型) 的預設值，然後選擇 Next (下一步)。
7. 在 [建立事件模式] 頁面上，針對 [事件來源] 選擇AWS 事件和 EventBridge 合作夥伴事件。
8. 在「事件模式」下，針對「事件來源」，選擇AWS 服務。
9. 在「事件模式」下 AWS 服務，選擇「Health」。
10. 針對「事件類型」，選擇下列其中一個選項。
    - 特定 Health 濫用事件 — 為 AWS Health 事件類型名稱中含有字詞Abuse的事件建立規則。
    - 特定 Health 事件 — 為特定 AWS 服務事件 (例如 Amazon EC2) 建立規則。
11. 您可以選擇任何服務或特定服務。如果您選擇特定服務，請選擇下列其中一個選項：
    - 選擇 [任何事件類型] 以建立套用至所有事件類別的規則。
    - 選擇特定事件類型分類，然後從清單中選擇值，例如問題、帳戶通知或 schedu ledChange。

    > **Tip**
    >
    > - 若要監視特定服務的所有 AWS Health 事件，建議您選擇 [任何事件類型] 和 [任何資源]。這樣可確保您的規則會監控指定服務的任何事件，包括任何新的事件類型代碼。AWS Health 如需規則範例，請參閱所有 Amazon EC2 事件。
    > - 您可以建立規則來監視多個服務或事件類型類別。若要這麼做，您必須手動更新規則的事件模式。如需詳細資訊，請參閱 為多個服務和類別建立規則。

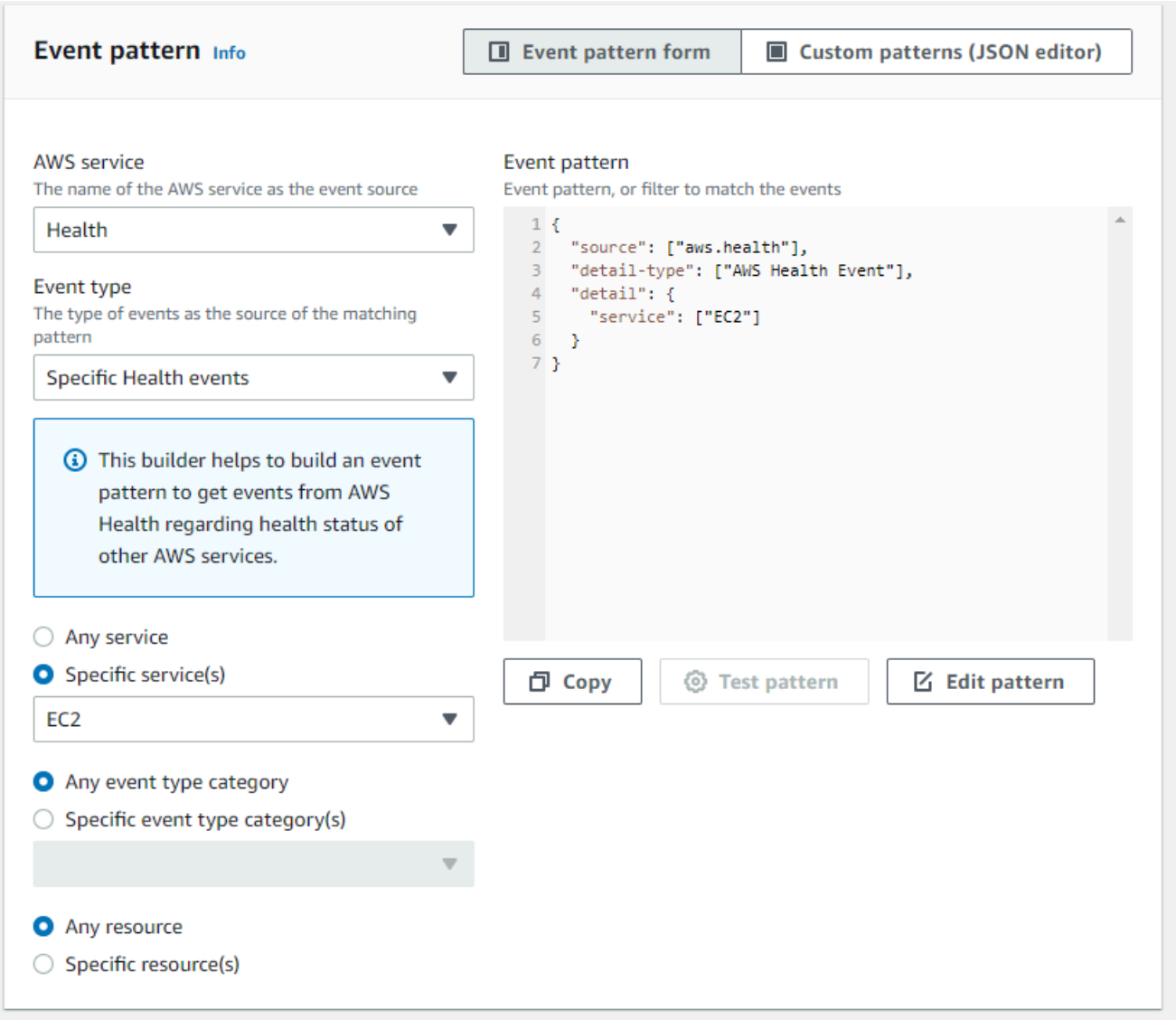
12. 如果您選擇特定的服務和事件類型類別，請為事件類型代碼選擇下列其中一個選項。
    - 選擇「任何事件類型代碼」以建立套用至所有事件類型代碼的規則。

- 選擇 [特定事件類型代碼]，然後從清單中選擇一或多個值。這會建立僅套用至特定事件類型代碼的規則。例如，如果您選擇**AWS_EC2_INSTANCE_STOP_SCHEDULED**和**AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED**，則您的規則只會在這些事件發生在您的帳戶中時套用至這些事件。

