使用者指南

AWS 韌性樞紐

AWS 韌性樞紐: 使用者指南

Table of Contents

什麼是 AWS Resilience Hub？

AWS Resilience Hub 是您管理和改善應用程式彈性姿勢的中心位置 AWS。 AWS Resilience Hub 使您能夠定義彈性目標，根據這些目標評估彈性姿勢，並根據 AWS Well-Architected 的框架實施改進建議。在中 AWS Resilience Hub，您也可以建立和執行 Amazon Fault Input Service 實驗，模擬應用程式的實際中斷情況，以協助您更好地瞭解相依性並發現潛在弱點。 AWS Resilience Hub 提供一個集中的地方，提供您需要的所有 AWS 服務和工具，以持續強化您的彈性姿勢。 AWS Resilience Hub 與其他服務搭配使用，以提供建議並協助您管理應用程式資源。如需詳細資訊，請參閱 使用其他 服務。

下表提供所有相關復原服務的文件連結。

相關 AWS 恢復服務和參考

AWS 彈性服務	文件連結
AWS Elastic Disaster Recovery	什麼是彈性災難復原
AWS Backup	什麼是 AWS Backup
Amazon Route 53 應用程序恢復控制器（路線 53 ARC）	什麼是 Amazon 路線 53 應用恢復控制器

主題

- AWS Resilience Hub — 復原力管理
- AWS Resilience Hub — 彈性測試
- AWS Resilience Hub 概念
- AWS Resilience Hub 支援的資源

AWS Resilience Hub — 復原力管理

AWS Resilience Hub 為您提供一個集中的位置來定義、驗證和追蹤 AWS 應用程式的恢復能力。 AWS Resilience Hub 協助您保護應用程式免受中斷的影響，並降低回復成本，以最佳化業務連續性，以協助符合法規遵循與法規要求。您可以使用 AWS Resilience Hub 來執行下列動作：

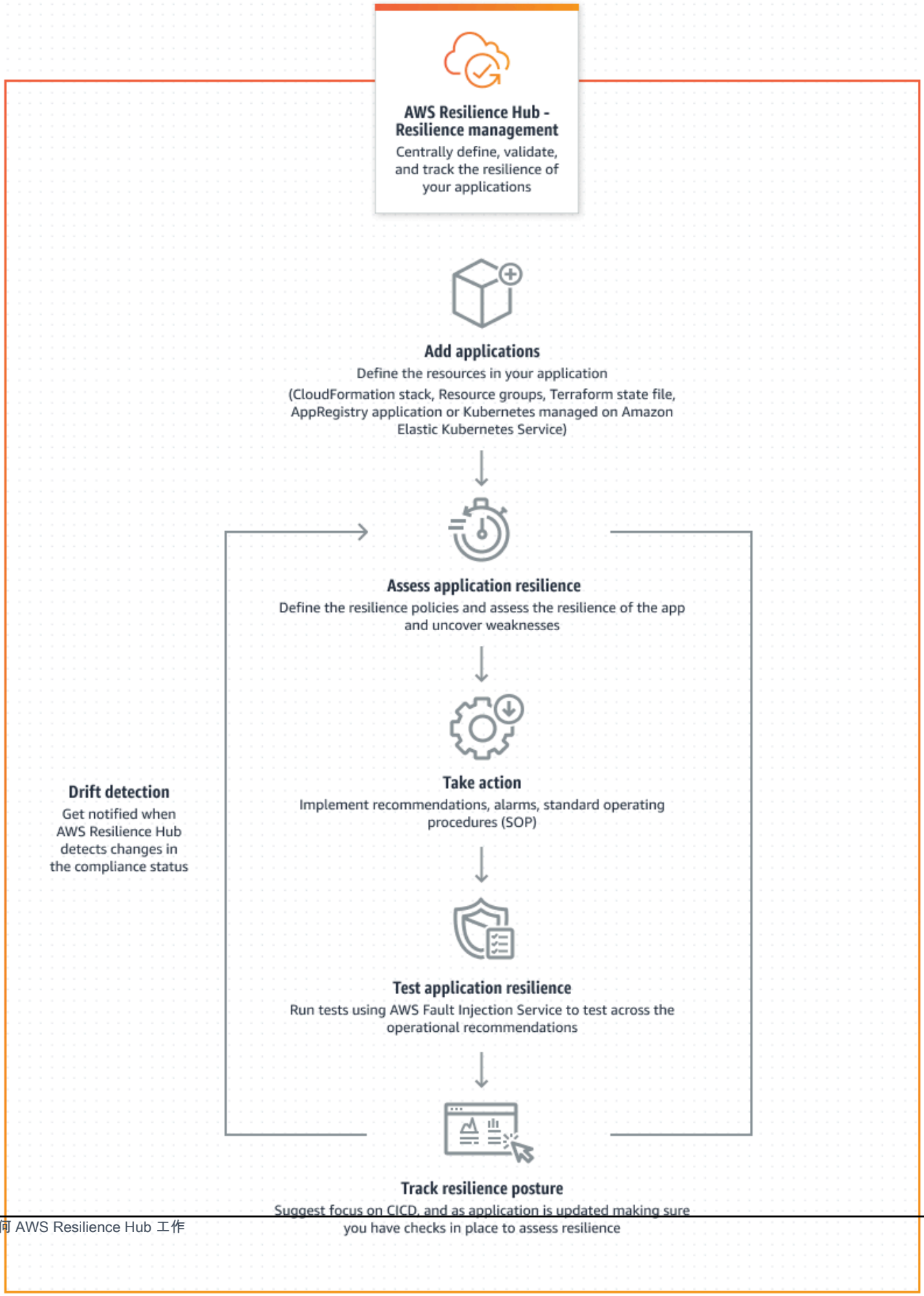
- 分析您的基礎架構並取得改善應用程式復原能力的建議。除了改善應用程式恢復能力的架構指導之外，這些建議還提供符合恢復原則、實作測試、警示和標準作業程序 (SOP) 的程式碼，您可以在整合和交付 (CI/CD) 管道中部署和執行應用程式。

- 評估不同條件下的復原時間目標 (RTO) 和復原點目標 (RPO) 目標。
- 優化業務連續性，同時降低回復成本。
- 在生產環境中發生之前找出問題並加以解決。

將應用程式部署到生產環境之後，您可以新增 AWS Resilience Hub 至 CI/CD 管線，以便在發行到生產環境之前驗證每個組建。

如何 AWS Resilience Hub 工作

下圖提供了如何 AWS Resilience Hub 工作的高層次概述。


AWS Resilience Hub - Resilience management
Centrally define, validate, and track the resilience of your applications
Add applications
Define the resources in your application
(CloudFormation stack, Resource groups, Terraform state file, AppRegistry application or Kubernetes managed on Amazon Elastic Kubernetes Service)
Assess application resilience
Define the resilience policies and assess the resilience of the app and uncover weaknesses
Take action
Implement recommendations, alarms, standard operating procedures (SOP)
Test application resilience
Run tests using AWS Fault Injection Service to test across the operational recommendations
Track resilience posture
Suggest focus on CICD, and as application is updated making sure you have checks in place to assess resilience
Drift detection
Get notified when AWS Resilience Hub detects changes in the compliance status

描述

透過從 AWS CloudFormation 堆疊、Terraform 狀態檔案、Amazon Elastic Kubernetes Service 叢集匯入資源來描述您的應用程式，或者您也可以從中已定義的應用程式中進行選擇。 AWS Resource Groups AWS Service Catalog AppRegistry

定義

定義應用程式的復原原則。這些原則包括適用於應用程式、基礎結構、可用區域和區域中斷的 RTO 和 RPO 目標。這些目標是用來估計應用程式是否符合復原原則。

評估

在您描述應用程式並將復原原則附加至應用程式之後，請執行復原評估。 AWS Resilience Hub 評估使用 AWS Well-Architected Framework 的最佳做法來分析應用程式的元件，並發現潛在的彈性弱點。這些弱點可能是由於基礎結構設定不完整、組態錯誤或需要其他組態改善的情況所導致。若要改善恢復能力，請根據評估報告的建議更新您的應用程式和復原政策。建議包括組件，警報，測試和恢復 SOP 的配置。然後，您可以執行另一個評估，並將結果與先前的報告進行比較，以查看有多少彈性提升。重申此程序，直到您估計的工作負載 RTO 和估計的工作負載 RPO 符合 RTO 和 RPO 目標為止。

驗證

執行測試以測量 AWS 資源的彈性，以及從應用程式、基礎結構、可用區域和 AWS 區域 事件復原所需的時間。為了測量彈性，這些測試會模擬資源中斷。 AWS 中斷的範例包括網路無法使用的錯誤、容錯移轉、已停止的程序、Amazon RDS 開機復原，以及可用區域的問題。

檢視和追蹤

將 AWS 應用程式部署到生產環境之後，您可以使用 AWS Resilience Hub 繼續追蹤應用程式的復原狀態。如果發生中斷，操作員可以檢視中斷， AWS Resilience Hub 並啟動相關的復原程序。

AWS Resilience Hub — 彈性測試

AWS Resilience Hub 可讓您對 AWS 工作負載執行 Amazon 故障注入服務 (AWS FIS) 測試和實驗，並維持最佳彈性。這些 stress 試透過建立破壞性事件來強調應用程式，以便觀察應用程式的回應方式。AWS FIS 提供多種預先建置的案例，以及可產生中斷的大量動作選擇。此外，它還包括您需要在生產中運行實驗的控件和護欄。控制項和護欄包括在滿足特定條件時執行自動倒回或停止實驗的選項。若要開始使用從AWS Resilience Hub 主控台執行實驗， AWS FIS 請完成the section called “必要條件”區段中定義的必要條件。

下表列出瀏覽窗格中的所有可用 AWS FIS 選項，以及相關 AWS FIS 文件的連結，其中包含從 AWS Resilience Hub 主控台開始使用 AWS FIS 測試的程序。

AWS FIS 導覽功能表選項和參考

AWS FIS 導航菜單選項	AWS FIS 文件
彈性測試	建立實驗範本
情境庫	AWS FIS 圖書館
实验模板	用於的實驗模板 AWS FIS

下表列出了「彈性測試」區段中下拉式功能表中的所有可用 AWS FIS 選項，以及相關 AWS FIS 文件的連結，其中包含從 AWS Resilience Hub 主控台開始使用 AWS FIS 測試的程序。

AWS FIS 下拉菜單選項和參考

AWS FIS 下拉菜單選項	AWS FIS 文件
建立實驗範本	建立實驗範本
從場景創建實驗	使用案例

AWS Resilience Hub 概念

這些概念可協助您進一步瞭解協助改善應用程式復原能力並防止應用程式中斷 AWS Resilience Hub的方法。

彈性

能夠在指定的時間範圍內維持可用性並從軟件和操作中斷中恢復。

復原點目標 (RPO)

自上次資料復原點以來可接受的時間上限。這決定了最後一個恢復點和服務中斷之間可接受的數據丟失。

復原時間目標 (RTO)

服務中斷與恢復服務之間的最大可接受延遲。這決定了當服務無法使用時，什麼被視為可接受的時間範圍。

預估的工作負載回復時間

預估的工作負載復原時間目標 (預估的工作負載 RTO) 是根據匯入的應用程式定義預估應用程式要符合的 RTO，然後執行評估。

預估工作負載復原點目標

預估的工作負載復原點目標 (預估的工作負載 RPO) 是根據匯入的應用程式定義預估應用程式要符合的 RPO，然後執行評估。

應用程式

AWS Resilience Hub 應用程式是受 AWS 支援的資源集合，這些資源會持續受到監控和評估，以管理其復原狀態。

應用組件

作為一個單元工作和失敗的一組相關 AWS 資源。例如，如果您有主要資料庫和複本資料庫，則這兩個資料庫都屬於相同的應用程式元件 (AppComponent)。

AWS Resilience Hub 決定哪些 AWS 資源可以屬於哪種類型的 AppComponent。例如，一個`DBInstance`可以屬於`AWS::ResilienceHub::DatabaseAppComponent`但不屬於`AWS::ResilienceHub::ComputeAppComponent`。

應用程式符合性

AWS Resilience Hub 報告您應用程式的下列合規狀態類型。

符合政策

估計應用程式符合其 RTO 和 RPO 目標，在原則中定義。其所有元件都符合定義的政策目標。例如，您選取的 RTO 和 RPO 目標為 24 小時，用於跨區域的中斷。 AWS AWS Resilience Hub 可以看到您的備份已複製到後備區域。您仍然需要從備份標準作業程序 (SOP) 維持復原，並進行測試和計時。這是操作建議和整體彈性得分的一部分。

違反政策

無法估計應用程式符合原則中定義的 RTO 和 RPO 目標。其中一個或多個 AppComponents 不符合政策目標。例如，您選取的 RTO 和 RPO 目標為 24 小時，跨區 AWS 域中斷，但您的資料庫組態不包括任何跨區域復原方法，例如全域複寫和備份副本。

未評估

該應用程序需要進行評估。目前尚未評估或追蹤。

偵測到變更

有一個新的發布版本的應用程序尚未進行評估。

彈性漂移

AWS Resilience Hub 執行漂移偵測，同時為您的應用程式執行評估，以檢查其是否符合其復原原則。為了進行比較，請 AWS Resilience Hub 使用先前成功評估應用程式中定義的恢復原則。

- Drided — 表示應用程式已違反其復原原則，且處於風險之中。
- 未漂移 — 表示應用程式的符合性並未從先前的評估變更。

彈性評估

AWS Resilience Hub 使用缺口和潛在補救措施的清單來衡量所選策略的有效性，以便從災難中恢復和繼續。它會使用原則評估每個應用程式元件或應用程式符合性狀態。此報告包含成本最佳化建議，以及潛在問題的參考資料。

彈性分數

AWS Resilience Hub 會產生分數，指出您的應用程式遵循我們的建議，以符合應用程式的彈性原則、警示、標準作業程序 (SOP) 和測試的程度。

中斷類型

AWS Resilience Hub 協助您針對下列類型的中斷評估彈性：

Application (應用程式)

基礎結構健康，但應用程式或軟體堆疊無法視需要運作。這可能會在部署新程式碼、組態變更、資料損毀或下游相依性故障之後發生。

雲基礎架構

由於中斷，雲端基礎架構未如預期般運作。由於一個或多個元件的本機錯誤，可能會發生中斷。在大多數情況下，這種類型的中斷可以通過重新啟動，回收或重新加載故障組件來解決。

雲端基礎架構 AZ 中斷

一或多個可用區域無法使用。此類型的中斷可透過切換至不同的可用區域來解決。

雲基礎設施區域事件

一個或多個區域無法使用。這種類型的事件可以通過切換到不同的來解決 AWS 區域。

故障注入實驗

AWS Resilience Hub 建議測試，以驗證應用程式恢復能力，以防止不同類型的中斷。這些中斷包括應用程式、基礎架構、可用區域 (AZ) 或應用程式元件的 AWS 區域 事件。

這些實驗可讓您執行以下操作：

- 注入失敗。
- 確認警示可以偵測中斷。
- 確認復原程序或標準作業程序 (SOP) 正常運作，以便從中斷復原應用程式。

SOP 測試可測量估計的工作量 RTO 和估計的工作負載 RPO。您可以測試不同的應用程式組態，並測量輸出 RTO 和 RPO 是否符合原則中定義的目標。

SOP

標準作業程序 (SOP) 是一組規定性的步驟，旨在在發生中斷或警示時有效地復原應用程式。根據應用程式評估， AWS Resilience Hub 建議一組 SOP，並建議在中斷之前準備、測試和測量 SOP，以確保及時復原。

AWS Resilience Hub 支援的資源

在中斷情況下影響應用程式效能的資源，可由 AWS Resilience Hub 頂層資源 (例如`AWS::RDS::DBInstance`和) 完整支援`AWS::RDS::DBCluster`。

若要進一步瞭解在評估中包含所有支援服務的資源所需的權限，請參閱the section called “AWSResilienceHubAsssessmentExecutionPolicy”。 AWS Resilience Hub

AWS Resilience Hub 支援來自下列 AWS 服務的資源：

- 運算
  - Amazon Elastic Compute Cloud (Amazon EC2)
  - AWS Lambda
  - Amazon Elastic Kubernetes Service (Amazon EKS)
  - Amazon Elastic Container Service (Amazon ECS)
  - AWS Step Functions
- 資料庫
  - Amazon Relational Database Service (Amazon RDS)
  - Amazon DynamoDB
  - Amazon DocumentDB
- 聯網與內容交付
  - Amazon Route 53
  - Elastic Load Balancing
  - 網路位址轉譯
- 儲存
  - Amazon Elastic Block Store (Amazon EBS)
  - Amazon Elastic File System (Amazon EFS)
  - Amazon Simple Storage Service (Amazon S3)
  - Amazon FSx for Windows File Server
- 其他
  - Amazon API Gateway
  - Amazon 路線 53 應用程序恢復控制器（Amazon Route 53 ARC）
  - Amazon Simple Notification Service
  - Amazon Simple Queue Service
  - AWS Auto Scaling
  - AWS Backup
  - AWS 彈性災難復原

Note

- AWS Resilience Hub 允許您檢視每個資源的支援執行個體，為您的應用程式資源提供額外的透明度。此外， AWS Resilience Hub 透過識別每個資源的唯一執行個體，同時在評估程序期間探索資源執行個體，以提供更準確的復原建議。如需將資源執行個體新增至應用程式的詳細資訊，請參閱編輯AWS Resilience Hub應用資源。
- AWS Resilience Hub 支持 Amazon EKS 和 Amazon ECS 上。 AWS Fargate
- AWS Resilience Hub 作為以下服務的一部分，支持 AWS Backup 資源評估：
  - Amazon EBS
  - Amazon EFS
  - Amazon S3
  - Amazon Aurora 全球數據
  - Amazon DynamoDB
  - Amazon RDS 服務
  - Amazon FSx for Windows File Server
- Amazon Route 53 ARC 僅 AWS Resilience Hub 評估 Amazon DynamoDB 全球、Elastic Load Balancing、Amazon RDS 和群組。 AWS Auto Scaling
- 若 AWS Resilience Hub 要評估跨區域資源，請將資源分組在單一應用程式元件下。如需每個「 AWS Resilience Hub 應用程式元件」所支援之資源與分組資源的詳細資訊，請參閱對資源進行分組 AppComponent。
- 目前， AWS Resilience Hub 如果 Amazon EKS 叢集位於 Amazon EKS 叢集，或是在啟用選擇加入的區域中建立應用程式，則目前不支援 Amazon EKS 叢集的跨區域評估。 AWS
- 目前，只會 AWS Resilience Hub 評估下列 Kubernetes 資源類型：
  - 部署
  - ReplicaSets
  - 豆莢

AWS Resilience Hub 會忽略下列類型的資源：

- 不影響預估工作負載 RTO 或預估工作負載 RPO 的資源 — 會忽略不影響預估工作負載 RTO 或預估工作負載 RPO 等資源。`AWS::RDS::DBParameterGroup` AWS Resilience Hub

- 非頂層資源 — AWS Resilience Hub 僅匯入頂層資源，因為它們可以透過查詢頂層資源的屬性來衍生其他屬性。例如，`AWS::ApiGateway::RestApi`並且`AWS::ApiGatewayV2::Api`是 Amazon API Gateway 支持的資源。但`AWS::ApiGatewayV2::Stage`是，不是頂級資源。因此，它不會由匯入 AWS Resilience Hub。

> **Note**
>
> 不支援資源
>
> - 您無法使用 AWS Resource Groups (Amazon 路線 53 RecordSets 和 API-GW HTTP) 和 Amazon Aurora 全球資源來識別多個資源。如果您想要將這些資源作為評估的一部分進行分析，則必須手動將資源新增至應用程式。但是，當您新增 Amazon Aurora 全球資源進行評估時，必須將其與 Amazon RDS 執行個體的應用程式元件分組。如需編輯資源的詳細資訊，請參閱the section called “編輯應用資源”。
> - 這些資源可能會影響應用程式復原，但目 AWS Resilience Hub 前並未完全支援這些資源。AWS Resilience Hub 如果應用程式受到 AWS CloudFormation 堆疊、Terraform 狀態檔案或 AppRegistry 應用程式的支援，會努力警告使用者有關不受支援的資源。 AWS Resource Groups

開始使用

本節介紹如何開始使用AWS Resilience Hub。這包括為帳戶建立 AWS Identity and Access Management (IAM) 許可。

必要條件

您必須先完成下列先決條件AWS Resilience Hub，才能使用：

- AWS帳號 — 為您要在其中使用的每個AWS帳號類型 (主要帳號/次要帳號/資源帳號) 建立一或多個帳號。AWS Resilience Hub如需建立和管理AWS帳戶的詳細資訊，請參閱下列內容：
  - 第一次AWS使用者 — 開始使用：您是第一次AWS使用嗎？
  - 管理AWS帳戶 — https://docs.aws.amazon.com/accounts/latest/reference/managing-accounts.html
- AWS Identity and Access Management(IAM) 許可 — 建立AWS帳戶後，您必須為所建立的每個帳戶配置必要的角色和 IAM 許可。例如，如果您已建立AWS帳戶來存取應用程式資源，則必須設定新角色並設定必要的 IAM 許可，AWS Resilience Hub才能從您的帳戶存取應用程式資源。若要進一步了解 IAM 許可，請參閱the section called “AWS 彈性中樞如何與 IAM 搭配運作”和如需將政策新增至角色的詳細資訊，請參閱the section called “使用 JSON 檔案定義信任原則”。

  若要快速開始向使用者、群組和角色新增 IAM 許可，您可以使用我們的AWS受管政策 (the section called “AWS 受管理政策”)。使用AWS受管政策來涵蓋您可用的常見使用案例，AWS 帳戶而不是自行編寫策略更容易。 AWS Resilience Hub將其他權限新增至受AWS管理的原則，以便將支援延伸至其他AWS服務並包含新功能。因此：
  - 如果您是現有客戶，而且希望應用程式在評估中使用最新的增強功能，則必須發佈新版本的應用程式，然後執行新的評估。如需詳細資訊，請參閱下列主題：
    - the section called “發佈新的應用程式版本”
    - the section called “執行復原能力評估”
  - 如果您未使用AWS受管政策將適當的 IAM 許可指派給使用者、群組和角色，則必須手動設定這些許可。如需 AWS 受管政策的詳細資訊，請參閱 the section called “AWSResilienceHubAsssessmentExecutionPolicy”。

將應用程式新增至 AWS Resilience Hub

AWS Resilience Hub 提供彈性評估和驗證，整合到您的軟體開發生命週期中。 AWS Resilience Hub 協助您主動準備和保護您的 AWS 應用程式免於中斷：

- 揭露彈性弱點。
- 估計是否可以達到目標復原時間目標 (RTO) 和復原點目標 (RPO)。
- 在問題發佈到生產環境之前先解決問題。

本節將引導您新增應用程式。您可以從現有的應用程式、 AWS CloudFormation 堆疊收集資源 AWS Resource Groups AppRegistry ，或建立適當的恢復原則。描述應用程式之後，您可以將其發佈到中 AWS Resilience Hub，並產生應用程式復原能力的評估報告。然後，您可以使用評估中的建議來改善彈性。您可以執行另一個評估、比較結果，然後重複執行，直到估計的工作負載 RTO 和估計的工作負載 RPO 達到您的 RTO 和 RPO 目標為止。

主題

步驟 1：透過新增應用程式開始使用

從描述 AWS 應用程式的詳細資料開始，並執行報告以評估復原能力。 AWS Resilience Hub

若要開始使用，請在 [開始使用] 下的 AWS Resilience Hub 首頁上，選擇 [新增應用程式]。

要進一步了解相關的成本和帳單 AWS Resilience Hub，請參閱AWS Resilience Hub 定價。

在中描述您的應用程序的詳細信息 AWS Resilience Hub

本節說明如何在中描述現有 AWS 應用程式的詳細資訊 AWS Resilience Hub。

描述您的應用程序的詳細信息

1. 輸入應用程式的名稱。
2. (選擇性) 輸入應用程式的說明。

下一頁

步驟 2：如何管理您的應用程式？

步驟 2：如何管理您的應用程式？

除了 AWS CloudFormation 堆疊 AWS Resource Groups、 AppRegistry 應用程式和 Terraform 狀態檔案之外，您還可以新增位於 Amazon Elastic Kubernetes Service (Amazon EKS) 叢集上的資源。也就是說，AWS 復原中樞可讓您將位於 Amazon EKS 叢集上的資源新增為選用資源。本節提供下列選項，可協助您判斷應用程式資源的位置。

- 資源集合 — 如果您想要從其中一個資源集合中探索資源，請選取此選項。資源集合包括 AWS CloudFormation 堆疊 AWS Resource Groups、 AppRegistry 應用程式和 Terraform 狀態檔案。

  如果選取此選項，則必須完成中的其中一個程序the section called “新增資源集合”。
- 僅限 EKS — 如果您想要從 Amazon EKS 叢集中的命名空間探索資源，請選取此選項。

  如果選取此選項，則必須完成中的程序 the section called “新增 EKS 叢集”
- 資源集合和 EKS — 如果您想要探索其中一個資源集合和 Amazon EKS 叢集的資源，請選取此選項。

  如果選取此選項，請完成中的其中一個程序，the section called “新增資源集合”然後完成中的程序the section called “新增 EKS 叢集”。

> **Note**
>
> 如需每個應用程式支援的資源數量的相關資訊，請參閱 Service Quotas。

下一頁

步驟 3：將資源添加到您的 AWS Resilience Hub 應用程序

步驟 3：將資源添加到您的 AWS Resilience Hub 應用程序

本節討論下列可用來構成應用模組結構基礎的選項：

- the section called “新增資源集合”
- the section called “新增 EKS 叢集”

新增資源集合

本節討論下列用來構成應用程式結構基礎的方法：

- 使用 AWS CloudFormation 堆疊
- 使用 AWS Resource Groups
- 使用 AppRegistry 應用
- 使用地形狀態檔
- 使用現有的應用 AWS Resilience Hub 程式

使用 AWS CloudFormation 堆疊

選擇包含您要在描述的應用程式中使用的資源的 AWS CloudFormation 堆疊。堆棧可以來自您用 AWS 帳戶 來描述應用程序的堆棧，也可以來自不同的帳戶或不同的區域。

探索構成應用程式結構基礎的資源

1. 選取CloudFormation 堆疊以探索堆疊式資源。
2. 從與您 AWS 帳戶 和區域相關聯的「選擇堆疊」 下拉式清單中選擇堆疊。

   若要使用位於不同 AWS 帳戶、不同區域或兩者的堆疊，請在 [AWS 區域外部新增堆疊] 方塊中輸入堆疊的 Amazon 資源名稱 (ARN)，然後選擇 [新增堆疊 AR N]。如需 ARN 的詳細資訊，請參閱《AWS 一般參考》中的 Amazon Resource Name (ARN)。

使用 AWS Resource Groups

選擇包 AWS Resource Groups 含您要在描述的應用程式中使用的資源的項目。

探索構成應用程式結構基礎的資源

1. 選取資源群組以探索包 AWS Resource Groups 含資源的群組。
2. 從選取資源群組下拉式清單中選擇資源。

   若 AWS Resource Groups 要在不同 AWS 帳戶、不同區域或兩者中使用，請在 [資源群組 ARN] 方塊中輸入堆疊的 Amazon 資源名稱 (ARN)，然後選擇 [新增資源群組 ARN]。如需 ARN 的詳細資訊，請參閱《AWS 一般參考》中的 Amazon Resource Name (ARN)。

使用 AppRegistry 應用

您一次只能新增一個 AppRegistry 應用程式。

選擇包含您要在描述的 AppRegistry 應用程式中使用之資源的應用程式。

探索構成應用程式結構基礎的資源

1. 選取AppRegistry以從中建立的應用程式清單中進行選取 AppRegistry。
2. 從選取應用程式下拉式清單中 AppRegistry選擇建立的應用程式。您一次只能選擇一個應用程序。

使用地形狀態檔

選擇 Terraform 狀態檔案，其中包含您要在所描述的應用程式中使用的 S3 儲存貯體資源。您可以導覽至 Terraform 狀態檔案的位置，或提供您可存取位於不同區域的 Terraform 狀態檔案的連結。

> **Note**
>
> AWS Resilience Hub 支持地形狀態文件版本`0.12`及更高版本。

探索構成應用程式結構基礎的資源

1. 選取地形狀態檔案以探索您的 S3 儲存貯體資源。
2. 在「選取狀態檔案」區段中，選擇「瀏覽 S3」以導覽至 Terraform 狀態檔案的位置。

   若要使用位於不同區域的 Terraform 狀態檔案，請在 S3 URL 欄位中提供 Terraform 狀態檔案位置的連結，然後選擇新增 S3 URL。

   地形表單狀態檔案的限制為 4 MB。

3. 從「儲存貯體」區段選取您的 S3 儲存貯體。
4. 從「物件」區段中，選取鍵，然後選擇「選擇」。

使用現有的應用 AWS Resilience Hub 程式

若要開始使用，請使用現有的應用程式。

探索構成應用程式結構基礎的資源

1. 選取現有應用程式，從現有的應用程式建置應用程式。
2. 從選取現有應用程式下拉式清單中選取應用程式。

新增 EKS 叢集

本節討論如何使用 Amazon EKS 叢集形成應用程式結構的基礎。

> **Note**
>
> 您必須擁有 Amazon EKS 許可和其他 IAM 角色才能連接到 Amazon EKS 叢集。如需新增單一帳戶和跨帳戶 Amazon EKS 許可和其他 IAM 角色以連接到叢集的詳細資訊，請參閱下列主題：
>
> - AWS Resilience Hub 存取權限參考
> - the section called “啟 AWS Resilience Hub 用對您的 Amazon EKS 叢集的存取”

