



使用者指南

AWS Health



AWS Health: 使用者指南

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

什麼是 AWS Health ?	1
的概念 AWS Health	2
AWS Health 事件	2
帳戶特定事件	3
公有事件	3
AWS Health 儀表板	3
AWS Health 儀表板 – 服務運作狀態	3
事件類型程式碼	4
事件類型類別	4
事件狀態	5
可操作性	5
角色	6
受影響的實體	6
AWS Health Amazon EventBridge 上的事件	6
AWS Health API	7
組織檢視	7
AWS 使用者通知	7
開始使用	8
設定	8
註冊 AWS 帳戶	8
建立具有管理存取權的使用者	9
在 AWS Health 儀表板中檢視帳戶事件	10
開啟和最近的問題	10
排程變更	12
其他通知	12
事件日誌	13
事件詳細資訊	14
事件類型	15
行事曆檢視	16
受影響的資源檢視	17
時區設定	18
您的組織運作狀態	18
AWS Health 事件的提醒	18
設定 Amazon EventBridge	19

在 中管理通知 AWS 使用者通知	20
設定事件的 AWS 受管通知訂閱 AWS Health	20
AWS 受管通知常見問答集	21
AWS Health 儀表板	23
的計劃生命週期事件 AWS Health	25
什麼是規劃的生命週期事件？	25
收到規劃的生命週期事件通知時，應預期會發生什麼情況？	26
彈性的共同責任模型	27
存取規劃的生命週期事件	28
使用 AWS Health API 與其他系統整合	29
簽署 AWS Health API 請求	29
選擇 AWS Health API 請求的端點	30
示範：以程式設計方式擷取過去七天的事件資料	31
示範：使用 Java 擷取過去七天 AWS Health 的事件資料	32
示範：使用 Python 擷取過去七天 AWS Health 的事件資料	35
教學課程：搭配 Java 範例使用 AWS Health API	37
步驟 1：初始化登入資料	37
步驟 2：初始化 AWS Health API 用戶端	38
步驟 3：使用 AWS Health API 操作來取得事件資訊	38
安全	42
資料保護	42
資料加密	43
身分與存取管理	44
目標對象	44
使用身分驗證	44
使用政策管理存取權	45
AWS Health 如何使用 IAM	47
身分型政策範例	51
疑難排解	63
使用服務連結角色	66
AWS 的 受管政策 AWS Health	67
在 中記錄和監控 AWS Health	72
法規遵循驗證	73
恢復能力	73
基礎設施安全性	73
組態與漏洞分析	73

安全最佳實務	74
授予 AWS Health 使用者最低可能許可	74
檢視 Health 儀板表	74
AWS Health 與 Amazon Chime 或 Slack 整合	74
監控 AWS Health 事件	74
彙總 AWS Health 事件	75
先決條件	75
啟用組織檢視	76
檢視組織檢視	79
停用組織檢視	84
管理組織的委派管理員檢視	85
註冊委派管理員帳戶	85
移除委派管理員帳戶	85
使用 EventBridge 監控運作狀態事件	87
建立涵蓋 AWS 區域 範圍的 EventBridge 規則	88
高可用性設定 (選用)	88
簡化整合	88
全域事件	89
監控 的帳戶特定和公有事件 AWS Health	89
AWS Health 事件的備份規則	90
檢視 EventBridge 上的 AWS Health 事件分頁清單	90
使用組織檢視和委派管理員存取權彙總 AWS Health 事件	91
將 AWS Health 事件監控和通知與 JIRA 和 ServiceNow 整合	91
設定 EventBridge 規則以傳送有關事件的通知	92
使用 API 或 AWS Command Line Interface	92
在聊天應用程式中設定 Amazon Q Developer 以傳送事件通知	94
先決條件	94
在 EC2 執行個體上自動執行操作以回應事件	96
先決條件	97
建立 EventBridge 的規則	100
參考：AWS Health 事件 Amazon EventBridge 結構描述	104
AWS Health 事件結構描述	104
公有運作狀態事件 - Amazon EC2 操作問題	113
帳戶特定 AWS Health 事件 - Elastic Load Balancing API 問題	114
帳戶特定 AWS Health 事件 - Amazon EC2 執行個體存放區磁碟機效能降低的備份事件	115
帳戶特定 AWS Health 事件 - Amazon EC2 執行個體淘汰	116

帳戶特定 AWS Health 事件 - Lambda 計劃生命週期事件	117
監控 AWS Health	119
使用 記錄 AWS Health API 呼叫 AWS CloudTrail	119
AWS Health CloudTrail 中的資訊	119
範例：AWS Health 日誌檔案項目	121
文件歷史紀錄	123
舊版更新	130
.....	cxxxii

什麼是 AWS Health ？

AWS Health 可讓您持續查看資源效能，以及 AWS 服務 和 帳戶的可用性。您可以使用 AWS Health 事件來了解服務和資源變更如何影響您在上執行的應用程式 AWS。AWS Health 提供相關且及時的資訊，協助您管理進行中的事件。AWS Health 也可協助您了解並準備規劃的活動。該服務提供由 AWS 資源運作狀態變更觸發的提醒和通知，以便您獲得近乎即時的事件可見性和指導，以協助加速故障診斷。

所有客戶都可以使用由 AWS Health API 提供支援的 [AWS Health Dashboard](#)。儀表板不需要設定，且可供 [已驗證 AWS 的使用者](#) 使用。如需更多服務重點，請參閱 [AWS Health 儀表板詳細資訊頁面](#)。

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

若要了解使用 服務時將遇到的 AWS Health 和 術語的基本概念，若要了解 的基本概念，AWS Health 請參閱 [的概念 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 客戶都可以透過 Amazon EventBridge 接收 AWS Health 事件，無需額外費用。
- 如果您有 AWS Business Support+、AWS Enterprise Support 或 AWS Unified Operations 計劃，您可以使用 AWS Health API 與內部和第三方系統整合。如果您所在的 AWS 區域 未提供其中一個 AWS 支援 計劃，或者您尚未轉換至其中一個計劃，則可以使用 AWS Health API 搭配 Business、Enterprise On-Ramp 或 Enterprise Support 計劃。如需詳細資訊，請參閱 [AWS Health API 參考](#)。
- 如需可用 AWS 支援 計劃的詳細資訊，請參閱 [AWS 支援](#)。

的概念 AWS Health

了解 AWS Health 概念，並了解如何使用 服務來維護 中應用程式、服務和資源的運作狀態 AWS 帳戶。

主題

- [AWS Health 事件](#)
- [AWS Health 儀表板](#)
- [事件類型程式碼](#)
- [事件類型類別](#)
- [事件狀態](#)
- [可操作性](#)
- [角色](#)
- [受影響的實體](#)
- [AWS Health Amazon EventBridge 上的事件](#)
- [AWS Health API](#)
- [組織檢視](#)
- [AWS 使用者通知](#)

AWS Health 事件

AWS Health 事件也稱為運作狀態事件，是代表其他服務 AWS Health 傳送的通知 AWS。您可以使用這些事件來了解可能會影響您帳戶的近期或排程變更。例如，如果 AWS Identity and Access Management (IAM) 計劃取代受管政策或 AWS Config 計劃取代受管規則，AWS Health 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。您可以檢閱事件描述以了解問題、識別任何受影響的資源，並採取任何建議的動作。

運作狀態事件有兩種類型：

內容

- [帳戶特定事件](#)
- [公有事件](#)

帳戶特定事件

帳戶特定事件是您 AWS 帳戶 或 AWS 組織中帳戶的本機事件。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，AWS Health 會提供事件和受影響資源名稱的相關資訊。

您可以從 [AWS Health 儀表板](#)、[AWS Health API](#) 找到帳戶特定的事件，或使用 [Amazon EventBridge](#) 或 [AWS 使用者通知](#) 來接收通知。

公有事件

公有事件是非特定於帳戶的服務事件。例如，如果美國東部（俄亥俄）區域中的 Amazon Simple Storage Service (Amazon S3) 發生服務問題，AWS Health 會提供事件的相關資訊，即使您未使用該服務或在該區域中有 S3 儲存貯體。我們建議您先檢閱公有通知，再對其採取行動。

您可以從 AWS Health 儀表板和 AWS Health 儀表板 – 服務運作狀態找到公有事件。

如果您有帳戶，請參閱 [AWS Health 儀表板入門](#)。

如果您沒有帳戶，請參閱 [AWS Health 儀表板](#)。

AWS Health 儀表板

如果您有 AWS 帳戶，AWS Health 儀表板會顯示公有事件和帳戶特定事件。

我們建議您使用 AWS Health Dashboard 來了解提供一般意識的事件，例如區域中服務即將發生的維護問題。您也可以使用 AWS Health 儀表板來了解可能直接影響您的事件，例如帳戶中已棄用的資源。

您可以在 <https://health.aws.amazon.com/health/home> 登入 AWS 管理主控台 以檢視您的 AWS Health Dashboard。

如需詳細資訊，請參閱 [AWS Health 儀表板入門](#)。

AWS Health 儀表板 – 服務運作狀態

如果您沒有帳戶，您可以使用位於 <https://health.aws.amazon.com/health/status> 的 AWS Health Dashboard – Service Health 來檢視公有事件。公有事件是回報的服務問題 AWS，可提供服務可用性的相關資訊。此網站只會顯示公有事件，這些事件並非特定於任何帳戶。您不需要登入或擁有帳戶即可檢視此頁面。

如需詳細資訊，請參閱 [AWS Health 儀表板](#)。

事件類型程式碼

運作狀態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AWS_EC2_SYSTEM_MAINTENANCE_EVENT事件類型代碼的運作狀態事件，這表示服務正在排程可能會影響您的維護事件。使用此資訊提前規劃或為您的帳戶採取動作。

事件類型類別

所有運作狀態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程式碼中，例如AWS_RDS_MAINTENANCE_SCHEDULED程式碼。在此範例中，已排程類別。您可以使用此資訊來了解高階的事件類別。

最佳實務是監控所有事件類型類別。請注意，每個類別都會針對不同類型的事件顯示。您也可以使用 [DescribeEventTypes](#) API 操作來尋找事件類型類別。

帳戶通知

這些事件提供有關帳戶和服務管理或安全性的資訊。這些事件可能具有資訊性，或者可能需要您採取緊急動作。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 – 您有一個可能允許公開存取的 Amazon S3 儲存貯體。
- AWS_BILLING_SUSPENSION_NOTICE – 您的帳戶有未結清的費用，並已暫停，或您已停用您的帳戶。
- AWS_WORKSPACES_OPERATIONAL_NOTIFICATION – Amazon WorkSpaces 發生服務問題。

問題

這些事件是會影響 AWS 服務或資源的非預期事件。此類別中的常見事件包括有關導致服務降級之操作問題的通訊，或用於您意識的本地化資源層級問題。

以下是問題的範例事件類型代碼：

- AWS_EC2_OPERATIONAL_ISSUE – 服務的操作問題，例如使用服務的延遲。
- AWS_EC2_API_ISSUE – 服務 API 的操作問題，例如 API 操作的延遲增加。
- AWS_EBS_VOLUME_ATTACHMENT_ISSUE – 可能影響 Amazon Elastic Block Store (Amazon EBS) 資源的當地語系化資源層級問題。

- `AWS_ABUSE_PII_CONTENT_REMOVAL_REPORT` – 此事件表示如果您不採取動作，您的帳戶可能會被暫停。

排定的變更

這些事件提供有關即將對您的服務和資源進行變更的資訊。這些事件包括計劃的生命週期事件，例如end-of-support通知和不同版本的自動升級。有些事件可能會建議您採取動作來避免服務中斷，而其他事件則會自動發生，而不需要採取任何動作。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的事件。

以下是排程變更的事件類型代碼範例：

- `AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED` – Amazon EC2 執行個體需要重新啟動。
- `AWS_SAGEMAKER_SCHEDULED_MAINTENANCE` – SageMaker AI 需要維護事件，例如修正服務問題。
- `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，這需要客戶動作。

Tip

如果您使用 AWS Health API 或 AWS Command Line Interface (AWS CLI) 傳回事件詳細資訊，Event 物件會包含具有 `ACCOUNT_SPECIFIC` 值 `eventScopeCode` 的欄位。如需詳細資訊，請參閱 [AWS Health API 參考](#)。

事件狀態

事件狀態會告訴您運作狀態事件是開啟、關閉還是即將發生。您可以在 AWS Health 儀表板或 AWS Health API 中檢視運作狀態事件長達 90 天。

可操作性

可操作性是一個欄位，可協助您根據是否需要您採取動作來排定運作狀態事件的優先順序。運作狀態事件包含可操作性狀態，指出是否需要採取動作來降低 AWS 資源的風險，或事件是否為資訊性質。

可操作性欄位可以包含下列其中一個值：

- `ACTION_REQUIRED`：具有此狀態的事件需要您採取動作，以減輕與 AWS 資源可用性、帳單或安全性相關的潛在影響。

- **ACTION_MAY_BE_REQUIRED**：具有此狀態的事件會根據您的特定實作、相依性和工作流程，傳達需要採取動作的變更。這些事件需要您檢閱，以判斷是否需要採取動作。
- **INFORMATIONAL**：具有此狀態的事件可讓您持續查看所使用 AWS 服務的操作資訊。預期不會立即採取任何動作。

Note

與服務問題相關的運作狀態事件不包含可操作性標籤，因為復原動作的需求取決於您的特定應用程式架構。

角色

角色欄位提供聯絡人清單，協助您將相關資訊路由到組織內適當的團隊。每個運作狀態事件可以包含下列一或多個角色：

- **OPERATIONS**：適用於與營運活動和服務可用性相關的事件。
- **SECURITY**：適用於與安全性考量相關的事件。
- **BILLING**：適用於具有潛在成本影響的事件。

例如，當 AWS 傳送有關轉換為延伸支援之標準支援結束的事件時，除了 OPERATIONS 之外，該事件 BILLING 還包含在角色清單中，以協助確保資訊到達負責成本管理的團隊。

受影響的實體

受影響的實體是可能受到事件影響 AWS 的資源。例如，如果您收到帳戶中使用之特定執行個體類型的 Amazon EC2 維護排程事件，您可以使用運作狀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，例如建立或取代資源。

AWS Health Amazon EventBridge 上的事件

您可以為您的帳戶設定 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到聊天介面。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 [AWS Health 使用 Amazon EventBridge 監控 中的事件](#)。

AWS Health API

您可以使用 AWS Health API 以程式設計方式存取 [AWS Health 儀表板](#) 中顯示的資訊，如下所示：

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

如需詳細資訊，請參閱 [AWS Health API 參考](#)。

Note

您必須擁有來自的 AWS Business Support+、AWS Enterprise Support 或 AWS Unified Operations 計劃 [AWS 支援](#)，才能使用 AWS Health API。如果您從沒有 AWS Business Support+、AWS Enterprise Support 或 AWS Unified Operations 計劃的帳戶呼叫 AWS Health API，您會收到 `SubscriptionRequiredException` 錯誤。

組織檢視

您可以使用此功能，將中 AWS 帳戶的所有運作狀態事件彙總 AWS Organizations 至 AWS Health 儀表板中的單一檢視。然後，您可以登入組織的管理帳戶，或使用 AWS Health API 檢視可能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。如需詳細資訊，請參閱 [跨帳戶彙總 AWS Health 事件](#)。

AWS 使用者通知

AWS Health 與整合 [AWS 使用者通知](#)，因此您可以輕鬆接收和控制影響 AWS 帳戶和服務的事件通知。預設使用者通知會提供 AWS Health 事件的受管通知。您可以設定這些訂閱，以控制透過以時間為基礎的彙總接收訊息的頻率、收到通知 AWS Health 的事件類型，以及通知的傳遞位置。若要開始使用，請在 [使用者通知](#) 中開啟 [AWS 管理主控台](#)。如需詳細資訊，請參閱 [在中管理 AWS Health 通知](#) [AWS 使用者通知](#)

AWS Health 儀表板入門

您可以使用 AWS Health 儀表板來了解 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](#) – 此頁面顯示您帳戶特有的事件。您可以檢視開啟、最近和排定的變更。您也可以檢視通知和事件日誌，其中顯示過去 90 天的所有事件。
- [您的組織事件](#) – 此頁面顯示您的組織特定的事件 AWS Organizations。您可以檢視組織的開啟中、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，您可以使用 [AWS Health 儀表板](#) 來了解一般服務可用性。如果您有帳戶，建議您登入 AWS Health 儀表板，以深入了解可能會影響您服務和資源的事件和近期變更。

主題

- [設定 AWS 您的帳戶](#)
- [在 AWS Health 儀表板中檢視您的帳戶事件](#)
- [設定 Amazon EventBridge](#)
- [在中管理 AWS Health 通知 AWS 使用者通知](#)

設定 AWS 您的帳戶

您必須先擁有 AWS Health，才能啟用 AWS 帳戶。如果您沒有 AWS 帳戶，請完成下列步驟來建立帳戶。

註冊 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個。

註冊 AWS 帳戶

1. 開啟 <https://portal.aws.amazon.com/billing/signup>。

2. 請遵循線上指示進行。

部分註冊程序需接收來電或簡訊，並在電話鍵盤輸入驗證碼。

當您註冊時 AWS 帳戶，AWS 帳戶根使用者會建立。根使用者有權存取該帳戶中的所有 AWS 服務和資源。作為安全最佳實務，請將管理存取權指派給使用者，並且僅使用根使用者來執行 [需要根使用者存取權的任務](#)。

AWS 會在註冊程序完成後傳送確認電子郵件給您。您可以隨時登錄 <https://aws.amazon.com/> 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

建立具有管理存取權的使用者

註冊後 AWS 帳戶，請保護 AWS 帳戶根使用者、啟用 AWS IAM Identity Center 和建立管理使用者，以免將根使用者用於日常任務。

保護您的 AWS 帳戶根使用者

1. 選擇根使用者並輸入 AWS 帳戶您的電子郵件地址，以帳戶擁有者 [AWS 管理主控台](#) 身分登入。在下一頁中，輸入您的密碼。

如需使用根使用者登入的說明，請參閱 AWS 登入使用者指南中的 [以根使用者身分登入](#)。

2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

如需說明，請參閱《IAM 使用者指南》中的 [為您的 AWS 帳戶根使用者（主控台）啟用虛擬 MFA 裝置](#)。

建立具有管理存取權的使用者

1. 啟用 IAM Identity Center。

如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的 [啟用 AWS IAM Identity Center](#)。

2. 在 IAM Identity Center 中，將管理存取權授予使用者。

如需使用 IAM Identity Center 目錄做為身分來源的教學課程，請參閱 AWS IAM Identity Center 《使用者指南》中的 [使用預設值設定使用者存取 IAM Identity Center 目錄](#)。

以具有管理存取權的使用者身分登入

- 若要使用您的 IAM Identity Center 使用者簽署，請使用建立 IAM Identity Center 使用者時傳送至您電子郵件地址的簽署 URL。

如需使用 IAM Identity Center 使用者登入的說明，請參閱AWS 登入 《使用者指南》中的[登入 AWS 存取入口網站](#)。

指派存取權給其他使用者

- 在 IAM Identity Center 中，建立一個許可集來遵循套用最低權限的最佳實務。

如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的[建立許可集](#)。

- 將使用者指派至群組，然後對該群組指派單一登入存取權。

如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的[新增群組](#)。

在 AWS Health 儀表板中檢視您的帳戶事件

您可以登入您的帳戶，以取得個人化事件和建議。

在 AWS Health 儀表板中檢視帳戶事件

- 在 <https://health.aws.amazon.com/health/home> 開啟您的 AWS Health 儀表板。
- 在導覽窗格中，針對您的帳戶運作狀態，您可以選擇下列選項：
 - [開啟和最近問題](#) – 檢視最近開啟和關閉的事件。
 - [排程變更](#) – 檢視可能影響您的服務和資源的近期事件。
 - [其他通知](#) – 檢視過去七天中可能會影響您帳戶的所有其他通知和持續事件。
 - [事件日誌](#) – 檢視過去 90 天的所有事件。


開啟和最近的問題

使用開啟和最近的問題索引標籤，檢視過去七天中可能影響您的帳戶的所有進行中事件。

當您從儀表板選擇事件時，詳細資訊窗格會顯示事件的相關資訊和受影響的資源清單。如需詳細資訊，請參閱[事件詳細資訊](#)。

您可以從篩選條件清單中選擇選項，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 AWS 服務等來縮小結果範圍。

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](#) 標籤。

 Note

目前，您無法刪除 AWS Health 儀表板中出現之事件的通知。在 AWS 服務 解析事件之後，通知會從儀表板檢視中移除。

Example : Amazon Elastic Compute Cloud (Amazon EC2) 的操作問題事件

下圖顯示 Amazon EC2 執行個體啟動失敗和連線問題的事件。

Your account health

Stay informed of important events affecting your AWS resources.