13. 針對受影響的資源選擇下列其中一個選項。
    - 選擇 [任何資源] 以建立套用至所有資源的規則。
    - 選擇特定資源，然後輸入一或多個資源的 ID。例如，您可以指定一個 Amazon EC2 執行個體識別碼 (例如 *I-Example 1B2C3de4)*，以監控僅影響此資源的事件。
14. 檢閱規則設定，使其符合您的事件監視需求。
15. 選擇下一步。
16. 在「選取目標」 頁面上，選擇您為此規則建立的目標類型，然後設定該類型所需的任何其他選項。例如，您可能會將事件匯流排傳送至 Amazon SQS 佇列或 Amazon SNS 主題。
17. 選擇下一步。
18. (選用) 在 設定標籤頁面，新增任何標籤，然後選擇下一步。
    - 注意：中的 aws.health 來源目前不會傳送標籤。 EventBridge
19. 在檢閱並建立頁面上，檢閱您的規則設定，並確定其符合您的事件監控要求。
20. 選擇建立規則。

Example ：所有 Amazon EC2 事件的規則

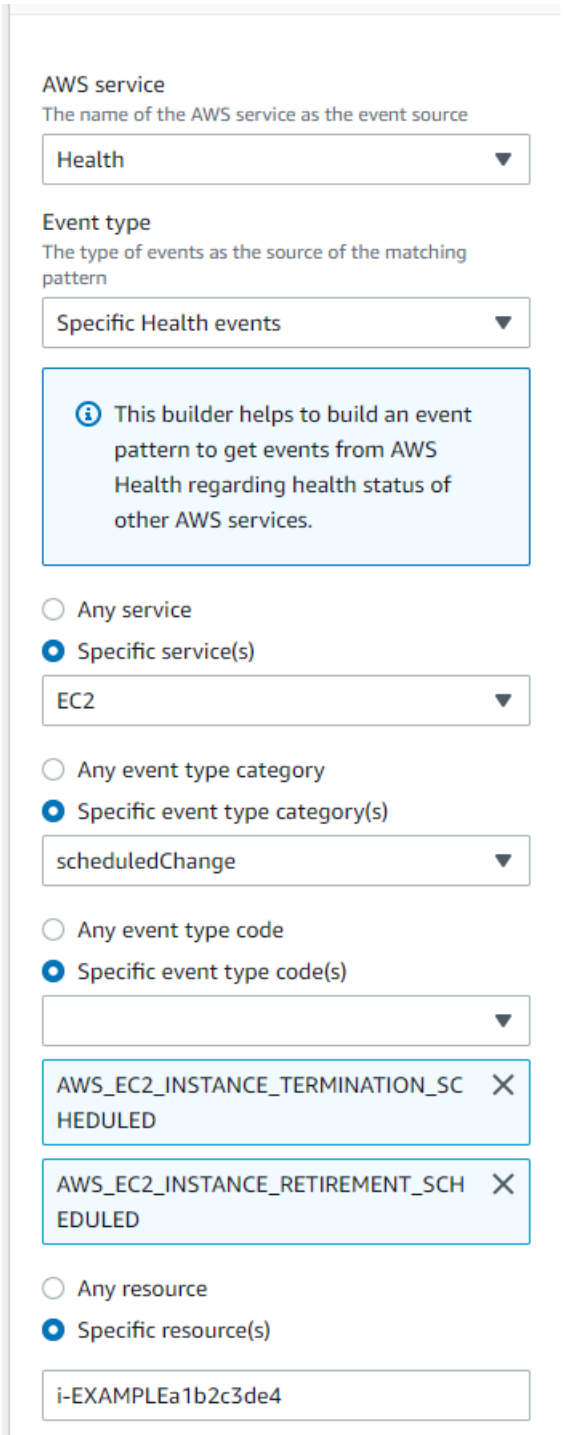
下列範例會建立規則，以便 EventBridge 監控所有 Amazon EC2 事件，包括事件類型類別、事件代碼和資源。



Example ：特定 Amazon EC2 事件的規則

下列範例會建立規則，以便 EventBridge 監視下列項目：

- Amazon EC2 服務
- scheduledChange 事件類型類別
- `AWS_EC2_INSTANCE_TERMINATION_SCHEDULED`和的事件類型代碼 `AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED`
- 具有 ID 的執行個體 `i-EXAMPLEa1b2c3de4`



為多個服務和類別建立規則

先前程序中的範例說明如何為單一服務和事件類型類別建立規則。您也可以為多個服務和事件類型類別建立規則。這表示您不必為要監視的每個服務和類別建立個別的規則。若要這麼做，您必須編輯事件模式，然後手動輸入變更。

您可以使用下列其中一個選項。

若要新增現有規則的服務和類別

1. 在 EventBridge 主控台的 [規則] 頁面上，選擇規則名稱。
2. 在右上角，選擇 Edit (編輯)。
3. 選擇下一步。
4. 在「事件模式」中，選擇 「編輯模式」，然後在文字欄位中輸入您的變更。
5. 選擇「下一步」，直到到達「檢閱和更新」頁面。
6. 選擇 [更新規則] 以儲存變更。

若要新增新規則的服務和類別

1. 遵循步驟 9 中建立 EventBridge 規則 AWS Health的程序。
2. 而不是從列表中選擇單個服務或類別，對於事件模式，選擇編輯模式。
3. 在文字欄位中輸入您的變更。請參閱下面的示例模式作為創建自己的事件模式的模型。
4. 檢閱您的事件模式，然後依照中的其餘程序建立 EventBridge 規則 AWS Health建立規則。

使用應用程式介面或 AWS Command Line Interface (AWS CLI)

對於新的或現有的規則，請使用 PutRuleAPI 作業或命`aws events put-rule`令來更新事件模式。如需 AWS CLI 指令範例，請參閱《指AWS CLI 令參考》中的 put-rule。

Example 範例：多個服務和事件類型類別

下列事件模式會建立規則來監控三種 AWS 服務的`issue`、`accountNotification`、和`scheduledChange`事件類型類別的事件：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 架構

以下是 AWS Health 事件的結構描述。舊版架構的變更或新增項目會反白顯示為「新增」。範例承載會在結構描述之後提供。

AWS Health 事件架構

AWS Health 事件架構

參數	描述	必要
version	EventBridge 版本，目前為「0」	是
id	事件的 uniqueEventBridge 識別碼	是
細節類型	描述詳細資料類型。對於 AWS Health 事件，這將是&AWS Health Event或 AWS Health	是