選擇包含您要在所描述的應用程式中使用之資源的 Amazon EKS 叢集和命名空間。Amazon EKS 叢集可以來自您用來 AWS 帳戶 描述應用程式的叢集，也可以來自不同的帳戶或不同區域。

> **Note**
>
> 若 AWS Resilience Hub 要評估 Amazon EKS 叢集，您必須手動將相關命名空間新增至 EKS 叢集和命名空間區段中的每個 Amazon EKS 叢集。命名空間名稱必須與 Amazon EKS 叢集上的命名空間名稱完全相符。

若要新增 Amazon EKS 叢集

1. 從與您 AWS 帳戶 和區域相關聯的選擇 EKS 叢集下拉式清單中選擇 Amazon EKS 叢集。

2. 若要使用位於不同 AWS 帳戶、不同區域或兩者的 Amazon EKS 叢集，請在 [跨帳戶] 或 [區域] 方塊中輸入堆疊的 Amazon 資源名稱 (ARN)，然後選擇 [新增 E KS ARN]。如需 ARN 的詳細資訊，請參閱《AWS 一般參考》中的 Amazon Resource Name (ARN)。

   如需新增許可以存取跨區域 Amazon Elastic Kubernetes Service 叢集的詳細資訊，請參閱。the section called “啟 AWS Resilience Hub 用對您的 Amazon EKS 叢集的存取”

若要從選取的 Amazon EKS 叢集新增命名空間

1. 在 [新增命名空間] 區段中，從 EKS 叢集和命名空間表格中，選取位於 Amazon EKS 叢集名稱左側的圓鈕，然後選擇 [更新命名空間]。

   您可以透過下列方式識別 Amazon EKS 叢集：

   - EKS 叢集名稱 — 指示所選 Amazon EKS 叢集的名稱。
   - 命名空間數量 — 表示在 Amazon EKS 叢集中選取的命名空間數目。
   - 狀態 — 指出是否 AWS Resilience Hub 已在應用程式中包含所選 Amazon EKS 叢集的命名空間。您可以使用下列選項來識別狀態：
     - 需要命名空間 — 表示您尚未包含 Amazon EKS 叢集中的任何命名空間。
     - 已新增命名空間 — 表示您已包含 Amazon EKS 叢集中的一或多個命名空間。
2. 若要新增命名空間，請在 [更新命名空間] 對話方塊中選擇 [新增命名空間]。

   更新命名空間對話方塊會將您從 Amazon EKS 叢集中選取的所有命名空間顯示為可編輯選項。
3. 在 [更新命名空間] 對話方塊中，您有下列編輯選項：

   - 若要新增命名空間，請選擇 [新增命名空間]，然後在命名空間中輸入命名空間名稱方塊。

     命名空間名稱必須與 Amazon EKS 叢集上的命名空間名稱完全相符。
   - 若要移除命名空間，請選擇命名空間旁邊的 [移除]。
   - 若要將選取的命名空間套用至所有 Amazon EKS 叢集，請選擇將命名空間套用至所有 EKS 叢集。

     如果選擇此選項，則其他 Amazon EKS 叢集中先前的命名空間選項將被目前的命名空間選擇覆寫。
4. 若要在應用程式中包含更新的命名空間，請選擇 [更新]。

下一頁

[第四步：設定 RTO 和 RPO]

第四步：設定 RTO 和 RPO

您可以使用自己的 RT/RPO 目標來定義新的恢復原則，也可以選擇具有預先定義的 RT/RPO 目標的現有恢復原則。如果您想要使用其中一個現有的恢復原則，請選取 [選擇現有原則選項]，然後從 [選項] 項目下拉式清單中選取現有的目標應用程式。

若要定義您自己的 RTO /RPO 目標

1. 選取 [建立新的恢復原則] 選項。
2. 輸入恢復原則的名稱。
3. (選擇性) 輸入恢復原則的說明。
4. 在 RT/RPO 目標區段中定義您的 RT/ R PO 目標。

> **Note**
>
> - 我們已為您的應用程式填入預設 RTO 和 RPO。您可以立即變更 RTO 和 RPO，或在評估應用程式之後變更。
> - AWS Resilience Hub 可讓您在復原原則的 RTO 和 R PO 欄位中輸入零值。但是，在評估您的申請時，盡可能低的評估結果接近零。因此，如果您在 RTO 和 R PO 欄位中輸入零值，則預估的工作負載 RTO 和預估的工作負載 RPO 結果將接近零，並且應用程式的「符合性」狀態將設定為違反原則。

5. 若要為您的基礎架構和 AZ 定義 RTO，請選擇向右箭號以展開「基礎結構 RTO 和 R PO」區段。
6. 在 RT/RPO 目標中，在方塊中輸入數值，然後選擇該值代表 RTO 和 R PO 的時間單位。

   針對基礎結構 RTO 和 RPO 區段中的基礎結構和可用區域重複這些項目。
7. (選擇性) 如果您有多區域應用程式，而且想要定義區域 RTO 和 RPO，請開啟 [區域-選擇性]。

   在 RT O 和 RPO 中，在方塊中輸入數值，然後選擇該值代表 RTO 和 R PO 的時間單位。

下一頁

[the section called “步驟 5：設定彈性漂移偵測”]

步驟 5：漂移偵測

AWS Resurability Hub 可讓您設定彈性漂移偵測，以便每天評估應用程式，並在偵測到任何漂移或評估失敗時收到通知。

若要設定彈性漂移偵測

1. 若要每天評估您的應用程式，請開啟每天自動評估此應用程式。

   如果開啟此選項，則每日評估排程只會在下列情況之後開始：

   - 首次成功手動評估應用程式。
   - 應用程式已設定適當的 IAM 角色。
   - 如果您的應用程式設定了目前的 IAM 使用者許可，您必須建立 `AwsResilienceHubPeriodicAssessmentRole`

     角色使用中的適當程序the section called “AWS 彈性中樞如何與 IAM 搭配運作”。
2. 若要在 AWS Resilience Hub 偵測到符合性狀態的任何漂移時收到通知，或者每日復原能力評估失敗，請開啟「取得任何彈性原則違規的通知」。

   如果開啟此選項，若要接收漂移通知，您必須指定 Amazon Simple Notification Service (Amazon SNS) 主題。若要提供 Amazon SNS 主題，請在提供 SNS 主題區段中選取選擇 SNS 主題選項，然後從選擇 SNS 主題下拉式清單中選取 Amazon SNS 主題。

   > **Note**
   >
   > - 若要讓 AWS 恢復中樞能夠將通知發佈到您的 Amazon SNS 主題，您的 Amazon SNS 主題必須設定適當的許可。如需設定權限的詳細資訊，請參閱the section called “能 AWS Resilience Hub 夠發佈到您的 Amazon SNS 主題”。
   > - 每日評估可能會影響您的執行配額。如需有關配額的詳細資訊，請參閱AWS 一般參考中的AWS Resilience Hub 端點和配額。

   若要使用位於不同 AWS 帳戶 或不同區域的 Amazon SNS 主題，請選取輸入 SNS 主題 ARN，然後在提供 SNS 主題方塊中輸入 Amazon SNS 主題的 Amazon 資源名稱 (ARN)。如需 ARN 的詳細資訊，請參閱《AWS 一般參考》中的 Amazon Resource Name (ARN)。

下一頁

步驟 6：設定權限

步驟 6：設定權限

AWS Resilience Hub 可讓您為主要帳戶和次要帳戶配置必要的權限，以探索和評估資源。不過，您必須個別執行程序來設定每個帳戶的權限。

若要設定 IAM 角色和 IAM 許可

1. 若要選取用於存取目前帳戶資源的現有 IAM 角色，請從 [選取 IAM 角色] 下拉式清單中選取 IAM 角色。

   > **Note**
   >
   > 對於跨帳戶設定，如果您未在輸入 IAM 角色 ARN 方塊中指定 IAM 角色的 Amazon 資源名稱 (ARN)， AWS Resilience Hub 將使用您從選取 IAM 角色下拉式清單中為所有帳戶選取的 IAM 角色。

   如果您的帳戶沒有附加現有的 IAM 角色，則可以使用下列其中一個選項來建立 IAM 角色：

   - AWS IAM 主控台 — 如果選擇此選項，則必須完成在 IAM 主控台中建立 AWS 彈性中樞角色中的程序。
   - AWS CLI — 如果您選擇此選項，則必須完成 AWS CLI 中的所有步驟。
   - CloudFormation template — 如果您選擇此選項，視帳戶類型 (主要帳戶或次要帳戶) 而定，您必須使用適當的 AWS CloudFormation 範本建立角色。
2. 選擇向右箭號以展開跨帳戶新增 IAM 角色-選用區段。
3. 若要從跨帳戶選取 IAM 角色，請在輸入 IAM 角色 ARN 方塊中輸入 IAM 角色的 ARN。確保您輸入的 IAM 角色的 ARN 不屬於目前帳戶。
4. 如果您想要使用目前的 IAM 使用者來探索您的應用程式資源，請選擇向右箭號以展開 [使用目前的 IAM 使用者許可] 區段，然後選取 [我了解必須手動設定許可以在其中啟用所需的功能 AWS Resilience Hub。

   如果選取此選項，某些 AWS Resilience Hub 功能 (例如彈性漂移偵測) 可能無法如預期般運作，並且會忽略您在步驟 1 和步驟 3 中提供的輸入。

下一頁

步驟 8：新增標籤

步驟 7：設定應用程式組態參數

本節可讓您使 AWS Elastic Disaster Recovery用提供跨區域容錯移轉支援的詳細資訊。 AWS Resilience Hub 將使用此資訊來提供復原建議。

如需應用程式組態參數的詳細資訊，請參閱應用組態參數。

若要新增應用程式組態參數 (選擇性)

1. 若要展開「應用程式組態參數」段落，請選擇向右鍵。
2. 在 [帳戶 ID] 方塊中輸入容錯移轉帳戶 ID。根據預設，我們已使用您的帳戶 ID 預先填入此欄位 AWS Resilience Hub，您可以變更該 ID。
3. 從 [區域] 下拉式清單中選取容錯移轉區域。

> **Note**
>
> 如果要停用此功能，請從下拉式清單中選取「—」。

下一頁

步驟 8：新增標籤

步驟 8：新增標籤

為 AWS 資源指派標籤或標籤，以搜尋和篩選資源，或追蹤 AWS 成本。

(選擇性) 若要將標籤新增至應用程式，請選擇 [新增標記] (如果您要將一或多個標記與應用程式產生關聯)。如需有關標籤的詳細資訊，請參閱AWS 一般參考中的標記資源。

選擇新增應用程式以建立應用程式。

下一頁

步驟 9：檢閱並發佈您的 AWS Resilience Hub 應用程式

步驟 9：檢閱並發佈您的 AWS Resilience Hub 應用程式

發佈之後，您仍然可以檢閱應用程式並編輯其資源。完成後，請選擇「發佈」以發佈應用程式。

如需有關檢閱應用程式及編輯其資源的詳細資訊，請參閱下列內容：

- the section called “檢視應用摘要”
- the section called “編輯應用資源”

下一頁

步驟 10：對您的 AWS Resilience Hub 應用程式執行評估

步驟 10：對您的 AWS Resilience Hub 應用程式執行評估

您發佈的應用程式會列在 [摘要] 頁面上。

發佈 AWS Resilience Hub 應用程式之後，系統會將您重新導向至應用程式摘要頁面，您可以在其中執行復原能力評估。評估會根據附加到應用程式的復原原則來評估您的應用程式組態。系統會產生一份評估報告，顯示您的應用程式如何針對彈性原則中的目標進行衡量。

執行恢復能力評估

1. 在 [應用程式摘要] 頁面上，選擇 [評估復原]。
2. 在 [執行復原能力評估] 對話方塊中，輸入報告的唯一名稱，或在 [報告名稱] 方塊中使用產生的名稱。
3. 選擇執行。
4. 收到評估報告已產生的通知後，請選擇「評量」標籤和您的評估以檢視報告。
5. 選擇 [檢閱] 索引標籤以檢視應用程式的評估報告。

使用 AWS Resilience Hub

AWS Resilience Hub協助您改善應用程式的復原能力AWS並在應用程序中斷時減少恢復時間。

若要使用AWS Resilience Hub，您：

- 描述你的AWS應用程式在AWS Resilience Hub。
- 管理您的AWS中的資源AWS Resilience Hub。
- 建立有效的恢復原則。
- 管理指出應用程式復原能力的評估。
- 管理應用程式的警示、標準作業程序 (SOP) 和測試。

描述和管理AWS Resilience Hub應用程式

AWS Resilience Hub應用程式是AWS資源的集合，其結構可防止和復原AWS應用程式中斷。

若要描述AWS Resilience Hub應用程式，您需要提供應用程式名稱、來自一或多個AWS CloudFormation堆疊的資源，以及適當的恢復原則。您也可以使用任何現有的AWS Resilience Hub應用程式做為範本來描述您的應用程式。

描述AWS Resilience Hub應用程式之後，您必須將其發佈，以便在其上執行復原能力評估。然後，您可以使用評估中的建議，透過執行另一個評估、比較結果，然後重申程序，直到估計的工作負載 RTO 和估計的工作負載 RPO 符合 RTO 和 RPO 目標為止，以改善彈性。

若要協助追蹤應用程式變更，請AWS Resilience Hub顯示應用程式建立時的先前版本AWS Resilience Hub。此可見性可協助您檢閱過去的應用程式組態，並協助您決定目前的應用程式組態。 AWS Resilience Hub使用下列狀態來識別應用程式版本：

- 草稿 — 指出應用程式版本正在修改且尚未發佈。
- 目前版本 — 指示此應用程式版本是最近發佈的版本。 AWS Resilience Hub使用此應用程式版本執行恢復能力評估。
- 檢視所有版本 — 選擇加號 (+) 以唯讀格式檢視所有先前版本。

您可以從 [應用程式] 頁面透過下列方式識別您的應用程式：

- 名稱 — 您在中定義應用程式時所提供的應用程式名稱AWS Resilience Hub。

- 說明 — 您在中定義應用程式時所提供之應用程式的說明AWS Resilience Hub。
- 符合性狀態 — 將應用程式狀態AWS Resilience Hub設定為「已評估」、「未評估」、「違反策略」或「偵測到變更」。
  - 評估-AWS Resilience Hub 已評估您的申請。
  - 未評估-尚AWS Resilience Hub未評估您的申請。
  - 違反原則-AWS Resilience Hub 判斷您的應用程式未符合復原時間目標 (RTO) 和復原點目標 (RPO) 的彈性原則目標。AWS Resilience Hub在重新評估應用程式的恢復能力之前，請檢閱並使用提供的建議。如需建議的詳細資訊，請參閱將應用程式新增至 AWS Resilience Hub。
  - 偵測到的變更-AWS Resilience Hub 已偵測到與應用程式相關聯的復原原則所做的變更。您必須重新評估您的應用程式，AWS Resilience Hub以判斷您的應用程式是否符合彈性原則的目標。
- 排程評估 — 資源類型可識別應用程式的元件資源。如需排程評估的詳細資訊，請參閱應用程式備援。
  - 作用中-這表示您的應用程式會由每天自動評估AWS Resilience Hub。
  - 停用-這表示您的應用程式不會每天自動評估AWS Resilience Hub，您必須手動評估您的應用程式。
- 彈性漂移狀態 — 指出您的應用程式是否已從先前的成功評估中漂移，並設定下列其中一種狀態：
  - Drided-表示應用程式在先前的成功評估中符合其復原原則，現在已違反復原則，且應用程式面臨風險。
  - 未漂移-表示應用程式估計仍符合原則中定義的 RTO 和 RPO 目標。
- 預估的工作負載 RTO — 指出應用程式可能的最大估計工作負載 RTO。此值是上次成功評估之所有中斷類型的最大估計工作負載 RTO。
- 預估的工作負載 RPO — 指出應用程式可能的最大估計工作負載 RPO。此值是上次成功評估之所有中斷類型的最大估計工作負載 RTO。
- 上次評估時間 — 指出上次成功評估申請的日期和時間。
- 建立時間 — 建立應用程式的日期和時間。
- ARN — 您的應用程式的亞馬遜資源名稱 (ARN)。如需 ARN 的詳細資訊，請參閱《AWS 一般參考》中的 Amazon Resource Name (ARN)。

> **Note**
>
> AWS Resilience Hub只有在將 Amazon ECR 用於映像儲存庫時，才能完全評估跨區域 Amazon ECS 資源的彈性。

此外，您也可以使用「應用程式」頁面中的下列其中一個選項來篩選應用程式清單：

- 尋找應用程式 — 輸入您的應用程式名稱，依應用程式名稱篩選結果。
- 依日期和時間範圍篩選上次評估時間 — 若要套用此篩選器，請選擇行事曆圖示，然後選取下列其中一個選項，以依符合時間範圍的結果進行篩選：
  - 相對範圍 — 選取其中一個可用選項，然後選擇「套用」。

    如果您選擇自定義範圍選項，請在輸入持續時間框中輸入持續時間，然後從「時間單位」下拉列表中選擇適當的時間單位，然後選擇「應用」。
  - 絕對範圍 — 若要指定日期和時間範圍，請提供開始時間和結束時間，然後選擇 [套用]。

下列主題顯示描述應用程式以及如何管理AWS Resilience Hub應用程式的不同方法。

主題

檢視AWS Resilience Hub應用程式摘要

AWS Resilience Hub主控台中的應用程式摘要頁面提供應用程式資訊和恢復健全狀況的概觀。

若要檢視應用程式摘要

1. 在導覽窗格中，選擇 Applications (應用程式)。
2. 在 [應用程式] 頁面上，選擇應用程式的名稱。

[應用程式摘要] 頁面包含下列段落。

主題

- 詳細資訊
- 應用程式備援
- 實施的警報
- 實施的實驗

詳細資訊

應用程式摘要詳細資訊段落會顯示應用程式選擇項目的摘要。

- 應用程式狀態 — 指出您的應用程式是否處於作用中狀態。
- 說明 — 應用程式的說明。
- 符合性狀態 — 指出應用程式的符合性狀態。
- 上次評估日期 — 指出上次評估您申請的日期和時間。
- 復原原則 — 顯示附加至應用程式的復原原則名稱。如需恢復原則的詳細資訊，請參閱管理復原原則。
- 排程評估 — 指出每日評估是作用中還是非作用中。
- 彈性漂移狀態 — 指出您的應用程式是否已從之前的成功評估中漂移。
- 上次漂移日期 — 指出檢查您的應用程式是否有漂移的日期和時間。

更新預約的評估

1. 若要更新應用程式的排程評估，請從 [動作] 中選擇 [更新彈性漂移偵測]。
2. 若要更新復原漂移偵測，請完成中的步驟步驟 5：漂移偵測 ，然後返回此程序。
3. 選擇 Update (更新)。

> **Note**
>
> 若要在現有應用程式上啟動彈性漂移偵測，您必須在首次啟用恢復性漂移偵測功能之後手動執行評估。如需執行評量的詳細資訊，請參閱執行復原能力評估。

應用程式備援

「應用程式備援」區段中顯示的指標來自應用程式的最新復原能力評估。

彈性分數

彈性分數可協助您量化處理潛在中斷的準備情況。此分數反映了您的應用程式遵循AWS Resilience Hub建議符合應用程式復原原則、警示、標準作業程序 (SOP) 和測試的程度。

您的應用程式可以達到的最大彈性分數為 100%。分數代表在預先定義的時間段內執行的所有建議測試。這表示測試正在啟動正確的警報，並且警報啟動正確的 SOP。

例如，假設AWS Resilience Hub建議使用一個警報和一個 SOP 進行一項測試。測試執行時，警示會起始關聯的 SOP，然後順利執行。如需復原分數的詳細資訊，請參閱了解彈性分數。

隨時間推移的彈性分數

透過一段時間的彈性分數，您可以檢視過去 30 天內應用程式恢復能力的圖表。雖然下拉式功能表可以列出 10 個應用程式，但一次最多AWS Resilience Hub只能顯示四個應用程式的圖表。如需排程評估的詳細資訊，請參閱步驟 5：漂移偵測 。

> **Note**
>
> AWS Resilience Hub不會同時執行排定的評估。因此，您可能需要稍後返回一段時間的復原分數圖表，以檢視應用程式的每日評估。

AWS Resilience Hub還使用亞馬遜 CloudWatch 來生成這些圖形。選擇在中檢視指標，在 CloudWatch CloudWatch 儀表板中建立和檢視有關應用程式恢復能力的更精細資訊。如需詳細資訊 CloudWatch，請參閱 Amazon 使用 CloudWatch 者指南中的使用儀表板。

實施的警報

應用程式摘要已實作警示區段會列出您在 Amazon 中設定用 CloudWatch 來監控應用程式的警示。如需警示的詳細資訊，請參閱管理警示。

實施的實驗

應用摘要故障注入實驗部分顯示了故障注入實驗的列表。如需故障注入實驗的詳細資訊，請參閱Amazon 故障注入服務實驗。

編輯AWS Resilience Hub應用資源

若要獲得準確且有用的彈性評估，請確保您的應用程式描述已更新，並符合您的實際AWS應用程式和資源。評估報告、驗證和建議均以列出的資源為基礎。如果您從應AWS用程式中新增或移除資源，則應在中反映這些變更AWS Resilience Hub。

AWS Resilience Hub提供應用程式來源的透明度。您可以識別和編輯應用程式中的資源和應用程式來源。

> **Note**
>
> 編輯資源只會修改應用程式的AWS Resilience Hub參考。不會對您的實際資源進行任何變更。

您可以新增遺失的資源、修改現有資源，或移除不需要的資源。資源會分組為邏輯應用程式元件 (AppComponents)。您可以編輯 AppComponents 以更好地反映應用程式的結構。

透過編輯應用程式的草稿版本，並將變更發佈至新 (發行) 版本，以新增或更新應用程式資源。 AWS Resilience Hub使用應用程式的發行版本 (其中包括更新的資源) 來執行復原能力評估。

評估應用程式的復原能力

1. 在導覽窗格中，選擇 Applications (應用程式)。
2. 在 [應用程式] 頁面上，選擇您要編輯的應用程式名稱。
3. 從「動作」功能表中選擇「評估復原」。
4. 在 [執行復原能力評估] 對話方塊中，輸入報告的唯一名稱，或在 [報告名稱] 方塊中使用產生的名稱。
5. 選擇執行。
6. 收到評估報告已產生的通知後，請選擇「評量」標籤和您的評估以檢視報告。
7. 選擇應用程式評估報告的 [檢閱] 索引標籤。

若要更新應用程式的彈性漂移偵測

1. 在導覽窗格中，選擇 Applications (應用程式)。
2. 在 [應用程式] 頁面上，選取您要啟用或停用復原漂移偵測的應用程式。
3. 從 [動作] 中選擇 [更新復原漂移偵測]。
4. 若要更新復原漂移偵測，請完成中的步驟步驟 5：漂移偵測 ，然後返回此程序。
5. 選擇 Update (更新)。

更新應用程式的安全性權限

1. 在導覽窗格中，選擇 Applications (應用程式)。

2. 在 [應用程式] 頁面上，選取您要更新其安全性權限的應用程式。
3. 從「動作」 中選擇「更新權限」。
4. 若要更新安全性權限，請完成中的步驟步驟 6：設定權限，然後返回此程序。
5. 選擇 [儲存並更新]。

將復原原則附加至您的應用程式

1. 在導覽窗格中，選擇 Applications (應用程式)。
2. 在 [應用程式] 頁面上，選擇您要編輯的應用程式名稱。
3. 從 [動作] 功能表中，選擇 [連接復原原則]。
4. 在 [連接原則] 對話方塊中，從 [選取復原原則] 下拉式清單中選取復原原則。
5. 選擇 Attach (連接)。

若要編輯應用程式 AppComponents 的輸入來源、資源和

1. 在導覽窗格中，選擇 Applications (應用程式)。
2. 在 [應用程式] 頁面上，選擇您要編輯的應用程式名稱。
3. 選擇應用程式結構索引標籤。
4. 選擇「版本」之前的加號 +，然後選取「草稿」狀態的應用程式版本。

5. 若要編輯輸入來源、資源和應用程式，請完成以下程序中 AppComponents 的步驟。

若要編輯應用程式的輸入來源

1. 若要編輯應用程式的輸入來源，請選擇 [輸入來源] 索引標籤。

   「輸入來源」區段會列出應用程式資源的所有輸入來源。您可以透過下列方式識別輸入來源：

   - 來源名稱 — 輸入來源的名稱。選擇來源名稱，即可在個別應用程式中檢視其詳細資訊。對於手動新增的輸入來源，連結將無法使用。例如，如果您選擇從AWS CloudFormation堆疊匯入的來源名稱，系統會將您重新導向至AWS CloudFormation主控台上的堆疊詳細資料頁面。
   - 來源 ARN — 輸入來源的亞馬遜資源名稱 (ARN)。選擇 ARN 以在個別應用程式中檢視其詳細資訊。對於手動新增的輸入來源，連結將無法使用。例如，如果您選擇從AWS CloudFormation堆疊匯入的 ARN，系統會將您重新導向至AWS CloudFormation主控台上的堆疊詳細資料頁面。

- 來源類型 — 輸入來源的類型。輸入來源包括 Amazon EKS 叢集、AWS CloudFormation堆疊、AppRegistry 應用程式AWS Resource Groups、Terraform 狀態檔案，以及手動新增的資源。
- 關聯資源 — 與輸入來源相關聯的資源數目。選擇一個數字，以在「資源」頁標中檢視輸入來源的所有相關資源。

2. 若要將輸入來源新增至您的應用程式，請從 [輸入來源] 區段中選擇 [新增輸入來源]。如需加入輸入來源的更多資訊，請參閱〈〉the section called “步驟 3：將資源添加到您的 AWS Resilience Hub 應用程序”。
3. 若要編輯輸入來源，請選取輸入來源，然後從「動作」中選擇下列其中一個選項：

- 重新匯入輸入來源 (最多 5 個) — 重新匯入最多五個選取的輸入來源。
- 刪除輸入來源 — 刪除選取的輸入來源。

若要發佈應用程式，應用程式必須至少包含一個輸入來源。如果您刪除所有輸入來源，則會停用「發佈新版本」。

若要編輯應用程式的資源

1. 若要編輯應用程式的資源，請選擇 [資源] 索引標籤。

> **Note**
>
> 若要查看未評估的資源清單，請選擇檢視未評估的資源。

[資源] 區段會列出您選擇做為應用程式說明範本之應用程式的資源。為了增強您的搜索體驗，AWS Resilience Hub已根據多個搜索條件對資源進行分組。這些搜尋條件包括 AppComponent 類型、不支援的資源和已排除的資源。若要根據「資源」(Resources) 表格中的搜尋條件來篩選資源，請選擇每個搜尋條件下方的編號。

您可以透過下列方式識別資源：

- 邏輯 ID — 邏輯 ID 是用來識別AWS CloudFormation堆疊、Terraform 狀態檔案、手動新增應用程式、 AppRegistry 應用程式或中資源的名稱。AWS Resource Groups

> **Note**
>
> - Terraform 可讓您針對不同的資源類型使用相同的名稱。因此，您會在共用相同名稱的資源的邏輯 ID 結尾看到「-資源類型」。

- 若要檢視所有應用程式資源的執行個體，請在邏輯 ID 之前選擇加號 (+)。若要檢視應用程式資源的所有執行個體，請在每個資源的邏輯 ID 之前選擇加號 (+)。

  如需支援資源的詳細資訊，請參閱the section called “支援的 AWS Resilience Hub 資源”。

- 資源類型 — 資源類型可識別應用程式的元件資源。例如，`AWS::EC2::Instance`宣告一個 Amazon EC2 執行個體。如需將 AppComponent資源分組的詳細資訊，請參閱對資源進行分組 AppComponent。
- 來源名稱 — 輸入來源的名稱。選擇來源名稱，即可在個別應用程式中檢視其詳細資訊。對於手動新增的輸入來源，連結將無法使用。例如，如果您選擇從AWS CloudFormation堆疊匯入的來源名稱，系統會將您重新導向至上的堆疊詳細資料頁面AWS CloudFormation。
- 來源類型 — 輸入來源的類型。輸入來源包括AWS CloudFormation堆疊、 AppRegistry 應用程式AWS Resource Groups、Terraform 狀態檔案，以及手動新增的資源。