Configure EventBridge

Get notifications for events that might affect your services and resources.

[Go to EventBridge](#) ↗

[Open and recent issues \(16\)](#) |
 [Scheduled changes \(0\)](#) |
 [Notifications \(3\)](#) |
 [Event log](#)

Open and recent issues (16)

View events that might affect your AWS infrastructure. [35 issues](#) were resolved in the past 24 hours.

Service: Elastic Compute Cloud ✕

Clear filter

< 1 >

Event summary

Operational issue - EC2 (Ohio)
 Last update: February 20, 2022 at 11:16:34 PM UTC-8
 us-east-2

Operational issue - EC2 (Ohio)
 Last update: February 17, 2022 at 11:56:09 PM UTC-8
 us-east-2

Operational issue - EC2 (N. Virginia)
 Last update: February 16, 2022 at 1:36:29 AM UTC-8
 us-east-1

Operational issue - EC2 (Ohio) [Back to list view](#) ↗

Details
Affected resources

Event data

<p>Service EC2</p> <p>Status Open</p> <p>Region / Availability Zone us-east-1</p> <p>Account specific No</p>	<p>Start time February 20, 2022 at 11:16:24 PM UTC-8</p> <p>End time -</p> <p>Category Issue</p> <p>Affected resources 1</p>
--	--

Description

[04:35 AM PST] We are investigating increased EC2 launch failures and networking connectivity issues for some instances in a single Availability Zone (USE1-AZ4) in the US-EAST-1 Region. Other Availability Zones within the US-EAST-1 Region are not affected by this issue.

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近期事件。這些事件可能包括服務的排程維護活動，以及需要動作才能解決的計劃生命週期事件。為了協助您規劃這些活動，我們提供行事曆檢視，讓您可以將這些排定的變更映射到每月行事曆。篩選條件可供使用。如需計劃生命週期事件的詳細資訊，請參閱 [的計劃生命週期事件 AWS Health](#)。

其他通知

使用通知索引標籤來檢視過去七天中可能會影響您帳戶的所有其他通知和持續事件。這可能包括事件，例如憑證輪換、帳單通知和安全漏洞。

事件日誌

使用事件日誌索引標籤來檢視所有 AWS Health 事件。日誌資料表包含額外的資料欄，讓您可以依狀態和開始時間進行篩選。

當您在事件日誌資料表中選擇事件時，詳細資訊窗格會顯示事件的相關資訊和受影響的資源清單。如需詳細資訊，請參閱[事件詳細資訊](#)。

您可以選擇下列篩選條件選項來縮小結果範圍：

- 可用區域
- 結束時間
- 事件
- 事件 ARN
- 事件類別
- 上次更新時間
- 區域
- 資源 ID/ARN
- 服務
- 開始時間
- 狀態

Example：事件日誌

下圖顯示美國東部（維吉尼亞北部）和美國東部（俄亥俄）區域的最新事件。

Event log

Q Add filter

Region: US East N. Virginia (us-east-1), US East Ohio (us-east-2) X Clear filter

Last refreshed less than 1 min ago

Event	Status	Event category	Region / Zone	Start time	Last update time	Affected resources
Lambda operational issue	Closed	Issue	us-east-1	October 9, 2020 at 2:03:48 AM UTC-7	October 9, 2020 at 3:11:09 AM UTC-7	-
EC2 operational issue	Closed	Issue	us-east-1	October 9, 2020 at 1:48:51 AM UTC-7	October 9, 2020 at 11:54:16 AM UTC-7	-
SNS operational issue	Closed	Issue	us-east-1	September 30, 2020 at 8:28:18 AM UTC-7	September 30, 2020 at 11:42:54 AM UTC-7	-
EC2 operational issue	Closed	Issue	us-east-1	September 16, 2020 at 7:30:41 AM UTC-7	September 16, 2020 at 7:45:03 AM UTC-7	-
Storagegateway operational issue	Closed	Issue	us-east-1	September 13, 2020 at 12:46:47 PM UTC-7	September 13, 2020 at 6:32:24 PM UTC-7	-
Deepracer operational issue	Closed	Issue	us-east-1	August 31, 2020 at 6:32:39 PM UTC-7	August 31, 2020 at 9:10:12 PM UTC-7	-

事件詳細資訊

當您選擇事件時，會出現兩個關於事件的標籤。詳細資訊索引標籤會顯示下列資訊：

- 服務
- 狀態
- 區域/可用區域
- 事件是否為帳戶特定
- 開始及結束時間
- Category
- 受影響的資源數量
- 有關事件的描述和更新時間表

受影響的資源索引標籤會顯示受事件影響之任何 AWS 資源的下列相關資訊：

- 資源 ID (例如, Amazon EBS 磁碟區 ID, 例如 vol-a1b2c34f) 或 Amazon Resource Name (ARN), 如果可用或相關。
- 對於計劃的生命週期事件, 此受影響的資源清單也包含資源的最新狀態 (待定、未知或已解決)。此清單通常每 24 小時重新整理一次, 但最多可能需要 72 小時才能反映目前的狀態。

您可以篩選資源中出現的項目。您可以依資源 ID 或 ARN 縮小結果範圍。

Example : AWS Health event for AWS Lambda

下列螢幕擷取畫面顯示 Lambda 的範例事件。

The screenshot displays the AWS Health console interface. On the left, the 'Event log' section includes a search bar with 'Add filter', a filter box for 'Region: US East N. Virginia (us-east-1), US East Ohio (us-east-2)', and a 'Clear filter' button. Below the filter is a pagination control showing '1'. The 'Event summary' section lists several operational issues, with the top one highlighted: 'Lambda operational issue' (Last update: October 9, 2020 at 3:11:09 AM UTC-7 us-east-1). On the right, the 'Lambda operational issue' details are shown, including 'Affected resources' and 'Event data'. The 'Event data' section contains a table with the following information:

Event	Start time
Lambda operational issue	October 9, 2020 at 2:03:48 AM UTC-7
Status	End time
Closed	October 9, 2020 at 3:11:08 AM UTC-7
Region / Availability Zone	Affected resources
us-east-1	-
Category	
Issue	

The 'Description' section provides details about the issue: [RESOLVED] Increased Invoke Error Rate. It includes two updates: [02:03 AM PDT] We have identified an increase in invoke error rates in the US-EAST-1 Region and are working towards resolution. and [03:11 AM PDT] Between October 8 10:35 PM and October 9 2:25 AM PDT we experienced increased Lambda invoke error rates in the US-EAST-1 Region. The issue has been resolved and the service is operating normally.

事件類型

AWS Health 事件有兩種類型：

- 公有事件是非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, AWS Health 會提供事件的相關資訊, 即使您在該區域中未使用服務或資源。

- 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 AWS 區域 使用的 中的 Amazon EC2 執行個體發生問題，AWS Health 會提供事件和受影響 Amazon EC2 執行個體清單的相關資訊。

您可以使用下列選項來識別事件是公有事件還是帳戶特定事件：

- 在 AWS Health 儀表板中，選擇事件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[AWS Health 儀表板入門](#)。
- 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 Health API 參考中的 [DescribeEventDetails](#) 操作。

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 事件投影至每月行事曆。此檢視可讓您查看過去最多 3 個月和未來一年的排程變更。

AWS Health 事件會依日期顯示。選取日期以顯示包含 AWS Health 事件進一步詳細資訊的側邊面板。近期和持續的事件會以黑色顯示。已完成的事件會以灰色顯示。如果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取事件，以顯示事件的相關資訊。側邊面板具有導覽列，可導覽至較早的檢視。

Scheduled changes Table Calendar

View upcoming events and ongoing events from the past seven days that might affect your AWS infrastructure, such as scheduled maintenance activities.

🔍 Add filter Any event

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday
28	29 2 Upcoming	30 2 Upcoming 1 Completed	31	1	2

30 January 2024

Scheduled events starting on 30 January 2024 (Showing 3 of 3) [View all on the table view](#)

- [EKS planned lifecycle event \(us-west-2\)](#)
Event status: **Upcoming**
- [EKS planned lifecycle event \(us-east-1\)](#)
Event status: **Upcoming**
- [EKS planned lifecycle event \(eu-west-1\)](#)
Event status: **Completed**

受影響的資源檢視

AWS Health 事件可能會指定受影響的精確資源。您可以在 AWS Health 事件的受影響資源索引標籤中檢視受影響的資源。若要檢視狀態，請選取 AWS Health 事件。狀態會顯示在側邊面板中受影響的資源索引標籤中。對於計劃的生命週期事件，AWS Health 事件會提供受影響資源狀態的每日更新。

帳戶層級 AWS Health 事件會在受影響的資源索引標籤上方顯示受影響資源狀態的摘要。受影響的資源清單與對應的狀態會顯示在資料表中。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。若要進一步了解規劃的生命週期事件，請參閱 [的計劃生命週期事件 AWS Health](#)。

當您存取組織檢視時，AWS Health 事件會顯示所有包含帳戶之所有受影響資源的狀態摘要。摘要列出受影響的帳戶，以及該帳戶的待定資源數量之後。選取帳號或待定資源的數量，以顯示帳戶檢視摘要。帳戶檢視摘要具有導覽列，可導覽回受影響帳戶的組織清單。受影響的資源狀態摘要會顯示在分割面板的頂端。

您可以在受影響的資源索引標籤中下載 CSV 或 JSON 格式的受影響資源清單。在組織檢視中，下載的檔案包含列出帳戶中的所有資源。導覽至組織檢視中的帳戶層級，以在下載的檔案中僅包含該帳戶的資源。下載的檔案中每個受影響的資源都包含 AWS 帳戶 ID、eventARN、實體名稱、entityARN、狀態，以及資源的上次更新時間。如果啟用篩選條件，下載的檔案只會包含篩選結果。

您一次只能下載一個檔案。檔案會自動下載到瀏覽器的預設下載資料夾中，並具有根據的預設檔案名稱 AWS 區域、事件標題、事件開始日期和下載日期。

The screenshot displays the AWS Health console interface for a 'Scheduled changes' event. The event is titled 'Lambda planned lifecycle event' and is currently in a 'Pending' state. A summary shows 4 pending resources (100%), 0 unknown, and 0 resolved. Below the summary is a table of affected resources.

Resource ID / ARN	Resource status	Last update time
arn:aws:lambda:us-east-1:959586608611:function:SpringClean-XUG3HH5R-AutoUpdateLambda-atNXDvDUU6P	Pending	3 months ago
arn:aws:lambda:us-east-1:959586608611:function:SpringClean-XUG3HH5R-FeatureCheckerFunction-cwZkcPWUtAGy	Pending	3 months ago

時區設定

您可以在本機時區或 UTC 的 AWS Health 儀表板中檢視事件。如果您變更 AWS Health 儀表板中的時區，儀表板中的所有時間戳記和公有事件都會更新為您指定的時區。

更新您的時區設定

1. 在 <https://health.aws.amazon.com/health/home> 開啟您的 AWS Health 儀表板。
2. 在頁面底部，選擇 Cookie 偏好設定。
3. 選取允許功能 Cookie。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)。




您的組織運作狀態

AWS Health 與 整合 AWS Organizations，因此您可以檢視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[跨帳戶彙總 AWS Health 事件](#)。

Enable organizational view

Key benefits

 <p>Organization-wide visibility</p> <p>Aggregate your Health events from all member AWS accounts in your AWS organization. This provides a centralized view for all events, such as operational issues, scheduled maintenance, and account notifications.</p>	 <p>API access</p> <p>If you have a Business or Enterprise Support plan, you can integrate with the AWS Health API to programmatically use organizational view and look up details for events that occur in your organization. Learn more</p>	 <p>Chat integration</p> <p>Using the AWS Health API, you can ingest events into your Amazon Chime or Slack channel to get notified when an event occurs. Filter events to get the ones that matter most to your organization. Learn more</p>
--	---	---

Get started

<p>1. Set up AWS Organizations</p> <p>You must have an AWS organization with all features enabled.</p> <p>Success</p> <p>Manage AWS Organizations View documentation</p>	<p>2. Enable organizational view for AWS Health</p> <p>After you set up AWS Organizations and sign in to the management account, you can enable AWS Health to aggregate all events. These events appear in the Personal Health Dashboard.</p> <p>Enable organizational view View documentation</p>
---	---

AWS Health 事件的提醒

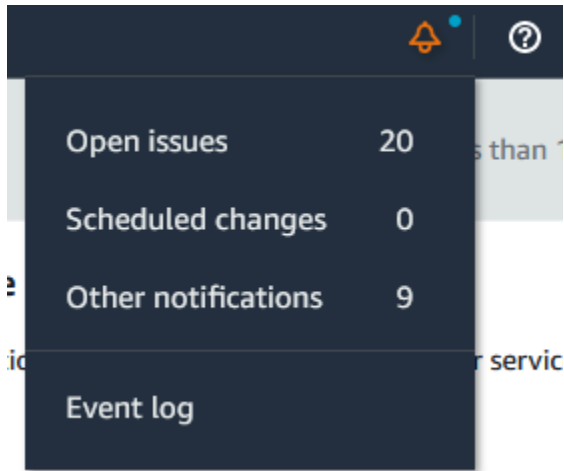
您的 AWS Health 儀表板在主控台導覽列中有一個鐘形圖示，其中包含提醒功能表。此功能會顯示每個類別中顯示在儀表板上的最近 AWS Health 事件數量。此鈴鐺圖示會顯示在數個 AWS 主控台上，例

如 Amazon EC2、Amazon Relational Database Service (Amazon RDS)、AWS Identity and Access Management (IAM) 和 的主控台 AWS Trusted Advisor。

選擇鈴鐺圖示，查看最近的事件是否會影響您的帳戶。然後，您可以選擇要導覽至 AWS Health 儀表板的事件，以取得更多資訊。

Example：開啟事件

下圖顯示 帳戶的開啟和通知事件。



設定 Amazon EventBridge

使用 EventBridge 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 通知您或您採取動作。

搭配 使用 EventBridge AWS Health

1. 在 <https://health.aws.amazon.com/health/home> 開啟您的 AWS Health 儀表板。
2. 若要導覽至 EventBridge 主控台以建立規則，請執行下列其中一項操作：
 - 從導覽窗格的運作狀態整合下，選擇 Amazon EventBridge。
 - 在設定 EventBridge 下，選擇移至 EventBridge。
3. 依照此程序建立規則並監控事件。請參閱 [AWS Health 使用 Amazon EventBridge 監控 中的事件](#)。

在中管理 AWS Health 通知 AWS 使用者通知

AWS 中的受管通知 AWS 使用者通知可讓您接收和管理影響 AWS 帳戶和服務的事件通知。當您在中使用 AWS 受管通知時 AWS 使用者通知，您可以指定要接收 AWS Health 的事件類別、設定電子郵件的組織檢視，以及取得合併通知，而非多個類似的電子郵件。

您可以選擇下列其他管道來接收您的 AWS Health 事件 AWS 使用者通知：

- Email
- 聊天
- 推送通知至 AWS Console Mobile Application

雖然這些通知不如直接 AWS Health 工具詳細，但它們提供了有效的方法來通知利益相關者問題和變更。

Note

若要全面了解 AWS Health 事件詳細資訊，包括受影響的資源 IDs、目前狀態（開啟或關閉）和資源狀態，最佳實務是使用下列其中一個 AWS Health 工具：

- AWS Health API
- Amazon EventBridge 中的 aws.health 來源
- 的 Health 儀板表

這些工具提供有關可能會影響工作負載的持續事件和變更的最詳細即時資訊。

設定事件的 AWS 受管通知訂閱 AWS Health

若要設定受 AWS 管通知訂閱，請完成下列步驟：

1. 在 使用者通知 中開啟 [AWS 管理主控台](#)。
2. 在導覽窗格中，選擇AWS 受管通知訂閱。
3. 您可以依類別管理您的 AWS Health 事件通知。如需詳細資訊，請參閱在 [中新增和移除 AWS 受管通知的帳戶聯絡人 AWS 使用者通知](#)。

Note

AWS Health 已將電子郵件交付遷移至 中的 AWS 受管通知 AWS 使用者通知。自 2025 年 12 月 15 日起，您會收到來自 AWS 受管通知的電子郵件。如需詳細資訊，請參閱《》中的遷移至 AWS 受管通知的變更？[AWS AWS 使用者通知常見問答集中的受管通知](#)。

AWS AWS 使用者通知常見問答集中的受管通知

遷移至 AWS 受管通知時有何變更？

根據預設，有關受管通知的電子郵件會傳送到您現有的帳戶聯絡人（根、操作、帳單和安全電子郵件地址）。您從 AWS 受管通知收到的電子郵件來自 `health@aws.com` 而非 `no-reply-aws@amazon.com`，且電子郵件的格式會變更。如果您先前已設定 AWS Health 通知的電子郵件規則，例如依寄件者 ID 轉送電子郵件或抓取電子郵件內容，則必須更新此設定以符合新的電子郵件格式。如果您需要透過推送通知進行自動化，建議您評估透過 Amazon EventBridge 傳送 AWS Health 的事件，以做為受管通知的替代方案。

彙總如何適用於電子郵件，以及如何啟用此功能？

AWS 受管通知會將影響相同組織內多個帳戶 AWS Health 的事件彙總 AWS Organizations 為單一彙總通知。您可以在管理帳戶的通知中心檢視彙總組織。受管通知會將彙總通知透過電子郵件傳送給管理帳戶的聯絡人。為了減少重複的電子郵件，AWS 受管通知會在管理和成員帳戶之間共用帳戶聯絡人時傳送一個通知。