參數	描述	必要
	`Abuse Event`	
source	事件匯流排來源。對於 AWS Health 事件，這將是 `aws.health`	是

參數	描述	必要
account	將 AWS Health 事件傳送到的 accountId。 Note 對於組織檢視，如果受影響的帳戶是在管理或委派的管理員帳戶中接收到的，這將與受影響的帳戶不同。	是

參數	描述	必要
time	通知傳送到的時間 EventBridge。格式:yyyy-mm-ddThh:mm:ssZ .	是
region	識別通 AWS 區域 知的傳遞目標。 Note 此欄位不表示此 AWS Health 事件的受影響地區。這是由「詳細活動園」提供。	是

參數	描述	必要
resources	說明帳號內受影響資源的清單 (如果有受影響的資源)。 Note 如果沒有參考資源，則此欄位可以為空白。	否
細節	本節包含 AWS Health 事件的所有詳細信息，如下所列。	是

參數		描述	必要
	事件集	特定地區之 AWS Health 事件的唯一識別碼，包括「地區」和「事件識別碼」。 Note EventARN 不是特定客戶帳戶或區域的唯一性。	是
	服務	AWS 服務 受 AWS Health 事件影響。例如，Amazon EC2，Amazon 簡單存儲服務，Amazon Redshift 或 Amazon Relational Database Service。	是

參數		描述	必要
	事件 TypeCode	事件類型的唯一辨識碼。例如：AWS_EC2_NSTANCE_NETWORK_MAINTENANCE_SCHEDULED 和 AWS_EC2_INSTANCE_REBOOT_MAINTENANCE_SCHEDULED 。包含的事件通常MAINTENANCE_SCHEDULED 會在 startTime 前約兩週推出。 Note 所有新的計劃生命週期事件都具有事件類型AWS_{SICE}_PLANNED_LIFI	是

參數		描述	必要
		YCLE_EVENT 。	
	事件 TypeCategory	事件的類別程式碼。可能的值為 issue、accountification n 、investigation 和 scheduledChange 。	是
	事件 ScopeCode	指出 AWS Health 事件是帳戶特定還是公用事件。可能的值為 ACCOUNT_SPECIFIC 或 PUBLIC。	是

參數		描述	必要
	通訊識別碼 (新增)	此 AWS Health 事件通訊的唯一識別碼。 具有相同通訊 ID 的訊息可能是單 AWS Health 一事件的備份訊息或頁面。此識別碼可與 accountId 搭配使用，以協助刪除重複郵件。 Note 隨著分頁功能發行版本，通訊 ID 包含頁碼，讓通訊 ID 在各個頁面中保持	是

參數	描述	必要
	唯一性，例如 1234567810-1。如需詳細資訊，請參閱「分頁上的 AWS Health 事件 EventBridge」。	

參數		描述	必要
	startTime	AWS Health 事件的開始時間，格式為：DoW, DD, MMM, YYYY, HH:MM:SS TZ。 Note 已排程事件的開始時間可能在 future。	是

參數		描述	必要
	endTime	AWS Health 事件的結束時間，格式為：DoW, DD MMM YYYY HH:MM:SS TZ。 **Note** endTime 可能不會針對 future 設定的事件提供。	否
	最後 UpdatedTime	AWS Health 事件的上次更新時間，格式為：DoW, DD MMM YYYY HH:MM:SS TZ。	是

參數		描述	必要
	statusCode	AWS Health 事件的狀態。類型分類具有不同的狀態。 Issue事件類別的可能值為 open、closed scheduledChanges 事件類別具有不同的狀態：Upcoming 或Completed 。 AccountNotifications 事件類別沒有狀態且設定為"-"。	是
	活动祇园	此 AWS Health 事件所描述的受影響地區。	是
	事件描述	描述 AWS Health 事件的區段。這包括描述事件的語言和文字欄位。	是

參數			描述	必要
		語言	AWS Health 活動中使用的語言。這通常由事件發佈至的地區決定。對於 us-east-1 區域，這通常是「en_US」。	是

參數			描述	必要
		最新描述	描述 AWS Health 事件從 AWS Health API 轉譯時，通常會顯示在 AWS Health 儀表板上。 Note 對於公開活動，這只包含最新的更新，而不包含事件的整個歷史記錄。	是
	事件元數據		可為事件提供的其他 AWS Health 事件中繼資料。	否

參數			描述	必要
		<metadata key 1>	元數據鍵，值字符串「鍵字符串 1」：「鍵值 1」 Note 事件中繼資料的索引鍵值配對是由傳送 AWS Health 事件的服務決定。	否
	情感		描述此 AWS Health 事件中受影響資源的資源值和狀態的陣列。	否
		實體值	資源/實體ID	否

參數			描述	必要
		最新更新時間（新）	上次以下列格式更新此資源/實體狀態的時間：DoW, DD MMM YYYY HH:MM:SS TZ	否
		狀態（新）	受影響的資源/實體的狀態。可能的值包括IMPAIREDUNKNOWN 、PENDING、	D

參數		描述	必要
	頁面（新）	此訊息所代表的頁面。如需詳細資訊，請參閱 分頁上的 AWS Health 事件 EventBridge。 Note 分頁只發生在資源上。256KB 大小限制違反的其他原因將導致通訊失敗。	是

參數		描述	必要
	總頁（新）	此健全狀況事件的總頁數。如需詳細資訊，請參閱 分頁上的 AWS Health 事件 EventBridge。 Note 您可以使用此功能來判斷您是否收到帳戶的多頁通訊的所有頁面。	是

參數		描述	必要
	受影響帳戶 (新增)	這是受影響帳戶的 accountId。 Note 如果此健全狀況事件傳送至屬於其一部分的帳戶，且在管理或委派的系統管理員帳戶中接收此狀況，則此欄位可能 AWS Organizations 與	是

參數		描述	必要
		「帳戶」欄位不同。	

公共 Health 事件-Amazon EC2 操作問題


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

帳戶特定 AWS Health 事件-Elastic Load Balancing API 問題

```
        {
          "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",
          }
```

```
        }
```

帳戶特定 AWS Health 事件-Amazon EC2 執行個體存放區磁碟機效能降低

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

分頁上的 AWS Health 事件 EventBridge

AWS Health 當「資源」或「受影響」清單導致郵 AWS Health 件大小超過 EventBridge 256KB 郵件大小限制時，支援分頁事件。之前，當資源超過此限制時， AWS Health 並未將完整的資源清單與事件通訊。