  > **Note**
  >
  > 若要編輯 Amazon EKS 叢集，AWS Resilience Hub請完成編輯應用程式程序的輸入來源中的步驟。

- 來源堆疊 — 包含資源的AWS CloudFormation堆疊。此欄取決於您選取的應用程式結構類型。
- 實體 ID — 該資源的實際指派識別碼，例如 Amazon EC2 執行個體 ID 或 S3 儲存貯體名稱。
- 已包含 — 這表示是否在應用程式中AWS Resilience Hub包含這些資源。
- 可評估 — 這表示是否AWS Resilience Hub會評估您的資源以獲得彈性。
- AppComponents— 探索到其應用程式結構時，指派給此資源的AWS Resilience Hub元件。
- 名稱 — 應用程式資源的名稱。
- 帳號 — 擁有實體資源的AWS帳號。

2. 若要尋找未列出的資源，請在搜尋方塊中輸入資源邏輯 ID。
3. 若要從應用程式中移除資源，請選取資源，然後選擇 [從動作排除資源]。
4. 若要解析應用程式上的資源，請選擇 [重新整理資源]。
5. 若要修改現有的應用程式資源，請完成以下步驟：

   a. 選取資源，然後從 [動作] 中選擇 [更新堆疊]。

   b. 在 [更新堆疊] 頁面中，若要更新資源，請完成中的適當程序步驟 3：將資源添加到您的 AWS Resilience Hub 應用程序，然後返回此程序。

c. 選擇 儲存 。

6. 若要將資源新增至您的應用程式，請從動作中選擇新增資源，然後完成下列步驟：

   a. 從 [資源類型] 下拉式清單中選取資源類型。

   b. AppComponent 從AppComponent下拉式清單中選取。

   c. 在 [資源名稱] 方塊中輸入資源邏輯 ID。

   d. 在「資源識別碼」方塊中輸入實際資源 ID、資源名稱或資源 ARN。

   e. 選擇 Add (新增)。

7. 若要編輯資源名稱，請選取資源，從 [動作] 中選擇 [編輯資源名稱]，然後完成下列步驟：

   a. 在 [資源名稱] 方塊中輸入資源邏輯 ID。

   b. 選擇 儲存 。

8. 若要編輯資源識別碼，請選取資源，從 [動作] 中選擇 [編輯資源識別碼]，然後完成下列步驟：

   a. 在「資源識別碼」方塊中輸入實際資源 ID、資源名稱或資源 ARN。

   b. 選擇 儲存 。

9. 若要變更 AppComponent，請選取資源， AppComponent從動作中選擇變更，然後完成下列步驟：

   a. AppComponent 從AppComponent下拉式清單中選取。

   b. 選擇 Add (新增)。

10. 若要刪除資源，請選取資源，然後從 [動作] 中選擇 [刪除資源]。

11. 若要包含資源，請選取資源，然後從 [動作] 中選擇 [包含資源]。

若要編輯您 AppComponents 的應用程式

1. 若要編輯應用程式 AppComponents 的，請選擇索AppComponents引標籤。

   > **Note**
   >
   > 如需將 AppComponent 資源分組的詳細資訊，請參閱對資源進行分組 AppComponent。

   此AppComponents段落會列出資源分組到的所有邏輯元件。您可以透 AppComponents 過下列方式識別：

- AppComponent name — 探索到此資源的應用程式結構時，指派給此資源的AWS Resilience Hub元件名稱。
- AppComponent 類型 — 元AWS Resilience Hub件的類型。
- 來源名稱 — 輸入來源的名稱。選擇來源名稱，即可在個別應用程式中檢視其詳細資訊。例如，如果您選擇從AWS CloudFormation堆疊匯入的來源名稱，系統會將您重新導向至上的堆疊詳細資料頁面AWS CloudFormation。
- 資源計數 — 與輸入來源相關聯的資源數目。選擇一個數字，以在「資源」頁標中檢視輸入來源的所有相關資源。

2. 若要建立 AppComponent，請從「動作」功能表中選擇「新建」， AppComponent然後完成下列步驟：

   a. 在名稱方塊 AppComponent 中輸入的AppComponent名稱。作為參考，我們已使用範例名稱預先填入此欄位。

   b. 從類型下拉式清單 AppComponent 中選取AppComponent類型。

   c. 選擇 儲存 。

3. 若要編輯 AppComponent，請選取一個 AppComponent，然後從「動作」 AppComponent 中選擇「編輯」。
4. 若要刪除 AppComponent，請選取 AppComponent，然後選擇「 AppComponent從動作刪除」。

變更資源清單後，您會收到警示，指出已對應用程式草稿版本進行變更。若要執行準確的恢復能力評估，您必須發佈應用程式的新版本。如需如何發佈新版本的詳細資訊，請參閱發佈新的AWS Resilience Hub應用程式版本。

對資源進行分組 AppComponent

A AppComponent 是一組作為單一單元運作和失敗的相關 AWS 資源。例如，如果您有主要資料庫和複本資料庫，則這兩個資料庫都屬於相同的應用程式元件 (AppComponent)。 AWS Resilience Hub 具有管理哪些 AWS 資源可以屬於哪種類型的規則 AppComponent。例如，一個`DBInstance`可以屬於`AWS::ResilienceHub::DatabaseAppComponent`但不屬於`AWS::ResilienceHub::ComputeAppComponent`。

將 AWS Resilience Hub 應用程式以 AWS CloudFormation 堆疊、Terraform 狀態檔案 AWS Resource Groups、Amazon Elastic Kubernetes Service 叢集或 AppRegistry 應用程式匯入時，會盡最大努力將相關資源分組為相同資源 AppComponent，但可能並非總是百分之百準確。 AWS Resilience Hub 您最了解應用程式的架構，因此您可以將已依據分組的資源重新分組 AWS Resilience Hub 為不同

AppComponent的資源。例如，如果一個 AWS CloudFormation 堆疊中有三個 EC2 執行個體，則會為 AppComponent 每個 EC2 執行個體 AWS Resilience Hub 建立一個執行個體，但這三個 EC2 執行個體可能都在執行相同的應用程式軟體。在此情況下，正確的選擇是將三個 EC2 執行個體重新分組為單ComputeAppComponent一執行個體。重新分組資源時，您應該只將資源重新群組為單一資源。AppComponent您也可以展開資源清單，並將未分組的資源合併為 AppComponent.

支 AWS Resilience Hub AppComponents 持以下資源：

- AWS::ResilienceHub::ComputeAppComponent
  - AWS::ApiGateway::RestApi
  - AWS::ApiGatewayV2::Api
  - AWS::AutoScaling::AutoScalingGroup
  - AWS::EC2::Instance
  - AWS::ECS::Service
  - AWS::EKS::Deployment
  - AWS::EKS::ReplicaSet
  - AWS::EKS::Pod
  - AWS::Lambda::Function
  - AWS::StepFunctions::StateMachine
- AWS::ResilienceHub::DatabaseAppComponent
  - AWS::DocDB::DBCluster
  - AWS::DynamoDB::Table
  - AWS::RDS::DBCluster
  - AWS::RDS::DBInstance
- AWS::ResilienceHub::NetworkingAppComponent
  - AWS::EC2::NatGateway
  - AWS::ElasticLoadBalancing::LoadBalancer
  - AWS::ElasticLoadBalancingV2::LoadBalancer
  - AWS::Route53::RecordSet
- AWS:ResilienceHub::NotificationAppComponent
  - AWS::SNS::Topic
- AWS::ResilienceHub::QueueAppComponent

  - `AWS::SQS::Queue`
- `AWS::ResilienceHub::StorageAppComponent`
  - `AWS::Backup::BackupPlan`
  - `AWS::EC2::Volume`
  - `AWS::EFS::FileSystem`
  - `AWS::FSx::FileSystem`
    -
> **Note**
>
> 目前，僅 AWS Resilience Hub 支援 FSx for Windows File Server 的 Amazon FSx。
  - `AWS::S3::Bucket`

以下是正確分組的範例：

- 將主要資料庫和複本分組在單 AppComponent一資料庫下。
- 將 Amazon S3 儲存貯體及其複寫分組在一個單一儲存貯體下 AppComponent。
- 將執行相同應用程式的 Amazon EC2 執行個體分組至單一執行個體 AppComponent。
- 將 Amazon SQS 佇列及其無效字母佇列分組到單一佇列之下。 AppComponent
- 將 Amazon ECS 服務分組在一個區域中，並在另一個區域以單一方式容錯移轉 Amazon ECS 服務。 AppComponent

> **Note**
>
> AWS Resilience Hub 需要正確的分組，以便計算估計的工作負載 RTO 和估計的工作負載 RPO 以產生建議。

若要將資源指定給 AppComponent

1. 在導覽窗格中，選擇 Applications (應用程式)。
2. 在 [應用程式] 頁面上，選擇包含您要重新群組之資源的應用程式名稱。
3. 選擇應用程式結構索引標籤。
4. 在版本下，選取狀態為草稿的應用程式版本。
5. 選擇 Resources (資源) 標籤。

6. 選取要重新分組的資源。
7. 從 [動作] 中選擇 [變更] AppComponent。

   將顯示 [變更] AppComponent 對話方塊。
8. 若要 AppComponent 從AppComponent區段中刪除目前的項目，請在顯示您目前 AppComponent 名稱的標籤右上角選擇 X。
9. 若要將資源分組為不同 AppComponent，請從「選擇」 AppComponent 下拉式清單 AppComponent中選擇不同的資源。
10. 選擇新增。
11. AppComponents 從AppComponents標籤中刪除任何空白。
12. 選擇 Publish new version (發佈新版本)。
13. 選擇應用程式結構索引標籤。
14. 若要檢視應用程式的已發佈版本，請完成以下步驟：

    a. 在版本選項卡下，選擇具有當前版本狀態的應用程序版本。
    b. 選擇 Resources (資源) 標籤。

若要分組資源

1. 在導覽窗格中，選擇 Applications (應用程式)。
2. 在 [應用程式] 頁面上，選擇包含您要分組之資源的應用程式名稱。
3. 選擇應用程式結構索引標籤。
4. 在版本索引標籤下，選取狀態為草稿的應用程式版本。
5. 選擇 Resources (資源) 標籤。
6. 選擇您要分組的資源。

   > **Note**
   >
   > 您無法選擇手動新增的資源。

7. 選擇 [動作]，然後選擇 [分組資源]。

   將顯示「合併 AppComponent」視窗。
8. AppComponent 從 [選擇] AppComponent 下拉式清單中選擇您要將資源分組的清單。
9. 選擇儲存。

10. 選擇 Publish new version (發佈新版本)。
11. 選擇應用程式結構索引標籤。
12. 若要檢視應用程式的已發佈版本，請完成以下步驟：

    a. 在版本選項卡下，選擇具有當前版本狀態的應用程序版本。
    b. 選擇 Resources (資源) 標籤。

發佈新的AWS Resilience Hub應用程式版本

如中所述對AWS Resilience Hub應用程式資源進行變更後編輯AWS Resilience Hub應用資源，您必須發佈應用程式的新版本，才能執行準確的恢復能力評估。此外，如果您在應用程式中新增了建議的警示、SOP 和測試，則可能需要發佈應用程式的新版本。

若要發佈應用程式的新版本

1. 在導覽窗格中，選擇 Applications (應用程式)。
2. 在 [應用程式] 頁面上，選擇應用程式的名稱。
3. 選擇應用程式結構索引標籤。
4. 選擇 Publish new version (發佈新版本)。
5. 在「發佈版本」對話方塊的「名稱」方塊中，輸入應用程式版本的名稱，或者您可以使用建議的預設名稱AWS Resilience Hub。
6. 選擇 Publish (發佈)。

   當您發佈應用程式的新版本時，這會成為執行恢復能力評估時評估的版本。此外，草稿版本將與發行版本相同，直到您進行任何變更為止。

在您發佈新版應用程式之後，我們建議您執行新的復原能力評估報告，以確認您的應用程式仍符合復原原則。如需有關執行評估的資訊，請參閱執行和管理 AWS Resilience Hub 恢復能力評估。

檢視所有AWS Resilience Hub應用程式版本

若要協助追蹤應用程式變更，請AWS Resilience Hub顯示應用程式建立時的先前版本AWS Resilience Hub。

若要檢視應用程式的所有版本

1. 在導覽窗格中，選擇 Applications (應用程式)。

2. 在 [應用程式] 頁面上，選擇應用程式的名稱。
3. 選擇應用程式結構索引標籤。
4. 若要檢視應用程式的所有先前版本，請在檢視所有版本之前選擇加號 (+)。 AWS Resilience Hub 指出使用「草稿」和「目前核發」狀態的應用程式的草稿版本與最近發行版本。您可以選擇任何版本的應用程式來檢視其資源 AppComponent、輸入來源及其他相關資訊。

   此外，您也可以使用下列其中一個選項來篩選清單：

   - 依版本名稱篩選 — 輸入名稱，以依應用程式版本的名稱篩選結果。
   - 依日期和時間範圍篩選 — 若要套用此篩選器，請選擇行事曆圖示，然後選取下列其中一個選項，以依符合時間範圍的結果進行篩選：
     - 相對範圍 — 選取其中一個可用選項，然後選擇「套用」。

       如果您選擇自定義範圍選項，請在輸入持續時間框中輸入持續時間，然後從中選擇適當的時間單位時間單位下拉列表，然後選擇登記。
     - 相對範圍 — 若要指定日期和時間範圍，請提供開始時間和結束時間，然後選擇 [套用]。

檢視AWS Resilience Hub應用程式的資源

若要檢視應用程式的資源

1. 在導覽窗格中，選擇 Applications (應用程式)。
2. 在 [應用程式] 頁面上，選取您要更新其安全性權限的應用程式。
3. 在動作中，選擇檢視資源。

   在「資源」標籤中，您可以透過下列方式識別「資源」表格中的資源：

   - 邏輯 ID — 邏輯 ID 是用來識別AWS CloudFormation堆疊、Terraform 狀態檔案、手動新增應用程式、 AppRegistry 應用程式或中資源的名稱。AWS Resource Groups

     > **Note**
     >
     > - Terraform 可讓您針對不同的資源類型使用相同的名稱。因此，您會在共用相同名稱的資源的邏輯 ID 結尾看到「-資源類型」。
     > - 若要檢視所有應用程式資源的執行個體，請在邏輯 ID 之前選擇加號 (+)。若要檢視應用程式資源的所有執行個體，請在每個資源的邏輯 ID 之前選擇加號 (+)。

如需支援資源的詳細資訊，請參閱the section called “支援的 AWS Resilience Hub 資源”。

- 狀態 — 這表示是否AWS Resilience Hub會評估您的資源以獲得復原能力。
- 資源類型 — 資源類型可識別應用程式的元件資源。例如，`AWS::EC2::Instance`宣告一個 Amazon EC2 執行個體。如需將 AppComponent 資源分組的詳細資訊，請參閱對資源進行分組 AppComponent。
- 來源名稱 — 輸入來源的名稱。選擇來源名稱，即可在個別應用程式中檢視其詳細資訊。對於手動新增的輸入來源，連結將無法使用。例如，如果您選擇從AWS CloudFormation堆疊匯入的來源名稱，系統會將您重新導向至上的堆疊詳細資料頁面AWS CloudFormation。
- 來源類型 — 輸入來源的類型。
- AppComponent type — 輸入來源的類型。輸入來源包括AWS CloudFormation堆疊、AppRegistry應用程式AWS Resource Groups、Terraform 狀態檔案，以及手動新增的資源。

> **Note**
>
> 若要編輯 Amazon EKS 叢集，AWS Resilience Hub請完成編輯應用程式程序的輸入來源中的步驟。

- 實體 ID — 該資源的實際指派識別碼，例如 Amazon EC2 執行個體 ID 或 S3 儲存貯體名稱。
- 已包含 — 這表示是否在應用程式中AWS Resilience Hub包含這些資源。
- AppComponents— 探索到其應用程式結構時，指派給此資源的AWS Resilience Hub元件。
- 名稱 — 應用程式資源的名稱。
- 帳號 — 擁有實體資源的AWS帳號。

4. 選擇 [儲存並更新]。

刪除AWS Resilience Hub應用程式

達到十個應用程式限制的上限之後，您必須先刪除一或多個應用程式，才能新增更多應用程式。

欲刪除應用程式

1. 在導覽窗格中，選擇 Applications (應用程式)。
2. 在 [應用程式] 頁面上，選取您要刪除的應用程式。
3. 選擇 Actions (動作)，然後選擇 Delete application (刪除應用程式)。

4. 若要確認刪除，請在「刪除」方塊中輸入 Delete，然後選擇「刪除」。

應用組態參數

AWS Resilience Hub提供輸入機制，以收集與應用程式相關聯之資源的其他資訊。有了這些資訊，AWS Resilience Hub就能更深入地瞭解您的資源，並提供更好的彈性建議。

「應用程式組態參數」段落會列出跨區域容錯移轉支援的所有組態參數。AWS Elastic Disaster Recovery您可以透過下列方式識別組態參數：

- 主題 — 指示已配置的應用程式區域。例如，容錯移轉組態。
- 目的 — 指示AWS Resilience Hub要求資訊的原因。
- 參數 — 指出應用程式區域特定的詳細資訊，這些詳細資訊AWS Resilience Hub將用來為您的應用程式提供建議。目前，此參數僅使用一個容錯移轉區域和一個關聯帳戶的索引鍵值。

更新應用程式組態參

本節可讓您更新應用程式的組態參數AWS Elastic Disaster Recovery並發佈應用程式，以包含復原能力評估的更新參數。

更新應用程式組態參數

1. 在導覽窗格中，選擇 Applications (應用程式)。
2. 在 [應用程式] 頁面上，選擇您要編輯的應用程式名稱。
3. 選擇應用程式組態參數索引標籤。
4. 選擇更新。
5. 在 [帳戶 ID] 方塊中輸入容錯移轉帳戶 ID。
6. 從 [區域] 下拉式清單中選取容錯移轉區域。

> **Note**
>
> 如果您要停用此功能，請從下拉式清單中選取「—」。

7. 選擇 [更新並發佈]。

管理復原原則

本節說明如何為您的應用程式建立復原原則。正確設定復原原則可讓您瞭解應用程式的彈性狀態。備援原則包含資訊和目標，您可用來評估應用程式是否會從中斷類型 (例如軟體、硬體、可用區AWS域或區域) 復原。這些原則不會變更或影響實際的應用程式。多個應用程式可以具有相同的恢復原則。

建立復原原則時，您可以定義目標目標：復原時間目標 (RTO) 和復原點目標 (RPO)。目標決定應用程式是否符合備援原則。將原則附加至您的應用程式，並執行復原評估。您可以為產品組合中不同類型的應用程式建立不同的政策。例如，實時交易應用程序將具有與每月報告應用程序不同的彈性政策。

> **Note**
>
> AWS Resilience Hub可讓您在復原原則的 RTO 和 R PO 欄位中輸入零值。但是，在評估您的申請時，盡可能低的評估結果接近零。因此，如果您在 RTO 和 R PO 欄位中輸入零值，則預估的工作負載 RTO 和預估的工作負載 RPO 結果將接近零，並且應用程式的「符合性」狀態將設定為違反原則。

評估會根據連接的恢復原則來評估您的應用程式組態。在程序結束時，AWS Resilience Hub提供應用程式如何針對復原原則中的復原目標進行測量的評估。

您可以在應用程式中建立復原原則，也可以在復原原則中建立復原原則。您可以存取有關您政策的相關詳細資訊，也可以修改和刪除它們。

AWS Resilience Hub使用 RTO 和 RPO 目標來測量下列潛在中斷類型的彈性：

- 應用程式 — 遺失必要的軟體服務或程序。
- 雲端基礎架構 — 硬體遺失，例如 EC2 執行個體。
- 雲端基礎架構可用區域 (AZ) — 一或多個可用區域無法使用。
- 雲端基礎架構區域 — 一個或多個區域無法使用。

AWS Resilience Hub可讓您建立自訂的備援原則，或使用我們建議的開放式標準備援原則。當您建立自訂原則時，請命名並說明您的原則，並選擇適當的層級或定義原則的層級。這些層級包括：基礎 IT 核心服務、關鍵任務、關鍵、重要和非關鍵。

選擇適合您應用程式類別的層級。例如，您可以將實時交易系統歸類為關鍵，而您可以將每月報告應用程序歸類為非關鍵。當您使用我們的標準原則時，您可以根據中斷類型選擇具有預先設定的層級和 RTO 和 RPO 目標值的恢復原則。如有必要，您可以變更層級以及 RTO 和 RPO 目標。

您可以在復原原則中建立復原原則，或在描述新應用程式時建立復原原則。

建立復原原則

在中AWS Resilience Hub，您可以建立恢復原則。備援原則包含資訊和目標，您可用來評估應用程式是否可從中斷類型 (例如軟體、硬體、可用區AWS域或區域) 復原。這些原則不會變更或影響實際的應用程式。多個應用程式可以具有相同的恢復原則。

建立復原原則時，您可以定義復原時間目標 (RTO) 和復原點目標 (RPO) 目標。執行評估時，AWS Resilience Hub會判斷應用程式是否預估為符合復原原則中定義的目標。

評估會根據連接的恢復原則來評估您的應用程式組態。在程序結束時，會AWS Resilience Hub針對您的應用程式如何針對彈性原則中的目標進行評估。

> **Note**
>
> AWS Resilience Hub可讓您在復原原則的 RTO 和 R PO 欄位中輸入零值。但是，在評估您的申請時，盡可能低的評估結果接近零。因此，如果您在 RTO 和 R PO 欄位中輸入零值，則預估的工作負載 RTO 和預估的工作負載 RPO 結果將接近零，並且應用程式的「符合性」狀態將設定為違反原則。

您可以在應用程式中建立復原原則，也可以在復原原則中建立復原原則。您可以存取有關您政策的相關詳細資訊，也可以修改和刪除它們。

若要在應用程式中建立復原原則

1. 在左側導覽選單中，選擇「應用程式」。
2. 從到完成程the section called “步驟 1：透過新增應用程式開始使用”序the section called “步驟 8：將標籤新增至您的應用程式 ”。
3. 在 [恢復原則] 區段中，選擇 [建立復原原則]。

   [建立恢復原則] 頁面隨即顯示。
4. 在 [選擇建立方法] 區段中，選取 [建立原則]。
5. 輸入政策的名稱。
6. (選用) 輸入政策的描述。
7. 從「階層」下拉式清單中選擇下列其中一項：

- 基礎 IT 核心服務
- 關鍵任務
- 嚴重
- Important (重要)
- 非重要

8. 對於 RTO 和 R PO 目標，在客戶應用模組 RTO 與 RPO 下，在方塊中輸入數值，然後選擇值所代表的時間單位。

   針對基礎結構和可用區域，在基礎結構 RTO 和 RPO 下重複這些項目。

9. (選擇性) 如果您有多區域應用程式，您可能想要定義「地區」的 RTO 和 RPO 目標。

   開啟區域。對於區域 RT O 與 RPO 目標，在客戶應用模組 RTO 與 RPO 下，在方塊中輸入數值，然後選擇值所代表的時間單位。

10. (選擇性) 如果您想要新增標籤，您可以稍後繼續建立原則。如需有關標籤的詳細資訊，請參閱AWS一般參考中的標記資源。

11. 若要建立原則，請選擇 [建立]。

若要在恢復原則中建立恢復原則

1. 在左側導覽功能表中，選擇 [策略]。
2. 在 [恢復原則] 區段中，選擇 [建立復原原則]。

   [建立恢復原則] 頁面隨即顯示。

3. 輸入政策的名稱。
4. (選用) 輸入政策的描述。
5. 從階層中選擇下列其中一項：

   - 基礎 IT 核心服務
   - 關鍵任務
   - 嚴重
   - Important (重要)
   - 非重要

6. 對於 RTO 和 R PO 目標，在客戶應用模組 RTO 與 RPO 下，在方塊中輸入數值，然後選擇值所代表的時間單位。

針對基礎結構和可用區域，在基礎結構 RTO 和 RPO 下重複這些項目。

7. (選擇性) 如果您有多區域應用程式，您可能想要定義「地區」的 RTO 和 RPO 目標。

   開啟區域。對於 RTO 和 R PO 目標，在客戶應用模組 RTO 與 RPO 下，在方塊中輸入數值，然後選擇值所代表的時間單位。

8. (選擇性) 如果您想要新增標籤，您可以稍後繼續建立原則。如需有關標籤的詳細資訊，請參閱AWS一般參考中的標記資源。

9. 若要建立原則，請選擇 [建立]。

根據建議的原則建立復原原則

1. 在左側導覽功能表中，選擇 [策略]。
2. 在 [選擇建立方法] 區段中，選取根據建議的原則選取策略。
3. 在 [恢復原則] 區段中，選擇 [建立復原原則]。

   [建立恢復原則] 頁面隨即顯示。

4. 輸入恢復原則的名稱。
5. (選用) 輸入政策的描述。
6. 在 [建議的恢復原則] 區段下，檢視並選擇下列其中一個預先決定的恢復原則層級：

   - 非關鍵應用
   - 重要應用
   - 關鍵應用
   - 全球關鍵應用
   - 關鍵任務應用
   - 全球關鍵任務應用
   - 基礎核心服務

7. 若要建立恢復原則，請選擇 [建立原則]。

存取恢復原則詳細資料

當您開啟恢復原則時，您會看到有關原則的重要詳細資料。您也可以編輯或刪除復原。

恢復原則詳細資料包含兩個主要檢視：摘要和標籤。

摘要

基本信息

提供有關恢復原則的下列資訊：名稱、說明、層級、成本層和建立日期。

估計的工作量 RTO 和估計的工作量 RPO

顯示與此恢復原則相關的預估工作負載 RTO 和預估的工作負載 RPO 中斷類型。

Tags (標籤)

使用此檢視可管理、新增和刪除此應用程式內部的標籤。

若要編輯恢復原則詳細資料中的恢復原則

1. 在左側導覽功能表中，選擇 [策略]。
2. 在恢復原則中，開啟恢復原則。
3. 選擇 編輯 。在 [基本資訊]、RTO 和 RPO 欄位中輸入適當的變更。接著選擇 Save changes (儲存變更)。

若要編輯恢復原則中的恢復原則

1. 在左側導覽功能表中，選擇 [策略]。
2. 在恢復原則中，選擇恢復原則。
3. 選擇 [動作]，然後選取 [編輯]。
4. 在 [基本資訊]、RTO 和 RPO 欄位中輸入適當的變更。接著選擇 Save changes (儲存變更)。

若要刪除恢復原則詳細資料中的恢復原則

1. 在左側導覽功能表中，選擇 [策略]。
2. 在恢復原則中，開啟恢復原則。
3. 選擇 刪除 。確認刪除，然後選擇 [刪除]。

若要刪除恢復原則中的恢復原則

1. 在左側導覽功能表中，選擇 [策略]。
2. 在恢復原則中，選擇恢復原則。

3. 選擇「動作」，然後選取「刪除」。
4. 確認刪除，然後選擇 [刪除]。

執行和管理 AWS Resilience Hub 恢復能力評估

當您的應用程式變更時，您應該執行復原能力評估。評估會將每個應用程式元件組態與原則進行比較，並提出警示、SOP 和測試建議。這些組態建議可以改善復原程序的速度。

警示建議可協助您設定偵測中斷的警示。SOP 建議提供管理常見復原程序的指令碼，例如從備份復原。測試建議提供建議，以確認您的組態是否正常運作。例如，您可以測試應用程式是否在自動復原程序期間復原，例如自動調整規模或負載平衡因為網路問題而復原。您可以測試是否在資源達到限制時觸發應用程式警示。您還可以在指定的條件下測試 SOP 的工作情況。

執行復原能力評估

您可以從中 AWS Resilience Hub的多個位置執行復原評估報告。如需有關應用程式的詳細資訊，請參閱the section called “應用程式”。

若要從動作功能表執行恢復能力評估

1. 在左側導覽選單中，選擇「應用程式」。
2. 從「應用程式」表格中選擇應用程式。
3. 從「動作」功能表選擇「評估復原」。
4. 在執行復原能力評估對話方塊中，您可以輸入唯一的名稱或使用產生的評估名稱。
5. 選擇執行。

   若要檢閱評估報告，請在應用程式中選擇評估。如需詳細資訊，請參閱 the section called “檢閱評估報告”。

若要從評估索引標籤執行恢復能力評估

您可以在應用程式或恢復原則變更時執行新的恢復能力評估。

1. 在左側導覽選單中，選擇「應用程式」。
2. 從「應用程式」表格中選擇應用程式。
3. 選擇「評估」標籤。
4. 選擇執行復原能力評估。

5. 在執行復原能力評估對話方塊中，您可以輸入唯一的名稱或使用產生的評估名稱。
6. 選擇執行。

   若要檢閱評估報告，請在應用程式中選擇評估。如需詳細資訊，請參閱 the section called “檢閱評估報告”。

檢閱評估報告

您可以在應用程式的 [評量] 檢視中找到評估報告。

尋找評估報告

1. 在左側導覽選單中，選擇「應用程式」。
2. 在應用程式中，開啟應用程式。
3. 在評估標籤中，從彈性評量表中選擇評估報告。

當您開啟報表時，您會看到下列內容：

- 評估報告的整體概述
- 改善彈性的建議。
- 設置警報，SOP 和測試的建議
- 如何創建和管理標籤以搜索和過濾您的 AWS 資源

檢閱

本節提供評估報告的概觀。 AWS Resilience Hub 列出每個中斷類型和相關的應用程式元件。它也會列出您實際的 RTO 和 RPO 原則，並決定應用程式元件是否可以達成原則目標。