若要啟用彙總，您必須 AWS Organizations 設定並授予管理帳戶與 AWS 使用者通知 服務之間的信任存取權。

如需詳細資訊，請參閱 [AWS 中的受管通知彙總 AWS 使用者通知](#)。

我是否必須啟用的 AWS Organizations 受信任存取 AWS 使用者通知，才能從 AWS 受管通知接收彙總電子郵件？

是，AWS 使用者通知 來自的受信任存取 AWS Organizations 是必要的。

AWS Organizations 使用 AWS Health 和 啟用受信任存取有何不同 AWS 使用者通知？

組織信任和相關聯的委派管理員權限由服務指派，並做為過度延伸許可的防護機制。的受信任存取 AWS Health 會啟用的組織檢視 Health 儀板表、AWS Health APIs、透過 Amazon EventBridge 傳送

AWS Health 的事件，以及 中的通知組態 使用者通知。的受信任存取會在 AWS 受管通知中 AWS 使用者通知 啟用彙總通知。由於信任存取不會共用，因此需要為每個服務分別新增設定委派管理員。

是否有方法可以為我的特定使用案例保留純文字電子郵件？

否。遷移完成後，目前的純文字 AWS Health 電子郵件會停用。如果您使用電子郵件規則來驅動不同的工作流程，我們建議您評估透過 Amazon EventBridge 傳送 AWS Health 的事件作為替代方案。

AWS 受管通知類別在 AWS Health 結構描述中對應到什麼？

運作狀態操作、安全性和帳單通知對應於分別具有操作、安全性和帳單角色的 AWS Health 帳戶通知和排程變更。具有多個角色標籤 AWS Health 的事件會透過安全性和帳單類別傳送。帳戶特定問題包括特有的問題類別運作狀態事件 AWS 帳戶。

公有服務事件無法透過 AWS 受管通知提供。

AWS Health 儀表板

您可以使用 AWS Health Dashboard – 服務運作狀態來檢視所有的運作狀態 AWS 服務。此頁面顯示跨服務回報的服務事件 AWS 區域。您不需要登入或擁有 AWS 帳戶即可存取 AWS Health Dashboard – 服務運作狀態頁面。

Tip

該網站僅顯示非特有的公有事件 AWS 帳戶。如果您已經有帳戶，我們建議您登入以檢視 AWS Health 儀表板，並隨時掌握可能影響您的帳戶和服務的事件。如需詳細資訊，請參閱 [AWS Health 儀表板入門](#)。

檢視 AWS Health 儀表板 – 服務運作狀態

1. 導覽至 <https://health.aws.amazon.com/health/status> 頁面。

Note

如果您已經登入您的頁面 AWS 帳戶，系統會將您重新導向至 AWS Health Dashboard – 您的帳戶運作狀態頁面。

2. 在服務運作狀態下，選擇開啟和最近的問題，以檢視最近報告的事件。您可以檢視事件的下列相關資訊：
 - 事件名稱和受影響的區域。例如，營運問題 – Amazon Elastic Compute Cloud（維吉尼亞北部）
 - 服務名稱
 - 事件的嚴重性，例如受影響或降級
 - 事件最近更新的時間表
 - 也受此事件影響 AWS 服務的清單

Note

您可以檢視本機時區或 UTC 中的事件。如需詳細資訊，請參閱 [時區設定](#)。

3. 選擇服務歷史記錄以檢視服務歷史記錄表格。此資料表顯示過去 12 個月的所有 AWS 服務中斷。

i Tip

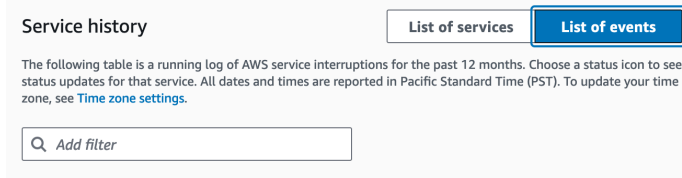
您可以依服務AWS 區域、 和日期進行篩選。

4. 在進行中的服務事件旁，選擇狀態圖示



以檢視事件的詳細資訊。

5. (選用) 若要將此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，以在快顯邊框中檢視該特定事件的詳細資訊。

**i** Note

選取 2023 年 9 月之後的任何公有事件，會在瀏覽器中填入該公有 AWS Health 事件的連結。選取此連結後，您可以使用該事件快顯視窗導覽至事件檢視清單。

6. (選用) 您可以檢視本機時區或 UTC 中的事件。如需詳細資訊，請參閱[時區設定](#)。
7. (選用) 如果您有帳戶，請選擇開啟您的帳戶運作狀態來登入。登入後，您可以檢視帳戶特定的事件。如需詳細資訊，請參閱[AWS Health 儀表板入門](#)。

i Note

雖然 RSS 摘要可用於運作狀態事件，但格式可能會有所變更。因此，抓取 RSS 摘要可能不會提供所有相關資料。若要以程式設計方式擷取運作狀態事件資料，建議您與 Amazon EventBridge 整合。如需詳細資訊，請參閱[AWS Health 使用 Amazon EventBridge 監控中的事件](#)。

的計劃生命週期事件 AWS Health

了解 的計劃生命週期事件 AWS Health。

主題

- [什麼是規劃的生命週期事件？](#)
- [收到規劃的生命週期事件通知時，應預期會發生什麼情況？](#)
- [彈性的共同責任模型](#)
- [存取規劃的生命週期事件](#)

什麼是規劃的生命週期事件？

AWS Health 會傳達可能影響應用程式可用性的重要變更。在 AWS 共同責任模型中，AWS 會採取動作，讓支援 資源的基礎硬體和基礎設施保持最新且安全。不過，某些變更需要客戶動作或協調，以避免影響您的應用程式。會在重要變更之前 AWS Health 通知您，例如：

- 開放原始碼軟體終止支援 - 有些 AWS 服務 執行開放原始碼版本的軟體。如果開放原始碼社群結束對軟體版本的支援，會在您需要採取動作來升級並避免影響應用程式時 AWS 通知您。
 - [Amazon RDS for MySQL 引擎版本終止支援](#)
 - [Amazon EKS Kubernetes 版本終止支援](#)
- 影響可能需要您動作 AWS 之擁有資源的變更。
 - [Amazon RDS Certificate Authority 憑證過期](#)。

Note

符合此條件的所有通知將透過 報告 AWS Health 為計劃生命週期事件。

- 動態資源縮減和改善中繼資料：從您收到通知到 AWS Health 事件的生命週期，您受影響的資源會以具有特定實體狀態的受影響實體與 AWS Health 事件相關聯。受影響的資源會在適用時以 ARN 格式指定。如果您受影響的資源需要客戶動作，則會以「待定」狀態列出這些資源。如果您受影響的資源已執行必要動作或資源已刪除，則狀態會更新為「RESOLVED」。

Note

- 資源狀態更新會以非同步和定期方式執行，在極少數情況下最多可延遲 72 小時。

- 在未提供動態更新的例外情況中，而不是具有「待定」或「已解決」狀態的資源，將不會指派任何狀態的資源。
- AWS GovCloud (US) 和中國區域不支援資源狀態更新。

收到規劃的生命週期事件通知時，應預期會發生什麼情況？

規劃生命週期事件 AWS Health 的體驗可協助您的團隊了解即將發生的生命週期變更，並追蹤動作完成。

類型類別：排程變更

事件類型代碼：AWS_{SERVICE}_PLANNED_LIFECYCLE_EVENT

事件開始時間：事件開始時間是資源受到變更影響的最快日期。

事件結束時間：事件結束時間是變更在所有 AWS 資源中完成的日期。請注意，不一定會指定結束時間。請務必將開始時間視為變更日期。

Note

組織可以預期收到每個計劃生命週期事件的單一事件 ARN，這些生命週期事件依受影響的資源區域分組。但是，如果組織有大量受影響的 AWS 帳戶或資源，他們可能會收到多個 ARNs。

提前了解計劃的生命週期事件：計劃的生命週期事件設計為在可能的情況下，主要版本/變更的最短前置時間為 180 天，次要版本/變更的最短前置時間為 90 天。

動態資源縮減和改善的中繼資料：從您收到通知到 AWS Health 事件的生命週期，您受影響的資源會作為具有特定實體狀態的**受影響實體**與 AWS Health 事件相關聯。受影響的資源會在適用時以 ARN 格式指定。如果您受影響的資源需要客戶動作，則會以「待定」狀態列出這些資源。如果您受影響的資源已執行必要動作或資源已刪除，則狀態會更新為「RESOLVED」。

Note

- AWS Health 通知會盡可能隨著時間提供狀態更新，但 AWS GovCloud (US) 和中國區域除外。
- 資源狀態更新會以非同步和定期方式執行，在極少數情況下最多可延遲 72 小時。

Open and recent issues | **Scheduled changes** | Other notifications | Event log

Scheduled changes

View upcoming events and ongoing events from the past seven days that might affect your AWS infrastructure, such as scheduled maintenance activities.

Q Add filter < 1 >

Event	Status	Region / Zone	Start time	End time	Affected resources
EKS planned lifecycle event	Upcoming	us-west-2	January 30, 2024 at 6:00:00 PM UTC-8		9 pending
DMS planned lifecycle event	Upcoming	us-east-1	January 29, 2024 at 6:00:00 PM UTC-8		1 pending
DMS planned lifecycle event	Upcoming	eu-west-1	January 29, 2024 at 6:00:00 PM UTC-8		10 pending
EKS planned lifecycle event	Completed	eu-west-1	January 30, 2024 at 6:00:00 PM UTC-8		-

EKS planned lifecycle event 🔍 ✕

Resource data is typically refreshed every 24 hours. ■ **0 Resolved** 0%
No actions required

Affected resources in account 745485236264 (5)

Q Add filter < 1 >

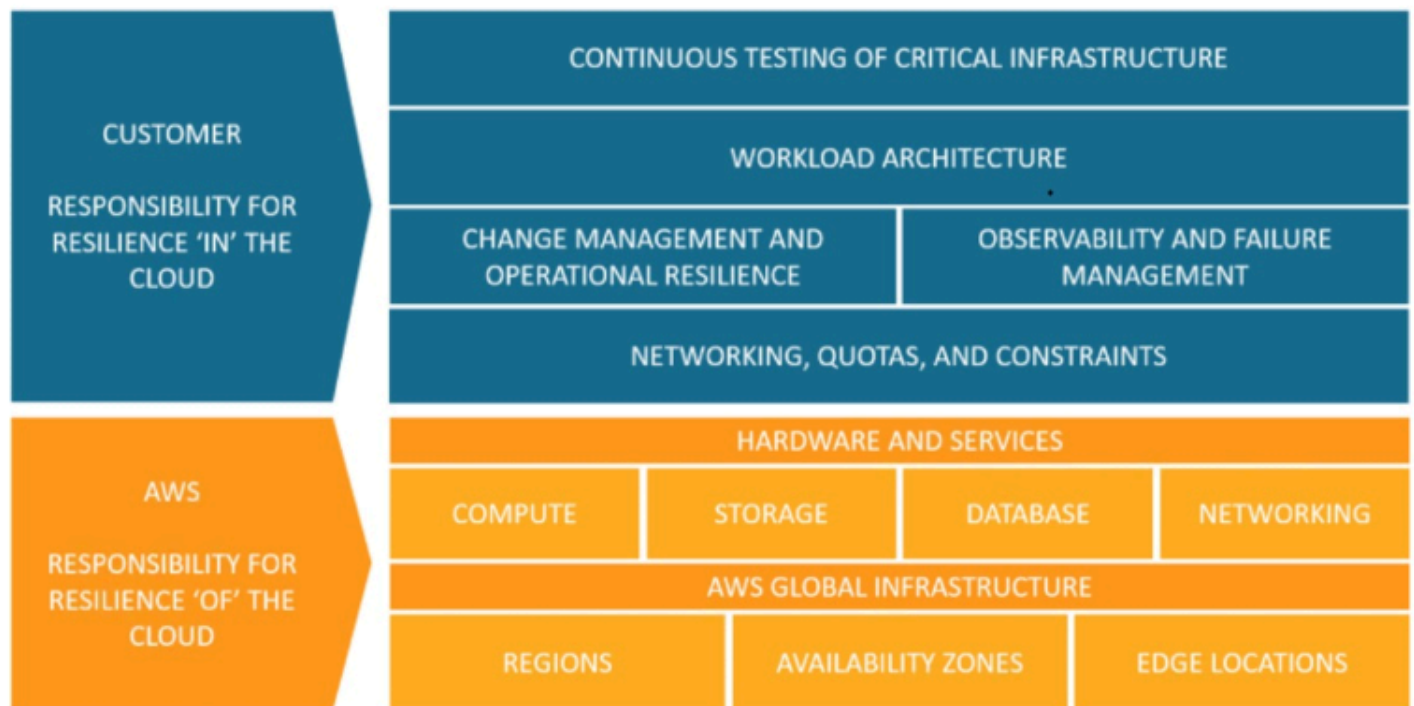
Resource ID / ARN	Resource status	Last update time
arn:aws:eks:us-west-2:745485236264:cluster/prod-ops-cluster	⊘ Pending	15 days ago
arn:aws:eks:us-west-2:745485236264:cluster/nonprod-dev5	⊘ Pending	15 days ago
arn:aws:eks:us-west-2:745485236264:cluster/n-preprd-eks	⊘ Pending	15 days ago
arn:aws:eks:us-west-2:745485236264:cluster/argoworkflows-refactor51	⊘ Pending	15 days ago
arn:aws:eks:us-west-1:745485236264:cluster/prod-refactor	⊘ Pending	15 days ago

在計劃的事件日期過後：

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作所描述的變更。
2. 如果您在支援結束日期之前解決所有資源，則您的 AWS Health 事件會變更為狀態 Closed。
3. 如果您在變更日期後仍有未解決的資源，則 AWS Health 事件會在事件開始或結束日期後 4 年（以較晚者為準）內保持開啟狀態。在此期間之後，會刪除 AWS Health 事件。

彈性的共同責任模型

安全與合規是 AWS 與客戶之間共同責任。根據部署的服務，此共用模型有助於減輕客戶的營運負擔。這是因為會 AWS 操作、管理和控制從主機作業系統和虛擬化層到服務操作所在設施實體安全性的元件。除了提供的安全群組防火牆組態之外，客戶還承擔訪客作業系統（包括更新和安全修補程式）和其他相關應用程式軟體的責任和管理 AWS。如需詳細資訊，請參閱[共同責任模式](#)。



存取規劃的生命週期事件

您可以使用幾個頻道來存取和監控規劃的生命週期事件：

- [使用 Amazon EventBridge](#)
- [使用 AWS Health 儀表板](#)
 - [行事曆檢視](#)
 - [受影響的資源檢視](#)
- [使用 AWS Health API](#)

使用 AWS Health API AWS Health 與其他系統整合

AWS Health 是一種 RESTful Web 服務，使用 HTTPS 做為傳輸，並使用 JSON 做為訊息序列化格式。您的應用程式程式碼能夠直接向 AWS Health API 發出請求。當您直接使用 REST API 時，您必須撰寫必要的程式碼來簽署和驗證您的請求。如需 AWS Health 操作和參數的詳細資訊，請參閱 [AWS Health API 參考](#)。

Note

您必須擁有來自的 AWS Business Support+、AWS Enterprise Support 或 AWS Unified Operations 計劃 [AWS 支援](#)，才能使用 AWS Health API。如果您所在的 AWS 區域未提供其中一個 AWS 支援計劃，或者您尚未轉換至其中一個計劃，則可以使用 AWS Health API 搭配 Business、Enterprise On-Ramp 或 Enterprise Support 計劃。如果您從 AWS 帳戶未註冊這些其中一個計劃的呼叫 AWS Health API，則會收到 `SubscriptionRequiredException` 錯誤。

您可以使用 AWS SDKs 來包裝 AWS Health REST API 呼叫，這可以簡化您的應用程式開發。您可以指定您的 AWS 登入資料，這些程式庫會為您處理身分驗證和請求簽署。

AWS Health 也在 [中](#) 提供 AWS Health 儀表板 AWS 管理主控台，可讓您用來檢視和搜尋事件和受影響的實體。請參閱 [AWS Health 儀表板入門](#)。

主題

- [簽署 AWS Health API 請求](#)
- [選擇 AWS Health API 請求的端點](#)
- [示範：以程式設計方式擷取過去七天 AWS Health 的事件資料](#)
- [教學課程：搭配 Java 範例使用 AWS Health API](#)

簽署 AWS Health API 請求

當您使用 AWS SDKs 或 AWS Command Line Interface (AWS CLI) 向提出請求時 AWS，這些工具會自動使用您在設定工具時指定的存取金鑰來簽署請求。例如，如果您將適用於 Java 的 AWS SDK 用於先前的高可用性端點示範，則不需要自行簽署請求。

Java 程式碼範例

如需如何搭配 使用 AWS Health API 的更多範例 適用於 Java 的 AWS SDK，請參閱此[範例程式碼](#)。

當您提出請求時，強烈建議您不要將 AWS 根帳戶登入資料用於定期存取 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 您的帳戶根使用者存取金鑰](#)。

如果您不使用 AWS SDKs 或 AWS CLI，則必須自行簽署請求。我們建議您使用 AWS Signature 第 4 版。如需詳細資訊，請參閱《》中的[簽署 AWS API 請求](#) AWS 一般參考。

選擇 AWS Health API 請求的端點

AWS Health API 遵循多區域應用程式架構，並在主動-被動組態中有兩個區域端點。為了支援主動-被動 DNS 容錯移轉，AWS Health 提供單一的全域端點。您可以在全域端點上執行 DNS 查詢，以判斷作用中端點和對應的簽署 AWS 區域。這可協助您了解要在程式碼中使用的端點，以便從中取得最新資訊 AWS Health。

當您向 全域端點提出請求時，您必須指定對目標區域端點的 AWS 存取憑證，並為區域設定簽署。否則，您的身分驗證可能會失敗。如需詳細資訊，請參閱[簽署 AWS Health API 請求](#)。

對於 IPv6-only 的請求，我們建議您在全域端點上執行 DNS 查詢，以判斷作用中的，AWS 區域 然後呼叫該區域的 IPv6 支援的雙堆疊端點。

下表代表預設組態。

Description	簽署區域	Endpoint	通訊協定
作用中	us-east-1	health.us-east-1.a amazonaws.com (僅限 IPv4) health.us-east-1.a pi.aws (支援 IPv4 和 IPv6)	HTTPS
被動	us-east-2	health.us-east-2.a amazonaws.com (僅限 IPv4)	HTTPS

Description	簽署區域	Endpoint	通訊協定
		health.us-east-2.amazonaws (支援 IPv4 和 IPv6)	
全域	us-east-1	global.health.amazonaws.com	HTTPS

Note
這是目前作用中端點的簽署區域。

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 查詢，然後從解析的名稱擷取 AWS 區域。

Example：全域端點上的 DNS 查詢

下列命令會在 global.health.amazonaws.com 端點上完成 DNS 查詢。命令接著會傳回 us-east-1 區域端點。此輸出會告訴您應使用哪個端點 AWS Health。

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

Tip

主動和被動端點都會傳回 AWS Health 資料。不過，最新的 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將與主動端點一致。我們建議您在作用中端點變更時重新啟動任何工作流程。

示範：以程式設計方式擷取過去七天 AWS Health 的事件資料

在下列程式碼範例中，針對全域端點 AWS Health 使用 DNS 查詢來判斷作用中的區域端點和簽署區域。AWS Health 會使用此資訊來擷取過去七天的事件資料報告。如果作用中端點變更，程式碼會重新啟動工作流程。