AWS Health 現在會在訊息中包含所有「資源」和「詳細資訊. 影響」。如果此「資源」和「詳細資訊. 影響識別」清單超過 256KB，則會將健全狀況事件 AWS Health 分割成多個頁面，並在中以個別訊息形式發佈這些頁面。 EventBridge每個頁面都保留相同的 EventARN 和通訊 ID，以幫助在收到所有頁面後重新組合「資源」或「詳細信息。影響」列表。

這些額外的訊息可能會導致不必要的訊息，例如當 EventBridge 規則導向至人類可讀的介面 (例如電子郵件或聊天室) 時。擁有人類可讀通知的客戶可以為「詳細.page」欄位新增篩選器，以便僅處理第一頁，從而消除從後續頁面建立的不必要訊息。

包含數個結構描述變更，以支援分頁啟動。即使只有 1 頁，每個通訊 ID 現在都會在通訊 ID 之後包含以連字符連接的頁碼。另外還有兩個新欄位，分別是詳細資料頁面和詳細資料。TotalPages，用來描述目前的頁碼和事件的總頁數。 AWS Health 除了「詳細資訊」或「資源」清單外，每個分頁郵件中包含的資訊都相同。收到所有頁面後，可以重建這些列表。受影響的資源和實體的頁面與訂單無關。

使用組織檢視和委派的管理員存取彙總 AWS Health 事件

AWS Health 支援在 Amazon 上發佈的 AWS Health 事件的組織檢視和委派管理員存取權 EventBridge。在中開啟組織檢視時 AWS Health，管理帳戶或委派的管理員帳戶會收到來自您組織中所有帳戶的單一 AWS Health 事件摘要 AWS Organizations。

此功能旨在提供集中式檢視，以協助管理整個組織的 AWS Health 事件。在管理帳戶中設定組織檢視和 EventBridge 規則不會停用組織中其他帳戶的規則。 EventBridge

如需啟用上的組織檢視和委派管理員存取權的詳細資訊 AWS Health，請參閱彙總 AWS Health 事件。

接收 AWS Health 事件 AWS Chatbot

您可以直接在聊天用戶端中接收 AWS Health 事件，例如 Slack 和 Amazon Chime。您可以使用此事件來識別最近可能會影響 AWS 應用程式和基礎結構的 AWS 服務問題。然後，您可以登錄AWS Health 儀表板以了解有關更新的更多信息。例如，如果您正在監控 AWS 帳戶中的`AWS_EC2_INSTANCE_STOP_SCHEDULED`事件類型，則該 AWS Health 事件可能會直接顯示在您的 Slack 頻道中。

必要條件

在開始之前，您必須具備以下條件：

- 設定的聊天用戶端 AWS Chatbot。您可以配置 Amazon Chime 聲和鬆弛。如需詳細資訊，請參閱《AWS Chatbot 管理員指南》 AWS Chatbot中的〈入門〉。
- 您建立並訂閱的 Amazon SNS 主題。如果您已經有 SNS 主題，則可以使用現有的主題。如需詳細資訊，請參閱《Amazon Simple Notification Service 開發人員指南》中的 Amazon SNS 入門。

若要接收 AWS Health 事件 AWS Chatbot

1. 按照步驟 13 中的程序建立 EventBridge 規則 AWS Health進行操作。

   a. 當您在步驟 13 中完成設定事件模式後，請在模式的最後一行加上逗號，並新增下列行，從分頁 AWS Health 事件中移除不必要的聊天訊息。請參閱分頁上的 AWS Health 事件 EventBridge。

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

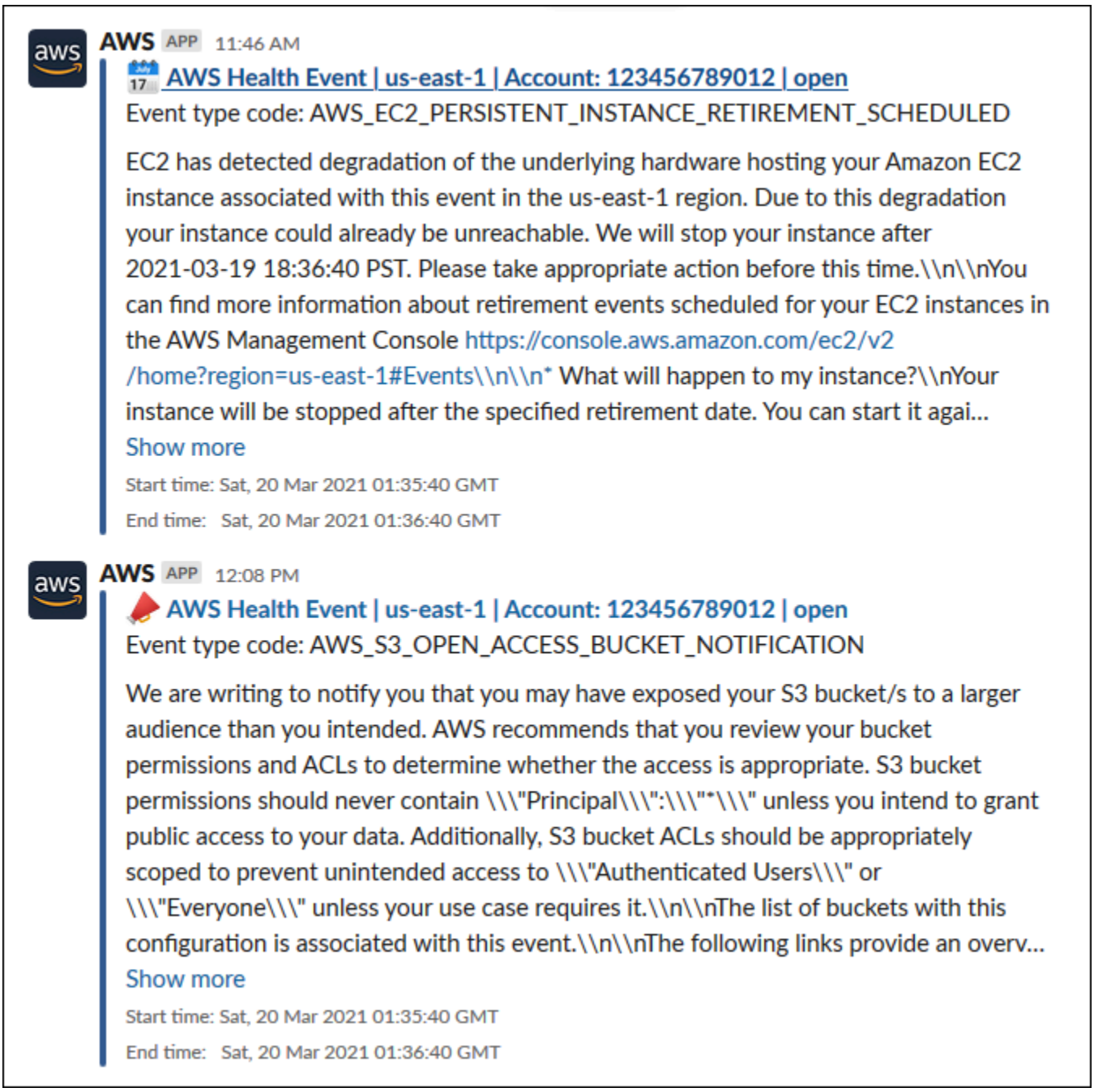
   b. 在步驟 14 中選擇目標時，請選擇 SNS 主題。您將在主 AWS Chatbot 控台中使用相同的 SNS 主題。