概觀

顯示應用程式的名稱、恢復原則的名稱以及報告的建立日期。

RTO

顯示預估應用程式是否符合復原原則目標的圖形表示。這是基於應用程序可以關閉的時間量而不會對組織造成重大損害。評估提供估計的工作量 RTO。

RPO

顯示預估應用程式是否符合復原原則目標的圖形表示。這是根據資料在企業造成重大傷害之前遺失的時間量而定。評估提供估計的工作負載 RPO。

詳細資訊

使用 [所有結果] 和 [應用程式符合性漂移] 索引標籤，提供各中斷類型的詳細 [所有結果] 索引標籤會顯示所有中斷，包括符合性漂移，而 [應用程式符合性漂移] 索引標籤只會顯示符合性漂移 中斷類型包括應用程式、雲端基礎結構 (基礎結構和可用區域) 和區域，並提供下列相關資訊：

- AppComponent

  構成應用程式的資源。例如，您的應用程式可能具有資料庫或運算元件。

- 估計 RTO

  指出您的原則組態是否符合您的原則需求。我們提供兩個值：我們的估計 RTO 和您的目標 RTO。例如，如果您在「目標 RTO」下看到 2h 值，在「估計工作負載 RTO」下看到 40m，表示我們提供 40 分鐘的估計工作負載 RTO，而您應用程式目前的 RTO 為兩小時。我們將估計的工作負載 RTO 計算基於配置，而不是策略。因此，無論您選取哪個原則，多重可用區域資料庫在可用區域失敗時，都會具有相同的預估工作負載 RTO。
- RTO 漂移

  指出您的應用程式偏離先前成功評估的預估工作負載 RTO 的持續時間。我們提供兩個值，即我們的估計 RTO 和 RTO 漂移。例如，如果您在「預估 RTO」下看到 2h 值，在 RT O 漂移下看到 40m，則表示您的應用程式偏離先前成功評估的估計工作負載 RTO 40 分鐘。

- 估計的投資回收

  根據您為每個應用程式元件設定的目標 RPO 原則，顯示預 AWS Resilience Hub 估的實際預估工作負載 RPO 原則。例如，您可能已將可用區域故障的恢復原則中的 RPO 目標設定為一小時。估計結果的計算結果可能接近零。這假設我們在其中提交每筆交易的 Amazon Aurora 在六個節點中的四個節點中成功，橫跨多個可用區域。 point-in-time 還原可能需要五分鐘。

  您可以選擇不提供的唯一 RTO 和 RPO 目標是「區域」。對於某些應用程式而言，當 AWS 服務存在關鍵依存時進行復原規劃，而該服務可能在整個區域無法使用時，這會很有用。

  如果您選擇此選項，例如為區域設定 RTO 或 RPO 目標，您將收到此類失敗的估計復原時間和作業建議。
- 反应组织漂移

指出您的應用程式偏離先前成功評估的預估工作負載 RPO 的持續時間。我們提供兩個值，即我們的估計 RPO 和 RPO 漂移。例如，如果您在「預估 RPO」下看到 2h 值，在 RPO 漂移下看到 40m，則表示您的應用程式偏離先前成功評估的估計工作負載 RPO 40 分鐘。

複查復原建議

備援建議會評估應用程式元件，並建議如何依據估計的工作負載 RTO 和估計的工作負載 RPO、成本和最小變更進行最佳化建議。

使用時 AWS Resilience Hub，您可以使用為什麼選擇此選項中的下列建議選項之一來最佳化恢復能力：

> **Note**
>
> - AWS Resilience Hub 最多提供三個 AWS Resilience Hub 建議選項。
> - 如果您設定區域 RTO 和 RPO 目標，則會在建議的選項中 AWS Resilience Hub 顯示針對區域 RTO /RPO 進行最佳化。如果未設定區域 RTO 和 RPO 目標，則會顯示最佳化可用區域 (AZ) RTO /R PO。如需在建立復原原則時設定區域性 RT/RPO 目標的詳細資訊，請參閱。建立復原原則
> - 應用程式及其組態的預估工作負載 RTO 和預估工作負載 RPO 值是透過考量資料量和個別來決定。 AppComponents但是，這些值只是估計值。您應該使用自己的測試 (例如 Amazon 故障注入服務) 來測試應用程式的實際復原時間。

針對可用性區域 RTO /RPO 進行最佳化

可用區域 (AZ) 中斷期間的最低估計工作負載回復時間 (RT/RPO)。如果您的組態無法充分變更以符合 RTO 和 RPO 目標，系統會通知您最低的預估工作負載 AZ 復原時間，讓您的組態接近符合原則的可能性。

針對區域 RTO /RPO 進行最佳化

區域中斷期間的最低估計工作負載回復時間 (RT/RPO)。如果您的組態無法充分變更以符合 RTO 和 RPO 目標，系統會通知您最低的預估工作負載區域復原時間，讓您的設定接近符合原則的可能性。

最佳化成本

您可以承擔的最低成本，但仍然符合您的恢復原則。如果您的組態無法充分變更以符合最佳化目標，系統會告知您可能產生的最低成本，讓組態接近符合原則的可能性。

優化最小的變化

達成政策目標所需的最低變更。如果您的組態無法充分變更以符合最佳化目標，系統會通知您建議的變更，這些變更可讓您的設定接近符合原則的可能性。

下列項目包含在最佳化類別劃分中：

- Description

  描述建議的組態 AWS Resilience Hub。
- 變更

  文字變更清單，說明切換至建議組態的必要工作。
- 基本成本

  與建議變更相關的預估成本。

  > **Note**
  >
  > 基本費用可能會根據使用情況而有所不同，並且不包括企業折扣計劃 (EDP) 的任何折扣或優惠。
- 估計的工作量 RTO 和 RPO

  預估的工作負載 RTO 和變更後的預估工作負載 RPO。

AWS 彈性中樞會評估應用程式元件 (AppComponent) 是否可以遵守復原政策。如果 AppComponent 不符合彈性政策，且 AWS Resurance Hub 無法提出任何建議以促進合規，則可能是因為 AppComponent 無法在限制範圍內達到所選取的復原時間。 AppComponent AppComponent 限制範例包括資源類型、儲存區大小或資源組態。

若要促進 AppComponent 與復原原則的符合性，請變更的資源類型 AppComponent 或更新恢復原則，以與資源可提供的內容保持一致。

檢閱作業建議

操作建議包含通過 AWS CloudFormation 模板設置警報，SOP 和 AWS FIS 實驗的建議。

AWS Resilience Hub 提供 AWS CloudFormation 範本檔案，供您下載及管理應用程式的基礎架構作為程式碼。因此，我們會在中提供建議，以 AWS CloudFormation 便您可以將它們新增至應用程式程式碼。如果 AWS CloudFormation 範本檔案的大小超過一 MB 且包含 500 個以上的資源，則 AWS Resilience Hub 會產生一個以上的 AWS CloudFormation 範本檔案，其中每個檔案的大小不超過一 MB 且最多包含 500 個資源。如果 AWS CloudFormation 範本檔案分割成多個檔案，則會附加 AWS CloudFormation 範本檔名`partXofY`，其中`X`表示順序中的檔案編號，並`Y`表示 AWS CloudFormation 樣板檔分成的檔案總數。例如，如果範本檔案分`big-app-template5-Alarm-104849185070-us-west-2.yaml`為四個檔案，檔案名稱將如下所示：

- `big-app-template5-Alarm-104849185070-us-west-2-part1of4.yaml`
- `big-app-template5-Alarm-104849185070-us-west-2-part2of4.yaml`
- `big-app-template5-Alarm-104849185070-us-west-2-part3of4.yaml`
- `big-app-template5-Alarm-104849185070-us-west-2-part4of4.yaml`

但是，如果是大型 AWS CloudFormation 範本，系統會要求您提供 Amazon 簡單儲存服務 URI，而不是將 CLI /API 與本機檔案作為輸入一起使用。

在中 AWS Resilience Hub，您可以執行下列動作：

- 您可以佈建所選警報、SOP 和 AWS FIS 實驗。若要佈建警示、SOP 和 AWS FIS 實驗，請選取適當的建議並輸入唯一名稱。 AWS Resilience Hub 根據您選取的建議建立範本。在範本中，您可以透過 Amazon 簡單儲存服務 (Amazon S3) URL 存取您建立的範本。
- 您可以隨時包含或排除針對應用程式建議的所選警示、SOP 和 AWS FIS 實驗。若要取得更多資訊，請參閱the section called “包括或排除操作建議”。
- 您也可以搜尋、建立、新增、移除和管理應用程式的標籤，並查看與該應用程式相關聯的所有標籤。

包括或排除操作建議

AWS Resilience Hub 提供包含或排除警示、SOP 和 AWS FIS 實驗 (測試) 的選項，這些建議用於在任何時間點提高應用程式的彈性分數。只有在您執行新的評估之後，包括和排除作業建議，才會影響應用程式的彈性分數。因此，我們建議您執行評估以取得更新的彈性分數，並瞭解其對應用程式的影響。

如需有關限制權限以包含或排除每個應用程式之建議的詳細資訊，請參閱the section called “限制權限以包含或排除 AWS Resilience Hub 建議”。

若要在應用程式中包含或排除作業建議

1. 在左側導覽選單中，選擇「應用程式」。
2. 在應用程式中，開啟應用程式。
3. 選擇「評估」，然後從「復原能力評量」表中選取評估。如果您沒有評估，請完成中的程序，the section called “執行復原能力評估”然後返回此步驟。
4. 選取作業建議索引標籤。
5. 若要在應用程式中包含或排除作業建議，請完成下列程序：

在應用程式中包含或排除建議的警示

1. 若要排除鬧鐘，請完成以下步驟：
   a. 在 [警示] 索引標籤下的 [警示] 表中，選取您要排除的所有警示 (具有 [未執行] 狀態)。您可以從「狀態」(State) 欄中識別警示的目前實作狀態。
   b. 從動作中，選擇排除選取項目。
   c. 從 [排除建議] 對話方塊中，選取下列其中一個原因 (選用)，然後選擇 [排除選取項目]，將選取的警示從應用程式中排除。
      - 已實作 — 如果您已在 Amazon 或任何其他第三方服務供應商等 AWS 服務中實作這些警示 CloudWatch，請選擇此選項。
      - 不相關 — 如果鬧鐘不符合您的業務需求，請選擇此選項。
      - 實施太複雜 — 如果您認為這些警報太複雜而無法實施，請選擇此選項。
      - 其他 — 選擇此選項可指定排除建議的任何其他原因。
2. 若要包含鬧鐘，請完成以下步驟：
   a. 在 [警示] 索引標籤下的 [警示] 表中，選取您要包含的所有警示 (具有已排除狀態)。您可以從「狀態」(State) 欄中識別警示的目前實作狀態。
   b. 在動作中，選擇包括所選項目。
   c. 從 [包含建議] 對話方塊中，選擇 [包含選取項目]，將所有選取的警示包含在應用

在您的應用程式中包含或排除建議的標準作業程序 (SOP)

1. 若要排除建議的 SOP，請完成以下步驟：

a. 在 [標準作業程序] 索引標籤下的 [SOP] 表中，選取您要排除的所有 SOP (具有 [已執行] 或 [未執行] 狀態)。您可以從 [狀態] 資料行識別 SOP 的目前實作狀態。

b. 在動作中，選擇排除選取項目，將選取的 SOP 從您的應用程式中排除。

c. 從 [排除建議] 對話方塊中，選取下列其中一個原因 (選用)，然後選擇 [排除選取項目]，將選取的 SOP 從應用程式中排除。

- 已實作 — 如果您已在服務或任何其他第三方 AWS 服務提供者中實作這些 SOP，請選擇此選項。
- 不相關 — 如果 SOP 不符合您的業務需求，請選擇此選項。
- 實施太複雜 — 如果您認為這些 SOP 太複雜而無法實施，請選擇此選項。
- 無 — 如果您不想指定原因，請選擇此選項。

2. 若要包含 SOP，請完成以下步驟：

a. 在標準操作程序選項卡下，從 SOP 表中，選擇要包含的所有警報（具有已排除狀態）。您可以從「狀態」(State) 欄中識別警示的目前實作狀態。

b. 在動作中，選擇包括所選項目。

c. 在「包含建議」對話方塊中，選擇「包含選取項目」，將所有選取的 SOP 包含在您的應用

在應用程式中包含或排除建議的測試

1. 若要排除建議的測試，請完成以下步驟：

a. 在故障注入實驗模板選項卡下，從故障注入實驗模板表中，選擇要排除的所有測試（具有「已實施」或「未實現」狀態）。您可以從「狀態」(State) 欄中識別測試的目前實作狀態。

b. 從動作中，選擇排除選取項目。

c. 從排除建議對話方塊中，選取下列其中一個原因 (選用)，然後選擇排除選取項以從應用程式中排除選取的 AWS FIS 實驗。

- 已實作 — 如果您已在服務或任何其他第三方 AWS 服務提供者中實作這些測試，請選擇此選項。
- 不相關 — 如果測試不符合您的業務需求，請選擇此選項。
- 實施太複雜 — 如果您認為這些測試太複雜而無法實施，請選擇此選項。
- 無 — 如果您不想指定原因，請選擇此選項。

2. 若要包含建議的測試，請完成以下步驟：

a. 在故障注入實驗模板選項卡下，從故障注入實驗模板表中，選擇要包含的所有測試（具有已排除狀態）。您可以從「狀態」(State) 欄中識別測試的目前實作狀態。

b. 在動作中，選擇包括所選項目。

c. 在「包含建議」對話方塊中，選擇「包含選取項目」，將所有選取的測試包括在您的

刪除恢復能力評估

您可以在應用程式的 [評估] 檢視中刪除恢復能力評估。

若要刪除恢復能力評估

1. 在左側導覽選單中，選擇「應用程式」。
2. 在應用程式中，開啟應用程式。
3. 在評估中，選擇彈性評估表格中的評估報告。
4. 如要確認刪除，請選擇 Delete (刪除)。

   報告不會再顯示在「復原能力評估」表格中。

管理警示

當您執行恢復能力評估時，作為操作建議的一部分， AWS Resilience Hub 建議設定 Amazon CloudWatch 警示以監控應用程式彈性。我們建議您根據目前應用程式組態的資源和元件來執行這些警示。如果應用程式中的資源和元件有所變更，您應執行復原能力評估，以確保針對更新的應用程式提供正確的警示。

AWS Resilience Hub 提供一個模板文件（`README.md`），允許您創建由 AWS Resilience Hub 內部 AWS （如 Amazon CloudWatch）或外部推薦的警報 AWS。警示中提供的預設值是以建立這些警示所使用的最佳作法為基礎。

主題

- 根據操作建議建立警示
- 檢視鬧鐘

根據操作建議建立警示

AWS Resilience Hub 創建一個包含詳細信息的 AWS CloudFormation 模板，以在 Amazon 中創建選定的警報 CloudWatch。產生範本後，您可以透過 Amazon S3 URL 存取該範本、下載該 URL 並將其放置在程式碼管道中，或透過 AWS CloudFormation 主控台建立堆疊。

若要根據建 AWS Resilience Hub 議建立警示，您必須為建議的警示建立 AWS CloudFormation 範本，並將它們包含在程式碼庫中。

若要在操作建議中建立警示

1. 在左側導覽選單中，選擇「應用程式」。
2. 在應用程式中選擇您的應用程式。
3. 選擇「評估」標籤。

   在彈性評估表格中，您可以使用下列資訊識別您的評量：

   - 名稱 — 您在建立時提供的評量名稱。
   - 狀態 — 指示評估的執行狀態。
   - 符合性狀態 — 指出評估是否符合復原原則。
   - 彈性漂移狀態 — 指出您的應用程式是否已從之前的成功評估中漂移。
   - 應用程式版本 — 應用程式的版本。
   - 呼叫者 — 指示呼叫評量的角色。
   - 開始時間 — 指示評估的開始時間。
   - 結束時間 — 指示評估的結束時間。
   - ARN — 評估的 Amazon 資源名稱 (ARN)。
4. 從「復原能力評估」表中選取評估。如果您沒有評估，請完成中的程序，the section called “執行復原能力評估”然後返回此步驟。
5. 選擇操作建議。
6. 如果預設未選取，請選擇 [警報] 索引標籤。

   在 [警示] 表格中，您可以使用下列指令來識別建議的警示：

   - 名稱 — 您為應用程式設定的警示名稱。
   - 描述 — 描述警示的目標。
   - 狀態 — 指出 Amazon CloudWatch 警示目前的實作狀態。

此欄會顯示下列其中一個值：

- 已實作 — 表示已在應用程式中實作建議的警示。 AWS Resilience Hub 選擇以下數字會篩選 [警報] 表格，以顯示應用程式中實作的所有建議警示。
- 未實作 — 表示建議的警示已包含 AWS Resilience Hub 在應用程式中，但未實作。選擇下列數字會篩選 [警報] 表格，以顯示應用程式中未實作的所有建議警示。
- 已排除 — 表示建議的警示已從您的應用程式中排除。 AWS Resilience Hub 選擇以下數字會篩選 [警報] 表格，以顯示從應用程式中排除的所有建議警示。如需包含和排除建議警示的詳細資訊，請參閱包含或排除操作建議。
- 非作用中 — 表示警示已部署到 Amazon CloudWatch，但在 Amazon 的狀態設定為不足。CloudWatch選擇下面的數字將過濾「警報」表，以顯示所有已實現和非活動的警報。

- 配置 — 指示是否有任何待處理的配置相依性需要解決。
- 類型 — 指示警示的類型。
- AppComponent— 指示與此警示相關聯的應用程式元件 (AppComponents)。
- 參照 ID — 指示中 AWS CloudFormation 堆疊事件的邏輯識別元 AWS CloudFormation。
- 建議 ID — 指示中 AWS CloudFormation 堆疊資源的邏輯識別元 AWS CloudFormation。

7. 在 [警示] 索引標籤中，若要根據特定狀態篩選 [警示] 表格中的警示建議，請選取相同狀態下的數字。
8. 選取您要為應用程式設定的建議警示，然後選擇 [建立 CloudFormation 範本]。
9. 在「建立 CloudFormation 樣板」對話方塊中，您可以使用自動產生的名稱，也可以在 AWS CloudFormation 範本名稱方塊中輸入CloudFormation 範本的名稱。
10. 選擇建立。這可能需要幾分鐘的時間來建立 AWS CloudFormation 範本。

    請完成下列程序，將建議包含在程式碼庫中。

包含您的代碼庫的 AWS Resilience Hub 建議

1. 選擇「範本」頁籤以檢視您剛建立的範本。您可以使用以下方法識別您的範本：

   - 名稱 — 您在建立時提供的評量名稱。
   - 狀態 — 指示評估的執行狀態。
   - 類型 — 指示作業建議的類型。
   - 格式 — 指示建立範本時所使用的格式 (JSON/ 文字)。
   - 開始時間 — 指示評估的開始時間。

- 結束時間 — 指示評估的結束時間。
- ARN-模板的 ARN

2. 在範本詳細資料下，選擇範本 S3 路徑下方的連結，以在 Amazon S3 主控台中開啟範本物件。
3. 在 Amazon S3 主控台的「物件」表格中，選擇 SOP 資料夾連結。
4. 若要複製 Amazon S3 路徑，請選取 JSON 檔案前面的核取方塊，然後選擇「複製 URL」。
5. 從 AWS CloudFormation 主控台建立 AWS CloudFormation 堆疊。如需建立 AWS CloudFormation 堆疊的詳細資訊，請參閱〈〉https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-create-stack.html。

   建立 AWS CloudFormation 堆疊時，您必須提供從上一步複製的 Amazon S3 路徑。

檢視鬧鐘

您可以檢視所有已設定用來監控應用程式恢復能力的作用中警示。 AWS Resilience Hub 使用 AWS CloudFormation 模板來存儲報警詳細信息，這些詳細信息依次用於在 Amazon CloudWatch 中創建警報。您可以使用 Amazon S3 URL 存取 AWS CloudFormation 範本，也可以下載範本並將其放置到程式碼管道中，或透過 AWS CloudFormation 主控台建立堆疊。

若要從儀表板檢視警示，請從左側導覽功能表中選擇 [儀表板]。在 [警示] 表格中，您可以使用下列資訊識別已實作的警示：

- 受影響的應用程式 — 已實作此警示的應用程式名稱。
- 作用中警報 — 指出從應用程式觸發的作用中警示數目。
- FIS 進行中 — 指出您的應用程式目前正在執行的 AWS FIS 實驗。

若要檢視應用程式中已實作的警示

1. 在左側導覽選單中，選擇「應用程式」。
2. 從「應用程式」表格中選取應用程式。
3. 在應用程式摘要頁面中，[已實作警示] 表格會顯示應用程式中實作的所有建議警示。

   若要在 [已實作警示] 表格中尋找特定警示，請在 [依文字、屬性或值尋找警示] 方塊中，選取下列其中一個欄位，選擇作業，然後輸入值。

   - 警示名稱 — 您為應用程式設定的警示名稱。

- 描述 — 描述警示的目標。
- 狀態 — 指示 Amazon CloudWatch 警示的目前實作狀態。

  此欄會顯示下列其中一個值：

  - 已實作 — 表示已在應用程式中實作建議的警示。 AWS Resilience Hub 選擇下面的數字，以在操作建議選項卡中查看所有建議和實施的警報。
  - 未實作 — 表示建議的警示已包含 AWS Resilience Hub 在應用程式中，但未實作。選擇下面的數字，以在操作建議標籤中檢視所有建議和未實作的警示。
  - 已排除 — 表示建議的警示已從您的應用程式中排除。 AWS Resilience Hub 選擇下面的數字，以在操作建議選項卡中查看所有建議警報和排除的警報。如需包含和排除建議警示的詳細資訊，請參閱包含或排除操作建議。
  - 非作用中 — 表示警示已部署到 Amazon CloudWatch，但在 Amazon 的狀態設定為不足。CloudWatch選擇下面的數字，以在「操作建議」標籤中檢視所有已導入和非作用中警示。
- 來源範本 — 提供包含警示詳細資訊之 AWS CloudFormation 堆疊的 Amazon 資源名稱 (ARN)。
- 資源 — 顯示此警示附加並實作的資源。
- 指標 — 顯示 CloudWatch 指派給警示的 Amazon 指標。如需有關 Amazon CloudWatch 指標的詳細資訊，請參閱 Amazon CloudWatch 指標。
- 上次變更 — 顯示上次修改警報的日期和時間。

若要檢視評估的建議警示

1. 在左側導覽選單中，選擇「應用程式」。
2. 從「應用程式」表格中選取應用程式。

   若要尋找應用程式，請在 [尋找應用程式] 方塊中輸入應用程式名稱。
3. 選擇「評估」標籤。

   在彈性評估表格中，您可以使用下列資訊識別您的評量：

   - 名稱 — 您在建立時提供的評量名稱。
   - 狀態 — 指示評估的執行狀態。
   - 符合性狀態 — 指出評估是否符合復原原則。
   - 彈性漂移狀態 — 指出您的應用程式是否已從之前的成功評估中漂移。
   - 應用程式版本 — 應用程式的版本。

- 呼叫者 — 指示呼叫評量的角色。
- 開始時間 — 指示評估的開始時間。
- 結束時間 — 指示評估的結束時間。
- ARN — 評估的 Amazon 資源名稱 (ARN)。

4. 從「復原能力評估」表中選取評估。
5. 選擇作業建議索引標籤。
6. 如果預設未選取，請選擇 [警報] 索引標籤。

   在 [警示] 表格中，您可以使用下列指令來識別建議的警示：

   - 名稱 — 您為應用程式設定的警示名稱。
   - 描述 — 描述警示的目標。
   - 狀態 — 指出 Amazon CloudWatch 警示目前的實作狀態。

     此欄會顯示下列其中一個值：

     - 已實作 — 表示警示已在您的應用程式中實作。選擇以下數字會篩選 [警報] 表格，以顯示應用程式中實作的所有建議警示。
     - 未實作 — 表示警示未實作或包含在您的應用程式中。選擇下列數字會篩選 [警報] 表格，以顯示應用程式中未實作的所有建議警示。
     - 已排除 — 表示警示已從應用程式中排除。選擇以下數字會篩選 [警報] 表格，以顯示從應用程式中排除的所有建議警示。如需包含和排除建議警示的詳細資訊，請參閱the section called “包括或排除操作建議”。
     - 非作用中 — 表示警示已部署到 Amazon CloudWatch，但在 Amazon 的狀態設定為不足。CloudWatch選擇下面的數字將過濾「警報」表，以顯示所有已實現和非活動的警報。
   - 配置 — 指示是否有任何待處理的配置相依性需要解決。
   - 類型 — 指示警示的類型。
   - AppComponent— 指示與此警示相關聯的應用程式元件 (AppComponents)。
   - 參照 ID — 指示中 AWS CloudFormation 堆疊事件的邏輯識別元 AWS CloudFormation。
   - 建議 ID — 指示中 AWS CloudFormation 堆疊資源的邏輯識別元 AWS CloudFormation。

標準作業程序

標準作業程序 (SOP) 是一組規定性的步驟，旨在在發生中斷或警示時有效地復原應用程式。事先準備、測試和測量 SOP，以確保在運營中斷時及時恢復。

根據您的應用程式元件，AWS Resilience Hub建議您應該準備的 SOP。 AWS Resilience Hub與 Systems Manager 合作，通過提供一些 SSM 文檔，您可以用作這些 SOP 的基礎來自動執行 SOP 的步驟。

例如，AWS Resilience Hub可能會根據現有的 SSM 自動化文件，建議使用 SOP 來新增磁碟空間。若要執行此 SSM 文件，您需要具有正確許可的特定 IAM 角色。 AWS Resilience Hub在應用程式中建立中繼資料，指出在磁碟不足時要執行的 SSM 自動化文件，以及執行該 SSM 文件所需的 IAM 角色。然後，此中繼資料會儲存在 SSM 參數中。

除了設定 SSM 自動化之外，最佳作法也是透過AWS FIS實驗進行測試。因此，AWS Resilience Hub還提供一個調用 SSM 自動化文檔的AWS FIS實驗-這樣，您可以主動測試應用程序，以確保您創建的 SOP 能夠完成預期的工作。

AWS Resilience Hub以您可以新增至應用程式程式碼基底的AWS CloudFormation範本形式提供建議。此範本提供：

- 具有執行 SOP 所需權限的 IAM 角色。
- 您可以用來測試 SOP 的AWS FIS實驗。
- SSM 參數，其中包含應用程式中繼資料，指出要做為 SOP 執行的 SSM 文件和哪個 IAM 角色，以及在哪個資源上執行。例如：`$(DocumentName) for SOP $(HandleCrisisA) on $(ResourceA)`。

創建 SOP 可能需要一些試驗和錯誤。針對您的應用程式執行復原能力評估，並從AWS Resilience Hub建議產生AWS CloudFormation範本是個好的開始。使用AWS CloudFormation範本產生AWS CloudFormation堆疊，然後在 SOP 中使用 SSM 參數及其預設值。運行 SOP 並查看您需要進行哪些改進。

因為所有應用程式都有不同的需求，所以AWS Resilience Hub提供的 SSM 文件預設清單不足以滿足您的所有需求。但是，您可以複製預設的 SSM 文件，並將其用作基礎，以建立專為您的應用程式量身打造的自訂文件。您也可以建立自己的全新 SSM 文件。如果您建立自己的 SSM 文件而不是修改預設值，則必須將它們與 SSM 參數產生關聯，以便在 SOP 執行時呼叫正確的 SSM 文件。

當您建立必要的 SSM 文件並視需要更新參數和文件關聯來完成 SOP 之後，請直接將 SSM 文件新增至程式碼基底，然後在該處進行任何後續變更或自訂。如此一來，每次部署應用程式時，您也會部署最多的 up-to-date SOP。

主題

- 根據建議構AWS Resilience Hub建 SOP

- 建立自訂 SSM 文件
- 使用自訂 SSM 文件而非預設文件
- 測試 SOP
- 檢視標準作業程序

根據建議構AWS Resilience Hub建 SOP

若要根據建AWS Resilience Hub議建置 SOP，您需要一個附加復原原則的AWS Resilience Hub應用程式，而且您必須針對該應用程式執行復原評估。復原能力評估會為您的 SOP 產生建議。