主題

- [示範：使用 Java 擷取過去七天 AWS Health 的事件資料](#)
- [示範：使用 Python 擷取過去七天 AWS Health 的事件資料](#)

示範：使用 Java 擷取過去七天 AWS Health 的事件資料

先決條件

您必須安裝 [Gradle](#)。

使用 Java 範例

1. 從 GitHub 下載 [AWS Health 高可用性端點示範](#)。
2. 導覽至示範專案 `high-availability-endpoint/java` 目錄。
3. 在命令列視窗中，輸入下列命令。

```
gradle build
```

4. 輸入下列命令來指定您的 AWS 登入資料。

```
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的 AWS Health 事件。在下列範例中，輸出包含 AWS Config 服務 AWS Health 的事件。

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

```
Service=CONFIG, EventTypeCode=AWS_CONFIG_OPERATIONAL_NOTIFICATION,  
  EventTypeCategory=accountNotification, Region=global,  
  StartTime=2020-09-11T02:55:49.899Z, LastUpdatedTime=2020-09-11T03:46:31.764Z,  
  StatusCode=open, EventScopeCode=ACCOUNT_SPECIFIC),  
  EventDescription=EventDescription(LatestDescription=As part of our ongoing efforts  
  to optimize costs associated with recording changes related to certain ephemeral  
  workloads,  
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 ## [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

- 如需詳細資訊，請參閱適用於 Java 的 AWS SDK API 參考中的[介面 HealthClient](#) 和[原始程式碼](#)。
- 如需此示範中用於 DNS 查詢的程式庫詳細資訊，請參閱 GitHub 中的 [dnsjava](#)。

示範：使用 Python 擷取過去七天 AWS Health 的事件資料

先決條件

您必須安裝 [Python 3](#)。

使用 Python 範例

1. 從 GitHub 下載[AWS Health 高可用性端點示範](#)。
2. 導覽至示範專案 `high-availability-endpoint/python` 目錄。
3. 在命令列視窗中，輸入下列命令。

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

Note

對於 Python 3.3 和更新版本，您可以使用內建 `venv` 模組來建立虛擬環境，而不是安裝 `virtualenv`。如需詳細資訊，請參閱 Python 網站上的 [venv - 虛擬環境的建立](#)。

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

4. 輸入下列命令以啟用虛擬環境。

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

5. 輸入下列命令來安裝相依性。

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

6. 輸入下列命令來指定您的 AWS 登入資料。

```
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的 AWS Health 事件。下列輸出會傳回 AWS 安全通知 AWS Health 的事件。

```
INFO:botocore.credentials:Found credentials in environment variables.
INFO:root:Details: {'arn': 'arn:aws:health:global::event/SECURITY/
AWS_SECURITY_NOTIFICATION/AWS_SECURITY_NOTIFICATION_0e35e47e-2247-47c4-
a9a5-876544042721',
'service': 'SECURITY', 'eventTypeCode': 'AWS_SECURITY_NOTIFICATION',
'eventTypeCategory': 'accountNotification', 'region': 'global', 'startTime':
datetime.datetime(2020, 8, 19, 23, 30, 42, 476000,
tzinfo=tzlocal()), 'lastUpdatedTime': datetime.datetime(2020, 8, 20, 20, 44, 9,
547000, tzinfo=tzlocal()), 'statusCode': 'open', 'eventScopeCode': 'PUBLIC'},
description:
{'latestDescription': 'This is the second notice regarding TLS requirements on FIPS
endpoints.\n\nWe
are in the process of updating all 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 ## [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?\n\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，請輸入下列命令來停用虛擬機器。

```
deactivate
```

Python 資源

- 如需的詳細資訊Health. Client，請參閱[AWS 適用於 Python \(Boto3\) 的 SDK API 參考](#)。
- 如需此示範中用於 DNS 查詢的程式庫詳細資訊，請參閱 GitHub 上的 [dnspython](#) 工具組和[原始程式碼](#)。

教學課程：搭配 Java 範例使用 AWS Health API

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

步驟 1：初始化登入資料

需要有效的登入資料才能與 AWS Health API 通訊。您可以使用與 AWS 帳戶相關聯之任何 IAM 使用者的金鑰對。

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 Health API 用戶端

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 Health API 操作來取得事件資訊

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.amdescribeEventDetailsRequestamazonaws.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

的雲端安全性 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，這些架構專為滿足最安全敏感組織的需求而建置。

安全性是 AWS 與您之間共同責任。[共同責任模式](#)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 Cloud AWS 中執行 AWS 服務的基礎設施。AWS 也為您提供可安全使用的服務。在[AWS 合規計畫](#)中，第三方稽核人員會定期測試和驗證我們安全的有效性。若要了解適用的合規計劃 AWS Health，請參閱[AWS 合規計劃的服務範圍](#)。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。您也必須負責其他因素，包括資料的機密性、公司的要求，以及適用的法律和法規。

本文件可協助您了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 以符合您的安全與合規目標。您也會了解如何使用其他 AWS 服務來協助您監控和保護 AWS Health 資源。

主題

- [中的資料保護 AWS Health](#)
- [的身分和存取管理 AWS Health](#)
- [在中記錄和監控 AWS Health](#)
- [的合規驗證 AWS Health](#)
- [中的彈性 AWS Health](#)
- [中的基礎設施安全 AWS Health](#)
- [中的組態和漏洞分析 AWS Health](#)
- [的安全最佳實務 AWS Health](#)

中的資料保護 AWS Health

AWS [共同責任模型](#)適用於 中的資料保護。如此模型所述，AWS 負責保護執行所有的全域基礎設施 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 共同責任模型和 GDPR](#) 部落格文章。

基於資料保護目的，我們建議您保護 AWS 帳戶 登入資料，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 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。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《使用者指南》中的[使用 CloudTrail 追蹤](#)。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 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 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-3 驗證的密碼編譯模組，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 \(FIPS\) 140-3](#)。

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 或使用主控台、API AWS CLI或其他 AWS 服務 AWS SDKs 時。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。

資料加密是指在傳輸中（從服務傳輸到 AWS 您的帳戶時）和靜態（存放在 AWS 服務中時）時保護資料。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 不會在事件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 AWS Health 都會靜態加密。

傳輸中加密

所有往返 傳送的資料 AWS Health 都會在傳輸中加密。

金鑰管理

AWS Health 對於在 AWS 雲端中加密的資料，不支援客戶受管加密金鑰。

的身分和存取管理 AWS Health

AWS Identity and Access Management (IAM) 是 AWS 服務，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行驗證（登入）和授權（具有許可）來使用 AWS Health 資源。IAM 是 AWS 服務您可以免費使用的。

主題

- [目標對象](#)
- [使用身分驗證](#)
- [使用政策管理存取權](#)
- [AWS Health 如何使用 IAM](#)
- [AWS Health 身分型政策範例](#)
- [對 AWS Health 身分和存取進行故障診斷](#)
- [使用的服務連結角色 AWS Health](#)
- [AWS 的受管政策 AWS Health](#)

目標對象

使用方式 AWS Identity and Access Management (IAM) 會根據您的角色而有所不同：

- 服務使用者 — 若無法存取某些功能，請向管理員申請所需許可 (請參閱 [對 AWS Health 身分和存取進行故障診斷](#))
- 服務管理員 — 負責設定使用者存取權並提交相關許可請求 (請參閱 [AWS Health 如何使用 IAM](#))
- IAM 管理員 — 撰寫政策以管理存取控制 (請參閱 [AWS Health 身分型政策範例](#))

使用身分驗證

身分驗證是您 AWS 使用身分憑證登入的方式。您必須以 AWS 帳戶根使用者、IAM 使用者或擔任 IAM 角色身分進行身分驗證。

您可以使用身分來源的登入資料，例如 AWS IAM Identity Center (IAM Identity Center)、單一登入身分驗證或 Google/Facebook 登入資料，以聯合身分的形式登入。如需有關登入的詳細資訊，請參閱《AWS 登入 使用者指南》中的 [如何登入您的 AWS 帳戶](#)。

對於程式設計存取，AWS 提供 SDK 和 CLI 以密碼編譯方式簽署請求。如需詳細資訊，請參閱《IAM 使用者指南》中的 [API 請求的 AWS 第 4 版簽署程序](#)。

AWS 帳戶根使用者

當您建立時 AWS 帳戶，您會從一個名為 AWS 帳戶 theroot 使用者的登入身分開始，該身分可完整存取所有 AWS 服務和資源。強烈建議不要使用根使用者來執行日常任務。有關需要根使用者憑證的任務，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https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html是一種身分具備單人或應用程式的特定許可權。建議以臨時憑證取代具備長期憑證的 IAM 使用者。如需詳細資訊，請參閱《IAM 使用者指南》中的[要求人類使用者使用聯合身分提供者來 AWS 使用臨時憑證存取](#)。

[IAM 群組](#)會指定 IAM 使用者集合，使管理大量使用者的許可權更加輕鬆。如需詳細資訊，請參閱《IAM 使用者指南》中的[IAM 使用者的使用案例](#)。

IAM 角色

IAM 角色https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html的身分具有特定許可權，其可以提供臨時憑證。您可以透過[從使用者切換到 IAM 角色（主控台）](#)或呼叫 AWS CLI 或 AWS API 操作來擔任角色。如需詳細資訊，請參閱《IAM 使用者指南》中的[擔任角色的方法](#)。

IAM 角色適用於聯合身分使用者存取、臨時 IAM 使用者許可、跨帳戶存取權與跨服務存取，以及在 Amazon EC2 執行的應用程式。如需詳細資訊，請參閱《IAM 使用者指南》中的[IAM 中的快帳戶資源存取](#)。

使用政策管理存取權

您可以透過建立政策並將其連接到身分或資源 AWS 來控制 AWS 中的存取。政策定義與身分或資源相關聯的許可。當委託人提出請求時 AWS，會評估這些政策。大多數政策會以 JSON 文件 AWS 的形式存放在中。如需進一步了解 JSON 政策文件，請參閱《IAM 使用者指南》中的[JSON 政策概觀](#)。

管理員會使用政策，透過定義哪些主體可在哪些條件下對哪些資源執行動作，以指定可存取的範圍。

預設情況下，使用者和角色沒有許可。IAM 管理員會建立 IAM 政策並將其新增至角色，供使用者後續擔任。IAM 政策定義動作的許可，無論採用何種方式執行。

身分型政策

身分型政策是附加至身分 (使用者、使用者群組或角色) 的 JSON 許可政策文件。這類政策控制身分可對哪些資源執行哪些動作，以及適用的條件。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的[透過客戶管理政策定義自訂 IAM 許可](#)。

身分型政策可分為內嵌政策 (直接內嵌於單一身分) 與受管政策 (可附加至多個身分的獨立政策)。如需了解如何在受管政策及內嵌政策之間做選擇，請參閱《IAM 使用者指南》中的[在受管政策與內嵌政策之間選擇](#)。

資源型政策

資源型政策是附加到資源的 JSON 政策文件。範例包括 IAM 角色信任政策與 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。您必須在資源型政策中[指定主體](#)。

資源型政策是位於該服務中的內嵌政策。您無法在資源型政策中使用來自 IAM 的 AWS 受管政策。

AWS Health 支援以資源為基礎的條件。您可以指定使用者可檢視哪一個 AWS Health 事件。例如，您可以建立僅允許 IAM 使用者存取 AWS Health Dashboard 中特定 Amazon EC2 事件的策略。

如需詳細資訊，請參閱[Resources](#)。

存取控制清單

存取控制清單 (ACL) 可控制哪些主體 (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 AWS WAF 和 Amazon VPC 是支援 ACLs 的服務範例。如需進一步了解 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 ACLs。

其他政策類型

AWS 支援其他政策類型，可設定更多常見政策類型授予的最大許可：

- 許可界限 — 設定身分型政策可授與 IAM 實體的最大許可。如需詳細資訊，請參閱《IAM 使用者指南》中的[IAM 實體許可界限](#)。
- 服務控制政策 (SCP) — 為 AWS Organizations 中的組織或組織單位指定最大許可。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的[服務控制政策](#)。
- 資源控制政策 (RCP) — 設定您帳戶中資源可用許可的上限。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的[資源控制政策 \(RCP\)](#)。
- 工作階段政策 — 在以程式設計方式為角色或聯合身分使用者建立臨時工作階段時，以參數形式傳遞的進階政策。如需詳細資訊，請參閱《IAM 使用者指南》中的[工作階段政策](#)。

多種政策類型

當多種類型的政策適用於請求時，產生的許可會更複雜而無法理解。若要了解如何 AWS 在涉及多種政策類型時決定是否允許請求，請參閱《IAM 使用者指南》中的[政策評估邏輯](#)。

AWS Health 如何使用 IAM

在您使用 IAM 管理對的存取之前 AWS Health，您應該了解哪些 IAM 功能可與搭配使用 AWS Health。若要全面了解 AWS Health 和其他 AWS 服務如何與 IAM 搭配使用，請參閱《IAM 使用者指南》中的與 IAM [AWS 搭配使用的服務](#)。

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。

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。政策會使用動作來授予執行相關聯動作的許可。

中的政策動作在動作之前 AWS Health 使用下列字首：health:。例如，若要授與某人許可，使其能使用 [DescribeEventDetails](#) API 操作，檢視特定事件的詳細資訊，您可以將 health:DescribeEventDetails 動作加入政策中。

政策陳述式必須包含 Action 或 NotAction element。AWS Health 定義自己的一組動作，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》中的 [定義的動作 AWS Health](#)。

Resources

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。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。最佳實務是使用其 [Amazon Resource Name \(ARN\)](#) 來指定資源。若動作不支援資源層級許可，使用萬用字元 (*) 表示該陳述式適用於所有資源。

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

AWS Health 事件具有下列 Amazon Resource Name (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"
```

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

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

如需 ARNs 格式的詳細資訊，請參閱 [Amazon Resource Name \(ARNs\) AWS 和服務命名空間](#)。

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

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

AWS Health API 操作可以涉及多個資源。例如，[DescribeEvents](#) 操作會傳回符合特定篩選條件之事件的資訊。這表示 IAM 使用者必須具有檢視此事件的許可。

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 僅支援運作狀態事件的資源層級許可，也僅支援 [DescribeAffectedEntities](#) 和 [DescribeEventDetails](#) API 操作。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 ARNs 的清單，請參閱《IAM 使用者指南》中的 [定義的資源 AWS Health](#)。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 元素會根據定義的條件，指定陳述式的執行時機。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。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的 [AWS 全域條件內容索引鍵](#)。

AWS Health 會定義自己的一組條件金鑰，也支援使用一些全域條件金鑰。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](#)。

[DescribeAffectedEntities](#) 和 [DescribeEventDetails](#) API 操作支援 health:eventTypeCode 與 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》中的 [的條件金鑰 AWS Health](#)。若要了解您可以使用條件金鑰的動作和資源，請參閱 [定義的動作 AWS Health](#)。

範例

若要檢視 AWS Health 身分型政策的範例，請參閱 [AWS Health 身分型政策範例](#)。

AWS Health 資源型政策

以資源為基礎的政策是 JSON 政策文件，指定指定委託人可在 AWS Health 資源上執行的動作，以及在何種條件下執行的動作。AWS Health 支援運作狀態事件的資源型許可政策。資源型政策可讓您依資源將使用許可授予至其他帳戶。您也可以使用資源型政策，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。當委託人和資源位於不同的 AWS 帳戶中時，您還必須授予委託人實體存取資源的許可。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 [DescribeAffectedEntities](#) 和 [DescribeEventDetails](#) API 操作的資源型政策。您可以在政策中指定這些動作，以定義哪些委託人實體（帳戶、使用者、角色和聯合身分使用者）可以對 AWS Health 事件執行動作。

範例

若要檢視以 AWS Health 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 不支援標記資源或根據標籤控制存取。

AWS Health IAM 角色

[IAM 角色](#)是您 AWS 帳戶中具有特定許可的實體。

搭配 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 [GetFederationToken](#) 等 AWS STS API 操作來取得臨時安全登入資料。

AWS Health 支援使用臨時登入資料。

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 支援與整合的服務連結角色 AWS Organizations。服務連結角色名為 `AWSServiceRoleForHealth_Organizations`。連接至角色是 [Health_OrganizationsServiceRolePolicy](#) AWS 受管政策。受管 AWS 政策允許存取組織中其他 AWS 帳戶 AWS Health 的運作狀態事件。

您可以使用 [EnableHealthServiceAccessForOrganization](#) 操作，以在帳戶中建立服務連結角色。不過，如果您想停用此功能，您必須先呼叫 [DisableHealthServiceAccessForOrganization](#) 操作。然後，您可以透過 IAM 主控台、IAM API 或 AWS Command Line Interface () 刪除角色AWS CLI。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[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 身分型政策範例

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 管理主控台 AWS CLI或 AWS API 執行任務。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](#)
- [使用 AWS Health 主控台](#)
- [允許使用者檢視他們自己的許可](#)

- [存取 AWS Health 儀表板和 AWS Health API](#)
- [根據資源與根據動作的條件](#)

政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 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 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。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](#)。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。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。如果透過特定 例如 使用服務動作 AWS 服務，您也可以使用條件來授予其存取權 CloudFormation。如需詳細資訊，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，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的 [使用 IAM Access Analyzer 驗證政策](#)。
- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的 [透過 MFA 的安全 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，您必須擁有一組最低許可。這些許可必須允許您列出和檢視 AWS 帳戶中 AWS Health 資源的詳細資訊。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。

為了確保這些實體仍然可以使用 AWS Health 主控台，您可以連接下列 AWS 受管政策 [AWSHealthFullAccess](#)。

此AWSHealthFullAccess政策會授予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 AWS 的組織檢視功能
- AWS Health 主控台內的 AWS Health 儀表板
- AWS Health API 操作和通知
- 檢視屬於您 AWS 組織一部分的帳戶相關資訊
- 檢視管理帳戶的組織單位 (OU)

Example: AWSHealthFullAccess

JSON

```
{
  "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 `Health_OrganizationsServiceRolePolicy` AWS 受管政策，讓 AWS Health 可以檢視組織中其他帳戶的事件。如需詳細資訊，請參閱 [使用的服務連結角色 AWS Health](#)。