   c. 完成程序的其餘部分以建立規則。
2. 導覽至 AWS Chatbot 主控台。
3. 選擇您的聊天客戶端，例如您的 Slack 頻道名稱，然後選擇編輯。
4. 在通知-選用區段中，對於主題，選擇您在步驟 1 中指定的相同 SNS 主題。
5. 選擇儲存。

   當 AWS Health 發送符合您規則 EventBridge 的事件時，該 AWS Health 事件將出現在您的聊天客戶端中。
6. 選擇事件名稱以在 AWS Health 儀表板中查看更多信息。

Example ：已傳送至 Slack 的 AWS Health 事件

以下是出現在 Slack 通道中的美國東部 (維吉尼亞北部) 區域的 Amazon EC2 和 Amazon 簡單儲存服務 (Amazon S3) 的兩個 AWS Health 事件範例。



自動執行 Amazon EC2 執行個體的動作

您可以自動執行動作，以回應 Amazon EC2 執行個體的排程事件。將事件 AWS Health 傳送到您的 AWS 帳戶時，您的 EventBridge 規則可以叫用目標 (例如 AWS Systems Manager 自動化文件)，以代表您自動執行動作。

例如，當針對 Amazon 彈性區塊存放區 (Amazon EBS) 支援的 EC2 執行個體排定 Amazon EC2 執行個體淘汰事件時， AWS Health 會

將AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED事件類型傳送到您 AWS Health 的儀表板。當您的規則偵測到此事件類型時，您可以自動執行個體的停止和啟動。如此一來，您就不必手動執行這些動作。

> **Note**
>
> 若要自動執行 Amazon EC2 執行個體的動作，執行個體必須由系統管理員管理。

如需詳細資訊，請參閱 Amazon EC2 使用者指南 EventBridge中的使用自動化 Amazon EC2。

必要條件

您必須先建立 AWS Identity and Access Management (IAM) 政策、建立 IAM 角色並更新角色的信任政策，然後才能建立規則。

建立 IAM 政策

請遵循此程序，為您的角色建立客戶管理政策。此原則授予角色代表您執行動作的權限。此程序在 IAM 主控台中使用 JSON 政策編輯器。

建立 IAM 政策

1. 登入 AWS Management Console 並開啟身分與存取權管理主控台，網址為 https://console.aws.amazon.com/iam/。
2. 在導覽窗格中，選擇政策。
3. 選擇 Create policy (建立政策)。
4. 請選擇 JSON 標籤。
5. 複製下列 JSON，然後取代編輯器中的預設 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參數中，對於 Amazon 資源名稱 (ARN)，輸入您的 AWS 帳戶 ID。

b. 您也可以取代角色名稱或使用預設值。此範例使用*### EvRole#*

6. 選擇下一步：標籤。
7. (選用) 您可使用標籤作為金鑰值對，將中繼資料新增至政策。
8. 選擇下一步：檢閱。
9. 在 [檢閱原則] 頁面上，輸入 [名稱]，例如 ***AutotionEV RolePolicy*** 和選用的 [說明]。
10. 檢閱 [摘要] 頁面以查看原則允許的權限。如果您滿意您的政策，請選擇 [建立政策]。

此政策定義角色可以採取的動作。若需詳細資訊，請參閱《IAM 使用者指南》中的建立 IAM 政策 (主控台)。

建立 IAM 角色

建立政策之後，必須建立 IAM 角色，並將政策連接到該角色。

若要建立 AWS 服務的角色

1. 登入 AWS Management Console 並開啟身分與存取權管理主控台，網址為 https://console.aws.amazon.com/iam/。
2. 在導覽窗格中，選擇 Roles (角色)，然後選擇 Create role (建立角色)。
3. 對於 Select type of trusted entity (選取信任的實體類型)，選擇 AWS service (服務)。
4. 針對您要允許擔任此角色的服務選擇 EC2。
5. 選擇下一步：許可。
6. 輸入您建立的策略名稱，例如 *AutotionEV RolePolicy*，然後選取策略旁邊的核取方塊。
7. 選擇下一步：標籤。
8. (選用) 您可使用標籤作為金鑰值對，將中繼資料新增至角色。
9. 選擇下一步：檢閱。
10. 針對角色名稱，輸入*### Ev* Role。此名稱必須與您建立的 IAM 政策的 ARN 中顯示的名稱相同。
11. (選用) 在 Role description (角色說明) 中，輸入角色的說明。
12. 檢閱角色，然後選擇建立角色。

如需詳細資訊，請參閱 IAM 使用者指南中的為 AWS 服務建立角色。

更新信任政策

最後，您可以更新所建立角色的信任原則。您必須完成此程序，才能在 EventBridge 主控台中選擇此角色。

更新角色的信任原則

1. 登入 AWS Management Console 並開啟身分與存取權管理主控台，網址為 https://console.aws.amazon.com/iam/。
2. 在導覽窗格中，選擇角色。
3. 在您 AWS 帳戶的角色清單中，選擇您建立的角色名稱，例如*### E* vRole。
4. 選擇 Trust Relationships (信任關係) 標籤，然後選擇 Edit Trust Relationship (編輯信任關係)。