要根據建議構建 SOP，您必須為建AWS Resilience Hub議的 SOP 創建一個AWS CloudFormation模板，並將它們包含在代碼庫中。

建立 SOP 建議的AWS CloudFormation範本

1. 開啟 AWS Resilience Hub 主控台。
2. 在導覽窗格中，選擇 Applications (應用程式)。
3. 從應用程式清單中，選擇您要為其建立 SOP 的應用程式。
4. 選擇「評估」標籤。
5. 從「復原能力評估」表中選取評估。如果您沒有評估，請完成中的程序，the section called “執行復原能力評估”然後返回此步驟。
6. 在作業建議下，選擇標準作業程序。
7. 選取您要包含的所有 SOP 建議。
8. 選擇 [建立 CloudFormation 範本]。這可能需要幾分鐘的時間來建立AWS CloudFormation範本。

   請完成下列程序，將 SOP 建議包含在程式碼庫中。

若要在程式碼庫中包含AWS Resilience Hub建議

1. 在 [作業建議] 中選擇 [範本]。
2. 在範本清單中，選擇您剛建立的 SOP 範本名稱。

   您可以使用下列資訊識別應用程式中實作的 SOP：

   - SOP 名稱 — 您為應用程式定義的 SOP 名稱。
   - 說明 — 說明 SOP 的目標。

- SSM 文件 — 包含 SOP 定義之 SSM 文件的 Amazon S3 網址。
- 測試回合 — 包含最新測試結果的文件的 Amazon S3 URL。
- 來源範本 — 提供包含 SOP 詳細資料之AWS CloudFormation堆疊的 Amazon 資源名稱 (ARN)。

3. 在範本詳細資料下，選擇範本 S3 路徑中的連結，以在 Amazon S3 主控台中開啟範本物件。
4. 在 Amazon S3 主控台的「物件」表格中，選擇 SOP 資料夾連結。
5. 若要複製 Amazon S3 路徑，請選取 JSON 檔案前面的核取方塊，然後選擇複製 URL。
6. 從AWS CloudFormation主控台建立AWS CloudFormation堆疊。如需建立AWS CloudFormation堆疊的詳細資訊，請參閱〈〉https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-create-stack.html。

   建立AWS CloudFormation堆疊時，您必須提供從上一步複製的 Amazon S3 路徑。

建立自訂 SSM 文件

若要完全自動化應用程式復原，您可能需要在 Systems Manager 主控台中為 SOP 建立自訂 SSM 文件。您可以將現有的 SSM 文件修改為基礎，也可以建立新的 SSM 文件。

如需有關使用 Systems Manager 建立 SSM 文件的詳細資訊，請參閱逐步解說：使用文件建立器建立自訂的 Runbook。

如需 SSM 文件語法的相關資訊，請參閱 SSM 文件語法。

如需自動執行 SSM 文件動作的相關資訊，請參閱 Systems Manager 自動化動作參考。

使用自訂 SSM 文件而非預設文件

若要以您建立的自訂文件取代 SOP AWS Resilience Hub 建議的 SSM 文件，請直接在程式碼庫中工作。除了新增新的自訂 SSM 自動化文件之外，您還可以：

1. 新增執行自動化所需的 IAM 許可。
2. 新增AWS FIS實驗以測試 SSM 文件。
3. 新增 SSM 參數，該參數指向您要用作 SOP 的自動化文件。

一般而言，使用中建議的預設值，AWS Resilience Hub並視需要自訂它們是最有效率的。例如，視需要新增或移除 IAM 角色的許可、將AWS FIS實驗設定變更為指向新 SSM 文件，或變更 SSM 參數以指向新的 SSM 文件。

測試 SOP

如前所述，最佳做法是將AWS FIS實驗新增至 CI/CD 管線，以定期測試 SOP；這樣可確保在發生中斷時，它們已準備就緒。

測試AWS Resilience Hub提供的和自定義 SOP。

檢視標準作業程序

若要從應用程式檢視已實作的 SOP

1. 在左側導覽選單中，選擇「應用程式」。
2. 在應用程式中，開啟應用程式。
3. 選擇標準作業程序頁標。

   在標準作業程序摘要區段中，「已導入的標準作業程序」表格會顯示從 SOP 建議產生的 SOP 清單。

   您可以通過以下方式識別您的 SOP：

   - SOP 名稱 — 您為應用程式定義的 SOP 名稱。
   - SSM 文件 — 包含 SOP 定義的 Amazon EC2 Systems Manager 文件的 S3 網址。
   - 說明 — 說明 SOP 的目標。
   - 測試回合 — 包含最新測試結果的文件 S3 URL。
   - 參照 ID — 參照 SOP 建議的識別碼。
   - 資源 ID — 實作 SOP 建議之資源的識別碼。

若要從評估中檢視建議的 SOP

1. 在左側導覽選單中，選擇「應用程式」。
2. 從「應用程式」表格中選取應用程式。

   若要尋找應用程式，請在 [尋找應用程式] 方塊中輸入應用程式名稱。
3. 選擇「評估」標籤。

   在彈性評估表格中，您可以使用下列資訊識別您的評量：

   - 名稱 — 您在建立時提供的評量名稱。

- 狀態 — 指示評估的執行狀態。
- 符合性狀態 — 指出評估是否符合復原原則。
- 彈性漂移狀態 — 指出您的應用程式是否已從之前的成功評估中漂移。
- 應用程式版本 — 應用程式的版本。
- 呼叫者 — 指示呼叫評量的角色。
- 開始時間 — 指示評估的開始時間。
- 結束時間 — 指示評估的結束時間。
- ARN — 評估的 Amazon 資源名稱 (ARN)。

4. 從「復原能力評估」表中選取評估。
5. 選擇作業建議索引標籤。
6. 選擇標準作業程序頁標。

   在「標準作業程序」表格中，您可以使用下列資訊瞭解有關建議 SOP 的更多資訊：

   - 名稱 — 建議 SOP 的名稱。
   - 說明 — 說明 SOP 的目標。
   - 狀態 — 指示 SOP 目前的實作狀態。也就是說，「已實作」、「未實作」和「已排除」。
   - 配置 — 指示是否有任何待處理的配置相依性需要解決。
   - 類型 — 指示 SOP 的類型。
   - AppComponent— 指示與此 SOP 相關聯的應用程式元件 (AppComponents)。如需有關支援的詳細資訊 AppComponents，請參閱將 AppComponent.
   - 參照 ID — 指示中AWS CloudFormation堆疊事件的邏輯識別元AWS CloudFormation。
   - 建議 ID — 指示中AWS CloudFormation堆疊資源的邏輯識別元AWS CloudFormation。

Amazon 故障注入服務實驗

本節說明如何在中建立和執行 Amazon 故障注入服務 (AWS FIS) 實驗 AWS Resilience Hub。您可以執行 AWS FIS 實驗來衡量 AWS 資源的彈性，以及從應用程式、基礎結構、可用區域和 AWS 區域 事件復原所需的時間。

為了衡量彈性，這些 AWS FIS 實驗會模擬資源中斷。 AWS 中斷的範例包括網路無法使用的錯誤、容錯移轉、Amazon EC2 或 AWS ASG 上已停止的程序、Amazon RDS 中的啟動復原，以及可用區域的問題。 AWS FIS 實驗結束時，您可以估計應用程式是否可以從復原原則 RTO 目標中定義的中斷類型中復原。

中的所有實驗都 AWS Resilience Hub 是使用構建的 AWS FIS ，它們執行 AWS FIS 操作。大多數 AWS FIS 實驗都會呼叫 Systems Manager 自動化動作來執行中斷並監控警示，而其他 AWS FIS 實驗僅使用針對特定 AWS 服務自訂的 AWS FIS 自動化動作 (例如 Amazon EKS 動作)。如需有關 AWS FIS 動作的詳細資訊，請參閱AWS FIS 動作參考。

您可以在預設狀態下使用 AWS FIS 實驗，也可以根據您的需求自訂實驗。 AWS FIS 可以從 AWS Resilience Hub （ the section called “檢視故障注入實驗” ）或 AWS FIS 控制台（ AWS FIS ）訪問實驗。

主題

- 根據操作建議創建 AWS FIS 實驗
- 從運行 AWS FIS 實驗 AWS Resilience Hub
- 檢視故障注入實驗
- Amazon 故障注入服務實驗故障/狀態檢查

根據操作建議創建 AWS FIS 實驗

AWS Resilience Hub 建議您在執行評估報告後測試應用程式。您可以從應用程式的評估報告存取並執行這些實驗。

AWS Resilience Hub 提供了一個 AWS FIS 實驗列表，這些實驗是具有測試參數的 Systems Manager 文檔。當您從清單中選取 AWS FIS 實驗時， AWS Resilience Hub 會使用您在「Systems Manager」文件中定義的參數建立 AWS CloudFormation 樣板。建立 AWS CloudFormation 堆疊之後，您可以看到針對應用程式佈建的 AWS FIS 實驗。

AWS CloudFormation 範本包含每個 Systems Manager 文件的 IAM 角色，以及執行所需的最低權限。

要根據建 AWS Resilience Hub 議創建 AWS FIS 實驗，您必須為推薦的測試創建一個 AWS CloudFormation 模板，並將它們包含在代碼庫中。

建立 AWS FIS 實驗 AWS CloudFormation 樣板的步驟

1. 開啟主 AWS Resilience Hub 控台。
2. 在導覽窗格中，選擇 Applications (應用程式)。
3. 從應用程式清單中，選擇您要建立測試的應用程式。
4. 選擇評估標籤。
5. 從「復原能力評估」表中選取評估。如果您沒有評估，請完成中的程序，the section called “執行復原能力評估”然後返回此步驟。

6. 在操作建議下，選擇故障注入實驗。
7. 選取您要包含的所有測試。
8. 選擇 [建立 CloudFormation 範本]。這可能需要幾分鐘的時間來建立 AWS CloudFormation 範本。
9. 選擇 Templates (範本)。

   您可以在「範本」表中檢視新建立 AWS CloudFormation 的範本。

   請完成下列程序，將建議包含在程式碼庫中。

若要在程式碼庫中包含 AWS Resilience Hub 建議

1. 在作業建議中，選擇範本。
2. 在範本清單中，選擇您剛建立的 AWS FIS 實驗範本名稱。

   您可以使用下列資訊識別在應用程式中實作的測試：

   - 測試名稱 — 您為應用程式建立的測試名稱。
   - 描述 — 描述測試的目標。
   - 狀態 — 指示測試的目前實行狀態。

     此欄會顯示下列其中一個值：

     - 已實作 — 表示測試已在您的應用程式中實作。
     - 未實作 — 表示測試未實作或包含在您的應用程式中。
     - 已排除 — 表示測試已從應用程式中排除。
     - 非作用中 — 表示測試已部署至 AWS FIS，但在過去 30 天內尚未執行。
   - 測試回合 — 包含最新測試結果的文件的 Amazon S3 URL。
   - 來源範本 — 提供包含實驗詳細資料之 AWS CloudFormation 堆疊的 Amazon 資源名稱 (ARN)。
3. 在範本詳細資料下，選擇範本 S3 路徑中的連結，以在 Amazon S3 主控台中開啟範本物件。
4. 在 Amazon S3 主控台的「物件」表格中，選擇測試資料夾連結。
5. 若要複製 Amazon S3 路徑，請選取 JSON 檔案前面的核取方塊，然後選擇複製 URL。
6. 從 AWS CloudFormation 主控台建立 AWS CloudFormation 堆疊。如需建立 AWS CloudFormation 堆疊的詳細資訊，請參閱〈〉https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-create-stack.html。

建立 AWS CloudFormation 堆疊時，您必須提供從上一步複製的 Amazon S3 路徑。

從運行 AWS FIS 實驗 AWS Resilience Hub

在您的應用程式中，您必須先從操作建議中建立 AWS FIS 實驗範本，然後才 AWS Resilience Hub 能執行 AWS FIS 實驗。

開始 AWS FIS 實驗的步驟

1. 在左側導覽選單中，選擇「應用程式」。
2. 在「應用程式」表中，開啟應用程式。
3. 選擇故障注入實驗標籤。
4. 從實驗模板表中選擇用於創建要運行的實驗模板之前的單選按鈕，然後選擇開始實驗。

停止 AWS FIS 實驗的步驟

1. 在左側導覽選單中，選擇「應用程式」。
2. 在「應用程式」表中，開啟應用程式。
3. 選擇故障注入實驗標籤。
4. 從 [實驗] 表格中選取實驗前的選項按鈕，然後選擇 [停止實驗]。

檢視故障注入實驗

在中 AWS Resilience Hub，檢視您設定用來衡量 AWS 資源彈性的 AWS FIS 實驗，以及從應用程式、基礎結構、可用區域和 AWS 區域 事件復原所需的時間。

若要從儀表板檢視 AWS FIS 實驗，請從左側導覽功能表中選擇「儀表板」。在「實驗」表中，您可以使用下列資訊來識別已 AWS FIS 實作的實驗：

- 實驗 ID — 實 AWS FIS 驗的標識符。
- 實驗模板 ID — 用於創建 AWS FIS 實驗的實驗模板的標 AWS FIS 識符。
- 來源範本 — 提供包含 AWS FIS 實驗詳細資訊之 AWS CloudFormation 堆疊的 Amazon 資源名稱 (ARN)。
- 狀態 — 指示 AWS FIS 實驗是否成功完成。

若要從應用程式檢視已 AWS FIS 實作的實驗

1. 在左側導覽選單中，選擇「應用程式」。
2. 在「應用程式」表中，開啟應用程式。
3. 選擇故障注入實驗。
4. 選擇實驗標籤。

   在 [實驗] 索引標籤中，您可以在 [AWS FIS 實驗] 表格中看到目前實驗的清單。

   在實驗表中，您可以使用以下信息識別 AWS FIS 實現的實驗：

   - 測試名稱 — 用於建立 AWS FIS 實驗的 AWS 彈性中樞建議測試的名稱。
   - 實驗 ID — 實 AWS FIS 驗的標識符。
   - 描述 — 描述 AWS FIS 實驗的目標。
   - 創建時間-創建 AWS FIS 實驗的日期和時間。
   - 上次更新時間 — 上次更新 AWS FIS 實驗的日期和時間。
   - 來源範本 — 提供包含 AWS FIS 實驗詳細資訊之 AWS CloudFormation 堆疊的 Amazon 資源名稱 (ARN)。

若要從評量檢視建議的實驗

1. 在左側導覽選單中，選擇「應用程式」。
2. 從「應用程式」表格中選取應用程式。

   若要尋找應用程式，請在 [尋找應用程式] 方塊中輸入應用程式名稱。
3. 選擇評估標籤。

   在彈性評估表格中，您可以使用下列資訊識別您的評量：

   - 名稱 — 您在建立時提供的評量名稱。
   - 狀態 — 指示評估的執行狀態。
   - 符合性狀態 — 指出評估是否符合復原原則。
   - 彈性漂移狀態 — 指出您的應用程式是否已從之前的成功評估中漂移。
   - 應用程式版本 — 應用程式的版本。
   - 呼叫者 — 指示呼叫評量的角色。
   - 開始時間 — 指示評估的開始時間。

- 結束時間 — 指示評估的結束時間。
- ARN — 評估的 Amazon 資源名稱 (ARN)。

4. 從「復原能力評估」表中選取評估。
5. 選擇作業建議索引標籤。
6. 選擇故障注入實驗標籤。

   在故障注入實驗模板表中，您可以使用以下信息了解有關建議測試的更多信息：

   - 名稱 — 建議測試的名稱。
   - 描述 — 描述測試的目標。
   - 狀態 — 指示測試的目前實行狀態。

     此欄會顯示下列其中一個值：

     - 已實作 — 表示測試已在您的應用程式中實作。
     - 未實作 — 表示測試未實作或包含在您的應用程式中。
     - 已排除 — 表示測試已從應用程式中排除。
     - 非作用中 — 表示測試已部署至 AWS FIS，但在過去 30 天內尚未執行。
   - 配置 — 指示是否有任何待處理的配置相依性需要解決。
   - 類型 — 指示測試的類型。
   - AppComponent— 指示與此測試相關聯的應用程式元件 (AppComponents)。如需有關支援的詳細資訊 AppComponents，請參閱將 AppComponent.
   - 風險 — 指示測試失敗的風險等級。風險等級分別使用「高」、「中」和「低」來表示高、中度和低風險等級。
   - 參照 ID — 指示中 AWS CloudFormation 堆疊事件的邏輯識別元 AWS CloudFormation。
   - 建議 ID — 指示中 AWS CloudFormation 堆疊資源的邏輯識別元 AWS CloudFormation。

Amazon 故障注入服務實驗故障/狀態檢查

AWS Resilience Hub 允許您跟踪已開始實驗的狀態。如需詳細資訊，請參閱中的欲從評估程序檢視建議的實驗the section called “檢視故障注入實驗”。

主題

- 使用 AWS Systems Manager 分析 AWS FIS 實驗執行
- AWS FIS 在測試在亞馬遜彈性 Kubernetes 服務叢集中執行的 Kubernetes 網繭時進行實驗失敗

使用 AWS Systems Manager 分析 AWS FIS 實驗執行

運行 AWS FIS 實驗後，您可以在 AWS Systems Manager 中查看執行詳細信息。

1. 移至 CloudTrail> 事件歷史記錄。
2. 使用實驗 ID 按用戶名過濾事件。
3. 檢視項 StartAutomationExecution 目。要求識別碼是 SSM 自動化識別碼。
4. 移至 AWS Systems Manager > 自動化。
5. 使用 SSM 自動化 ID 依執行 ID 篩選，並檢視自動化詳細資料。

   您可以使用任何 Systems Manager 自動化來分析執行。如需詳細資訊，請參閱 AWS Systems Manager Automation 使用者指南。執行輸入參數會顯示在「執行詳細資訊」的「輸入參數」區段中，並包含未出現在 AWS FIS 實驗中的選用參數。

   您可以向下鑽研至「執行」步驟中的特定步驟，來尋找有關步驟狀態和其他步驟詳細資訊的資訊。

常見故障

以下是執行評估報告時遇到的常見失敗：

- 在執行測試 /SOP 實驗之前，未部署警報範本。這會在自動化步驟期間產生錯誤訊息。
  - 失敗訊息：`The following parameters were not found: [/ResilienceHub/Alarm/3dee49a1-9877-452a-bb0c-a958479a8ef2/nat-gw-alarm-bytes-out-to-source-2020-09-21_nat-02ad9bc4fbd4e6135]. Make sure all the SSM parameters in automation document are created in SSM Parameter Store.`
  - 修復：在重新執行故障注入實驗之前，請確保呈現相關警示並部署產生的範本。
- 缺少執行角色的權限。如果提供的執行角色缺少權限並出現在步驟詳細資料中，就會發生此錯誤訊息。
  - 失敗訊息：`An error occurred (Unauthorized Operation) when calling the DescribeInstanceStatus operation: You are not authorized to perform this operation. Please Refer to Automation Service Troubleshooting Guide for more diagnosis details。`
  - 補救：確認您提供了正確的執行角色。如果這樣做，請新增所需的權限，然後重新執行評估。
- 執行成功，但沒有預期的結果。這是參數不正確或內部自動化問題所造成的結果。
  - 失敗訊息：執行成功，因此不會顯示錯誤訊息。

- 補救：檢查輸入參數並查看分析 AWS FIS 實驗執行中所述的執行步驟，然後檢查各個步驟以獲得預期的輸入和輸出。

AWS FIS 在測試在亞馬遜彈性 Kubernetes 服務叢集中執行的 Kubernetes 網繭時進行實驗失敗

以下是在測試 Amazon EKS 叢集中執行的 Kubernetes 網繭時遇到的常見亞馬遜彈性 Kubernetes 服務 (Amazon EKS) 故障：

- 針對 AWS FIS 實驗或 Kubernetes 服務帳戶設定不正確的 IAM 角色。
  - 失敗訊息：
    - `Error resolving targets. Kubernetes API returned ApiException with error code 401.`
    - `Error resolving targets. Kubernetes API returned ApiException with error code 403.`
    - `Unable to inject AWS FIS Pod: Kubernetes API returned status code 403. Check Amazon EKS logs for more details.`
  - 修正：確認下列項目。
    - 請確定您已遵循使用 AWS FISaws:eks:pod動作中的指示。
    - 請確定您已建立並設定具有必要 RBAC 權限和正確命名空間的 Kubernetes 服務帳戶。
    - 確定您已將提供的 IAM 角色 (請參閱測試 AWS CloudFormation 堆疊的輸出) 對應至 Kubernetes 使用者。
- 無法啟動 AWS FIS Pod：已達到最大失敗的邊車容器。這通常發生在內存不足以運行 AWS FIS 側車容器時。
  - 失敗訊息：`Unable to heartbeat FIS Pod: Max failed sidecar containers reached`。
  - 修復：避免此錯誤的一個選項是降低目標負載百分比，使其與可用記憶體或 CPU 保持一致。
- 警報斷言在實驗開始時失敗。因為相關警示沒有資料點，就會發生這個錯誤。
  - 失敗訊息：`Assertion failed for the following alarms`。列出宣告失敗的所有警示。
  - 補救：確定已針對警示正確安裝容器見解，且警示未開啟 (ALARM處於狀態)。

了解彈性分數

本節說明如何 AWS Resilience Hub 量化不同中斷案例中的應用程式準備程度。

AWS Resilience Hub 提供彈性分數，代表應用程式的彈性狀態。此分數反映了應用程式遵循我們針對符合應用程式彈性原則、警示、標準作業程序 (SOP) 和測試的建議的程度。根據應用程式使用的資源類型，針對每種中斷類型 AWS Resilience Hub 建議警示、SOP 和一組測試。

最高彈性得分為 100 分。若要取得最佳分數或最高分，您必須在應用程式中實作所有建議的警示、SOP 和測試。例如， AWS Resilience Hub 建議使用一個警報和一個 SOP 進行一次測試。測試會執行並觸發警示，並啟動相關聯的 SOP。如果它們成功執行，且應用程式符合復原原則，則會收到接近或等於 100 點的復原分數。

執行第一次評估之後， AWS Resilience Hub 提供從應用程式中排除作業建議的選項。若要瞭解排除的建議對恢復能力分數的影響，您必須執行新的評估。不過，您可以隨時在應用程式中包含排除的建議，並執行新的評估。如需包含和排除警示、SOP 和測試建議的詳細資訊，請參閱the section called “包括或排除操作建議”。

存取應用程式的彈性分數

您可以從導覽功能表中選擇 [儀表板] 或 [應用程式]，以檢視應用程式的備援分數。

從儀表板存取彈性分數

1. 在左側導覽功能表中，選擇 [儀表板]。
2. 在隨時間推移的應用程式復原分數中，從選擇最多 4 個應用程式下拉式清單中選擇一或多個應用程式。
3. 復原分數圖表會顯示所有選取之應用程式的復原分數。

從應用程式存取彈性分數

1. 在左側導覽選單中，選擇「應用程式」。
2. 在應用程式中，開啟應用程式。
3. 選擇摘要。

   彈性分數圖表會顯示應用程式彈性分數最多一年的趨勢。 AWS Resilience Hub 顯示行動項目、彈性原則違規，以及使用下列項目改善和達到最大可能彈性分數所需解決的作業建議：

- 若要檢視需要完成以改善和達到最大可能恢復能力分數的行動項目，請選擇 [動作項目] 索引標籤。選取此選項後， AWS Resilience Hub 會顯示下列內容：
  - RT/RPO — 指出需要修復以解決應用程式彈性原則中違規的復原時間 (RT/RPO) 數目。選擇要在應用程式評估報告中檢視 RT/RPO 詳細資料的值。
  - 警示 — 指出需要在應用程式中實作的建議 Amazon CloudWatch 警示數量。選擇值以在應用程式的評估報告中檢視需要修復的 Amazon CloudWatch 警示。
  - SOP — 表示需要在您的應用程式中實作的建議 SOP 數目。選擇值以檢視應用程式評估報告中需要修正的 SOP。
  - FIS — 指出需要在應用程式中實作的建議測試數目。選擇值以檢視應用程式評估報告中需要修正的測試。
- 若要檢視影響彈性分數的每個元件的分數，請選擇「分數劃分」。選取此選項後， AWS Resilience Hub 會顯示下列內容：
  - RT/RPO 相容性 — 指出應用程式元件 (AppComponents) 與預估工作負載復原時間的相容性，以及應用程式復原原則中定義的目標復原時間。選擇要在應用程式評估報告中檢視 RT/RPO 估計值的值。
  - 實作警示 — 表示已實作 Amazon CloudWatch 警示的實際貢獻與其對應用程式彈性分數的最大可能貢獻比較。選擇值以在應用程式的評估報告中檢視已實作的 Amazon CloudWatch 警示。
  - SOP 實作 — 指出已實作 SOP 的實際貢獻與其對應用程式彈性分數的最大可能貢獻相比。選擇要在應用程式評估報告中檢視已實作 SOP 的值。
  - 實作 FIS 實驗 — 指出已實作測試的實際貢獻與其對應用程式彈性得分的最大可能貢獻相比。選擇要在應用程式評估報告中檢視已實作測試的值。
- 若要檢視彈性政策違規情況和作業建議，請選擇向右箭號以展開「政策違規與作業建議細分」區段。展開時， AWS Resilience Hub 會顯示以下內容：
  - 彈性原則違規 — 指出違反應用程式復原原則的應用程式元件數量。選擇 RTO /RPO 旁邊的值，即可在應用程式評估報告的 [備援建議] 索引標籤中檢視詳細資料。
  - 操作建議 — 指出尚未實作或執行的作業建議，使用 [未完成] 和 [已排除] 索引標籤來增強應用程式的復原能力。作業建議包括所有處於非作用中的建議，以及尚未實作的建議。

    若要檢視需要實行的作業建議，請選擇 [未完成] 索引標籤。選取此選項後， AWS Resilience Hub 會顯示下列內容：
    - 警示 — 指出需要實作的建議 Amazon CloudWatch 警示數量。
    - SOP — 指示需要實施的建議 SOP 數量。

- FIS — 指出需要執行的建議測試數目。

若要檢視從應用程式中排除的作業建議，請選擇 [已排除] 索引標籤。選取時， AWS Resilience Hub 會顯示下列內容：

- 警示 — 指出從應用程式中排除的建議 Amazon CloudWatch 警示數量。
- SOP — 指出從您的應用程式中排除的建議 SOP 數目。
- FIS — 指出從應用程式中排除的建議測試數目。

計算彈性分數

本節中的表格說明決定每個建議類型的評分元件和應用程式的彈性分數所 AWS Resilience Hub 使用的公式。 AWS Resilience Hub 針對每個建議類型的評分元件和應用程式的彈性分數所決定的所有結果值，都會四捨五入至最接近的點。例如，如果實施了三個警報中的兩個，則分數將是 13.33（2/3）* 20）分。此值將四捨五入至 13 點。如需有關表格內公式中使用之權重的詳細資訊，請參閱一the section called “重量 AppComponents 和中斷類型”節。

部分評分元件只能透過 `ScoringComponentResiliencyScore` API 取得。如需這種 API 的詳細資訊，請參閱 ScoringComponentResiliencyScore。

資料表

- 計算各建議類型評分元件的公式
- 計算彈性得分的公式
- 用於計算彈性分數 AppComponents 和中斷類型的公式

下表說明用 AWS Resilience Hub 來計算每個建議類型評分元件的公式。

計算各建議類型評分元件的公式

評分元件	描述	公式	範例
測試覆蓋範圍 (T)	根據成功實施和排除的測試次數，超出 AWS Resilience Hub 建議測試總數的標準化分數（0 -100 分）。	`T = ((Total number of tests implemented) + (Total number of tests excluded)) / (Total number`	如果您在 20 個 AWS Resilience Hub 建議測試中實施了 10 個並排除了 5 個測試，則測試

評分元件	描述	公式	範例
	Note 若要計算彈性分數，建議的測試必須在過去 30 天內成功執行，才能 AWS Resilience Hub 將其視為已實作。	of tests recommended) 公式的各個部分如下： • 配置的測試總數 — 指示在 AWS CloudFormation 控制台中創建和上傳 AWS CloudFormation 模板時配置的測試總數。 • 建議的測試總數 — 指出 AWS Resilience Hub 根據應用程式資源建議的測試。 • 排除的測試總數 — 指出您已從應用程式中排除的建議測試次數。	涵蓋範圍的計算方式如下： T = (10 + 5) / 20 那就是 T = .75 or 75 points

評分元件	描述	公式	範例
警報覆蓋範圍 (A)	標準化分數 (0 -100 分) 是根據成功實作和排除的 Amazon CloudWatch 警示數量，超出 AWS Resilience Hub 建議的 Amazon CloudWatch 警示總數。 **Note** 若要計算彈性分數，建議的警示應處於 [就緒] 狀態，以 AWS Resilience Hub 便將其視為已實作。	`A = ((Total number of alarms implemented) + (Total number of alarms excluded)) / (Total number of alarms recommended)` 公式的各個部分如下： • 設定的警示總數 — 指出在 AWS CloudFormation 主控台中建立和上傳 AWS CloudFormation 範本時設定的 Amazon CloudWatch 警報總數。 • 建議的警示總數 — 指出 AWS Resilience Hub 根據應用程式資源建議的 Amazon CloudWatch 警示。 • 排除的警示總數 — 指出您從應用程式中排除的建議 Amazon CloudWatch 警示數量。	如果您在 20 個 AWS Resilience Hub 建議的 Amazon CloudWatch 警報中實施了 10 個並排除了 5 個 Amazon CloudWatch 警報，則 Amazon CloudWatch 警報涵蓋範圍的計算方式如下： `A = (10 + 5) / 20` 那就是 `A = .75 or 75 points`