對於僅呼叫 AWS CLI 或 AWS API 的使用者，您不需要允許最低主控台許可。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。此政策包含在主控台或使用或 AWS CLI AWS API 以程式設計方式完成此動作的許可。

```

{
  "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 儀表板和 AWS Health API

AWS Health 儀表板適用於所有 AWS 帳戶。AWS Health API 僅適用於具有 AWS Business Support +、AWS Enterprise Support 或 AWS Unified Operations 計劃的帳戶。如需詳細資訊，請參閱[支援](#)。

您可以使用 IAM 建立實體（使用者、群組或角色），然後授予這些實體存取 AWS Health Dashboard 和 AWS Health API 的許可。

根據預設，IAM 使用者無法存取 AWS Health Dashboard 或 AWS Health API。您可以將 IAM 政策連接至單一使用者、使用者群組或角色，讓使用者存取帳戶 AWS Health 的資訊。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，他們可以登入您的帳戶，並使用帳戶特定的登入頁面來檢視 AWS Health 資訊。如需詳細資訊，請參閱[使用者如何登入您的帳戶](#)。

Note

具有檢視 AWS Health Dashboard 許可的 IAM 使用者對帳戶上所有 AWS 服務的運作狀態資訊具有唯讀存取權，包括但不限於 AWS 資源 IDs，例如 Amazon EC2 執行個體 IDs、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 API 的 AWS Health 存取權，則政策套用的使用者或角色可以存取有關 AWS 服務和相關資源發佈的所有資訊，即使其他 IAM 政策不允許該存取權。

您可以使用兩個 APIs 群組 AWS Health。

- 個別帳戶 – 您可以使用 [DescribeEvents](#) 和 [DescribeEventDetails](#) 等操作來取得您帳戶 AWS Health 事件的相關資訊。
- 組織帳戶 – 您可以使用 [DescribeEventsForOrganization](#) 和 [DescribeEventDetailsForOrganization](#) 等操作，以取得屬於您組織之帳戶 AWS Health 的事件相關資訊。

如需可用 API 操作的詳細資訊，請參閱 [AWS Health API 參考](#)。

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 儀表板和 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

此政策陳述式授予對 AWS Health Dashboard 和任何 `Describe*` AWS Health API 操作的存取權。例如，具有此政策的 IAM 使用者可以存取 中的 AWS Health 儀表板，AWS 管理主控台 並呼叫 `DescribeEvents` API AWS Health 操作。

Example：描述存取權

JSON

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

拒絕存取

此政策陳述式拒絕存取 AWS Health Dashboard 和 AWS Health API。具有此政策的 IAM 使用者無法檢視 中的 AWS Health 儀表板 AWS 管理主控台 ，也無法呼叫任何 AWS Health API 操作。

Example : 拒絕存取

JSON

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

組織檢視

如果您想要啟用的組織檢視 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

若要了解每個 APIs 所需的確切許可，請參閱《IAM 使用者指南》中的 [AWS Health APIs 和通知定義的動作](#)。

Note

您必須使用來自管理帳戶的登入資料，組織才能存取 AWS Health APIs AWS Organizations。如需詳細資訊，請參閱[跨帳戶彙總 AWS Health 事件](#)。

允許存取 AWS Health 組織檢視

此政策陳述式會授予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

JSON

```
{
  "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

此政策陳述式拒絕存取 AWS Organizations 動作，但允許存取個別帳戶 AWS Health 的動作。

Example：拒絕 AWS Health 組織檢視存取

JSON

```

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

```

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

Note

如果您想要授予許可的使用者或群組已有 IAM 政策，您可以將 AWS Health 特定政策陳述式新增至該政策。

根據資源與根據動作的條件

AWS Health 支援 [DescribeAffectedEntities](#) 和 [DescribeEventDetails](#) API 操作的 [IAM 條件](#)。您可以使用資源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。

若要這樣做，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。

當您在政策中指定 AWS Health 事件時，可以使用下列欄位：

- eventTypeId
- service

備註

- [DescribeAffectedEntities](#) 和 [DescribeEventDetails](#) API 操作支援資源層級許可。例如，您可以建立政策來允許或拒絕特定 AWS Health 事件。

- [DescribeAffectedEntitiesForOrganization](#) 和 [DescribeEventDetailsForOrganization](#) API 操作不支援資源層級許可。
- 如需詳細資訊，請參閱《服務授權參考》中的 [AWS Health APIs 和通知的動作、資源和條件索引鍵](#)。

Example：以動作為基礎的條件

此政策陳述式授予對 AWS Health Dashboard 和 Describe* API 操作的 AWS Health 存取權，但拒絕存取與 Amazon EC2 相關的任何 AWS Health 事件。

JSON

```
{
  "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。

JSON

```
{
  "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

此政策陳述式會授予對 AWS Health Dashboard 和 Describe* API 操作的 AWS Health 存取權，但拒絕存取任何與 eventTypeCode 相符 AWS Health 的事件 AWS_EC2_*。

JSON

```
{
  "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 [DescribeAffectedEntities](#) 和 [DescribeEventDetails](#) 操作，而且沒有存取 AWS Health 事件的許可，則會顯示 `AccessDeniedException` 錯誤。如需詳細資訊，請參閱 [對 AWS Health 身分和存取進行故障診斷](#)。

對 AWS Health 身分和存取進行故障診斷

使用下列資訊來診斷和修正使用 和 IAM AWS Health 時可能遇到的常見問題。

主題

- [我未獲授權在 中執行動作 AWS Health](#)
- [我未獲授權執行 iam:PassRole](#)
- [我想要檢視我的存取金鑰](#)
- [我是管理員，想要允許其他人存取 AWS Health](#)
- [我想要允許 AWS 帳戶外的人員存取我的 AWS Health 資源](#)

我未獲授權在 中執行動作 AWS Health

如果 AWS 管理主控台 告訴您無權執行 動作，則必須聯絡您的管理員尋求協助。您的管理員是為您提供使用者名稱和密碼的人員。

當使用者沒有使用 AWS Health Dashboard 或 AWS Health API 操作的許可時，會顯示 `AccessDeniedException` 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 需要來自的 AWS Business Support+、AWS Enterprise Support 或 AWS Unified Operations 計劃[AWS 支援](#)。如果您從沒有 AWS Business Support+、AWS Enterprise Support 或 AWS Unified Operations 計劃的帳戶呼叫 AWS Health API，則會傳回下列錯誤碼：SubscriptionRequiredException。

我未獲授權執行 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 服務可讓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 沒有將角色傳遞給服務的許可。

```
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 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](#)。透過這樣做，您可以讓某人永久存取您的 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，您必須將許可授予需要存取的人員或應用程式。如果您使用 AWS IAM Identity Center 管理人員和應用程式，您可以將許可集指派給使用者或群組，以定義其存取層級。許可集會自動建立 IAM 政策，並將其指派給與該人員或應用程式相關聯的 IAM 角色。如需詳細資訊，請參閱 AWS IAM Identity Center 《使用者指南》中的[許可集](#)。

如果您不是使用 IAM Identity Center，則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）。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。授予許可後，請將登入資料提供給使用者或應用程式開發人員。他們將使用這些登入資料來存取 AWS。若要進一步了解如何建立 IAM 使用者、群組、政策和許可，請參閱《IAM [使用者指南](#)》中的 [IAM 身分](#)和[政策和許可](#)。

我想要允許 AWS 帳戶外的人員存取我的 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：

- 若要了解 是否 AWS Health 支援這些功能，請參閱 [AWS Health 如何使用 IAM](#)。
- 若要了解如何提供您擁有 AWS 帳戶 的資源存取權，請參閱《[IAM 使用者指南](#)》中的[在您擁有 AWS 帳戶 的另一個 中為 IAM 使用者提供存取權](#)。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的[將存取權提供給第三方 AWS 帳戶 擁有](#)。
- 如需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 中的跨帳戶資源存取](#)。

使用的服務連結角色 AWS Health

AWS Health use AWS Identity and Access Management (IAM) [服務連結角色](#)。服務連結角色是直接連結至的唯一 IAM 角色類型 AWS Health。服務連結角色由預先定義，AWS Health 並包含服務 AWS 服務為您呼叫其他所需的所有許可。

您可以使用服務連結角色進行設定 AWS Health，以避免手動新增必要的許可。AWS Health 會定義其服務連結角色的許可，除非另有定義，否則只能 AWS Health 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。

的服務連結角色許可 AWS Health

AWS Health 有兩個服務連結角色：

- [AWSServiceRoleForHealth_Organizations](#) – 此角色信任 AWS Health (health.amazonaws.com) 擔任角色來 AWS 服務為您存取。連接到此角色是 Health_OrganizationsServiceRolePolicy AWS 受管政策。
- [AWSServiceRoleForHealth_EventProcessor](#) – 此角色信任 AWS Health 服務委託人 (event-processor.health.amazonaws.com) 為您擔任該角色。連接到此角色是 AWSHealth_EventProcessorServiceRolePolicy AWS 受管政策。服務主體使用角色來建立 AWS 事件偵測和回應的 Amazon EventBridge 受管規則。此規則是中從您的帳戶 AWS 帳戶交付警示狀態變更資訊所需的基礎設施 AWS Health。

如需 AWS 受管政策的詳細資訊，請參閱 [AWS 的受管政策 AWS Health](#)。

為建立服務連結角色 AWS Health

您不需要建立 AWSServiceRoleForHealth_Organizations 服務連結角色。當您呼叫 [EnableHealthServiceAccessForOrganization](#) 操作時，會在帳戶中為您 AWS Health 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](#)」。

編輯的服務連結角色 AWS Health

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](#)。

刪除的服務連結角色 AWS Health

若要刪除AWSServiceRoleForHealth_Organizations角色，您必須先呼叫 [DisableHealthServiceAccessForOrganization](#) 操作。然後，您可以透過 IAM 主控台、IAM API 或 AWS Command Line Interface () 刪除角色AWS CLI。

若要刪除AWSServiceRoleForHealth_EventProcessor角色，請聯絡 AWS 支援 並要求他們從 AWS 事件偵測和回應中移出您的工作負載。此程序完成後，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 的 受管政策 AWS Health

AWS 受管政策是由 AWS AWS 受管政策建立和管理的獨立政策旨在為許多常用案例提供許可，以便您可以開始將許可指派給使用者、群組和角色。

請記住，AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為這些許可可供所有 AWS 客戶使用。我們建議您定義特定於使用案例的 [客戶管理政策](#)，以便進一步減少許可。

您無法變更 AWS 受管政策中定義的許可。如果 AWS 更新受 AWS 管政策中定義的許可，則更新會影響政策連接的所有委託人身分（使用者、群組和角色）。當新的 AWS 服務 啟動或新的 API 操作可供現有服務使用時，AWS 最有可能更新 AWS 受管政策。

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 受管政策。

內容

- [AWS 受管政策：AWSHealth_EventProcessorServiceRolePolicy](#)
- [AWS 受管政策：Health_OrganizationsServiceRolePolicy](#)
- [AWS 受管政策：AWSHealthFullAccess](#)
- [AWS Health AWS 受管政策的更新](#)

AWS 受管政策：AWSHealth_EventProcessorServiceRolePolicy

AWS Health 使用 [AWSHealth_EventProcessorServiceRolePolicy](#) AWS 受管政策。此受管政策連接至 `AWSServiceRoleForHealth_EventProcessor` 服務連結角色。此政策允許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 [使用的服務連結角色 AWS Health](#)。

受管政策具有下列許可，AWS Health 允許存取 AWS 事件偵測和回應的 Amazon 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，並描述和更新這些規則的目標。

JSON

```
{
  "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"
}
]
}

```

如需政策變更的清單，請參閱 [AWS Health AWS 受管政策的更新](#)。

AWS 受管政策：Health_OrganizationsServiceRolePolicy

AWS Health 使用 [Health_OrganizationsServiceRolePolicy](#) AWS 受管政策。此受管政策連接至 `AWSServiceRoleForHealth_Organizations` 服務連結角色。此政策允許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 [使用的服務連結角色 AWS Health](#)。

此政策授予許可，AWS Health 允許存取運作狀態組織檢視的必要 AWS Organizations 詳細資訊。

許可詳細資訊

此政策包含以下許可。

- `organizations` – 說明中的帳戶 AWS 服務，AWS Organizations 以及可與 Organizations 搭配使用的。

JSON

```

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

```

```

    ],
    "Resource": "*"
  }
]
}

```

如需政策變更的清單，請參閱 [AWS Health AWS 受管政策的更新](#)。

AWS 受管政策：AWSHealthFullAccess

AWS Health 使用 [AWSHealthFullAccess](#) AWS 受管政策。政策會授予實體 (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 AWS 的組織檢視功能，並檢視管理帳戶的組織單位 (OU)
- health – 存取 AWS Health API 操作和通知
- iam – 建立連結服務的 AWS Health IAM 角色

JSON

```

{
  "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"
      }
    }
  }
]
}

```

如需政策變更的清單，請參閱 [AWS Health AWS 受管政策的更新](#)。

AWS Health AWS 受管政策的更新

檢視自此服務開始追蹤這些變更 AWS Health 以來，AWS 受管政策更新的詳細資訊。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 AWS Health 受管政策的重要更新。

AWS Health

變更	描述	日期
AWS 受管政策：AWSHealth FullAccess - 更新現有政策	AWS Health 已將 AWSHealth FullAccess 政策擴展至 AWS GovCloud (US) Regions 和中國區域。	2023 年 10 月 16 日
AWS 受管政策：Health_OrganizationsServiceRolePolicy - 更新現有政策	AWS Health 新增 AWS Organizations 動作，以允許服務連結角色描述可與搭配使用的帳戶 AWS 和服務 AWS Organizations。	2023 年 7 月 19 日
變更發佈的日誌	變更 AWS Health 受管政策的日誌。	2023 年 1 月 13 日

在中記錄和監控 AWS Health

監控是維護 AWS Health 和其他 AWS 解決方案的可靠性、可用性和效能的重要部分。AWS 提供下列監控工具，讓您監看 AWS Health、回報錯誤，並適時採取動作：

- Amazon CloudWatch AWS 會即時監控您的 AWS 資源和您在 上執行的應用程式。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，您可以讓 CloudWatch 追蹤 CPU 使用量或其他 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體指標，並在需要時自動啟動新的執行個體。如需詳細資訊，請參閱《[Amazon CloudWatch 使用者指南](#)》。
- Amazon EventBridge 提供near-real-time的系統事件串流，描述 AWS 資源的變更。EventBridge 支援自動化事件驅動型運算。您可以編寫規則，在其他 AWS 服務內監看特定事件，並在這些事件發生時觸發自動化動作。如需詳細資訊，請參閱[AWS Health 使用 Amazon EventBridge 監控 中的事件](#)。
- AWS CloudTrail 會擷取由您的帳戶發出或代表 AWS 您的帳戶發出的 API 呼叫和相關事件，並將日誌檔案交付至您指定的 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 地址，以及呼叫的時間。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](#)。

的合規驗證 AWS Health

若要了解 是否 AWS 服務 在特定合規計劃的範圍內，請參閱[AWS 服務 合規計劃範圍內](#) 然後選擇您感興趣的合規計劃。如需一般資訊，請參閱[AWS 合規計劃](#)。

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[下載報告 in AWS Artifact](#)

您使用 時的合規責任 AWS 服務 取決於資料的機密性、您公司的合規目標，以及適用的法律和法規。如需使用 時合規責任的詳細資訊 AWS 服務，請參閱 [AWS 安全文件](#)。

中的彈性 AWS Health

AWS 全球基礎設施是以 AWS 區域和可用區域為基礎建置。AWS 區域提供多個實體分隔和隔離的可用區域，這些可用區域與低延遲、高輸送量和高備援聯網連接。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存放和複寫。此方法可確保您可以從 Health 儀板表 或 AWS Health API 操作存取它們。您 AWS Health 最多可以檢視事件發生後的 90 天。

如需 AWS 區域和可用區域的詳細資訊，請參閱 [AWS 全球基礎設施](#)。

中的基礎設施安全 AWS Health

作為受管服務，AWS Health 受到 [Amazon Web Services : 安全程序概觀](#) 白皮書中所述的 AWS 全球網路安全程序的保護。

您可以使用 AWS 發佈的 API 呼叫，AWS Health 透過網路存取。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。

中的組態和漏洞分析 AWS Health

組態和 IT 控制是客戶 AWS 與您之間共同責任。如需詳細資訊，請參閱 AWS [共同的責任模型](#)。

的安全最佳實務 AWS Health

請參閱下列使用的最佳實務 AWS Health。

授予 AWS Health 使用者最低可能許可

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，您可以允許 AWS Identity and Access Management (IAM) 使用者存取 Health 儀板表。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 身分型政策範例](#)。

檢視 Health 儀板表

Health 儀板表 經常檢查您的，以識別可能影響您的帳戶或應用程式的事件。例如，您可能會收到 資源的事件通知，例如需要更新的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體。

如需詳細資訊，請參閱[AWS Health 儀表板入門](#)。

AWS Health 與 Amazon Chime 或 Slack 整合

您可以 AWS Health 與您的聊天工具整合。此整合可讓您和您的團隊即時收到 AWS Health 事件的通知。如需詳細資訊，請參閱 GitHub 中的 [AWS Health 工具](#)。

監控 AWS Health 事件

您可以 AWS Health 與 Amazon CloudWatch Events 整合，以便針對特定事件建立規則。當 CloudWatch Events 偵測到符合您規則的事件時，您會收到通知，然後可以採取動作。CloudWatch Events 事件是區域特定的，因此您必須在應用程式或基礎設施所在的區域中設定此服務。

在某些情況下，無法判斷 AWS Health 事件的區域。如果發生這種情況，事件預設會出現在美國東部（維吉尼亞北部）區域。您可以在此區域中設定 CloudWatch Events，以確保您監控這些事件。

如需詳細資訊，請參閱[AWS Health 使用 Amazon EventBridge 監控 中的事件](#)。

跨帳戶彙總 AWS Health 事件

根據預設，您可以使用 AWS Health 來檢視單一 AWS 帳戶 AWS Health 的事件。如果您使用 AWS Organizations，也可以集中檢視整個組織的 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，或收到安全漏洞的通知。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。使用此功能來隨時了解可能需要更新或程式碼變更 AWS 的服務即將發生的變更。

最佳實務是使用[委派管理員](#)功能，將 AWS Health 組織檢視的存取權委派給成員帳戶。這可讓營運團隊更輕鬆地存取組織中 AWS Health 的事件。委派管理員功能可讓您限制管理帳戶，同時為團隊提供對事件採取行動 AWS Health 所需的可見性。

Important

- AWS Health 為組織中的帳戶傳送的事件，只要事件可用，就會顯示在組織檢視中，最長可達 90 天，即使其中一或多個帳戶離開您的組織。
- 組織事件在刪除前可使用 90 天。此配額無法增加。

先決條件

在使用組織檢視之前，您必須：

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

您也可以以組織的管理帳戶中的根使用者身分登入（不建議）。如需詳細資訊，請參閱《IAM 使用者指南》中的[鎖定 AWS 您的帳戶根使用者存取金鑰](#)。

- 如果您以 IAM 使用者身分登入，請使用授予 AWS Health 和 Organizations 動作存取權的 IAM 政策，例如 [AWSHealthFullAccess](#) 政策。如需詳細資訊，請參閱[AWS Health 身分型政策範例](#)。

主題

- [啟用組織檢視](#)

- [檢視組織檢視](#)
- [停用組織檢視](#)
- [管理組織的委派管理員檢視](#)

啟用組織檢視

您可以使用 AWS Health 主控台來取得 AWS 組織中運作狀態事件的集中式檢視。

所有 AWS 支援 計劃都可以在 AWS Health 主控台中使用組織檢視，無需額外費用。

Note

如果您想要允許使用者存取 管理帳戶中的此功能，他們必須擁有 [AWSHealthFullAccess](#) 政策等許可。如需詳細資訊，請參閱 [AWS Health 身分型政策範例](#)。

Enabling organizational view (Console)

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。

檢視組織的 AWS Health 儀表板

1. 在 <https://health.aws.amazon.com/health/home> 開啟您的 AWS Health 儀表板。
2. 在導覽窗格中，在您的組織運作狀態下，選擇組態。
3. 在啟用組織檢視頁面上，選擇啟用組織檢視。
4. (選用) 如果您想要變更 AWS 組織，例如建立組織單位 (OUs)，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