5. 對於「策略文件」，請複製下列 JSON、移除預設政策，然後將複製的 JSON 貼到其位置。

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

6. 選擇 Update Trust Policy (更新信任政策)。

如需詳細資訊，請參閱《IAM 使用者指南》中的修改角色信任政策 (主控台)。

建立規則 EventBridge

遵循此程序在 EventBridge 主控台中建立規則，以便您可以自動執行排定要停用的 EC2 執行個體的停止和啟動。

建立 Systems Manager 自動化動作 EventBridge 的規則

1. 在以下位置打開 Amazon EventBridge 控制台 https://console.aws.amazon.com/events/。
2. 在導覽窗格的 Events (事件) 下，選擇 Rules (規則)。
3. 在 [建立規則] 頁面上，輸入規則的 [名稱] 和 [說明]。
4. 在 Define pattern (定義模式) 下，選擇 Event pattern (事件模式)，然後選擇 Pre-defined pattern by service (依服務預先定義模式)。
5. 針對服務供應商，選擇 AWS。
6. 針對服務名稱，選擇 Health。
7. 針對事件類型，選擇特定 Health 事件。
8. 選擇 [特定服務]，然後選擇 [EC2]。
9. 選擇 [特定事件類型]，然後選擇 [scheduled Change]。

10. 選擇 [特定事件類型程式碼]，然後選擇事件類型代碼。

    例如，對於 Amazon EC2 EBS 支援的執行個體，請選擇。**AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED**對於 Amazon EC2 執行個體商店支援的執行個體，請選擇。**AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED**

11. 選擇 Any resource (任何資源)。

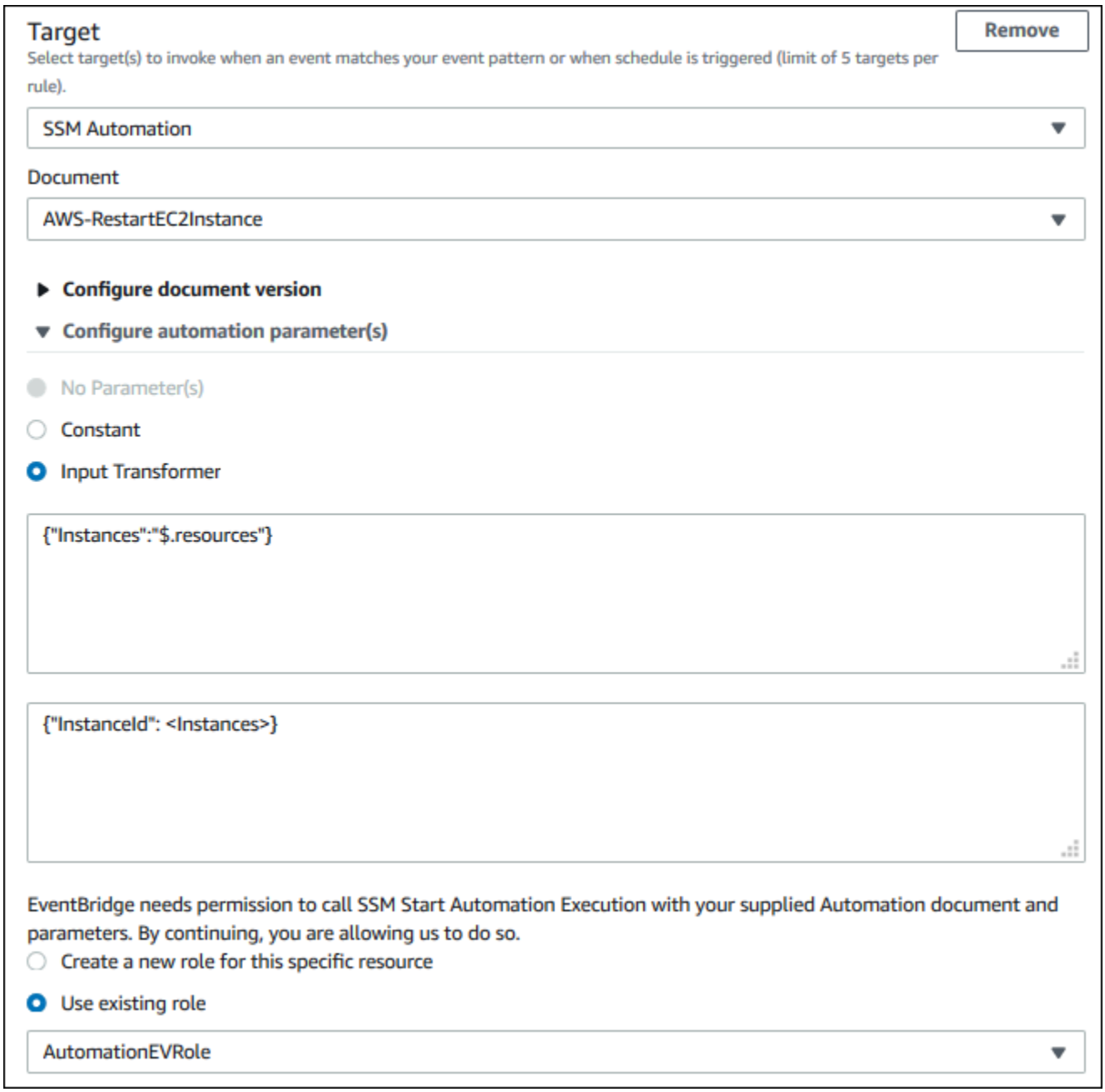
    您的事件模式看起來會類似下列範例。

    Example

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

12. 新增系 Systems Manager 自動化文件目標。在「選取目標」 下，選擇「SSM 自動化」做為「目標」。
13. 對於 Document (文件)，請選擇 AWS-RestartEC2Instance。
14. 展開 [設定自動化參數]，然後選擇 [輸入變壓器]。
15. 在「輸入路徑」欄位中輸入**{"Instances":"$.resources"}**。
16. 對於第二個欄位，輸入**{"InstanceId": <Instances>}**。
17. 選擇 [使用現有角色]，然後選擇您建立的 IAM 角色，例如### *E* vRole。