評分元件	描述	公式	範例
SOP 覆蓋範圍 (S)	基於成功實施和排除的 SOP 數量，超出建議的 SOP 總數的標準化分數（0 -100 分 AWS Resilience Hub ）。	`S = ((Total number of SOPs implemented) + (Total number of SOPs excluded)) / (Total number of SOPs recommended)` 公式的各個部分如下： • 配置的 SOP 總數 — 指示在控制台中創建和上傳 AWS CloudFormation 模板時配置的 SOP 總數。 AWS CloudFormation • 建議的 SOP 總數 — 指示 AWS Resilience Hub 根據應用程式資源建議的 SOP。 • 排除的 SOP 總數 — 指出您已從應用程式中排除的建議 SOP 數目。	如果您在 20 個 AWS Resilience Hub 建議的 SOP 中實施了 10 個並排除了 5 個 SOP，則 SOP 涵蓋範圍的計算方式如下： `S = (10 + 5) / 20` 那就是 `S = .75 or 75 points`

評分元件	描述	公式	範例

RT/RPO 法規遵循 () P	以符合其彈性原則的應用程式為基礎的標準化分數 (0 -100 分)。	`P = Total weights of disruption types meeting the application's resiliency policy / Total weights of all disruption types .`	如果您的應用程式恢復原則僅符合可用區域 (AZ) 和基礎架構中斷類型，則恢復原則分數 (P) 的計算方式如下：
			• 如果您已設定區域 RTO 和 RPO 目標，計算P方式如下：
			`P = (20 + 30)/ 100`
			那就是 `P = .5 or 50 points`
			• 如果您尚未設定區域 RTO 和 RPO 目標，計算方P式如下：
			`P = (22.22 + 33.33)/ 99.9`
			那就是 `P = .55 or 55 points`

下表說明用來計算整個應用程式彈性分數的公式。 AWS Resilience Hub

計算彈性得分的公式

評分元件	描述	公式	範例
應用程式的彈性分數 () RS	根據您的應用程式符合其復原原則的標準化彈性分數 (0-100 分)。每個應用程式的彈性分數是所有建議類型的加權平均值。那就是：RS = Weighted Average (T, A, S, P)	每個應用程式的彈性分數是使用下列公式計算：RS = (T * Weight(T) + A * Weight(A) + S * Weight(S) + P * Weight(P)) / (Weight(T) + Weight(A) + Weight(S) + Weight(P))	計算每個建議類型表格涵蓋範圍的公式如下： • Test coverage (T) = .75 • Alarms (A) = .75 • SOPs (S) = .75 • Meeting resiliency policy (P) = .5 每個應用程式的彈性分數計算方式如下： RS = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) /(.2 + .2 + .2 + .4) 那就是 RS = .65 or 65 points

下表說明用來計算應用程 AWS Resilience Hub 式元件 (AppComponents) 和中斷類型之復原分數的公式。不過，您只能透過下列 AWS 彈性中樞 API 取得彈性分數 AppComponents 和中斷類型：

- DescribeAppAssessment以獲得 RSo
- ListAppComponentCompliances獲得RSao和 RSA

用於計算彈性分數 AppComponents 和中斷類型的公式

評分元件	描述	公式	範例
每個中斷類型 AppComponent 和每個中斷類型的彈性分數 () RSao	一個標準化分數（0 -100 分），根據每個中斷類型的 AppComponent 滿足其彈性政策。每個中斷類型 AppComponent 和每個中斷類型的彈性分數是所有建議類型的加權平均值。 那就是：RSao = Weighted Average (T, A, S, P) 的值T, A, S, P是針對和中斷類型的所有建議測試、警示、SOP 和會議恢復原則計算的。AppComponent	每個中斷類型 AppComponent 和每個中斷類型的彈性分數是使用下列公式計算： RSao = (T * Weight(T) + A * Weight(A) + S * Weight(S) + P * Weight(P)) / (Weight(T) + Weight(A) + Weight(S) + Weight(P))	RSao所有建議類型的假設如下： • Test coverage (T) = .75 • Alarms (A) = .75 • SOPs (S) = .75 • Meeting resiliency policy (P) = .5 每個 AppComponent 和中斷類型的彈性分數計算方式如下： RSao = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) / (.2 + .2 + .2 + .4) 那就是 RSao = .65 or 65 points

評分元件	描述	公式	範例

每 () 的彈性分 AppCompon ent 數 RSa	基於滿足其彈性政策的標準化分數 (0 -100 分) 。每個彈性分數 AppCompon ent 是所有建議類型的加權平均值。那就是：RSa = Weighted Average (T, A, S, P)
	
	的值T, A, S, P是針對所有建議的測試、警示、SOP 和符合恢復原則計算的. AppCompon ent
		每個彈性分數 AppComponent 是使用下列公式計算：
		
		`RSa = (T * Weight(T) +`
		
		`A * Weight(A) +`
		
		`S * Weight(S) +`
		
		`P * Weight(P)) /`
		
		`(Weight(T) + Weight(A) + Weight(S) + Weight(P))`
			RSa所有建議類型的假設如下：
			
			• `Test coverage (T) = .75`
			• `Alarms (A) = .75`
			• `SOPs (S) = .75`
			• `Meeting resiliency policy (P) = .5`
			
			每個彈性分數的計算 AppComponent 方式如下：
			
			`RSa = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) / (.2 + .2 + .2 + .4)`
			
			那就是 RSa = .65 or 65 points

評分元件	描述	公式	範例
每個中斷類型的彈性分數 () RSo	基於滿足其彈性政策的標準化分數（0 -100 分）。每個中斷類型的彈性分數是所有建議類型的加權平均值。那就是：RSo = Weighted Average (T, A, S, P) 的值會針T, A, S, P對中斷類型的所有建議測試、警示、SOP 和會議恢復原則計算。	每個中斷類型的彈性分數是使用下列公式計算： RSo = (T * Weight(T) + A * Weight(A) + S * Weight(S) + P * Weight(P)) / (Weight(T) + Weight(A) + Weight(S) + Weight(P))	RSo所有建議類型的假設如下： • Test coverage (T) = .75 • Alarms (A) = .75 • SOPs (S) = .75 • Meeting resiliency policy (P) = .5 每個中斷類型的彈性分數計算方式如下： RSo = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 *.4)) / (.2 + .2 + .2 + .4) 那就是 RSo = .65 or 65 points

重量

AWS Resilience Hub 為每個建議類型指派一個權重，以取得總彈性分數。

下表顯示警示、SOP、測試、會議恢復原則和中斷類型的權重。中斷類型包括應用程式、基礎架構、可用區域和區域。

> **Note**
>
> 如果您選擇不為您的原則定義區域 RTO 或 RPO 目標，其他中斷類型的加權會相應增加，如未定義區域時的權重欄中所示。

警示、SOP、測試、原則目標的權重

推薦類型	Weight
警示	二十個積分
麵包片	二十個積分
測試	二十個積分
會議恢復原則	四十點積分

中斷類型的權重

中斷類型	定義區域時的權重	未定義「區域」時的權重
應用程式	四十點積分	7 点和平原则
基礎設施	三十個積分	三十三点和平
可用區域	二十個積分	2 點評分
區域	十點積分	N/A

將操作建議整合到您的應用程式中 AWS CloudFormation

在 [作業建議] 頁面中選擇 [建 CloudFormation 立AWS CloudFormation範本] 之後，AWS Resilience Hub會建立描述應用程式之特定警示、標準作業程序 (SOP) 或AWS FIS實驗的範本。AWS CloudFormation範本存放在 Amazon S3 儲存貯體中，您可以在操作建議頁面的範本詳細資料索引標籤中查看範本的 S3 路徑。

例如，下列清單顯示 JSON 格式的範本，該AWS CloudFormation範本描述由所呈現的警示建議。AWS Resilience Hub這是一個名為的 DynamoDB 表的讀取節流警報。`Employees`

範本Resources區段說明 DynamoDB 表的讀取節流事件數目超過 1 時啟動的AWS::CloudWatch::Alarm警示。而這兩個AWS::SSM::Parameter資源定義的元數據，AWS Resilience Hub允許識別已安裝的資源，而無需掃描實際的應用程序。

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",
  "Parameters" : {
    "SNSTopicARN" : {
      "Type" : "String",
      "Description" : "The ARN of the SNS topic to which alarm status changes are to be
 sent. This must be in the same region being deployed.",
      "AllowedPattern" : "^arn:(aws|aws-cn|aws-iso|aws-iso-[a-z]{1}|aws-us-gov):sns:
([a-z]{2}-((iso[a-z]{0,1}-)|(gov-)){0,1}[a-z]+-[0-9]):[0-9]{12}:[A-Za-z0-9/][A-Za-
z0-9:_/+=,@.-]{1,256}$"
    }
  },
  "Resources" : {

 "ReadthrottleeventsthresholdexceededEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm" :
 {
      "Type" : "AWS::CloudWatch::Alarm",
      "Properties" : {
        "AlarmDescription" : "An Alarm by AWS Resilience Hub that alerts when the
 number of read-throttle events are greater than 1.",
        "AlarmName" : "ResilienceHub-ReadThrottleEventsAlarm-2020-04-01_Employees-ON-
DEMAND-0-DynamoDBTable-PXBZQYH3DCJ9",
        "AlarmActions" : [ {
          "Ref" : "SNSTopicARN"
        } ],
        "MetricName" : "ReadThrottleEvents",
        "Namespace" : "AWS/DynamoDB",
        "Statistic" : "Sum",
        "Dimensions" : [ {
          "Name" : "TableName",
          "Value" : "Employees-ON-DEMAND-0-DynamoDBTable-PXBZQYH3DCJ9"
        } ],
        "Period" : 60,
        "EvaluationPeriods" : 1,
        "DatapointsToAlarm" : 1,
        "Threshold" : 1,
        "ComparisonOperator" : "GreaterThanOrEqualToThreshold",
        "TreatMissingData" : "notBreaching",
        "Unit" : "Count"
```

```
      },
      "Metadata" : {
        "AWS::ResilienceHub::Monitoring" : {
          "recommendationId" : "dynamodb:alarm:health-read_throttle_events:2020-04-01"
        }
      }
    },

 "dynamodbalarmhealthreadthrottleevents20200401EmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm
 {
      "Type" : "AWS::SSM::Parameter",
      "Properties" : {
        "Name" : "/ResilienceHub/Alarm/3f904525-4bfa-430f-96ef-58ec9b19aa73/dynamodb-
alarm-health-read-throttle-events-2020-04-01_Employees-ON-DEMAND-0-DynamoDBTable-
PXBZQYH3DCJ9",
        "Type" : "String",
        "Value" : {
          "Fn::Sub" :
 "${ReadthrottleeventsthresholdexceededEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm}"
        },
        "Description" : "SSM Parameter for identifying installed resources."
      }
    },

 "dynamodbalarmhealthreadthrottleevents20200401EmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm
 {
      "Type" : "AWS::SSM::Parameter",
      "Properties" : {
        "Name" : "/ResilienceHub/Info/Alarm/3f904525-4bfa-430f-96ef-58ec9b19aa73/
dynamodb-alarm-health-read-throttle-events-2020-04-01_Employees-ON-DEMAND-0-
DynamoDBTable-PXBZQYH3DCJ9",
        "Type" : "String",
        "Value" : {
          "Fn::Sub" : "{\"alarmName\":
\"${ReadthrottleeventsthresholdexceededEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm}\",
\"referenceId\":\"dynamodb:alarm:health_read_throttle_events:2020-04-01\",
\"resourceId\":\"Employees-ON-DEMAND-0-DynamoDBTable-PXBZQYH3DCJ9\",\"relatedSOPs\":
[\"dynamodb:sop:update_provisioned_capacity:2020-04-01\"]}"
        },
        "Description" : "SSM Parameter for identifying installed resources."
      }
    }
  }
```

```
}
```

修改AWS CloudFormation範本

將警示、SOP 或AWS FIS資源整合到主應用程式中最簡單的方法，就是將其新增為範本中描述您應用程式範本的另一個資源。下面提供的 JSON 格式檔案提供了如何在範本中描述 DynamoDB 表的基本概述。AWS CloudFormation真正的應用程式可能會包含更多資源，例如其他資料表。

```
{
   "AWSTemplateFormatVersion": "2010-09-09T00:00:00.000Z",
   "Description": "Application Stack with Employees Table",
   "Outputs": {
      "DynamoDBTable": {
         "Description": "The DynamoDB Table Name",
         "Value": {"Ref": "Employees"}
      }
   },
   "Resources": {
      "Employees": {
         "Type": "AWS::DynamoDB::Table",
         "Properties": {
            "BillingMode": "PAY_PER_REQUEST",
            "AttributeDefinitions": [
               {
                  "AttributeName": "USER_ID",
                  "AttributeType": "S"
               },
               {
                  "AttributeName": "RANGE_ATTRIBUTE",
                  "AttributeType": "S"
               }
            ],
            "KeySchema": [
               {
                  "AttributeName": "USER_ID",
                  "KeyType": "HASH"
               },
               {
                  "AttributeName": "RANGE_ATTRIBUTE",
                  "KeyType": "RANGE"
               }
            ],
            "PointInTimeRecoverySpecification": {
```

```
            "PointInTimeRecoveryEnabled": true
         },
         "Tags": [
            {
               "Key": "Key",
               "Value": "Value"
            }
         ],
         "LocalSecondaryIndexes": [
            {
               "IndexName": "resiliencehub-index-local-1",
               "KeySchema": [
                  {
                     "AttributeName": "USER_ID",
                     "KeyType": "HASH"
                  },
                  {
                     "AttributeName": "RANGE_ATTRIBUTE",
                     "KeyType": "RANGE"
                  }
               ],
               "Projection": {
                  "ProjectionType": "ALL"
               }
            }
         ],
         "GlobalSecondaryIndexes": [
            {
               "IndexName": "resiliencehub-index-1",
               "KeySchema": [
                  {
                     "AttributeName": "USER_ID",
                     "KeyType": "HASH"
                  }
               ],
               "Projection": {
                  "ProjectionType": "ALL"
               }
            }
         ]
      }
   }
}
```

```
}
```

若要允許警示資源與應用程式一起部署，您現在需要在應用程式堆疊中以動態參考來取代硬式編碼資源。

因此，在AWS::CloudWatch::Alarm資源定義中，變更下列項目：

```
"Value" : "Employees-ON-DEMAND-0-DynamoDBTable-PXBZQYH3DCJ9"
```

到以下內容：

```
"Value" : {"Ref": "Employees"}
```

並在AWS::SSM::Parameter資源定義下，更改以下內容：

```
"Fn::Sub" : "{\"alarmName\":
\"${ReadthrottleeventsthresholdexceededDynamoDBEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm
\"referenceId\":\"dynamodb:alarm:health_read_throttle_events:2020-04-01\",
\"resourceId\":\"Employees-ON-DEMAND-0-DynamoDBTable-PXBZQYH3DCJ9\",\"relatedSOPs\":
[\"dynamodb:sop:update_provisioned_capacity:2020-04-01\"]}"
```

到以下內容：

```
"Fn::Sub" : "{\"alarmName\":
\"${ReadthrottleeventsthresholdexceededEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm}\",
\"referenceId\":\"dynamodb:alarm:health_read_throttle_events:2020-04-01\",\"resourceId
\":\"${Employees}\",\"relatedSOPs\":
[\"dynamodb:sop:update_provisioned_capacity:2020-04-01\"]}"
```

修改 SOP 和AWS FIS實驗的AWS CloudFormation模板時，您將採取相同的方法，將硬編碼的參考 ID 替換為動態引用，即使在硬件更改後也可以繼續工作。

透過使用 DynamoDB 表格的參照，您可AWS CloudFormation以執行下列動作：

- 首先創建數據庫表。
- 始終在警報中使用生成資源的實際 ID，並在AWS CloudFormation需要替換資源時動態更新警報。

> **Note**
>
> 您可以選擇更高級的方法來管理應用程序資源，AWS CloudFormation例如嵌套堆棧或引用單獨AWS CloudFormation堆棧中的資源輸出。（但是，如果您想要將建議堆疊與主堆疊分開，則需要設定一種在兩個堆疊之間傳遞資訊的方式。）
> 此外，第三方工具，例如 Terraform by HashiCorp，也可以用來佈建基礎結構作為程式碼 (IaC)。

使用 AWS Resilience Hub API 描述和管理應用程式

作為使用AWS Resilience Hub控制台描述和管理應用程序的替代方法，AWS Resilience Hub可讓您使用 AWS Resilience Hub API 描述和管理應用程序。本章介紹如何創建使用 AWS Resilience Hub API 的應用程序。它也會定義您需要執行 API 的順序，以及必須提供適當範例的參數值。如需詳細資訊，請參閱下列主題：

- the section called “準備申請”
- the section called “執行和分析應用程式”
- the section called “修改您的應用”

步驟 1：準備申請

若要準備應用程式，您必須先建立應用程式、指派復原則，然後從輸入來源匯入應用程式資源。如需用來準備應用程式之 AWS Resilience Hub API 的相關資訊，請參閱下列主題：

- the section called “建立應用程式”
- the section called “建立復原原則”
- the section called “匯入應用程式資源並監控匯入狀態”
- the section called “發佈應用程式並指派復原原則”

建立應用程式

若要在中建立新的應用程式AWS Resilience Hub，您必須呼叫 `CreateApp` API 並提供唯一的應用程式名稱。如需這種 API 的詳細資訊，請參閱 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateApp.html。

下面的例子演示了如何newApp在AWS Resilience Hub使用 `CreateApp` API 創建一個新的應用程序。

請求

```
aws resiliencehub create-app --name newApp
```

回應

```
{
```

```
    "app": {
        "appArn": "<App_ARN>",
        "name": "newApp",
        "creationTime": "2022-10-26T19:48:00.434000+03:00",
        "status": "Active",
        "complianceStatus": "NotAssessed",
        "resiliencyScore": 0.0,
        "tags": {},
        "assessmentSchedule": "Disabled"
    }
}
```

建立復原原則

建立應用程式之後，您必須建立復原原則，讓您能夠使用 API 瞭解應用`CreateResiliencyPolicy`程式的彈性狀態。如需這種 API 的詳細資訊，請參閱 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateResiliencyPolicy.html。

下面的例子演示了如何在AWS Resilience Hub使用 `CreateResiliencyPolicy` API `newPolicy` 為您的應用程序創建。

請求

```
aws resiliencehub create-resiliency-policy \
--policy-name newPolicy --tier NonCritical \
--policy '{"AZ": {"rtoInSecs": 172800,"rpoInSecs": 86400}, \
"Hardware": {"rtoInSecs": 172800,"rpoInSecs": 86400}, \
"Software": {"rtoInSecs": 172800,"rpoInSecs": 86400}}'
```

回應

```
{
    "policy": {
        "policyArn": "<Policy_ARN>",
        "policyName": "newPolicy",
        "policyDescription": "",
        "dataLocationConstraint": "AnyLocation",
        "tier": "NonCritical",
        "estimatedCostTier": "L1",
        "policy": {
            "AZ": {
```

```
                "rtoInSecs": 172800,
                "rpoInSecs": 86400
            },
            "Hardware": {
                "rtoInSecs": 172800,
                "rpoInSecs": 86400
            },
            "Software": {
                "rtoInSecs": 172800,
                "rpoInSecs": 86400
            }
        },
        "creationTime": "2022-10-26T20:48:05.946000+03:00",
        "tags": {}
    }
}
```

從輸入來源匯入資源並監視匯入狀態

AWS Resilience Hub提供下列 API 以將資源匯入您的應用程式：

- `ImportResourcesToDraftAppVersion`— 此 API 可讓您將資源從不同的輸入來源匯入應用程式的草稿版本。如需這種 API 的詳細資訊，請參閱 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_ImportResourcesToDraftAppVersion.html。
- `PublishAppVersion`— 此 API 發布了應用程序的新版本以及更新版本 AppComponents。如需這種 API 的詳細資訊，請參閱 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_PublishAppVersion.html。
- `DescribeDraftAppVersionResourcesImportStatus`— 此 API 可讓您監控資源到應用程式版本的匯入狀態。如需這種 API 的詳細資訊，請參閱 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeDraftAppVersionResourcesImportStatus.html。

下面的例子演示了如何AWS Resilience Hub使用 `ImportResourcesToDraftAppVersion` API 將資源導入到您的應用程序。

請求

```
aws resiliencehub import-resources-to-draft-app-version \
--app-arn <App_ARN> \
--terraform-sources '[{"s3StateFileUrl": <S3_URI>}]'
```

回應

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "sourceArns": [],
    "status": "Pending",
    "terraformSources": [
        {
            "s3StateFileUrl": <S3_URI>
        }
    ]
}
```

下面的示例演示了如何在AWS Resilience Hub使用 `CreateAppVersionResource` API 手動添加資源到您的應用程序。

請求

```
aws resiliencehub create-app-version-resource \
--app-arn <App_ARN> \
--resource-name "backup-efs" \
--logical-resource-id '{"identifier": "backup-efs"}' \
--physical-resource-id '<Physical_resource_id_ARN>' \
--resource-type AWS::EFS::FileSystem \
--app-components '["new-app-component"]'
```

回應

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "physicalResource": {
        "resourceName": "backup-efs",
        "logicalResourceId": {
            "identifier": "backup-efs"
        },
        "physicalResourceId": {
            "identifier": "<Physical_resource_id_ARN>",
            "type": "Arn"
        },
```

```
        "resourceType": "AWS::EFS::FileSystem",
        "appComponents": [
            {
                "name": "new-app-component",
                "type": "AWS::ResilienceHub::StorageAppComponent",
                "id": "new-app-component"
            }
        ]
    }
}
```

下列範例顯示如何在AWS Resilience Hub使用 `DescribeDraftAppVersionResourcesImportStatus` API 時監控資源的匯入狀態。

請求

```
aws resiliencehub describe-draft-app-version-resources-import-status \
--app-arn <App_ARN>
```

回應

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "status": "Success",
    "statusChangeTime": "2022-10-26T19:55:18.471000+03:00"
}
```

發佈應用程式的草稿版本並指派恢復原則

在執行評估之前，您必須先發佈應用程式的草稿版本，並將復原原則指派給應用程式的已發行版本。

若要發佈應用程式的草稿版本並指派恢復原則

1. 若要發佈應用程式的草稿版本，請使用 `PublishAppVersion` API。如需這種 API 的詳細資訊，請參閱 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_PublishAppVersion.html。

   下面的示例演示了如何AWS Resilience Hub使用 `PublishAppVersion` API 發布應用程序的草稿版本。

請求

```
aws resiliencehub publish-app-version \
 --app-arn <App_ARN>
```

回應

```
{
    "appArn": "<App_ARN>",
    "appVersion": "release"
}
```

2. 使用 UpdateApp API 將恢復原則套用至應用程式的發行版本。如需這種 API 的詳細資訊，請參閱 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_UpdateApp.html。

下列範例顯示如何在AWS Resilience Hub使用 UpdateApp API 時，將復原原則套用至已發行版本的應用程式。

請求

```
aws resiliencehub update-app \
--app-arn <App_ARN> \
--policy-arn <Policy_ARN>
```

回應

```
{
    "app": {
        "appArn": "<App_ARN>",
        "name": "newApp",
        "policyArn": "<Policy_ARN>",
        "creationTime": "2022-10-26T19:48:00.434000+03:00",
        "status": "Active",
        "complianceStatus": "NotAssessed",
        "resiliencyScore": 0.0,
        "tags": {
            "resourceArn": "<App_ARN>"
```

```
        },
        "assessmentSchedule": "Disabled"
    }
}
```

步驟 2：執行和管理AWS Resilience Hub復原能力評估

發佈新版應用程式之後，您必須執行新的恢復能力評估並分析結果，以確保您的應用程式符合復原原則中定義的估計工作負載 RTO 和預估的 RPO。評估會將每個應用程式元件組態與原則進行比較，並提出警示、SOP 和測試建議。

如需詳細資訊，請參閱下列主題：

- the section called “執行和監控恢復能力評估”
- the section called “建立復原原則”

執行和監控AWS Resilience Hub恢復能力評估

若要在中執行恢復能力評估AWS Resilience Hub並監控其狀態，您必須使用下列 API：

- `StartAppAssessment`— 此 API 會為應用程式建立新的評估。如需這種 API 的詳細資訊，請參閱 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_StartAppAssessment.html。
- `DescribeAppAssessment`— 此 API 描述了應用程序的評估，並提供評估的完成狀態。如需這種 API 的詳細資訊，請參閱 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeAppAssessment.html。

下列範例顯示如何在AWS Resilience Hub使用 `StartAppAssessment` API 中開始執行新評估。

請求

```
aws resiliencehub start-app-assessment \
--app-arn <App_ARN> \
--app-version release \
--assessment-name first-assessment
```

回應

```
{
```

```
    "assessment": {
        "appArn": "<App_ARN>",
        "appVersion": "release",
        "invoker": "User",
        "assessmentStatus": "Pending",
        "startTime": "2022-10-27T08:15:10.452000+03:00",
        "assessmentName": "first-assessment",
        "assessmentArn": "<Assessment_ARN>",
        "policy": {
            "policyArn": "<Policy_ARN>",
            "policyName": "newPolicy",
            "dataLocationConstraint": "AnyLocation",
            "policy": {
                "AZ": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                },
                "Hardware": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                },
                "Software": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                }
            }
        },
        "tags": {}
    }
}
```

下列範例顯示如何在AWS Resilience Hub使用 `DescribeAppAssessment` API 監控評估狀態。您可以從`assessmentStatus`變數擷取評估狀態。

請求

```
aws resiliencehub describe-app-assessment \
--assessment-arn <Assessment_ARN>
```

回應

```
{
```

```
    "assessment": {
        "appArn": "<App_ARN>",
        "appVersion": "release",
        "cost": {
            "amount": 0.0,
            "currency": "USD",
            "frequency": "Monthly"
        },
        "resiliencyScore": {
            "score": 0.27,
            "disruptionScore": {
                "AZ": 0.42,
                "Hardware": 0.0,
                "Region": 0.0,
                "Software": 0.38
            }
        },
        "compliance": {
            "AZ": {
                "achievableRtoInSecs": 0,
                "currentRtoInSecs": 4500,
                "currentRpoInSecs": 86400,
                "complianceStatus": "PolicyMet",
                "achievableRpoInSecs": 0
            },
            "Hardware": {
                "achievableRtoInSecs": 0,
                "currentRtoInSecs": 2595601,
                "currentRpoInSecs": 2592001,
                "complianceStatus": "PolicyBreached",
                "achievableRpoInSecs": 0
            },
            "Software": {
                "achievableRtoInSecs": 0,
                "currentRtoInSecs": 4500,
                "currentRpoInSecs": 86400,
                "complianceStatus": "PolicyMet",
                "achievableRpoInSecs": 0
            }
        },
        "complianceStatus": "PolicyBreached",
        "assessmentStatus": "Success",
        "startTime": "2022-10-27T08:15:10.452000+03:00",
        "endTime": "2022-10-27T08:15:31.883000+03:00",
```

```
        "assessmentName": "first-assessment",
        "assessmentArn": "<Assessment_ARN>",
        "policy": {
            "policyArn": "<Policy_ARN>",
            "policyName": "newPolicy",
            "dataLocationConstraint": "AnyLocation",
            "policy": {
                "AZ": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                },
                "Hardware": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                },
                "Software": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                }
            }
        },
        "tags": {}
    }
}
```

檢查評估結果

成功完成評估後，您可以使用以下 API 檢查評估結果。

- `DescribeAppAssessment`— 此 API 允許您根據恢復原則跟踪應用程序的當前狀態。此外，您也可以從`complianceStatus`變數擷取合規狀態，以及從`resiliencyScore`結構中擷取每種中斷類型的復原分數。如需這種 API 的詳細資訊，請參閱 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeAppAssessment.html。
- `ListAlarmRecommendations`— 此 API 可讓您使用評估的 Amazon 資源名稱 (ARN) 取得警示建議。如需這種 API 的詳細資訊，請參閱 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_ListAlarmRecommendations.html。

> **Note**
>
> 若要取得 SOP 和 FIS 測試建議，請使用`ListSopRecommendations`和`ListTestRecommendations` API。

下列範例顯示如何使用 `ListAlarmRecommendations` API 使用評估的 Amazon 資源名稱 (ARN) 取得警示建議。

> **Note**
>
> 若要取得 SOP 和 FIS 測試建議，請以`ListSopRecommendations`或`ListTestRecommendations`取代。

請求

```
aws resiliencehub list-alarm-recommendations \
--assessment-arn <Assessment_ARN>
```