- 當您啟用 AWS Health 組織檢視時，初始帳戶載入程序會在背景執行，可能需要幾分鐘的時間才能完成。您可以關閉 AWS Health 主控台，稍後再返回，因為您不需要等待程序完成。歷史運作狀態事件（在您啟用此功能之前建立的事件）最多可能需要 24 小時才會出現在您的組織檢視中。

- 如果您有 AWS Business Support+、AWS Enterprise Support 或 AWS Unified Operations 計劃，您可以呼叫 [DescribeHealthServiceStatusForOrganization](#) API 操作來檢查程序的狀態。
- 當您啟用此功能時，具有 Health_OrganizationsServiceRolePolicy AWS 受管政策 AWSServiceRoleForHealth_Organizations 的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 [使用的服務連結角色 AWS Health](#)。

Enabling organizational view (CLI)

您可以使用 [EnableHealthServiceAccessForOrganization](#) API 操作來啟用組織檢視。

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 [Business](#)、[Enterprise On-Ramp](#) 或 [Enterprise](#) Support 計劃才能呼叫 AWS Health API。
- 您必須使用美國東部（維吉尼亞北部）區域端點。

Example

下列 AWS CLI 命令會從您的帳戶啟用此功能 AWS。您可以從管理帳戶或從可擔任具有必要許可之角色的帳戶使用此命令。

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

下列程式碼範例會呼叫 [EnableHealthServiceAccessForOrganization](#) API 操作。

Python

```
import boto3

client = boto3.client('health', region_name='us-east-1')

response = client.enable_health_service_access_for_organization()
```

```
print(response)
```

Java

您可以針對下列範例使用適用於 Java 2.0 版的 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.EnableHealthServiceAccessForOrganizationRequest;
import
    software.amazon.awssdk.services.health.model.EnableHealthServiceAccessForOrganizationResponse;
import
    software.amazon.awssdk.services.health.model.DescribeHealthServiceStatusForOrganizationRequest;
import
    software.amazon.awssdk.services.health.model.DescribeHealthServiceStatusForOrganizationResponse;

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

import software.amazon.awssdk.regions.Region;

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

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

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

```
    }

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

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

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，具有 Health_OrganizationsServiceRolePolicy AWS 受管政策 AWSServiceRoleForHealth_Organizations [的服務連結角色](#) 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](#) 操作來檢查程序的狀態。

檢視組織檢視

您可以使用 AWS Health 主控台來取得 AWS 組織中運作狀態事件的集中式檢視。

所有 AWS 支援 計劃都可以在 AWS Health 主控台中使用組織檢視，無需額外費用。

Note

如果您想要允許使用者存取 管理帳戶中的此功能，他們必須擁有 [AWSHealthFullAccess](#) 政策等許可。如需詳細資訊，請參閱 [AWS Health 身分型政策範例](#)。

Viewing organizational view events (Console)

啟用組織檢視後，AWS Health 會顯示組織中所有帳戶的運作狀態事件。

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 從管理員帳戶關閉的生效日期起，會保留帳戶的政策資料 90 天。在 90 天期間結束時，會 AWS 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 保留政策資料，當您重新開啟已關閉的帳戶時，會將該帳戶重新 AWS 指派為服務管理員，並復原該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) 區域中的客戶：

- 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

當您啟用此功能時，AWS Health 主控台可以從[AWS Health 儀表板 – 服務運作](#)狀態顯示過去 7 天的公有事件。這些公有事件並非專屬於您組織中的帳戶。AWS Health 儀表板中的事件 – 服務運作狀態提供有關 AWS 服務區域可用性的公開資訊。

您可以在以下頁面中檢視組織檢視事件：

開啟和最近的問題

您可以使用開啟和最近的問題索引標籤來檢視可能影響 AWS 基礎設施的事件，例如對 AWS 服務的變更，以及影響您組織的資源。

檢視組織檢視事件

1. 在 <https://health.aws.amazon.com/health/home> 開啟您的 AWS Health 儀表板。
2. 在導覽窗格的組織運作狀態下，選擇開啟和最近的問題，以檢視最近報告的事件。
3. 選擇事件。在詳細資訊索引標籤上，您可以檢閱事件的下列相關資訊：
 - 事件名稱
 - 狀態
 - 區域/可用區域
 - 受影響的帳戶
 - 開始時間
 - 結束時間
 - 類別
 - 描述

排定的變更

使用排程變更索引標籤來檢視可能影響組織的近期事件。這些事件可以包含服務的排程維護活動。

其他通知

使用通知索引標籤來檢視過去七天中可能影響組織的所有其他通知和持續事件。這可能包括事件，例如憑證輪換、帳單通知和安全漏洞。

事件日誌

您也可以使用事件日誌索引標籤來檢視 AWS Health 組織檢視的事件。資料欄配置和行為類似於開啟和最近的問題索引標籤，但事件日誌索引標籤包含額外的資料欄和篩選條件選項，例如事件類別、狀態和開始時間。

在事件日誌索引標籤中檢視組織檢視事件

1. 在 <https://health.aws.amazon.com/health/home> 開啟您的 AWS Health 儀表板。
2. 在導覽窗格中，在您的組織運作狀態下，選擇事件日誌。
3. 在事件日誌下，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
- 區域/可用區域
- 受影響的帳戶
- 開始時間
- 結束時間
- 類別
- 描述

Viewing affected accounts and resources (Console)

在組織運作狀態下，您可以檢視組織中受事件和任何相關資源影響的帳戶。例如，如果 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體維護即將發生事件，組織中具有 Amazon EC2 執行個體的帳戶可能會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。

檢視受影響的帳戶和資源

1. 在 <https://health.aws.amazon.com/health/home> 開啟您的 AWS Health 儀表板。
2. 在導覽窗格的組織運作狀態下，選擇其中一個索引標籤。
3. 選擇具有受影響帳戶值的事件。
4. 選擇受影響的帳戶索引標籤。
5. 選擇顯示帳戶詳細資訊以檢視帳戶的下列資訊：
 - 帳戶 ID
 - 帳戶名稱
 - 主要電子郵件
 - 組織單位 (OU)
6. 展開帳戶以檢視受影響的資源。
7. 如果有 10 個以上的資源，請選擇檢視所有資源以進行檢視。
8. 若要依此特定事件的帳戶 ID 進行篩選，請執行下列動作：
 - a. 在受影響的帳戶索引標籤上，選擇新增篩選條件，選擇帳戶 ID，然後輸入帳戶 ID。您一次只能輸入一個帳戶 ID。
 - b. 選擇套用。您輸入的帳戶會顯示在清單中。

Viewing organizational view events (CLI)

啟用此功能後，會 AWS Health 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 在您啟用組織檢視之前，不會記錄組織中發生的事件。

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 從管理員帳戶關閉的生效日期起，會保留帳戶的政策資料 90 天。在 90 天期間結束時，會 AWS 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 保留政策資料，當您重新開啟已關閉的帳戶時，會將該帳戶重新 AWS 指派為服務管理員，並復原該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) 區域中的客戶：

- 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。

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
```

停用組織檢視

如果您不想彙總組織的事件，您可以從管理帳戶關閉此功能，也可以使用 [DisableHealthServiceAccessForOrganization](#) API 操作來停用組織檢視。

Disabling organizational view events (Console)

AWS Health 會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中先前的事件，直到刪除為止。

停用組織檢視

1. 在 <https://health.aws.amazon.com/health/home> 開啟您的 AWS Health 儀表板。
2. 在導覽窗格的組織運作狀態下，選擇組態。
3. 在啟用組織檢視頁面上，選擇停用組織檢視。

關閉此功能後，AWS Health 不會再彙總組織中的事件。不過，服務連結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 Command Line Interface () 將其刪除為止AWS CLI。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](#)。

Disabling organizational view events (CLI)

Example

下列 AWS CLI 命令會從您的帳戶停用此功能。

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

Note

您也可以使用 Organizations [DisableAWSServiceAccess](#) API 操作來停用組織功能。呼叫此操作之後，會 AWS Health 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，會 AWS Health 傳回錯誤。AWS Health 會繼續彙總您 AWS 帳戶的運作狀態事件。

停用此功能後，AWS Health 不會再彙總組織中的事件。不過，服務連結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 或將其刪除為止 AWS CLI。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](#)。

管理組織的委派管理員檢視

透過 AWS Health，您可以利用的委派管理員功能 AWS Organizations，允許管理帳戶以外的帳戶在 [AWS Health 儀表板](#) 上或透過 [AWS Health API](#) 以程式設計方式檢視彙總 AWS Health 事件。委派管理員功能可讓不同團隊彈性檢視和管理整個組織的運作狀態事件。盡可能將責任委派給管理帳戶以外的 AWS 安全最佳實務。

內容

- [為您的組織檢視註冊委派管理員](#)
- [從組織檢視中移除委派管理員](#)

為您的組織檢視註冊委派管理員

為組織啟用組織檢視後，您最多可以將組織中的五個成員帳戶註冊為委派管理員。若要這樣做，請呼叫 [RegisterDelegatedAdministrator](#) API 操作。註冊成員帳戶後，他們將被委派管理帳戶，並且可以從 AWS Health 儀表板存取 AWS Health 組織檢視。如果帳戶有 [商業](#)、[Enterprise On-Ramp](#) 或 [企業](#) 支援計劃，則委派管理員可以使用 AWS Health API 存取 AWS Health 組織檢視。

若要建立委派管理員，請從組織中的管理帳戶呼叫 following AWS Command Line Interface (AWS CLI) 命令。您可以從管理帳戶或從可擔任具有必要 AWS Identity and Access Management 許可之角色的帳戶使用此命令。在下列範例命令中，將 ACCOUNT_ID 取代為您要與服務 AWS Health 委託人 "health.amazonaws.com" 一起註冊的成員帳戶 ID。

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

註冊委派管理員後，您可以查看影響整個組織帳戶的所有 AWS Health 事件。您可以檢視過去 90 天或自組織檢視功能首次啟用以來的歷史事件，以較新者為準。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管理員

若要移除委派管理員的存取權，請呼叫 [DeregisterDelegatedAdministrator](#) API 操作。

從組織的管理帳戶中，呼叫下列 AWS CLI 命令，將成員帳戶移除為委派管理員。在下列範例命令中，將 ACCOUNT_ID 取代為您要移除的成員帳戶 ID。

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

AWS Health 使用 Amazon EventBridge 監控 中的事件

您可以使用 Amazon EventBridge 來偵測和回應 AWS Health 事件。然後，當事件符合您在規則中指定的值時，EventBridge 會根據您建立的規則叫用一或多個目標動作。根據事件類型，您可以擷取事件資訊、啟動其他事件、傳送通知、採取修正動作或執行其他動作。例如，如果您的 中有 AWS 帳戶 排定更新 AWS 的資源，例如 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，您可以使用 來 AWS Health 接收電子郵件通知。

備註

- AWS Health 會持久地交付事件，並嘗試至少將事件成功交付至 EventBridge 一次。
- 您建立的任何 EventBridge 規則只能接收 的通知 AWS 帳戶。若要接收您 內其他帳戶的組織事件 AWS Organizations，請參閱[使用組織檢視和委派管理員存取權彙總 AWS Health 事件](#)。
- 建立 EventBridge 規則後，公有運作狀態事件最多可能需要一小時才會開始傳送。

您可以在 AWS Health 工作流程中為 EventBridge 選擇多個目標類型，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至 Slack 頻道。或者，您可以使用 Lambda 和 EventBridge，在 AWS Health 事件發生時透過 Amazon SNS 傳送自訂文字或簡訊通知。

如需您可以為回應 AWS Health 事件而建立的自動化和自訂提醒範例，請參閱 GitHub 中的[AWS Health 工具](#)。

主題

- [建立涵蓋 AWS 區域 範圍的 EventBridge 規則](#)

- [監控的帳戶特定和公有事件 AWS Health](#)
- [檢視 EventBridge 上的 AWS Health 事件分頁清單](#)
- [使用組織檢視和委派管理員存取權彙總 AWS Health 事件](#)
- [將 AWS Health 事件監控和通知與 JIRA 和 ServiceNow 整合](#)
- [設定 EventBridge 規則以傳送中事件的通知 AWS Health](#)
- [在聊天應用程式中設定 Amazon Q Developer 以傳送中事件的通知 AWS Health](#)
- [在 EC2 執行個體上自動執行操作，以回應中的事件 AWS Health](#)
- [參考：AWS Health 事件 Amazon EventBridge 結構描述](#)

建立涵蓋 AWS 區域範圍的 EventBridge 規則

您可以為要接收 AWS Health 事件的每個區域建立 EventBridge 規則。例如，若要從歐洲（法蘭克福）區域接收事件，您可以為此區域建立規則。

若要增強 AWS Health 通知的可靠性，您可以在專用備份區域中設定規則。在標準 AWS 分割區中，美國西部（奧勒岡）區域做為所有其他區域的備份區域，而美國東部（維吉尼亞北部）區域則做為美國西部（奧勒岡）區域的備份。當運作狀態事件發生時，它們會自動傳送至主要區域及其指定的備份區域。例如，如果您要監控歐洲（法蘭克福）區域中的事件，則任何運作狀態事件都會傳送至歐洲（法蘭克福）區域和美國西部（奧勒岡）區域。即使主要區域遇到問題，此系統仍會確保您繼續接收運作狀態通知。若要建立備份規則，請遵循的程序[設定 EventBridge 規則以傳送中事件的通知 AWS Health](#)。

如果您不想使用備份功能，則必須將篩選條件新增至備份區域規則。例如，為實作篩選條件 `detail.backupEvent = False`。這可防止您從其他區域接收備份事件。

高可用性設定（選用）

如果您想要建立具有高可用性的 EventBridge 整合，請確定您已在相關和備份區域中實作規則，然後使用實作重複資料刪除 `detail.communicationId`。這可確保您接收所有事件，同時避免重複。如需詳細資訊，請參閱[參考：AWS Health 事件 Amazon EventBridge 結構描述](#)。

簡化整合

如果您想要從多個擷取事件 AWS 區域，但偏好只設定單一規則，則簡化整合是適當的選項。若要從標準 AWS 分割區中的所有區域接收 AWS Health 事件，您可以在美國西部（奧勒岡）區域中設定中

央規則。此單一規則會自動彙總來自您接收運作狀態事件之所有標準分割區區域的事件。不過，您不會有高可用性組態。

全域事件

有些 AWS Health 事件並非區域特定。非特定區域的事件稱為全域事件。這些包括針對 AWS Identity and Access Management (IAM) 傳送的事件。若要接收全域事件，您必須為美國東部（維吉尼亞北部）區域建立規則。

監控的帳戶特定和公有事件 AWS Health

當您建立 EventBridge 規則來監控事件時 AWS Health，規則會同時提供帳戶特定的事件和公有事件：

- 帳戶特定事件會影響您的帳戶和資源，例如事件，告訴您 Amazon EC2 執行個體或其他排程變更事件的必要更新。
- 公有事件會出現在[AWS Health 儀表板 – 服務運作狀態](#)。公有事件並非專屬於 AWS 帳戶，並提供有關服務區域可用性的公有資訊。

Important

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

您可以使用 eventScopeCode 參數，在 EventBridge 中識別事件為公有或帳戶特定。事件可以有 PUBLIC 或 ACCOUNT_SPECIFIC。您也可以在此參數上篩選規則。

範例：Amazon Elastic Compute Cloud 的公有事件

下列事件顯示美國東部（維吉尼亞北部）區域中 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"
}
}
```

AWS Health 事件的備份規則

如果您是從 監控公有事件 AWS 區域，建議您建立備份規則。在受影響的區域中設定有效的規則時，的公有事件 AWS Health 會同時傳送至受影響的區域和備份區域。

AWS Health 無論受影響區域中設定的任何規則為何，都會將帳戶特定事件傳送至受影響的區域和備份區域。

我們建議您使用 eventARN 和 刪除重複 AWS Health 事件，communicationId 因為這些值對於傳送至備份區域 AWS Health 的訊息，會保持一致。

檢視 EventBridge 上的 AWS Health 事件分頁清單

AWS Health 當 AWS Health resources 或 的清單 affectedEntities 導致訊息大小超過 EventBridge 的 256KB 訊息大小限制時，支援事件分頁。

AWS Health 包含訊息中的所有 `resources` 和 `detail.affectedEntities` 欄位。如果此清單的 `resources` 和 `detail.affectedEntities` 值超過 256KB，則會將運作狀態事件 AWS Health 分割成多個頁面，並在 EventBridge 中將這些頁面發佈為個別訊息。每個頁面會保留相同的 `eventARN` 和 `communicationId` 值，以協助在收到所有頁面 `detail.affectedEntities` 之後重新組合 `resources` 或的清單。

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取的界面時，例如電子郵件或聊天。具有人類可讀通知的客戶可以為 `detail.page` 欄位新增篩選條件，以僅處理第一頁，從而消除從後續頁面建立的不必要訊息。

在結構描述中，即使只有 1 頁，每個 `communicationId` 也會包含 `communicationId` 之後的連字號頁碼。欄位 `detail.page` 和 `detail.totalPages` 說明 AWS Health 事件的目前頁碼和總頁數。每個分頁訊息中包含的資訊都相同，但 `detail.affectedEntities` 或的清單除外 `resources`。在收到所有頁面後，即可重建這些清單。受影響資源和實體的頁面與順序無關。

使用組織檢視和委派管理員存取權彙總 AWS Health 事件

AWS Health 支援在 Amazon EventBridge 上發佈 AWS Health 之事件的組織檢視和委派管理員存取權。在中開啟組織檢視時 AWS Health，管理帳戶或委派管理員帳戶會收到來自中組織內所有帳戶的單一 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 EventBridge 規則。

如需在上啟用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](#)。

將 AWS Health 事件監控和通知與 JIRA 和 ServiceNow 整合

您可以將 AWS Health 事件與 JIRA 和 ServiceNow 整合，以接收操作和帳戶資訊、準備排定的變更，以及使用 Service Management Connector (SMC) 管理運作狀態事件。與整合的 SMC AWS Health 可以使用透過 EventBridge 傳送的運作狀態事件，自動建立、映射和更新 JIRA 票證和 ServiceNow 事件。

您可以使用組織檢視和委派管理員存取權，在 JIRA 和 ServiceNow 內輕鬆管理整個組織的運作狀態事件，並將資訊直接整合 AWS Health 到團隊的工作流程中。

如需使用 SMC 進行 ServiceNow 整合的詳細資訊，請參閱 [ServiceNow AWS Health 中的整合](#)。

如需使用 SMC 進行 JIRA Management Cloud 整合的詳細資訊，請參閱 [AWS Health JIRA 中的](#)。

設定 EventBridge 規則以傳送 中事件的通知 AWS Health

您可以建立 Amazon EventBridge 規則，以程式設計方式將 AWS Health 事件與其他 服務、應用程式和工作負載整合。EventBridge 提供拖放主控台界面和 API，以設定在為您的帳戶或組織建立相符 AWS Health 事件時觸發的規則。若要了解如何在 EventBridge 中設定規則以擷取 AWS Health 事件，請參閱 [《Amazon EventBridge 使用者指南》中的在 Amazon EventBridge 中建立規則和在 Amazon EventBridge 中建立對事件做出反應的規則](#)。 EventBridge

根據您的整合，EventBridge 可讓您將參數新增至 EventBridge 規則，以僅篩選您要與使用案例整合 AWS Health 的事件。對於事件回應使用案例，您可能想要專注於issue事件類別和某些關鍵服務。對於計劃的生命週期事件等變更管理使用案例，您可能想要在可操作性欄位中將重點放在具有 AWS Health 的事件ACTION_REQUIRED上。為了與安全使用案例整合，您可能想要使用SECURITY角色欄位專注於所有 AWS Health 濫用事件和 AWS Health 事件。

您可以使用範例使用案例來驗證您的規則擷取您需要的事件。範例使用案例可在 中取得[參考：AWS Health 事件 Amazon EventBridge 結構描述](#)。您也可以在 EventBridge 主控台的測試事件模式 - 選用面板的使用範例事件提供的選項下找到它們

使用 API 或 AWS Command Line Interface

對於新的或現有的規則，請使用 [PutRule](#) API 操作或 `aws events put-rule`命令來更新事件模式。若要檢視範例 AWS CLI 命令，請參閱《AWS CLI 命令參考》中的 [put-rule](#)。

Example範例：為僅 Amazon EC2 服務的問題設定規則

下列事件模式會建立規則來監控 Amazon EC2 服務的問題事件。

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