    您的目標應該看起來像下面的例子。



> **Note**
>
> 如果您沒有具有所需 EC2 和 Systems Manager 許可和受信任關係的現有 IAM 角色，則您的角色將不會顯示在清單中。如需詳細資訊，請參閱 必要條件。

18. 選擇 Create（建立）。

如果您的帳戶中發生與規則相符的事件，則 EventBridge 會將事件傳送至您指定的目標。

設定 SMC 連接器 AWS Health

您可以將 AWS Health 事件與 JIRA 整合， ServiceNow 以及使用服務管理連接器 (SMC) 接收作業和帳戶資訊、準備排定的變更，以及管理 Health 事件。SMC 整合 AWS Health 可以使用傳送至的 Health 全狀況事件 EventBridge 來自動建立、對應及更新 JIRA 票證和 ServiceNow事件。

您可以使用組織檢視和委派的系統管理員存取權，輕鬆管理 JIRA 內整個組織的 Health 事件 ServiceNow，並將 AWS Health 資訊直接納入團隊的工作流程中。

如需有關使用 SMC 進行 ServiceNow 整合的詳細資訊，請參閱整合 AWS Health 於 ServiceNow。

如需使用 SMC 的 JIRA 管理雲端整合的詳細資訊，請參閱 JIRA AWS Health 中的。

監控 AWS Health

監控是維持其他 AWS 解決方案的可靠性、可用性和效能的 AWS Health 重要組成部分。 AWS 提供下列監控工具來監視 AWS Health、回報錯誤，並在適當時採取行動：

- Amazon 會即時 CloudWatch 監控您的 AWS 資源和執行 AWS 的應用程式。您可以收集和追蹤指標、建立自訂儀板表，以及設定警示，在特定指標達到您指定的閾值時通知您或採取動作。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。

  您可以使用 Amazon，以 EventBridge 便您收到可能影響服務和資源的 AWS Health 事件的通知。例如，如果 AWS Health 發佈有關 Amazon EC2 執行個體的事件，您可以使用這些通知採取行動，並視需要更新或更換資源。如需詳細資訊，請參閱 使用 Amazon 監控 AWS Health 事件 EventBridge。
- AWS CloudTrail 擷取您帳戶或代表您 AWS 帳戶發出的 API 呼叫和相關事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。如需詳細資訊，請參閱 AWS CloudTrail 使用者指南。

主題

使用記錄 AWS Health API 呼叫 AWS CloudTrail

AWS Health 與 (提供中的使用者 AWS CloudTrail、角色或服務所採取的動作記錄) 的 AWS 服務整合 AWS Health。 CloudTrail 擷取 AWS Health 做為事件的 API 呼叫。擷取的呼叫包括來自 AWS Health 主控台的呼叫和 AWS Health API 作業的程式碼呼叫。如果您建立追蹤，您可以啟用持續交付 CloudTrail 事件到 Amazon S3 儲存貯體，包括 AWS Health. 如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。使用收集的資訊 CloudTrail，您可以判斷提出的要求 AWS Health、提出要求的來源 IP 位址、提出要求的人員、提出要求的時間以及其他詳細資訊。

若要進一步了解 CloudTrail，包括如何設定和啟用它，請參閱AWS CloudTrail 使用者指南。

AWS Health 中的資訊 CloudTrail

CloudTrail 在您創建 AWS 帳戶時，您的帳戶已啟用。當受支援的事件活動發生在中時 AWS Health，該活動會與 CloudTrail 事件歷史記錄中的其他 AWS 服務事件一起記錄在事件中。您可以在帳戶中查看，搜索和下載最近的事 AWS 件。如需詳細資訊，請參閱檢視具有事 CloudTrail 件記錄的事件。

如需 AWS 帳戶中持續記錄事件 (包括的事件) AWS Health，請建立追蹤。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。根據預設，當您在主控台中建立追蹤時，追蹤會套用至所有 AWS 區域。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 Amazon S3 儲存貯體。此外，您還可以設定其他 AWS 服務，以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務與整合
- 設定 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 記錄檔並從多個帳戶接收 CloudTrail 記錄檔

所有 AWS Health API 操作都會記錄在 API 參考中， CloudTrail 並記錄在 AWS Health API 參考中。例如，呼叫`DescribeEventsDescribeEventDetails`、和`DescribeAffectedEntities`作業會在 CloudTrail 記錄檔中產生項目。

AWS Health 支援將下列動作記錄為記 CloudTrail 錄檔中的事件：

- 請求是使用根登入資料還是 IAM 登入資料提出
- 提出該請求時，是否使用了特定角色或聯合身分使用者的臨時安全憑證
- 請求是否由其他 AWS 服務提出

如需詳細資訊，請參閱CloudTrail 使 userIdentity 元素。

您可以視需要將日誌檔存放在 Amazon S3 儲存貯體中。您也可以定義 Amazon S3 生命週期規則以自動封存或刪除日誌檔案。您的日誌檔案預設使用 Amazon S3 伺服器端加密 (SSE) 加密。

若要在日誌檔交付時收到通知，您可以設定 CloudTrail 為在交付新的日誌檔時發佈 Amazon SNS 通知。如需詳細資訊，請參閱為 CloudTrail.

您也可以將來自多個 AWS 區域和多個 AWS 帳戶的 AWS Health 日誌檔彙總到單一 Amazon S3 儲存貯體。

如需詳細資訊，請參閱從多個區域接 CloudTrail 收 CloudTrail 記錄檔和從多個帳戶接收記錄檔。

範例： AWS Health 記錄檔項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。事件代表來自任何來源的單一請求，包括有關請求的操作，動作的日期和時