回應

```
{
    "alarmRecommendations": [
        {
            "recommendationId": "78ece7f8-c776-499e-baa8-b35f5e8b8ba2",
            "referenceId": "app_common:alarm:synthetic_canary:2021-04-01",
            "name": "AWSResilienceHub-SyntheticCanaryInRegionAlarm_2021-04-01",
            "description": "A monitor for the entire application, configured to
 constantly verify that the application API/endpoints are available",
            "type": "Metric",
            "appComponentName": "appcommon",
            "items": [
                {
                    "resourceId": "us-west-2",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ],
```

```
            "prerequisite": "Make sure CloudWatch Synthetics is setup to monitor the
 application (see the <a href=\"https://docs.aws.amazon.com/AmazonCloudWatch/latest/
monitoring/CloudWatch_Synthetics_Canaries.html\" target=\"_blank\">docs</a>). \nMake
 sure that the Synthetics Name passed in the alarm dimension matches the name of the
 Synthetic Canary. It Defaults to the name of the application.\n"
        },
        {
            "recommendationId": "d9c72c58-8c00-43f0-ad5d-0c6e5332b84b",
            "referenceId": "efs:alarm:percent_io_limit:2020-04-01",
            "name": "AWSResilienceHub-EFSHighIoAlarm_2020-04-01",
            "description": "Alarm by AWS ResilienceHub that reports when EFS I/O load
 is more than 90% for too much time",
            "type": "Metric",
            "appComponentName": "storageappcomponent-rlb",
            "items": [
                {
                    "resourceId": "fs-0487f945c02f17b3e",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "09f340cd-3427-4f66-8923-7f289d4a3216",
            "referenceId": "efs:alarm:mount_failure:2020-04-01",
            "name": "AWSResilienceHub-EFSMountFailureAlarm_2020-04-01",
            "description": "Alarm by AWS ResilienceHub that reports when volume failed
 to mount to EC2 instance",
            "type": "Metric",
            "appComponentName": "storageappcomponent-rlb",
            "items": [
                {
                    "resourceId": "fs-0487f945c02f17b3e",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ],
            "prerequisite": "* Make sure Amazon EFS utils are installed(see the <a
 href=\"https://github.com/aws/efs-utils#installation\" target=\"_blank\">docs</a>).
\n* Make sure cloudwatch logs are enabled in efs-utils (see the <a href=\"https://
github.com/aws/efs-utils#step-2-enable-cloudwatch-log-feature-in-efs-utils-config-
file-etcamazonefsefs-utilsconf\" target=\"_blank\">docs</a>).\n* Make sure that
```

```
you've configured `log_group_name` in `/etc/amazon/efs/efs-utils.conf`, for example:
`log_group_name = /aws/efs/utils`.\n* Use the created `log_group_name` in the
generated alarm. Find `LogGroupName: REPLACE_ME` in the alarm and make sure the
`log_group_name` is used instead of REPLACE_ME.\n"
        },
        {
            "recommendationId": "b0f57d2a-1220-4f40-a585-6dab1e79cee2",
            "referenceId": "efs:alarm:client_connections:2020-04-01",
            "name": "AWSResilienceHub-EFSHighClientConnectionsAlarm_2020-04-01",
            "description": "Alarm by AWS ResilienceHub that reports when client
connection number deviation is over the specified threshold",
            "type": "Metric",
            "appComponentName": "storageappcomponent-rlb",
            "items": [
                {
                    "resourceId": "fs-0487f945c02f17b3e",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "15f49b10-9bac-4494-b376-705f8da252d7",
            "referenceId": "rds:alarm:health-storage:2020-04-01",
            "name": "AWSResilienceHub-RDSInstanceLowStorageAlarm_2020-04-01",
            "description": "Reports when database free storage is low",
            "type": "Metric",
            "appComponentName": "databaseappcomponent-hji",
            "items": [
                {
                    "resourceId": "terraform-20220623141426115800000001",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "c1906101-cea8-4f77-be7b-60abb07621f5",
            "referenceId": "rds:alarm:health-connections:2020-04-01",
            "name": "AWSResilienceHub-RDSInstanceConnectionSpikeAlarm_2020-04-01",
            "description": "Reports when database connection count is anomalous",
            "type": "Metric",
```

```
            "appComponentName": "databaseappcomponent-hji",
            "items": [
                {
                    "resourceId": "terraform-20220623141426115800000001",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "f169b8d4-45c1-4238-95d1-ecdd8d5153fe",
            "referenceId": "rds:alarm:health-cpu:2020-04-01",
            "name": "AWSResilienceHub-RDSInstanceOverUtilizedCpuAlarm_2020-04-01",
            "description": "Reports when database used CPU is high",
            "type": "Metric",
            "appComponentName": "databaseappcomponent-hji",
            "items": [
                {
                    "resourceId": "terraform-20220623141426115800000001",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "69da8459-cbe4-4ba1-a476-80c7ebf096f0",
            "referenceId": "rds:alarm:health-memory:2020-04-01",
            "name": "AWSResilienceHub-RDSInstanceLowMemoryAlarm_2020-04-01",
            "description": "Reports when database free memory is low",
            "type": "Metric",
            "appComponentName": "databaseappcomponent-hji",
            "items": [
                {
                    "resourceId": "terraform-20220623141426115800000001",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "67e7902a-f658-439e-916b-251a57b97c8a",
```

```
            "referenceId": "ecs:alarm:health-service_cpu_utilization:2020-04-01",
            "name": "AWSResilienceHub-ECSServiceHighCpuUtilizationAlarm_2020-04-01",
            "description": "Alarm by AWS ResilienceHub that triggers when CPU
utilization of ECS tasks of Service exceeds the threshold",
            "type": "Metric",
            "appComponentName": "computeappcomponent-nrz",
            "items": [
                {
                    "resourceId": "aws_ecs_service_terraform-us-east-1-demo",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "fb30cb91-1f09-4abd-bd2e-9e8ee8550eb0",
            "referenceId": "ecs:alarm:health-service_memory_utilization:2020-04-01",
            "name": "AWSResilienceHub-ECSServiceHighMemoryUtilizationAlarm_2020-04-01",
            "description": "Alarm by AWS ResilienceHub for Amazon ECS that indicates if
the percentage of memory that is used in the service, is exceeding specified threshold
limit",
            "type": "Metric",
            "appComponentName": "computeappcomponent-nrz",
            "items": [
                {
                    "resourceId": "aws_ecs_service_terraform-us-east-1-demo",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "1bd45a8e-dd58-4a8e-a628-bdbee234efed",
            "referenceId": "ecs:alarm:health-service_sample_count:2020-04-01",
            "name": "AWSResilienceHub-ECSServiceSampleCountAlarm_2020-04-01",
            "description": "Alarm by AWS Resilience Hub for Amazon ECS that triggers if
the count of tasks isn't equal Service Desired Count",
            "type": "Metric",
            "appComponentName": "computeappcomponent-nrz",
            "items": [
                {
                    "resourceId": "aws_ecs_service_terraform-us-east-1-demo",
```

```
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ],
            "prerequisite": "Make sure the Container Insights on Amazon ECS is enabled:
 (see the <a href=\"https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/
deploy-container-insights-ECS-cluster.html\" target=\"_blank\">docs</a>)."
        }
    ]
}
```

下列範例顯示如何使用 ListAppComponentRecommendations API 取得組態建議 (有關如何改善目前恢復能力的建議)。

請求

```
aws resiliencehub list-app-component-recommendations \
--assessment-arn <Assessment_ARN>
```

回應

```
{
    "componentRecommendations": [
        {
            "appComponentName": "computeappcomponent-nrz",
            "recommendationStatus": "MetCanImprove",
            "configRecommendations": [
                {
                    "cost": {
                        "amount": 0.0,
                        "currency": "USD",
                        "frequency": "Monthly"
                },
                    "appComponentName": "computeappcomponent-nrz",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
 cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
```

```
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        }
                    },
                    "optimizationType": "LeastCost",
                    "description": "Current Configuration",
                    "suggestedChanges": [],
                    "haArchitecture": "BackupAndRestore",
                    "referenceId": "original"
                },
                {
                    "cost": {
                        "amount": 0.0,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "computeappcomponent-nrz",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
backups"
```

```
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        }
                    },
                    "optimizationType": "LeastChange",
                    "description": "Current Configuration",
                    "suggestedChanges": [],
                    "haArchitecture": "BackupAndRestore",
                    "referenceId": "original"
                },
                {
                    "cost": {
                        "amount": 14.74,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "computeappcomponent-nrz",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 0,
                            "expectedRtoDescription": "No expected downtime. You're
launching using EC2, with DesiredCount > 1 in multiple AZs and CapacityProviders with
MinSize > 1",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "ECS Service state is saved on
EFS file system. No data loss is expected as objects are be stored in multiple AZs."
                        },
```

```
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 0,
                            "expectedRtoDescription": "No expected downtime. You're
launching using EC2, with DesiredCount > 1 and CapacityProviders with MinSize > 1",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "ECS Service state is saved on
EFS file system. No data loss is expected as objects are be stored in multiple AZs."
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        }
                    },
                    "optimizationType": "BestAZRecovery",
                    "description": "Stateful ECS service with launch type EC2 and EFS
storage, deployed in multiple AZs. AWS Backup is used to backup EFS and copy snapshots
in-region.",
                    "suggestedChanges": [
                        "Add Auto Scaling Groups and Capacity Providers in multiple
AZs",
                        "Change desired count of the setup",
                        "Remove EBS volume"
                    ],
                    "haArchitecture": "BackupAndRestore",
                    "referenceId": "ecs:config:ec2-multi_az-efs-backups:2022-02-16"
                }
            ]
        },
        {
            "appComponentName": "databaseappcomponent-hji",
            "recommendationStatus": "MetCanImprove",
            "configRecommendations": [
                {
                    "cost": {
                        "amount": 0.0,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
```

```
                    "appComponentName": "databaseappcomponent-hji",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": "Estimated time to restore from
an RDS backup. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": "Estimated time to restore from
snapshot. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": "Estimated time to restore from
snapshot. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        }
                    },
                    "optimizationType": "LeastCost",
                    "description": "Current Configuration",
                    "suggestedChanges": [],
                    "haArchitecture": "BackupAndRestore",
                    "referenceId": "original"
                },
                {
                    "cost": {
```

```
                        "amount": 0.0,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "databaseappcomponent-hji",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": "Estimated time to restore from
an RDS backup. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": "Estimated time to restore from
snapshot. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": "Estimated time to restore from
snapshot. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        }
                    },
                    "optimizationType": "LeastChange",
                    "description": "Current Configuration",
                    "suggestedChanges": [],
                    "haArchitecture": "BackupAndRestore",
```

```
                    "referenceId": "original"
                },
                {
                    "cost": {
                        "amount": 76.73,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "databaseappcomponent-hji",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 120,
                            "expectedRtoDescription": "Estimated time to promote a
secondary instance.",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "Aurora data is automatically
replicated across multiple Availability Zones in a Region."
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 120,
                            "expectedRtoDescription": "Estimated time to promote a
secondary instance.",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "Aurora data is automatically
replicated across multiple Availability Zones in a Region."
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 900,
                            "expectedRtoDescription": "Estimate time to backtrack to a
stable state.",
                            "expectedRpoInSecs": 300,
                            "expectedRpoDescription": "Estimate for latest restorable
time for point in time recovery."
                        }
                    },
                    "optimizationType": "BestAZRecovery",
                    "description": "Aurora database cluster with one read replica, with
backtracking window of 24 hours.",
                    "suggestedChanges": [
                        "Add read replica in the same region",
                        "Change DB instance to a supported class (db.t3.small)",
```

```
                        "Change to Aurora",
                        "Enable cluster backtracking",
                        "Enable instance backup with retention period 7"
                    ],
                    "haArchitecture": "WarmStandby",
                    "referenceId": "rds:config:aurora-backtracking"
                }
            ]
        },
        {
            "appComponentName": "storageappcomponent-rlb",
            "recommendationStatus": "BreachedUnattainable",
            "configRecommendations": [
                {
                    "cost": {
                        "amount": 0.0,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "storageappcomponent-rlb",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 0,
                            "expectedRtoDescription": "No data loss in your system",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "No data loss in your system"
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyBreached",
                            "expectedRtoInSecs": 2592001,
                            "expectedRtoDescription": "No recovery option configured",
                            "expectedRpoInSecs": 2592001,
                            "expectedRpoDescription": "No recovery option configured"
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 900,
                            "expectedRtoDescription": "Time to recover EFS from backup.
(Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Recovery Point Objective for EFS
from backups, derived from backup frequency"
                        }
```

```
                    },
                    "optimizationType": "BestAZRecovery",
                    "description": "EFS with backups configured",
                    "suggestedChanges": [
                        "Add additional availability zone"
                    ],
                    "haArchitecture": "MultiSite",
                    "referenceId": "efs:config:with_backups:2020-04-01"
                },
                {
                    "cost": {
                        "amount": 0.0,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "storageappcomponent-rlb",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 0,
                            "expectedRtoDescription": "No data loss in your system",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "No data loss in your system"
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyBreached",
                            "expectedRtoInSecs": 2592001,
                            "expectedRtoDescription": "No recovery option configured",
                            "expectedRpoInSecs": 2592001,
                            "expectedRpoDescription": "No recovery option configured"
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 900,
                            "expectedRtoDescription": "Time to recover EFS from backup.
(Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Recovery Point Objective for EFS
from backups, derived from backup frequency"
                        }
                    },
                    "optimizationType": "BestAttainable",
                    "description": "EFS with backups configured",
                    "suggestedChanges": [
```

```
                        "Add additional availability zone"
                    ],
                    "haArchitecture": "MultiSite",
                    "referenceId": "efs:config:with_backups:2020-04-01"
                }
            ]
        }
    ]
}
```

步驟 3：修改您的應用程式

AWS Resilience Hub可讓您編輯應用程式的草稿版本，並將變更發佈至新 (已發佈) 版本，以修改應用程式資源。 AWS Resilience Hub使用已發佈的應用程式版本 (包括更新的資源) 來執行復原能力評估。

如需詳細資訊，請參閱下列主題：

- the section called “手動新增資源”
- the section called “將資源分組到單一應用程式元件”
- the section called “排除資源 AppComponent”

手動將資源新增至應用程式

如果資源未部署為輸入來源的一部分，AWS Resilience Hub可讓您使用 `CreateAppVersionResource` API 手動將資源新增至應用程式。如需這種 API 的詳細資訊，請參閱 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateAppVersionResource.html。

您必須為此 API 提供下列參數：

- 應用程式的 Amazon 資源名稱 (ARN)
- 資源的邏輯 ID
- 資源的實體 ID
- AWS CloudFormation 類型

下面的示例演示了如何在AWS Resilience Hub使用 `CreateAppVersionResource` API 手動添加資源到您的應用程序。

請求

```
aws resiliencehub create-app-version-resource \
--app-arn <App_ARN> \
--resource-name "backup-efs" \
--logical-resource-id '{"identifier": "backup-efs"}' \
--physical-resource-id '<Physical_resource_id_ARN>' \
--resource-type AWS::EFS::FileSystem \
--app-components '["new-app-component"]'
```

回應

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "physicalResource": {
        "resourceName": "backup-efs",
        "logicalResourceId": {
            "identifier": "backup-efs"
        },
        "physicalResourceId": {
            "identifier": "<Physical_resource_id_ARN>",
            "type": "Arn"
        },
        "resourceType": "AWS::EFS::FileSystem",
        "appComponents": [
            {
                "name": "new-app-component",
                "type": "AWS::ResilienceHub::StorageAppComponent",
                "id": "new-app-component"
            }
        ]
    }
}
```

將資源分組到單一應用程式元件

應用程序組件（AppComponent）是一組作為一個單元工作和失敗的相關AWS資源。例如，當您擁有用作待命部署的跨區域工作負載時。 AWS Resilience Hub具有管理哪些AWS資源可以屬於哪種類型的規則 AppComponent。 AWS Resilience Hub可讓您 AppComponent 使用下列資源管理 API 將資源分組為單一資源。

- `UpdateAppVersionResource`— 此 API 更新應用程序的資源詳細信息。如需這種 API 的詳細資訊，請參閱 UpdateAppVersionResource。
- `DeleteAppVersionAppComponent`— 此 API 會從應用程式 AppComponent 中刪除。如需這種 API 的詳細資訊，請參閱 DeleteAppVersionAppComponent。

下面的示例演示了如何在AWS Resilience Hub使用 `DeleteAppVersionAppComponent` API 更新應用程序的資源詳細信息。

請求

```
aws resiliencehub delete-app-version-app-component \
--app-arn <App_ARN> \
--id new-app-component
```

回應

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "appComponent": {
        "name": "new-app-component",
        "type": "AWS::ResilienceHub::StorageAppComponent",
        "id": "new-app-component"
    }
}
```

下面的示例演示了如何刪除在AWS Resilience Hub使用 `UpdateAppVersionResource` API 的先前示例中創建的空 AppComponent 。

請求

```
aws resiliencehub delete-app-version-app-component \
--app-arn <App_ARN> \
--id new-app-component
```

回應

```
{
    "appArn": "<App_ARN>",
```

```
    "appVersion": "draft",
    "appComponent": {
        "name": "new-app-component",
        "type": "AWS::ResilienceHub::StorageAppComponent",
        "id": "new-app-component"
    }
}
```

排除資源 AppComponent

AWS Resilience Hub可讓您使用 UpdateAppVersionResource API 將資源排除在評估之外。計算應用程式的復原能力時，不會考慮這些資源。如需這種 API 的詳細資訊，請參閱 https://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_UpdateAppVersionResource.html。

> **Note**
>
> 您只能排除從輸入來源匯入的那些資源。

下面的示例演示了如何在AWS Resilience Hub使用 UpdateAppVersionResource API 排除應用程序的資源。

請求

```
aws resiliencehub update-app-version-resource \
--app-arn <App_ARN> \
--resource-name "ec2instance-nvz" \
--excluded
```

回應

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "physicalResource": {
        "resourceName": "ec2instance-nvz",
        "logicalResourceId": {
            "identifier": "ec2",
            "terraformSourceName": "test.state.file"
        },
```

```
        "physicalResourceId": {
            "identifier": "i-0b58265a694e5ffc1",
            "type": "Native",
            "awsRegion": "us-west-2",
            "awsAccountId": "123456789101"
        },
        "resourceType": "AWS::EC2::Instance",
        "appComponents": [
            {
                "name": "computeappcomponent-nrz",
                "type": "AWS::ResilienceHub::ComputeAppComponent"
            }
        ]
    }
}
```

中的安全性 AWS Resilience Hub

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

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

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

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

目錄

資料保護 AWS Resilience Hub

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

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

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源進行通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用設定 API 和使用者活動記錄 AWS CloudTrail。

- 使用 AWS 加密解決方案以及其中的所有默認安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2 概觀。

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

靜態加密

AWS Resilience Hub 加密您的靜態資料。中的 AWS Resilience Hub 資料會使用透明伺服器端加密進行靜態加密。這可協助降低保護敏感資料所涉及的操作負擔和複雜性。您可以透過靜態加密，建立符合加密合規和法規要求，而且對安全性要求甚高的應用程式。

傳輸中加密

AWS Resilience Hub 加密服務與其他整合式 AWS 服務之間傳輸中的資料。在 AWS Resilience Hub 與整合式服務之間傳遞的所有資料都會使用傳輸層安全性 (TLS) 加密。 AWS Resilience Hub 針對跨 AWS 服務的特定類型目標提供預先設定的動作，並支援目標資源的動作。

AWS 復原中樞的 Identity and Access Management

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

主題

- 物件
- 使用身分驗證
- 使用政策管理存取權
- AWS 彈性中樞如何與 IAM 搭配運作
- 設定 IAM 角色和許可

- AWS 復原中樞身分識別與存取疑難
- AWS Resilience Hub 存取權限參考
- AWS 受管理的政策 AWS Resilience Hub
- 將地形狀態檔案匯入 AWS Resilience Hub
- 啟 AWS Resilience Hub 用對 Amazon Elastic Kubernetes Service 叢集的存取
- 啟用發佈 AWS Resilience Hub 到您的 Amazon 簡易通知服務主題
- 限制權限以包含或排除 AWS Resilience Hub 建議

物件

您的使用方式 AWS Identity and Access Management (IAM) 會有所不同，具體取決於您在 AWS 彈性集線器中執行的工作。

服務使用者 — 如果您使用 AWS Resliance Hub 服務執行工作，則系統管理員會為您提供所需的認證和權限。當您使用更多 AWS 彈性中樞功能來完成工作時，您可能需要額外的權限。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法存取 AWS 彈性中樞中的功能，請參閱AWS 復原中樞身分識別與存取疑難。

服務管理員 — 如果您負責公司的 AWS 韌性中樞資源，您可能擁有完整存取 AWS 復原力集線器。判斷您的服務使用者應該存取哪些 AWS 彈性中樞功能和資源是您的工作。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步了解貴公司如何搭配 AWS 彈性中樞使用 IAM，請參閱AWS 彈性中樞如何與 IAM 搭配運作。

IAM 管理員 — 如果您是 IAM 管理員，您可能想要瞭解如何撰寫政策以管理 AWS 復原中樞存取權的詳細資訊。若要檢視您可以在 IAM 中使用的 AWS 彈性中樞身分型政策範例，請參閱。復原中樞的身分識別型原則範例 AWS

使用身分驗證

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

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

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

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

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

AWS 帳戶 根使用者

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

聯合身分

最佳作法是要求人類使用者 (包括需要系統管理員存取權的使用者) 使用與身分識別提供者的同盟，才能使用臨時認證 AWS 服務 來存取。

聯合身分識別是來自企業使用者目錄的使用者、Web 身分識別提供者、Identi ty Center 目錄，或使用透過身分識別來源提供的認證進行存取 AWS 服務 的任何使用者。 AWS Directory Service同盟身分存取時 AWS 帳戶，他們會假設角色，而角色則提供臨時認證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連線並同步到自己身分識別來源中的一組使用者和群組，以便在所有應用程式 AWS 帳戶 和應用程式中使用。如需 IAM Identity Center 的相關資訊，請參閱 AWS IAM Identity Center 使用者指南中的什麼是 IAM Identity Center？。

IAM 使用者和群組

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

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

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

IAM 角色

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

使用暫時憑證的 IAM 角色在下列情況中非常有用：

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

- 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon EC2 上執行的應用程式 — 您可以使用 IAM 角色來管理在 EC2 執行個體上執行的應用程式以及發出 AWS CLI 或 AWS API 請求的臨時登入資料。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並提供給其所有應用程式，請建立連接至執行個體的執行個體設定檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得暫時憑證。如需更多資訊，請參閱 IAM 使用者指南中的利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式。

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

使用政策管理存取權

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

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

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

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

身分型政策

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

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶. 受管政策包括 AWS 受管政策和客戶管理

的策略。若要了解如何在受管政策及內嵌政策間選擇，請參閱 IAM 使用者指南中的在受管政策和內嵌政策間選擇。

資源型政策

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

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

存取控制清單 (ACL)

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

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

其他政策類型

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

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

階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需更多資訊，請參閱 IAM 使用者指南中的工作階段政策。

多種政策類型

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

AWS 彈性中樞如何與 IAM 搭配運作

在您使用 IAM 管理 AWS 復原中樞的存取權限之前，請先了解哪些 IAM 功能可搭配 AWS 彈性中樞使用。

您可以搭配 AWS 彈性中樞使用的 IAM 功能

IAM 功能	AWS 彈性中樞支援
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵 (服務特定)	是
ACL	否
ABAC(政策中的標籤)	部分
臨時憑證	是
轉送存取工作階段 (FAS)	是
服務角色	是

若要深入瞭解 AWS 彈性中樞和其他 AWS 服務如何與大多數 IAM 功能搭配運作，請參閱 IAM 使用者指南中的搭配 IAM 使用的AWS 服務。

復原中樞的身分識別型原則 AWS

支援身分型政策	是

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

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素參考。

復原中樞的身分識別型原則範例 AWS

若要檢視 AWS 復原中樞身分識別型原則的範例，請參閱。復原中樞的身分識別型原則範例 AWS

AWS 復原中樞內的資源型政策

支援以資源基礎的政策	否

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

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，作為資源型政策的主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主體和資源不同時 AWS 帳戶，受信任帳戶中的 IAM 管理員也必須授與主體實體 (使用者或角色) 權限，才能存取資源。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，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 角色與資源型政策有何差異。

AWS 彈性中樞的政策動作

支援政策動作	是

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

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

政策會使用動作來授予執行相關聯動作的許可。

若要查看 AWS 復原中樞動作清單，請參閱服務授權參考中的AWS 復原中樞定義的動作。

AWS 復原中樞中的原則動作會在動作之前使用下列前置詞：

```
resiliencehub
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [
      "resiliencehub:action1",
      "resiliencehub:action2"
         ]
```

若要檢視 AWS 復原中樞身分識別型原則的範例，請參閱。復原中樞的身分識別型原則範例 AWS

AWS 彈性中樞的政策資源

支援政策資源	是

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

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

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

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

若要查看 AWS 復原中樞資源類型及其 ARN 的清單，請參閱服務授權參考資料中由 AWS 復原中樞定義的資源。若要瞭解您可以使用哪些動作指定每個資源的 ARN，請參閱AWS 復原中樞定義的動作。

若要檢視 AWS 復原中樞身分識別型原則的範例，請參閱。復原中樞的身分識別型原則範例 AWS

AWS 復原中樞的原則條件金鑰

支援服務特定政策條件金鑰	是

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

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

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

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

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

若要查看 AWS 復原中樞條件金鑰清單，請參閱服務授權參考中的AWS 復原中樞的條件金鑰。若要瞭解您可以使用條件金鑰的動作和資源，請參閱AWS 彈性中樞定義的動作。

若要檢視 AWS 復原中樞身分識別型原則的範例，請參閱。復原中樞的身分識別型原則範例 AWS

AWS 彈性中樞中的 ACL

支援 ACL	否

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。

ABAC 與 AWS 彈性樞紐

支援 ABAC (政策中的標籤)	部分

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。在中 AWS，這些屬性稱為標籤。您可以將標籤附加到 IAM 實體 (使用者或角色) 和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。您接著要設計 ABAC 政策，允許在主體的標籤與其嘗試存取的資源標籤相符時操作。

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

若要根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件金鑰，在政策的條件元素中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的什麼是 ABAC?。如要查看含有設定 ABAC 步驟的教學課程，請參閱《IAM 使用者指南》中的使用屬性型存取控制 (ABAC)。

搭配 AWS 復原集線器使用臨時登入

支援臨時憑證	是

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配AWS 服務 使用，請參閱 IAM 使用者指南中的 IAM。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立暫時認證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱《IAM 使用者指南》中的切換至角色 (主控台)。

您可以使用 AWS CLI 或 AWS API 手動建立臨時登入資料。然後，您可以使用這些臨時登入資料來存取 AWS。 AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱 IAM 中的暫時性安全憑證。

AWS 復原中樞的轉寄存取工作階段

支援轉寄存取工作階段 (FAS)	是

當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。

AWS 恢復中樞的服務角色

支援服務角色	是

服務角色是服務擔任的 IAM 角色，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需更多資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務。

> **Warning**
>
> 變更服務角色的權限可能會中斷 AWS 復原中樞功能。只有在 AWS 復原中樞提供指引時，才編輯服務角色。

復原中樞的身分識別型原則範例 AWS

根據預設，使用者和角色沒有建立或修改 AWS 彈性中樞資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行工作。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

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》中的建立 IAM 政策。

如需有關 AWS 彈性中樞所定義之動作和資源類型的詳細資訊，包括每個資源類型的 ARN 格式，請參閱服務授權參考中AWS 彈性中樞的動作、資源和條件金鑰。

主題

- 政策最佳實務
- 使用 AWS 復原中樞主控台
- 允許使用者檢視他們自己的許可
- 列出可用的 AWS Resilience Hub 應用
- 開始應用程式評估
- 刪除應用程式評估
- 為特定應用程式建立建議範本
- 刪除特定應用程式的建議範本
- 使用特定恢復原則更新應用程式

政策最佳實務

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

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始授與使用者和工作負載的權限，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們可用在您的 AWS 帳戶. 建議您透過定義特定於您的使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低許可許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的權限。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需更多資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。
- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫 API 作業時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 API 存取。

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

使用 AWS 復原中樞主控台

若要存取 AWS 彈性中樞主控台，您必須擁有最少一組權限。這些權限必須允許您列出並檢視有關 AWS 帳戶. AWS 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 (使用者或角色) 而言，主控台就無法如預期運作。

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

若要確保使用者和角色仍然可以使用 AWS Resurability Hub 主控台，請同時將 AWS 復原中樞*ConsoleAccess*或*ReadOnly* AWS 受管理的原則附加至實體。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。

下列策略授與使用者在 AWS Resilience Hub 主控台中列出和檢視所有資源的權限，但不能建立、更新或刪除這些資源。

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

允許使用者檢視他們自己的許可

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

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

```
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

列出可用的 AWS Resilience Hub 應用

下列原則授與使用者列出可用 AWS Resilience Hub 應用程式的權限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:ListApps"
      ],
      "Resource": [
        "*"
```

```
      ]
    }
  ]
}
```

開始應用程式評估

下列策略授與使用者啟動特定 AWS Resilience Hub 應用程式評估的權限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:StartAppAssessment"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
  ]
}
```