```
]
}
```

Example範例：設定所有動作所需 AWS Health 事件的規則，包括規劃的生命週期事件

下列事件模式會建立規則來監控需要 動作的所有 AWS Health 事件，包括計劃的生命週期事件。

```
{
  "detail": {
    "eventTypeCategory": [
      "accountNotification",
      "scheduledChange"
    ],
    "actionability": [
      "ACTION_REQUIRED"
    ]
  },
  "detail-type": [
    "AWS Health Event"
  ],
  "source": [
    "aws.health"
  ]
}
```

Example範例：為多個服務和 AWS Health 事件類型類別的所有事件設定規則

下列事件模式會建立規則來監控三種 AWS 服務之 issue、accountNotification和 scheduledChange事件類型類別的事件：Amazon EC2 Auto Scaling、Amazon VPC 和 Amazon EC2。

```
{
  "detail": {
    "eventTypeCategory": [
      "issue",
      "accountNotification",
      "scheduledChange"
    ],
    "service": [
      "AUTOSCALING",
      "VPC",
      "EC2"
    ]
  }
}
```

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

在聊天應用程式中設定 Amazon Q Developer 以傳送 中事件的通知 AWS Health

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可能影響應用程式 AWS 和基礎設施的最新 AWS 服務問題。然後，您可以登入您的 [AWS Health Dashboard](#) 以進一步了解更新。例如，如果您正在監控 AWS 帳戶中 AWS_EC2_INSTANCE_STOP_SCHEDULED 的事件類型，則 AWS Health 事件可以直接顯示到您的 Slack 頻道。

先決條件

開始使用之前，您必須具備下列項目：

- 在聊天應用程式中使用 Amazon Q Developer 設定的聊天用戶端。您可以設定 Amazon Chime 和 Slack。如需詳細資訊，請參閱 [《聊天應用程式管理員指南》](#) 中的在聊天應用程式中開始使用 Amazon Q 開發人員。
- 您建立和訂閱的 Amazon SNS 主題。如果您已有 SNS 主題，您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](#)。

在聊天應用程式中使用 Amazon Q Developer 接收 AWS Health 事件

1. 依照中的程序 [設定 EventBridge 規則以傳送 中事件的通知 AWS Health](#) 執行步驟 13。
 - a. 當您完成步驟 13 中的事件模式設定時，請在模式的最後一行新增逗號，並新增以下行以從分頁 AWS Health 事件中移除不必要的聊天訊息。請參閱 [檢視 EventBridge 上的 AWS Health 事件分頁清單](#)。

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



- b. 當您在步驟 16 選擇目標時，請選擇 SNS 主題。您將在聊天應用程式主控台的 Amazon Q Developer 中使用相同的 SNS 主題。
 - c. 完成其餘程序以建立規則。
2. 在聊天應用程式主控台中導覽至 [Amazon Q Developer](#)。
 3. 選擇您的聊天用戶端，例如您的 Slack 頻道名稱，然後選擇編輯。
 4. 在通知 - 選用區段中，針對主題選擇您在步驟 1 中指定的相同 SNS 主題。
 5. 選擇儲存。



當 AWS Health 將事件傳送至符合您規則的 EventBridge 時，AWS Health 事件會出現在您的聊天用戶端中。

6. 選擇事件名稱，即可在 AWS Health 儀表板中查看更多資訊。

Example：AWS Health 事件傳送至 Slack

以下是美國東部（維吉尼亞北部）區域中 Amazon EC2 和 Amazon Simple Storage Service (Amazon S3) 在 Slack 頻道中出現的兩個 AWS Health 事件範例。

**AWS** APP 11:46 AM
 [AWS Health Event | us-east-1 | Account: 123456789012 | open](#)
Event type code: AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED
EC2 has detected degradation of the underlying hardware hosting your Amazon EC2 instance associated with this event in the us-east-1 region. Due to this degradation your instance could already be unreachable. We will stop your instance after 2021-03-19 18:36:40 PST. Please take appropriate action before this time.\\n\\nYou can find more information about retirement events scheduled for your EC2 instances in the AWS Management Console <https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#Events>\\n\\n* What will happen to my instance?\\nYour instance will be stopped after the specified retirement date. You can start it agai...
[Show more](#)
Start time: Sat, 20 Mar 2021 01:35:40 GMT
End time: Sat, 20 Mar 2021 01:36:40 GMT

**AWS** APP 12:08 PM
 [AWS Health Event | us-east-1 | Account: 123456789012 | open](#)
Event type code: AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION
We are writing to notify you that you may have exposed your S3 bucket/s to a larger audience than you intended. AWS recommends that you review your bucket permissions and ACLs to determine whether the access is appropriate. S3 bucket permissions should never contain \\\"Principal\\\": \\\"*\\\" unless you intend to grant public access to your data. Additionally, S3 bucket ACLs should be appropriately scoped to prevent unintended access to \\\"Authenticated Users\\\" or \\\"Everyone\\\" unless your use case requires it.\\n\\nThe list of buckets with this configuration is associated with this event.\\n\\nThe following links provide an overv...
[Show more](#)
Start time: Sat, 20 Mar 2021 01:35:40 GMT
End time: Sat, 20 Mar 2021 01:36:40 GMT

在 EC2 執行個體上自動執行操作，以回應 中的事件 AWS Health

您可以自動化回應 Amazon EC2 執行個體排程事件的動作。當 AWS Health 將事件傳送到 AWS 您的帳戶時，您的 EventBridge 規則接著可以叫用 AWS Systems Manager 自動化文件等目標，以代表您自動執行動作。

例如，當排程 Amazon EC2 執行個體的 Amazon EC2 執行個體淘汰事件時，AWS Health 會將 AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED 事件類型傳送至您的 AWS Health

Dashboard。當您的規則偵測到此事件類型時，您可以自動停止和啟動執行個體。如此一來，您就不必手動執行這些動作。

Note

若要自動化 Amazon EC2 執行個體的動作，執行個體必須由 Systems Manager 管理。

如需詳細資訊，請參閱《[Amazon EC2 使用者指南](#)》中的使用 [EventBridge 自動化 Amazon EC2](#)。

先決條件

您必須建立 AWS Identity and Access Management (IAM) 政策、建立 IAM 角色，以及更新角色的信任政策，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。此政策提供角色代表您執行動作的許可。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 管理主控台 並開啟位於 <https://console.aws.amazon.com/iam/> 的 IAM 主控台。
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，然後在編輯器中取代預設 JSON。

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，針對 Amazon Resource Name (ARN) 輸入 AWS 您的帳戶 ID。
 - b. 您也可以取代角色名稱或使用預設值。此範例使用 *AutomationEVRole*。
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. 在檢閱政策頁面上，輸入名稱，例如 *AutomationEVRolePolicy* 和選用的描述。
10. 檢閱摘要頁面以查看政策允許的許可。如果您對政策感到滿意，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。

為 AWS 服務建立角色

1. 登入 AWS 管理主控台 並開啟位於 <https://console.aws.amazon.com/iam/> 的 IAM 主控台。
2. 在導覽窗格中，選擇角色，然後選擇建立角色。
3. 對於 Select type of trusted entity (選取信任的實體類型)，選擇 AWS service (服務)。
4. 為您要允許 擔任此角色的服務選擇 EC2。
5. 選擇下一步：許可。
6. 輸入您建立的政策名稱，例如 *AutomationEVRolePolicy*，然後選取政策旁的核取方塊。
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 *AutomationEVRole*。此名稱必須與您建立之 IAM 政策的 ARN 中出現的名稱相同。
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政策。您必須完成此程序，才能在 EventBridge 主控台中選擇此角色。

更新角色的信任政策

1. 登入 AWS 管理主控台 並開啟位於 <https://console.aws.amazon.com/iam/> 的 IAM 主控台。
2. 在導覽窗格中，選擇角色。
3. 在 AWS 帳戶中的角色清單中，選擇您建立的角色名稱，例如 *AutomationEVRole*。
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. 針對政策文件，複製下列 JSON、移除預設政策，並將複製的 JSON 貼到其位置。

JSON

```
{
  "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 EventBridge 的規則

請依照此程序在 EventBridge 主控台中建立規則，以便您可以自動停止和啟動排程淘汰的 EC2 執行個體。

建立適用於 Systems Manager 自動化動作的 EventBridge 規則

1. 造訪 <https://console.aws.amazon.com/events/> 開啟 Amazon EventBridge 主控台。

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，輸入規則的名稱和描述。
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，選擇運作狀態。
7. 針對事件類型，選擇特定運作狀態事件。
8. 選擇特定 (特定) 服務，然後選擇 EC2。
9. 選擇特定事件類型類別 (s)，然後選擇 scheduledChange。
10. 選擇特定事件類型程式碼 (程式碼)，然後選擇事件類型程式碼。

例如，對於 Amazon EC2 EBS 支援的執行個體，選擇

AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED。針對 Amazon EC2 執行個體後端執行個體，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與下列範例類似。

Example

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

```
}
```

12. 新增 Systems Manager Automation 文件目標。在選取目標下，針對目標選擇 SSM 自動化。
13. 對於 Document (文件)，請選擇 `AWS-RestartEC2Instance`。
14. 展開設定自動化參數 (設定)，然後選擇輸入轉換器。
15. 在輸入路徑欄位中，輸入 `{"Instances": "$resources"}`。
16. 針對第二個欄位，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 `AutomationEVRole`。

您的目標看起來應該如下範例所示。

Target Remove

Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule).

SSM Automation

Document

AWS-RestartEC2Instance

▶ Configure document version

▼ Configure automation parameter(s)

No Parameter(s)

Constant

Input Transformer

```
["Instances": "$resources"]
```

```
["InstanceId": <Instances>]
```

EventBridge needs permission to call SSM Start Automation Execution with your supplied Automation document and parameters. By continuing, you are allowing us to do so.

Create a new role for this specific resource

Use existing role

AutomationEVRole

Note

如果您沒有具有必要 EC2 和 Systems Manager 許可和信任關係的現有 IAM 角色，您的角色將不會出現在清單中。如需詳細資訊，請參閱[先決條件](#)。

18. 選擇建立。

如果您的帳戶中發生符合您規則的事件，EventBridge 會將事件傳送至您指定的目標。

參考：AWS Health 事件 Amazon EventBridge 結構描述

以下是 AWS Health 事件的結構描述。在第二個資料表中，詳細資訊參數的內容如下。範例承載是在結構描述資料表之後提供。

AWS Health 事件結構描述

AWS Health 事件結構描述

參數	Description	必要
version	EventBridge 版本，目前為 "0"。	是
id	EventBridge 事件的唯一識別符。	是
detail-type	詳細資訊的類型。對於 AWS Health 事件，支援的值為 &AWS Health Event 和 AWS Health Abuse Event	是
source	事件匯流排來源。對於 AWS Health 事件，支援的值為 <code>aws.health</code>	是

參數	Description	必要
account	<p>傳送 AWS Health 事件的目標帳戶 ID。</p> <div data-bbox="1068 445 1269 1621"><p> Note</p><p>對於組織檢視，如果在管理帳戶或委派管理員帳戶中收到，則這是與受影響帳戶不同的帳戶。</p></div>	是


參數	Description	必要
time	通知傳送至 EventBridge 的時間。格式：yyyy-mm-d dThh:mm:ssZ。	是
region	<p>通知傳送到 AWS 區域的。</p> <div data-bbox="1068 768 1271 1751" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>此欄位不會指出此 AWS Health 事件受影響的區域。該資訊會在中報告detailentRegion。</p> </div>	是

參數	Description	必要
resources	描述帳戶內受影響的資源清單，如果有的話。 如果沒有參考的資源，此欄位為空白。	否
詳細資訊	包含 AWS Health 事件詳細資訊的區段，如此事件後面的資料表所述。	是

'details' 參數的結構描述內容

下表記錄 AWS Health 事件結構描述中詳細資訊參數的內容。

AWS Health 事件結構描述：詳細資訊參數內容

'detail' 參數內容	Description	必要
eventArn	特定區域 AWS Health 事件的唯一識別符，包括區域和事件 ID。 <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E1F5FE;"> <p> Note 事件 ARN 對特定 AWS 帳戶或區域來說不是唯一的。</p> </div>	是
服務	受 AWS Health 事件 AWS 服務影響的。例如，Amazo	是

'detail' 參數內容	Description	必要
	n EC2、Amazon Simple Storage Service、Amazon Redshift 或 Amazon Relational Database Service。	
eventTypeCode	<p>事件類型的唯一辨識碼。例如：AWS_EC2_INSTANCE_NETWORK_MAINTENANCE_SCHEDULED 和 AWS_EC2_INSTANCE_REBOOT_MAINTENANCE_SCHEDULED。包含的事件通常會 MAINTENANCE_SCHEDULED 在開始時間前約兩週推出。</p> <div data-bbox="591 940 1029 1356" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>所有新的計劃生命週期事件都具有事件類型 AWS_{SERVICE}_PLANNED_LIFECYCLE_EVENT。</p> </div>	是
eventTypeCategory	事件的類別程式碼。支援的值包括 issue、investigation、accountNotification 和 scheduledChange。	是
eventScopeCode	指出 AWS Health 事件是帳戶特定還是公有。支援的值為 ACCOUNT_SPECIFIC 或 PUBLIC。	是

'detail' 參數內容	Description	必要
communicationId	<p>此 AWS Health 事件通訊的唯一識別符。</p> <p>具有相同通訊 ID 的訊息可能是備份訊息或單一 AWS Health 事件的頁面。此識別符可與帳戶 ID 搭配使用，以協助刪除重複的訊息。</p> <p>使用 AWS Health 事件分頁支援時，通訊 ID 會包含頁面號碼，讓通訊 ID 在各頁面中保持唯一，例如 12345678910-1。如需詳細資訊，請參閱檢視 EventBridge 上的 AWS Health 事件分頁清單。</p>	是
startTime	<p>AWS Health 事件的開始時間，格式為 DoW, DD, MMM, YYYY, HH:MM:SS TZ。</p> <p>排程事件的開始時間可以是未來的時間。</p>	是
endTime	<p>AWS Health 事件的結束時間，格式為 : DoW, DD MMM YYYY HH:MM:SS TZ。</p> <p>無法為排程在未來時間的事件提供結束時間。</p>	否
lastUpdatedTime	<p>AWS Health 事件的上次更新時間，格式為 DoW, DD MMM YYYY HH:MM:SS TZ。</p>	是

'detail' 參數內容	Description	必要
statusCode	<p>AWS Health 事件的狀態。</p> <p>支援的值包括 open、closed和 upcoming。</p>	是
eventRegion	此 AWS Health 事件描述受影響的區域。	是
eventDescription	<p>描述 AWS Health 事件的區段。這包括用於描述事件的語言和文字欄位。</p> <ul style="list-style-type: none"> • language – AWS Health 事件中所用語言的程式碼。這通常由發佈事件的區域決定。例如，在 us-east-1 區域中，這通常是 en_US。 • latestDescription – 描述從 AWS Health API 轉譯 AWS Health 的事件，通常出現在 AWS Health 儀表板上。 <div data-bbox="623 1255 1029 1570" style="border: 1px solid #add8e6; border-radius: 15px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>對於公有事件，這只包含最新的更新，不包含事件的完整歷史記錄。</p> </div>	是

'detail' 參數內容	Description	必要
eventMetadata	<p>可為事件提供 AWS Health 的其他事件中繼資料。</p> <ul style="list-style-type: none"> • <中繼資料金鑰 1> – 中繼資料金鑰/值對字串："keystring1" : "keyvalue1" <p>事件中繼資料的鍵/值對取決於傳送 AWS Health 事件的服務。</p>	否
affectedEntities	<p>描述 AWS Health 事件中受影響資源的資源值和狀態的陣列。</p> <ul style="list-style-type: none"> • entityValue – 資源/實體 ID。 • lastUpdatedtime – 此資源/實體狀態上次更新的時間，格式為 DoW, DD MMM YYYY HH:MM:SS TZ。 • 狀態 – 受影響資源/實體的狀態。支援的值包括 IMPAIRED、UNIMPAIRED、RESOLVED、PENDING 和 UNKNOWN。 	否

'detail' 參數內容	Description	必要
頁面	<p>此訊息代表的頁面。如需詳細資訊，請參閱檢視 EventBridge 上的 AWS Health 事件分頁清單。</p> <div data-bbox="591 447 1029 762" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note</p> <p>分頁只會發生在資源上。如果因為其他原因超過 256KB 大小限制，則通訊會失敗。</p> </div>	是
totalPages	<p>此運作狀態事件的頁面總數。如需詳細資訊，請參閱檢視 EventBridge 上的 AWS Health 事件分頁清單。</p> <p>您可以使用此值來判斷您是否收到帳戶多頁通訊的所有頁面。</p>	是
backupEvent	<p>如果客戶不想利用備援，此旗標會篩選掉分割區中指定備份區域中的備份事件。此值可以是 true 或 false。</p>	是
affectedAccount	<p>受影響帳戶的帳戶 ID。</p> <p>如果此運作狀態事件傳送到屬於的帳戶，AWS Organizations 並在管理帳戶或委派管理員帳戶中收到，則可能與 account 欄位的值不同。</p>	是

'detail' 參數內容	Description	必要
可操作性	中繼資料可啟用哪些事件需要動作的程式設計判斷，無需手動檢查。可能的（單一）值可以是 ACTION_REQUIRED、ACTION_MAY_BE_REQUIRED 或 INFORMATIONAL。	否
角色	此中繼資料清單會啟用將事件路由到哪個利益相關者的程式設計判斷。可能（多個）的值為 OPERATIONAL、SECURITY 和 BILLING。	否

公有運作狀態事件 - 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",
    "backupEvent": "false",
    "affectedAccount": "123456789012",
    "personas": ["OPERATIONS"]
}
}

```

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",
    "backupEvent": "false",
    "affectedAccount": "123456789012",
    "personas": ["OPERATIONS"]
  }
}
```