間，請求參數等信息。 CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

下列範例顯示示範DescribeEntity彙總作業的 CloudTrail 記錄項目。

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

的文件歷史記錄 AWS Health

下表說明此版本的文件 AWS Health。

- API 版本：2016-08-04

下表說明 AWS Health 文件的重要更新，從 2020 年 8 月 28 日開始。您現在可以訂閱 RSS 摘要，接收有關更新的通知。

變更	描述	日期
已從「 AWS Health 安全性」區段文件移除網路間流量隱私權	如需詳細資訊，請參閱中的安全性AWS Health	2024年3月27日
更新了 AWS Health 儀表板-服務健康狀態和計劃生命週期事 AWS Health 件的文檔。	如需詳細資訊，請參閱AWS Health 儀表板 — 的服務健康狀況和計劃生命週期事件 AWS Health。	2024年2月15日
移除建立 EventBridge 規則中的重複 bullet 點 AWS Health	在建立 EventBridge 規則中移除重複的 bullet 點 AWS Health。	2023 年 12 月 4 日
新增規劃生命週期事件的文件	如需詳細資訊，請參閱的計劃生命週期事件 AWS Health。	2023 年 10 月 31 日
更新 AWSHealthFullAccess 的說明文件	您現在可以使用中的 AWSHealthFullAccess 受管理策略 AWS GovCloud (US) Regions。請參閱的AWS 受管政策 AWS Health。	2023 年 10 月 16 日
已新增在中設定 AWS 使用者通知的文件 AWS Health。	您現在可以在中設定 AWS 使用者通知 AWS Health。如需詳細資訊，請參閱設定的 AWS 使用者通知 AWS Health。	2023 年 8 月 30 日

已將委派管理員功能的文件新增至「彙總 AWS Health 事件」區段。	如需詳細資訊，請參閱委派管理員組織檢視。	2023 年 7 月 27 日
單反政策更新	AWS 受管理策略的更新：健康 _ OrganizationsServiceRolePolicy。如需詳細資訊，請參閱 AWS Health的AWS 受管政策。	2023 年 7 月 19 日
AWS Health 模式現在支持事件元數據	您現在可以從事件接收事件中 AWS Health 繼資料。如需詳細資訊，請參閱使用 Amazon 監控 AWS Health 事件 EventBridge。	2023 年 6 月 20 日
Amazon 更新的文檔 EventBridge	您現在可以使用 Amazon EventBridge 規則來監控帳戶特定事件和公開事件。如需詳細資訊，請參閱使用 Amazon 監控 AWS Health 事件 EventBridge。	2023 年 5 月 2 日
已新增 AWS 受管理原則的文件	已新增針對以 AWS Health及使用服務連結角色之AWS 受管理策略的 AWS Health文件。	2023 年 1 月 18 日
添加時區設置文檔	使用新的時區功能，以當地時區或 UTC 檢視「 AWS Health 儀表板」。如需詳細資訊，請參閱AWS Health 儀表板入門 — 您的帳戶健康狀態和AWS Health 儀表板 — 服務健康狀態。	2022 年 9 月 21 日
已更新的文件	已新增 AWS Health Aware 的文件。如需詳細資訊，請參閱 AWS Health Aware。	2022 年 5 月 25 日

已更新的文件	Service Health Dashboard 和AWS Personal Health Dashboard已重新命名為「 AWS Health 儀表板」。 如需詳細資訊，請參閱AWS Health 儀表板入門 — 您的帳戶健康狀態和AWS Health 儀表板 — 服務健康狀態。	2022 年 2 月 28 日
Amazon 更新的文檔 EventBridge	使用 Amazon EventBridge 監控 Health 事件的新主題。AWS Health 如需詳細資訊，請參閱使用 Amazon 監控 AWS Health 事件 EventBridge。	2022 年 2 月 3 日
已更新的文件	如果您有企業版支 Support 方案，則可以使用 AWS Health API。	2021 年 11 月 24 日
添加的文檔	AWS Health 概念的新主題。如需詳細資訊，請參閱 AWS Health.	2021 年 7 月 29 日
對於 CloudWatch 事件更新的文檔	已新增有關如何為多個服務和事件類型類別建立規則的章節。如需詳細資訊，請參閱為多個服務和類別建立規則。	2021 年 5 月 7 日
對於 CloudWatch 事件更新的文檔	更新區段以自動執 AWS Systems Manager 行 Amazon CloudWatch 活動規則的動作。如需詳細資訊，請參閱自動執行 Amazon EC2 執行個體的動作。	2021 年 4 月 28 日

對於 CloudWatch 事件更新的文檔	新增區段可在聊天用戶端中接收 AWS Health 事件。如需詳細資訊，請參閱使用接收 AWS Health 事件 AWS Chatbot。	2021 年 3 月 16 日
已更新的文件	下列主題更新： • 更新了彙總 AWS Health 事件主題 • 使用 Amazon AWS Health 事件主題重新組織和更新監控 CloudWatch 事件 • 更新了基於資源和行動的條件部分	2021 年 1 月 29 日
在主控台中新增組織檢 AWS Health 視的 AWS Health 儀表板	您可以使用主 AWS Health 控台來啟用組織檢視功能。然後，您可以檢視 AWS 組織中成員帳戶的健康事件。	2020 年 12 月 14 日
高可用性端點示範	您可以使用範例程式碼來判斷的作用中地區端點和簽署 AWS 區域 AWS Health。	2020 年 10 月 22 日
AWS Health 使用者指南的更新	組織會更新並新增 RSS 摘要，以便您可以訂閱 AWS Health 文件的最新更新。	2020 年 8 月 28 日

舊版更新

變更	描述	日期
更新組織檢視主題以包含範例。	請參閱使用組織檢視跨帳戶彙總 AWS Health 事件。	2020 年 6 月 3 日

變更	描述	日期
安全性和 AWS Health	新增了關於使用 AWS Health 時，安全性考量的資訊。請參閱中的安全性 AWS Health。	二零二零年五月五日
已新增章節說明如何對 AWS Organizations中所有帳戶之間彙總的事件使用組織檢視。	請參閱使用組織檢視跨帳戶彙總 AWS Health 事件。	2019 年 12 月 18 日
添加了新的「基於資源和操作的條件」部分，以解釋 API 提供的事件限制。 AWS Health	請參閱適用於 AWS Health 的 Identity and Access Management。	2018 年 8 月 2 日
已新增有關 AWS Health 資訊可見度的附註。	請參閱適用於 AWS Health 的 Identity and Access Management。	2017 年 8 月 16 日
服務版本。	AWS Health 已發行。	2016 年 12 月 1 日

AWS 詞彙表

如需最新的 AWS 術語，請參閱《AWS 詞彙表 參考》中的 AWS 詞彙表。

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。