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

```
{
  "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-east-1::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-east-1",
    "eventDescription": [{
      "language": "en_US",
      "latestDescription": "A description of the event will be provided here"
    }],
    "affectedEntities": [{
      "entityValue": "i-abcd1111"
    }],
    "page": "1",
    "totalPages": "1",
  }
}
```

```

    "backupEvent": "true",
    "affectedAccount": "123456789012",
    "personas": ["OPERATIONS"]
  }
}

```

帳戶特定 AWS Health 事件 - Amazon EC2 執行個體淘汰

```

{
  "version": "0",
  "id": "7bf73129-1428-4cd3-a780-95db273d1602",
  "detail-type": "AWS Health Event",
  "source": "aws.health",
  "account": "123456789012",
  "time": "2026-01-27T01:43:21Z",
  "region": "us-east-1",
  "detail": {
    "eventArn": "arn:aws:health:us-east-1::event/
AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED_90353408594353983",
    "service": "EC2",
    "eventTypeCode": "AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED",
    "eventTypeCategory": "scheduledChange",
    "eventScopeCode": "ACCOUNT_SPECIFIC",
    "communicationId": "1234abc01232a4012345678-1",
    "startTime": "Thu, 27 Aug 2026 13:19:03 GMT",
    "lastUpdatedTime": "Thu, 27 Jan 2026 13:44:13 GMT",
    "statusCode": "open",
    "eventRegion": "us-east-1",
    "eventDescription": [{
      "language": "en_US",
      "latestDescription": "A description of the event will be provided here"
    }],
    "eventMetadata": {
      "keystring1": "valuestring1",
      "keystring2": "valuestring2",
      "keystring3": "valuestring3",
      "keystring4": "valuestring4",
      "truncated": "true"
    },
    "affectedEntities": [{
      "entityValue": "arn:aws:ec2:us-east-1:123456789012:instance/
i-1234567890abcdef0",
      "lastUpdatedTime": "Thu, 26 Jan 2026 19:01:55 GMT",

```

```

        "status": "PENDING"
    }],
    "affectedAccount": "123456789012",
    "page": "1",
    "totalPages": "1",
    "backupEvent": "false",
    "personas": ["OPERATIONS"],
    "actionability": "ACTION_REQUIRED"
}
}

```

帳戶特定 AWS Health 事件 - Lambda 計劃生命週期事件

```

{
  "version": "0",
  "id": "7bf73129-1428-4cd3-a780-95db273d1602",
  "detail-type": "AWS Health Event",
  "source": "aws.health",
  "account": "123456789012",
  "time": "2023-01-27T01:43:21Z",
  "region": "us-west-2",
  "resources": ["arn:lambda-1-101002929", "arn:lambda-1-101002930",
    "arn:lambda-1-101002931", "arn:lambda-1-101002932"],
  "detail": {
    "eventArn": "arn:aws:health:us-west-2::event/
    AWS_LAMBDA_PLANNED_LIFECYCLE_EVENT_90353408594353980",
    "service": "LAMBDA",
    "eventTypeCode": "AWS_LAMBDA_PLANNED_LIFECYCLE_EVENT",
    "eventTypeCategory": "scheduledChange",
    "eventScopeCode": "ACCOUNT_SPECIFIC",
    "communicationId": "1234abc01232a4012345678-1",
    "startTime": "Thu, 27 Aug 2026 13:19:03 GMT",
    "lastUpdatedTime": "Thu, 27 Jan 2026 13:44:13 GMT",
    "statusCode": "open",
    "eventRegion": "us-west-2",
    "eventDescription": [{
      "language": "en_US",
      "latestDescription": "A description of the event will be provided here"
    }],
    "eventMetadata": {
      "keystring1": "valuestring1",
      "keystring2": "valuestring2",
      "keystring3": "valuestring3",
    }
  }
}

```

```
    "keystring4": "valuestring4",
    "truncated": "true"
  },
  "affectedEntities": [{
    "entityValue": "arn:lambda-1-101002929",
    "lastUpdatedTime": "Thu, 26 Jan 2026 19:01:55 GMT",
    "status": "PENDING"
  }, {
    "entityValue": "arn:lambda-1-101002930",
    "lastUpdatedTime": "Thu, 26 Jan 2026 19:05:12 GMT",
    "status": "PENDING"
  }, {
    "entityValue": "arn:lambda-1-101002931",
    "lastUpdatedTime": "Thu, 26 Jan 2026 19:07:13 GMT",
    "status": "PENDING"
  }, {
    "entityValue": "arn:lambda-1-101002932",
    "lastUpdatedTime": "Thu, 26 Jan 2026 19:10:59 GMT",
    "status": "RESOLVED"
  }],
  "affectedAccount": "123456789012",
  "page": "1",
  "totalPages": "10",
  "backupEvent": "false",
  "personas": ["OPERATIONS"],
  "actionability": "ACTION_REQUIRED"
}
}
```

監控 AWS Health

監控是維護 AWS Health 及其他 AWS 解決方案的可靠性、可用性和效能的重要部分。AWS 提供下列監控工具，讓您監看 AWS Health、回報錯誤，並適時採取動作：

- Amazon CloudWatch AWS 會即時監控您的 AWS 資源和您在 上執行的應用程式。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 EventBridge，以便收到可能影響服務和資源 AWS Health 的事件通知。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動作，並視需要更新或取代資源。如需詳細資訊，請參閱 [AWS Health 使用 Amazon EventBridge 監控 中的事件](#)。

- AWS CloudTrail 會擷取由您的帳戶 AWS 或代表您的帳戶發出的 API 呼叫和相關事件，並將日誌檔案交付至您指定的 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 地址，以及呼叫的時間。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](#)

使用 記錄 AWS Health API 呼叫 AWS CloudTrail

AWS Health 已與 服務整合 AWS CloudTrail，此服務可提供使用者、角色或 AWS 服務在其中採取之動作的記錄 AWS Health。CloudTrail 會擷取 AWS Health 的 API 呼叫當作事件。擷取的呼叫包括來自 AWS Health 主控台的呼叫，以及對 AWS Health API 操作的程式碼呼叫。如果您建立線索，您可以將 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 的事件 AWS Health。即使您未設定追蹤，依然可以透過 CloudTrail 主控台 中的事件歷史記錄檢視最新事件。您可以使用 CloudTrail 所收集的資訊來判斷提出的請求 AWS Health、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，包括如何設定及啟用，請參閱 [《AWS CloudTrail 使用者指南》](#)。

AWS Health CloudTrail 中的資訊

當您建立 AWS 帳戶時，會在您的帳戶上啟用 CloudTrail。在 中發生支援的事件活動時 AWS Health，該活動會與事件歷史記錄中的其他 AWS 服務事件一起記錄在 CloudTrail 事件中。您可以在 AWS 帳

戶中檢視、搜尋和下載最近的事件。如需詳細資訊，請參閱《使用 CloudTrail 事件歷史記錄檢視事件》<https://docs.aws.amazon.com/awsccloudtrail/latest/userguide/view-cloudtrail-events.html>。

若要持續記錄您 AWS 帳戶中的事件，包括的事件 AWS Health，請建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。根據預設，當您在主控台中建立線索時，線索會套用至所有 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，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- [建立追蹤的概觀](#)
- [CloudTrail 支援的服務和整合](#)
- [設定 CloudTrail 的 Amazon SNS 通知](#)
- [從多個區域接收 CloudTrail 日誌檔案](#)，以及[從多個帳戶接收 CloudTrail 日誌檔案](#)

CloudTrail 會記錄所有 AWS Health API 操作，並記錄在 [AWS Health API 參考](#)中。例如，對 DescribeEvents、DescribeEventDetails 和 DescribeAffectedEntities 操作的呼叫都會在 CloudTrail 日誌檔案中產生項目。

AWS Health 支援將下列動作記錄為 CloudTrail 日誌檔案中的事件：

- 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 userIdentity 元素](#)。

您可以視需要將日誌檔案存放在 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。

若要在日誌檔案交付時收到通知，您可以設定 CloudTrail 在新日誌檔案交付時發佈 Amazon SNS 通知。如需詳細資訊，請參閱 [CloudTrail 設定 Amazon SNS 通知](#)。

您也可以將多個 AWS 區域和多個 AWS 帳戶的 AWS Health 日誌檔案彙整至單一 Amazon S3 儲存貯體。

如需詳細資訊，請參閱[從多個區域接收 CloudTrail 日誌檔案](#)和[從多個帳戶接收 CloudTrail 日誌檔案](#)。

範例：AWS Health 日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

下列範例顯示示範 [DescribeEntityAggregates](#) 操作的 CloudTrail 日誌項目。

```
{
  "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-8515-73e8abcbcb29b",
    "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
已更新設定 EventBridge 規則以傳送 中事件的通知 AWS Health	連結至一般規則建立步驟的 Amazon EventBridge 使用者指南，簡化建立 EventBridge 規則的程序。主題現在著重於 AWS Health 特定的篩選和使用案例。如需詳細資訊，請參閱 設定 EventBridge 規則以傳送 中事件的通知 AWS Health 。	2026 年 3 月 13 日
更新 AWS Health 事件 Amazon EventBridge 結構描述 範例	更新結構描述範例，以包含角色和可操作性欄位。範例包括 Amazon EC2 操作問題的公有運作狀態事件、Elastic Load Balancing API 問題和 Amazon EC2 執行個體存放區磁碟機效能降級備份事件的帳戶特定事件，以及 Lambda 計劃生命週期事件。如需詳細資訊，請參閱 參考：AWS Health 事件 Amazon EventBridge 結構描述 。	2026 年 3 月 13 日
在 中更新管理 AWS Health 通知 AWS 使用者通知	更新本節的資訊，以反映 AWS Health 事件遷移至。AWS 使用者通知如需詳細資訊，請參	2025 年 12 月 22 日

	閱管理中的 AWS Health 通知 AWS 使用者通知。	
已更新的監控帳戶特定和公有事件 AWS Health	新增本節的詳細資訊，詳細說明公有事件和帳戶特定事件的備份規則行為。如需詳細資訊，請參閱 AWS Health 事件的備份規則 。	2025 年 12 月 11 日
新增運作狀態事件的動作能力和角色欄位的相關資訊	已新增 概念 AWS Health 章節 中可操作性和人物角色欄位的資訊，以及參考： AWS Health 事件結構描述 章節中 'details' 參數的 Amazon EventBridge 結構描述內容。如需詳細資訊，請參閱 和 Reference : events 結構描述的概念 AWS Health 。 AWS HealthAmazon EventBridge	2025 年 11 月 20 日
更新章節：建立涵蓋 AWS 區域範圍的 EventBridge 規則	更新資訊以建立 EventBridge 規則。如需詳細資訊，請參閱 建立涵蓋 AWS 區域範圍的 EventBridge 規則 。	2025 年 11 月 3 日
更新章節：在中管理 AWS Health 通知 AWS 使用者通知	更新設定 AWS Health 事件 AWS 受管通知訂閱的步驟資訊。如需詳細資訊，請參閱 管理中的 AWS Health 通知 AWS 使用者通知 。	2025 年 9 月 16 日
更新章節：AWS Health 使用 Amazon EventBridge 監控中的事件	更新中的資訊，以將事件 AWS Health 交付至 EventBridge。如需詳細資訊，請參閱 AWS Health 使用 Amazon EventBridge 在中監控事件 。	2025 年 9 月 15 日

更新章節：AWS Health 儀表板	移除訂閱運作狀態事件 RSS 摘要的選用步驟。新增注意事項，若要接收運作狀態事件的通知，客戶可以使用 EventBridge。如需詳細資訊，請參閱 AWS Health 儀表板 。	2025 年 8 月 15 日
更新章節：AWS Health 使用 Amazon EventBridge 監控中的事件	移除主題，安裝服務連結角色以使用 AWS Health Amazon EventBridge 在中監控事件時使用 AWS 事件偵測和回應	2025 年 8 月 8 日
更新章節：AWS Health 使用 Amazon EventBridge 監控中的事件	已將資訊新增至備註區段，指出在您開始接收公有運作狀態事件的通知之前，可能會有長達一小時的延遲。如需詳細資訊，請參閱 AWS Health 使用 Amazon EventBridge 在中監控事件	2025 年 7 月 22 日
更新章節：啟用組織檢視	新增資訊至備註區段，指出當您啟用組織檢視時，AWS Health 會自動彙總整個組織的所有歷史運作狀態事件。歷史事件最多可能需要 24 小時才會出現在您的組織檢視中。如需詳細資訊，請參閱 啟用組織檢視	2025 年 6 月 27 日
更新章節：跨帳戶彙總 AWS Health 事件	移除的備註 AWS Health 不會顯示在您啟用組織檢視之前發生的事件。如需詳細資訊，請參閱 跨帳戶彙總 AWS Health 事件	2025 年 6 月 27 日

WorkDocs 已棄用	已移除 已規劃生命週期事件 AWS Health 中已棄用 WorkDocs 的參考。	2025 年 6 月 19 日
新增 AWS 受管通知遷移時間軸的注意事項	已新增有關電子郵件遷移至中 AWS 受管通知之金鑰日期的備註 AWS 使用者通知。如需詳細資訊，請參閱 管理中的 AWS Health 通知 AWS 使用者通知 。	2025 年 4 月 28 日
更新計劃的生命週期事件	更新計劃的生命週期事件，指出 AWS Health 事件會保持開啟 4 年，而不是未解決資源的 90 天。如需詳細資訊，請參閱規劃生命週期事件中收到規劃的生命週期事件通知時應預期什麼？一節。 AWS Health	2025 年 4 月 18 日
更新已規劃生命週期事件之受影響資源清單的描述	計劃生命週期事件受影響的資源清單通常每 24 小時重新整理一次，但最多可能需要 72 小時才能反映目前的資源狀態。如需詳細資訊，請參閱 AWS Health 儀表板中檢視帳戶事件的事件詳細資訊 一節。	2025 年 4 月 7 日
新增在中管理 AWS Health 通知的常見問答集 AWS 使用者通知	如需詳細資訊，請參閱在 AWS 使用者通知 常見問答集中管理通知 。	2025 年 2 月 18 日
已新增端點IPv6-only 請求的相關資訊。	如需詳細資訊，請參閱 選擇 AWS Health API 請求的端點 。	2025 年 1 月 28 日
在中管理 AWS Health 通知 AWS 使用者通知	如需詳細資訊，請參閱 管理中的通知 AWS 使用者通知 。	2025 年 1 月 16 日

已更正使用 Amazon EventBridge 監控 AWS Health 事件中的 JSON	如需詳細資訊，請參閱 使用 Amazon EventBridge 監控 AWS Health 事件 。	2024 年 9 月 3 日
更新了有關下載受影響資源的資訊	如需詳細資訊，請參閱 受影響的資源檢視 。	2024 年 7 月 27 日
從安全區段 AWS Health 文件中移除網際網路流量隱私權	如需詳細資訊，請參閱 中的安全性 AWS Health 。	2024 年 3 月 27 日
已更新 AWS Health 儀表板 – AWS Health 文件的服務運作狀態和規劃生命週期事件。	如需詳細資訊，請參閱 AWS Health 儀表板 – 服務運作狀態和的計劃生命週期事件 AWS Health 。	2024 年 2 月 15 日
移除建立的 EventBridge 規則中的重複項目符號點 AWS Health	移除 建立 EventBridge 規則 AWS Health 中的重複項目符號點。	2023 年 12 月 4 日
新增計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	您現在可以在 中使用 AWSHealthFullAccess 受管政策 AWS GovCloud (US) Regions。請參閱 AWS 的受管政策 AWS Health 。	2023 年 10 月 16 日
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 AWS 的使用者通知 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

SLR 政策更新	AWS 受管政策的更新：Health_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 結構描述現在支援事件中繼資料	您現在可以從事件接收 AWS Health 事件中繼資料。如需詳細資訊，請參閱 使用 Amazon EventBridge 管理 AWS Health 事件 。	2023 年 6 月 20 日
已更新 Amazon EventBridge 的文件	您現在可以使用 Amazon EventBridge 規則來監控帳戶特定和公有事件。如需詳細資訊，請參閱 使用 Amazon EventBridge 管理 AWS Health 事件 。	2023 年 5 月 2 日
新增 AWS 受管政策的文件	新增和 使用服務連結角色 AWS Health 的受管政策 AWS Health 文件。	2023 年 1 月 18 日
新增時區設定文件	使用新的時區功能，在本機時區或 UTC 中檢視 AWS Health 儀表板。如需詳細資訊，請參閱 AWS Health 儀表板入門 – 您的帳戶運作狀態和 AWS Health 儀表板 – 服務運作狀態 。	2022 年 9 月 21 日
已更新的文件	新增 AWS Health Aware 的文件。如需詳細資訊，請參閱 AWS Health 感知 。	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 Dashboard。 如需詳細資訊，請參閱 儀表板入門 AWS Health – 您的帳戶運作狀態 和 AWS Health 儀表板 – 服務運作狀態 。	2022 年 2 月 28 日
已更新 Amazon EventBridge 的文件	AWS Health 使用 Amazon EventBridge 監控運作狀態事件的新主題。如需詳細資訊，請參閱 使用 Amazon EventBridge 管理 AWS Health 事件 。	2022 年 2 月 3 日
已更新的文件	如果您有 Enterprise On-Ramp Support 計劃，您可以使用 AWS Health API。	2021 年 11 月 24 日
新增的文件	AWS Health 概念的新主題。如需詳細資訊，請參閱 的概念 AWS Health 。	2021 年 7 月 29 日
更新 CloudWatch Events 的文件	新增了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
更新 CloudWatch Events 的文件	更新章節以自動化 Amazon CloudWatch Events 規則 AWS Systems Manager 的動作。如需詳細資訊，請參閱 自動化 Amazon EC2 執行個體的動作 。	2021 年 4 月 28 日

更新 CloudWatch Events 的文件	新增章節以接收聊天用戶端中的 AWS Health 事件。如需詳細資訊，請參閱 聊天應用程式中使用 Amazon Q Developer 接收 AWS Health 事件 。	2021 年 3 月 16 日
已更新的文件	下列主題更新： <ul style="list-style-type: none"> 更新彙總 AWS Health 事件主題 重組和更新使用 Amazon CloudWatch Events AWS Health 監控事件主題 更新資源型和動作型條件區段 	2021 年 1 月 29 日
在 AWS Health 主控台中新增組織檢視的 AWS Health 儀表板	您可以使用 AWS Health 主控台來啟用組織檢視功能。然後，您可以檢視組織中 AWS 成員帳戶的運作狀態事件。	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作用中的區域端點和簽署 AWS 區域 AWS Health。	2020 年 10 月 22 日
AWS Health 使用者指南的更新	組織更新並新增 RSS 摘要，讓您可以訂閱 AWS Health 文件的最新更新。	2020 年 8 月 28 日

舊版更新

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

變更	描述	Date
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 。	2020 年 5 月 5 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 跨帳戶彙總 AWS Health 事件 。	2019 年 12 月 18 日
新增了「資源和動作型條件」一節，以說明 AWS Health API 提供的事件限制。	請參閱 的身分和存取管理 AWS Health 。	2018 年 8 月 2 日
新增有關 AWS Health 資訊可見性的備註。	請參閱 的身分和存取管理 AWS Health 。	2017 年 8 月 16 日
服務版本。	AWS Health 已發佈。	2016 年 12 月 1 日

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。