刪除應用程式評估

下列策略授與使用者刪除特定 AWS Resilience Hub 應用程式評估的權限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:DeleteAppAssessment"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
```

```
  ]
}
```

為特定應用程式建立建議範本

下列原則授與使用者針對特定應用 AWS Resilience Hub 程式建立建議範本的權限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:CreateRecommendationTemplate"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
  ]
}
```

刪除特定應用程式的建議範本

下列原則授與使用者刪除特定 AWS Resilience Hub 應用程式之建議範本的權限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:DeleteRecommendationTemplate"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
  ]
}
```

使用特定恢復原則更新應用程式

下列原則授與使用者使用特定復原原則更新 AWS Resilience Hub 應用程式的權限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:UpdateApp"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ],
      "Condition": {
        "StringLike" : { "resiliencehub:policyArn" : "arn:aws:resiliencehub:us-
west-2:111122223333:resiliency-policy/*" }
      }
    }
  ]
}
```

設定 IAM 角色和許可

AWS Resilience Hub 可讓您設定要在為應用程式執行評估時使用的 IAM 角色。您可以透過多種方式進行設定， AWS Resilience Hub 以取得應用程式資源的唯讀存取權。但是， AWS Resilience Hub 建議使用以下方法：

- 基於角色的訪問 — 此角色在當前帳戶中定義和使用。 AWS Resilience Hub 將扮演此角色來存取應用程式的資源。

  若要提供以角色為基礎的存取權，角色必須包含下列項目：

  - 讀取資源的唯讀權限 (AWS Resilience Hub 建議您使用受`AwsResilienceHubAssessmentPolicy`管政策)。
  - 信任原則會擔任此角色，可讓 AWS Resilience Hub 服務主體擔任此角色。如果您的帳戶中沒有設定此類角色， AWS Resilience Hub 將會顯示建立該角色的指示。如需詳細資訊，請參閱 the section called “步驟 6：設定權限”。

> **Note**
>
> 如果您僅提供呼叫者角色名稱，而且您的資源位於其他帳戶中，則 AWS Resilience Hub 會在其他帳號中使用此角色名稱來存取跨帳戶資源。或者，您可以為其他帳號設定角色 ARN，這些帳號將用來取代呼叫者角色名稱。

- 目前的 IAM 使用者存取權限 — AWS Resilience Hub 將使用目前的 IAM 使用者存取您的應用程式資源。當您的資源位於不同的帳戶中時， AWS Resilience Hub 將採用以下 IAM 角色來存取資源：
  - `AwsResilienceHubAdminAccountRole`在當前帳戶
  - `AwsResilienceHubExecutorAccountRole`在其他帳戶

  此外，當您設定排程的評估時， AWS Resilience Hub 會擔任該`AwsResilienceHubPeriodicAssessmentRole`角色。不過，不建議使用`AwsResilienceHubPeriodicAssessmentRole`，因為您必須手動設定角色和權限，而且某些功能 (例如彈性漂移偵測) 可能無法如預期般運作。

AWS 復原中樞身分識別與存取疑難

使用下列資訊可協助您診斷和修正使用 AWS 彈性中樞和 IAM 時可能會遇到的常見問題。

主題

- 我沒有授權在 AWS 彈性集線器中執行操作
- 我沒有授權執行 iam：PassRole
- 我想允許我以外的人訪問我 AWS 帳戶 的 AWS 彈性中心資源

我沒有授權在 AWS 彈性集線器中執行操作

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

下列範例錯誤會在`mateojackson` IAM 使用者嘗試使用主控台檢視一個虛構 *`my-example-widget`* 資源的詳細資訊，但卻無虛構 `resiliencehub:`*`GetWidget`* 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 resiliencehub:GetWidget on resource: my-example-widget
```

在此情況下，必須更新 mateojackson 使用者的政策，允許使用 resiliencehub:*GetWidget* 動作存取 *my-example-widget* 資源。

如果您需要協助，請聯絡您的 AWS 系統管理員。您的管理員提供您的簽署憑證。

我沒有授權執行 iam：PassRole

如果您收到未授權執行iam:PassRole動作的錯誤訊息，則必須更新您的原則，以允許您將角色傳遞至 AWS Resurability Hub。

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

當名為的 IAM 使用者marymajor嘗試使用主控台在 AWS 彈性中樞執行動作時，就會發生下列範例錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

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

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

如果您需要協助，請聯絡您的 AWS 系統管理員。您的管理員提供您的簽署憑證。

我想允許我以外的人訪問我 AWS 帳戶 的 AWS 彈性中心資源

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

如需進一步了解，請參閱以下內容：

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

AWS Resilience Hub 存取權限參考

您可以使用 AWS Identity and Access Management (IAM) 管理應用程式資源的存取權限，並建立適用於使用者、群組或角色的 IAM 政策。

每個 AWS Resilience Hub 應用程式都可以設定為使用 the section called “呼叫者角色” (IAM 角色)，或使用目前的 IAM 使用者許可 (以及一組用於跨帳戶和排程評估的預先定義角色)。在此角色中，您可以附加定義存取其他 AWS 資源或應用程式資源所需權限的原則。 AWS Resilience Hub 呼叫者角色必須具有新增至 AWS Resilience Hub 服務主體的信任原則。

若要管理應用程式的權限，建議您使用the section called “AWS 受管理政策”. 您可以在不進行任何修改的情況下使用這些受管理的策略，也可以使用它們作為編寫自己的限制性策略的起點。策略可以使用其他選用條件，在資源層級限制不同動作的使用者權限。

如果您的應用程式資源位於不同的帳號 (次要帳號/資源帳號) 中，您必須在每個包含應用程式資源的帳號中設定新角色。

主題

- the section called “使用 IAM 角色”
- the section called “使用目前的 IAM 使用者許可”

使用 IAM 角色

AWS Resilience Hub 將使用預先定義的現有 IAM 角色來存取主要帳戶或次要/資源帳戶中的資源。這是存取資源的建議權限選項。

主題

- the section called “呼叫者角色”
- the section called “跨帳戶存取不同 AWS 帳戶的角色”

呼叫者角色

AWS Resilience Hub 呼叫者角色是 AWS Resilience Hub 假設存取 AWS 服務和資源的 AWS Identity and Access Management (IAM) 角色。例如，您可以建立呼叫者角色，該角色具有存取 CFN 範本及其建立之資源的權限。本頁提供如何建立、檢視及管理應用程式呼叫者角色的相關資訊。

當您建立應用程式時，您會提供呼叫者角色。 AWS Resilience Hub 當您匯入資源或開始評估時，假定此角色可存取您的資源。若 AWS Resilience Hub 要正確承擔呼叫者角色，角色的信任原則必須將 AWS Resilience Hub 服務主體 (彈性 hub.amaz onaws.com) 指定為受信任的服務。

若要檢視應用程式的呼叫者角色，請從導覽窗格中選擇 [應用程式]，然後從 [應用程式] 頁面的 [動作] 功能表選擇 [更新權限]。

您可以隨時從應用程式呼叫者角色新增或移除權限，或將應用程式設定為使用不同的角色來存取應用程式資源。

主題

- the section called “在 IAM 主控台中建立呼叫者角色”
- the section called “使用 IAM API 管理角色”
- the section called “使用 JSON 檔案定義信任原則”

在 IAM 主控台中建立呼叫者角色

若 AWS Resilience Hub 要啟用存取 AWS 服務和資源，您必須使用 IAM 主控台在主要帳戶中建立叫用者角色。如需使用 IAM 主控台建立角色的詳細資訊，請參閱建立 AWS 服務角色 (主控台)。

使用 IAM 主控台在主要帳戶中建立呼叫者角色

1. 在 `https://console.aws.amazon.com/iam/` 開啟 IAM 主控台。
2. 在導覽窗格中，選擇 [角色]，然後選擇 [建立角色]。
3. 選取 [自訂信任原則]，在 [自訂信任原則] 視窗中複製下列原則，然後選擇 [下一步]。

> **Note**
>
> 如果您的資源位於不同的帳戶中，則必須在每個帳戶中建立角色，並針對其他帳戶使用次要帳號信任策略。

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

```
        "Service": "resiliencehub.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. 在 [新增權限] 頁面的 [權限原則] 區段AWSResilienceHubAsssessmentExecutionPolicy中，輸入 [依內容或原則名稱篩選原則]，然後按 Enter 方塊。
5. 選取原則，然後選擇 [下一步]。
6. 在 [角色詳細資料] 區段中，在 [角色名稱] 方塊中輸入唯一的角色名稱 (例如AWSResilienceHubAssessmentRole)。

   此欄位僅接受字母數字和 '+=,.@-_/' 字元。
7. (選擇性) 在 [說明] 方塊中輸入有關角色的說明。
8. 選擇建立角色。

   若要編輯使用案例和權限，請在步驟 6 中選擇位於「步驟 1：選取信任的實體」或「步驟 2：新增權限」區段右側的「編輯」按鈕。

建立呼叫者角色和資源角色 (如果適用) 之後，您可以將應用程式設定為使用這些角色。

> **Note**
>
> 建立或更新應用程式時，您必須在目前的 IAM 使用者/角色中具有呼叫者角色的iam:passRole權限。但是，您不需要此權限即可執行評估。

使用 IAM API 管理角色

角色的信任原則會授予指定主體擔任該角色的權限。若要使用 AWS Command Line Interface (AWS CLI) 建立角色，請使用create-role指令。使用此命令時，您可以內嵌指定信任原則。下列範例顯示如何授與 AWS Resilience Hub 服務的主體權限來擔任您的角色。

> **Note**
>
> JSON 字串中逸出引號 (' ') 的要求可能會因您的殼層版本而有所不同。

樣品 create-role

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-role-policy-
document '{
  "Version": "2012-10-17","Statement":
  [
    {
      "Effect": "Allow",
      "Principal": {"Service": "resiliencehub.amazonaws.com"},
      "Action": "sts:AssumeRole"
    }
  ]
}'
```

使用 JSON 檔案定義信任原則

您可以使用個別的 JSON 檔案定義角色的信任原則，然後執行create-role命令。在下列範例中，**trust-policy.json**是包含目前目錄中信任原則的檔案。此原則會藉由執行**create-role**命令附加至角色。**create-role**命令的輸出顯示在「樣本輸出」中。若要將權限新增至角色，請使用attach-policy-to-role命令，然後您可以先新增受AWSResilienceHubAsssessmentExecutionPolicy管理的原則。如需有關此受管理原則的詳細資訊，請參閱the section called “AWSResilienceHubAsssessmentExecutionPolicy”。

樣品 trust-policy.json

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

樣品 create-role

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-
role-policy-document file://trust-policy.json
```

範例輸出

```
{
    "Role": {
        "Path": "/",
        "RoleName": "AWSResilienceHubAssessmentRole",
        "RoleId": "AROAQFOXMPL6TZ6ITKWND",
        "Arn": "arn:aws:iam::123456789012:role/AWSResilienceHubAssessmentRole",
        "CreateDate": "2020-01-17T23:19:12Z",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [{
                "Effect": "Allow",
                "Principal": {
                    "Service": "resiliencehub.amazonaws.com"
                },
                "Action": "sts:AssumeRole"
            }]
        }
    }
}
```

樣品 **attach-policy-to-role**

```
aws iam attach-role-policy --role-name AWSResilienceHubAssessmentRole --
policy-arn arn:aws:iam::aws:policy/
AWSResilienceHubAsssessmentExecutionPolicy
```

跨帳戶存取不同 AWS 帳戶的角色-選擇性

當您的資源位於次要/資源帳號中時，您必須在每個帳號中建立角色，才能成功評估您的應 AWS Resilience Hub 用程式。角色建立程序與呼叫者角色建立程序類似，信任原則組態除外。

> **Note**
>
> 您必須在資源所在的次要帳號中建立角色。

主題

- the section called “在IAM 主控台中為次要/資源帳戶建立角色”
- the section called “使用 IAM API 管理角色”
- the section called “使用 JSON 檔案定義信任原則”

在IAM 主控台中為次要/資源帳戶建立角色

若 AWS Resilience Hub 要啟用存取其他 AWS 帳號中的 AWS 服務和資源，您必須在每個帳號中建立角色。

使用IAM 主控台為次要/資源帳戶在IAM 主控台中建立角色

1. 在 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 在導覽窗格中，選擇 [角色]，然後選擇 [建立角色]。
3. 選取 [自訂信任原則]，在 [自訂信任原則] 視窗中複製下列原則，然後選擇 [下一步]。

> **Note**
>
> 如果您的資源位於不同的帳戶中，則必須在每個帳戶中建立角色，並針對其他帳戶使用次要帳號信任策略。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::primary_account_id:role/InvokerRoleName"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. 在 [新增權限] 頁面的 [權限原則] 區段AWSResilienceHubAsssessmentExecutionPolicy中，輸入 [依內容或原則名稱篩選原則]，然後按 Enter 方塊。
5. 選取原則，然後選擇 [下一步]。
6. 在 [角色詳細資料] 區段中，在 [角色名稱] 方塊中輸入唯一的角色名稱 (例如AWSResilienceHubAssessmentRole)。
7. (選擇性) 在 [說明] 方塊中輸入有關角色的說明。

8. 選擇建立角色。

   若要編輯使用案例和權限，請在步驟 6 中選擇位於「步驟 1：選取信任的實體」或「步驟 2：新增權限」區段右側的「編輯」按鈕。

此外，您還需要將呼叫者角色的`sts:assumeRole`權限新增至呼叫者角色，才能使其在次要帳戶中擔任角色。

針對您建立的每個次要角色，將下列原則新增至呼叫者角色：

```
{
    "Effect": "Allow",
    "Resource": [
      "arn:aws:iam::secondary_account_id_1:role/RoleInSecondaryAccount_1",
      "arn:aws:iam::secondary_account_id_2:role/RoleInSecondaryAccount_2",
      ...
      ],
      "Action": [
        "sts:AssumeRole"
      ]
}
```

使用 IAM API 管理角色

角色的信任原則會授予指定主體擔任該角色的權限。若要使用 AWS Command Line Interface (AWS CLI) 建立角色，請使用`create-role`指令。使用此命令時，您可以指定內嵌信任政策。下列範例顯示如何授與 AWS Resilience Hub 服務主體承擔您的角色的權限。

> **Note**
>
> JSON 字串中逸出引號 (' ') 的要求可能會因您的殼層版本而有所不同。

樣品 `create-role`

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-role-policy-
document '{"Version": "2012-10-17","Statement": [{"Effect": "Allow","Principal":
 {"AWS": ["arn:aws:iam::primary_account_id:role/InvokerRoleName"]},"Action":
 "sts:AssumeRole"}]}'
```

您也可使用單獨的 JSON 檔案來定義角色的信任政策。在下列範例中，trust-policy.json 為當前目錄中的檔案。

使用 JSON 檔案定義信任原則

您可以使用個別的 JSON 檔案定義角色的信任原則，然後執行create-role命令。在下列範例中，**trust-policy.json**是包含目前目錄中信任原則的檔案。此原則會藉由執行**create-role**命令附加至角色。**create-role**命令的輸出顯示在「樣本輸出」中。若要將權限新增至角色，請使用attach-policy-to-role命令，然後您可以先新增受AWSResilienceHubAsssessmentExecutionPolicy管理的原則。如需有關此受管理原則的詳細資訊，請參閱the section called “AWSResilienceHubAsssessmentExecutionPolicy”。

樣品 trust-policy.json

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::primary_account_id:role/InvokerRoleName"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

樣品 create-role

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-role-policy-
document file://trust-policy.json
```

範例輸出

```
{
    "Role": {
        "Path": "/",
        "RoleName": "AWSResilienceHubAssessmentRole2",
        "RoleId": "AROAT2GICMEDJML6EVQRG",
        "Arn": "arn:aws:iam::262412591366:role/AWSResilienceHubAssessmentRole2",
```

```
        "CreateDate": "2023-08-02T07:49:23+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": [
                            "arn:aws:iam::262412591366:role/
AWSResilienceHubAssessmentRole"
                        ]
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }
    }
}
```

樣品 attach-policy-to-role

```
aws iam attach-role-policy --role-name AWSResilienceHubAssessmentRole --
policy-arn arn:aws:iam::aws:policy/
AWSResilienceHubAsssessmentExecutionPolicy.
```

使用目前的 IAM 使用者許可

如果您想要使用目前的 IAM 使用者許可建立和執行評估，請使用此方法。您可以將受AWSResilienceHubAsssessmentExecutionPolicy管政策附加到 IAM 使用者或與使用者相關聯的角色。

單一帳戶設定

使用上述受管政策足以在與 IAM 使用者在相同帳戶中管理的應用程式上執行評估。

排程評估設定

您必須建立新角色，AwsResilienceHubPeriodicAssessmentRole才能執 AWS Resilience Hub 行排程的評估相關工作。

> **Note**
>
> - 使用基於角色的訪問（具有上面提到的調用者角色）時，不需要此步驟。

- 角色名稱必須是AwsResilienceHubPeriodicAssessmentRole。

啟用執 AWS Resilience Hub 行預約評估相關工作

1. 將AWSResilienceHubAsssessmentExecutionPolicy受管理的原則附加至角色。
2. 新增下列策略，其中primary_account_id是定義應用程式並執行評估的 AWS 帳戶。此外，您必須針對已排程評估的角色新增相關聯的信任原則 (AwsResilienceHubPeriodicAssessmentRole)，以授予 AWS Resilience Hub 服務承擔排定評估角色的權限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "sts:AssumeRole"
      ],
      "Resource": "arn:aws:iam::primary_account_id:role/
AwsResilienceHubAdminAccountRole"
    },
    {
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": [
        "arn:aws:iam::primary_account_id:role/
AwsResilienceHubAssessmentEKSAccessRole"
      ]
    }
  ]
}
```

已排程評估角色的信任原則 (**AwsResilienceHubPeriodicAssessmentRole**)

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "resiliencehub.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

跨帳戶設定

如果您使用多個帳戶的 AWS 彈性中樞，則需要以下 IAM 許可政策。根據您的使用案例，每個 AWS 帳戶可能需要不同的權限。設 AWS Resilience Hub 定跨帳戶存取時，會考慮下列帳戶和角色：

- 主要帳戶 — 您要在其中建立應用程式並執行評估的 AWS 帳戶。
- 次要/資源帳號 — 資源所在的 AWS 帳號。

> **Note**
>
> - 使用基於角色的訪問（具有上面提到的調用者角色）時，不需要此步驟。
> - 如需設定許可以存取 Amazon Elastic Kubernetes Service 的詳細資訊，請參閱。the section called “啟 AWS Resilience Hub 用對您的 Amazon EKS 叢集的存取”

主要帳戶設定

您必須在主要帳戶`AwsResilienceHubAdminAccountRole`中建立新角色，並啟用 AWS Resilience Hub 存取權才能擔任該角色。此角色將用於存取您 AWS 帳戶中包含您資源的其他角色。它不應該具有讀取資源的權限。

> **Note**
>
> - 角色名稱必須是`AwsResilienceHubAdminAccountRole`。
> - 它必須在主要帳戶中建立。
> - 您目前的 IAM 使用者/角色必須具有擔任此角色的`iam:assumeRole`權限。

- 以相關secondary_account_id_1/2/...的次要帳戶識別碼取代。

下列原則提供您角色的執行者權限，以存取 AWS 帳戶中其他角色的資源：

```
{
  {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Resource": [
        "arn:aws:iam::secondary_account_id_1:role/AwsResilienceHubExecutorAccountRole",
        "arn:aws:iam::secondary_account_id_2:role/AwsResilienceHubExecutorAccountRole",
        ...
      ],
      "Action": [
        "sts:AssumeRole"
      ]
    }
  ]
}
```

管理員角色 (AwsResilienceHubAdminAccountRole) 的信任原則如下：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::primary_account_id:role/caller_IAM_role"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::primary_account_id:role/
AwsResilienceHubPeriodicAssessmentRole"
      },
      "Action": "sts:AssumeRole"
```

```
    }
  ]
}
```

次要/資源帳號設定

在每個次要帳戶中，您必須建立新帳戶AwsResilienceHubExecutorAccountRole並啟用上述建立的管理員角色，才能擔任此角色。由 AWS Resilience Hub 於此角色將用於掃描和評估您的應用程式資源，因此也需要適當的權限。

不過，您必須將AWSResilienceHubAsssessmentExecutionPolicy受管理的原則附加至角色，並附加 Executor 角色原則。

執行者角色信任策略如下：

```
{
  {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::primary_account_id:role/AwsResilienceHubAdminAccountRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

AWS 受管理的政策 AWS Resilience Hub

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

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

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

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

AWSResilienceHubAsssessmentExecutionPolicy

您可以將其附加AWSResilienceHubAsssessmentExecutionPolicy到您的 IAM 身分。執行評估時，此原則會授與其他 AWS 服務的存取權限，以便執行評估。

許可詳細資訊

此政策提供足夠的許可以將警示 AWS FIS 和 SOP 範本發佈到您的 Amazon Simple Storage Service (Amazon S3) 儲存貯體。Amazon S3 存儲桶名稱必須以開頭aws-resilience-hub-artifacts-。如果您希望發佈到另一個 Amazon S3 儲存貯體，可以在呼叫 CreateRecommendationTemplate API 時執行此操作。如需詳細資訊，請參閱CreateRecommendationTemplate。

此政策包含以下許可：

- Amazon CloudWatch (CloudWatch) — 獲取您在 Amazon 中設置的所有實施警報 CloudWatch 以監控應用程序。此外，我們還會用cloudwatch:PutMetricData來發佈ResilienceHub命名空間中應用程式彈性分數的 CloudWatch 指標。
- Amazon Data Lifecycle Manager — 取得與您 AWS 帳戶相關聯之 Amazon Data Lifecycle Manager 資源並提供Describe許可。
- Amazon DevOps 大師 — 列出並提供與您 AWS 帳戶相關聯的 Amazon DevOps 大師資源的Describe許可。
- 亞馬遜動 DynamoDB 資源 — 列出並提供與您帳戶相關聯的 Amazon DynamoDB 資源的Describe許可。 AWS
- Amazon ElastiCache (ElastiCache) — 為與您的 AWS 帳戶相關聯的 ElastiCache 資源提供Describe許可。
- 亞馬遜彈性運算雲端 (Amazon EC2) — 列出和提供與您 AWS 帳戶相關聯的 Amazon EC2 資源的Describe許可。
- Amazon Elastic Container Registry (Amazon ECR) — 為與您 AWS 的帳戶相關聯的 Amazon ECR 資源提供Describe許可。
- Amazon Elastic Container Service (Amazon ECS) — 為與您 AWS 的帳戶相關聯的 Amazon ECS 資源提供Describe許可。

- Amazon Elastic File System (Amazon EFS) — 為與您的 AWS 帳戶相關聯的 Amazon EFS 資源提供Describe許可。
- Amazon Elastic Kubernetes Service (Amazon EKS) — 列出並提供與您帳戶相關聯的 Amazon EKS 資源的Describe許可。 AWS
- Amazon EC2 Auto Scaling — 列出和提供與您 AWS 帳戶相關聯的 Amazon EC2 Auto Scaling 資源的Describe許可。
- Amazon EC2 Systems Manager (SSM) — 為與您 AWS 的帳戶相關聯的 SSM 資源提供Describe許可。
- Amazon 故障注入服務 (AWS FIS) — 列出並提供與您 AWS 帳戶相關聯的 AWS FIS 實驗和實驗範本的Describe許可。
- Amazon FSx FSx for Windows File Server (Amazon FSx) — 列出並提供與您Describe帳戶相關聯的 Amazon FSx 資源的許可。 AWS
- Amazon RDS — 列出和提供與您 AWS 帳戶相關聯的 Amazon RDS 資源的Describe許可。
- Amazon 路線 53 (路線 53) — 列出和提供與您 AWS 帳戶關聯的 Route 53 資源的Describe許可。
- Amazon Route 53 Resolver — 列出並提供與您 AWS 帳戶相關聯之 Amazon Route 53 Resolver 資源的Describe權限。
- 亞馬遜簡單通知服務 (Amazon SNS) — 列出並提供與您 AWS 帳戶相關聯的 Amazon SNS 資源的Describe許可。
- Amazon Simple Queue Service (Amazon SQS) — 列出並提供與您 AWS 帳戶相關聯的 Amazon SQS 資源的Describe許可。
- 亞馬遜簡單儲存服務 (Amazon S3) — 列出並提供與您 AWS 帳戶相關聯的 Amazon S3 資源的Describe許可。

> **Note**
>
> 執行評估時，如果有任何遺失的權限需要從受管政策更新，則 AWS Resilience Hub 會使用 s3: GetBucketLogging 權限順利完成評估。不過， AWS Resilience Hub 會顯示一則警告訊息，其中列出遺失的權限，並提供寬限期來新增相同權限。如果您未在指定的寬限期內新增遺失的權限，評估將會失敗。

- AWS Backup — 列出和Describe取得與您 AWS 帳戶相關聯的 Amazon EC2 Auto Scaling 資源的許可。

- AWS CloudFormation — 列出並Describe取得與您 AWS 帳戶相關聯之 AWS CloudFormation 堆疊資源的權限。
- AWS DataSync — 列出並提供與您 AWS 帳戶相關聯之 AWS DataSync 資源的Describe權限。
- AWS Directory Service — 列出並提供與您 AWS 帳戶相關聯之 AWS Directory Service 資源的Describe權限。
- AWS Elastic Disaster Recovery (彈性災難復原) — 提供與您 AWS 帳戶相關聯的彈性災難復原資源的Describe權限。
- AWS Lambda (Lambda) — 列出並提供與您 AWS 帳戶相關聯的 Lambda 資源的Describe許可。
- AWS Resource Groups (Resource Groups) — 列出並提供與您 AWS 帳號相關聯之 Resource Groups 資源的Describe權限。
- AWS Service Catalog (Service Catalog) — 列出並提供與您 AWS 帳戶相關聯的 Service Catalog 資源的Describe權限。
- AWS Step Functions — 列出並提供與您 AWS 帳戶相關聯之 AWS Step Functions 資源的Describe權限。
- Elastic Load Balancing — 列出並提供與您 AWS 帳戶相關聯的 Elastic Load Balancing 資源的Describe權限。
- ssm:GetParametersByPath— 我們使用此權限來管理針對您的應用程序配置的 CloudWatch 警報，測試或 SOP。

AWS 帳戶需要下列 IAM 政策，才能為使用者、使用者群組和角色新增許可，這些許可為團隊提供執行評估時存取 AWS 服務所需的權限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "application-autoscaling:DescribeScalableTargets",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:DescribeBackupVault",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
```

```
        "cloudformation:ValidateTemplate",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "datasync:DescribeTask",
        "datasync:ListLocations",
        "datasync:ListTasks",
        "devops-guru:ListMonitoredResources",
        "dlm:GetLifecyclePolicies",
        "dlm:GetLifecyclePolicy",
        "drs:DescribeJobs",
        "drs:DescribeSourceServers",
        "drs:GetReplicationConfiguration",
        "ds:DescribeDirectories",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DescribeFleets",
        "ec2:DescribeHosts",
        "ec2:DescribeInstances",
        "ec2:DescribeNatGateways",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpoints",
        "ecr:DescribeRegistry",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeNodegroup",
```

```
        "eks:ListFargateProfiles",
        "eks:ListNodegroups",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "fis:GetExperimentTemplate",
        "fis:ListExperimentTemplates",
        "fis:ListExperiments",
        "fsx:DescribeFileSystems",
        "lambda:GetFunctionConcurrency",
        "lambda:GetFunctionConfiguration",
        "lambda:ListAliases",
        "lambda:ListVersionsByFunction",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBInstances",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBSnapshots",
        "rds:DescribeGlobalClusters",
        "resource-groups:GetGroup",
        "resource-groups:ListGroupResources",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-readiness:GetReadinessCheckStatus",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53:GetHealthCheck",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListResourceRecordSets",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverEndpointIpAddresses",
        "s3:GetBucketLocation",
```

```
        "s3:GetBucketLogging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetMultiRegionAccessPointRoutes",
        "s3:GetReplicationConfiguration",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "servicecatalog:GetApplication",
        "servicecatalog:ListAssociatedResources",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "ssm:DescribeAutomationExecutions",
        "states:DescribeStateMachine",
        "states:ListStateMachineVersions",
        "states:ListStateMachineAliases",
        "tag:GetResources"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "apigateway:GET"
      ],
      "Resource": [
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/usageplans"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource": "arn:aws:s3:::aws-resilience-hub-artifacts-*"
```

```
    },
    {
      "Effect": "Allow",
      "Action": [
        "cloudwatch:PutMetricData"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "cloudwatch:namespace": "ResilienceHub"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:GetParametersByPath"
      ],
      "Resource": "arn:aws:ssm:*:*:parameter/ResilienceHub/*"
    }
  ]
}
```

AWS Resilience HubAWS 受管理策略的更新

檢視 AWS Resilience Hub 自此服務開始追蹤這些變更以來的 AWS 受管理策略更新詳細資料。如需有關此頁面變更的自動警示，請訂閱「 AWS Resilience Hub 文件歷史記錄」頁面上的 RSS 摘要。

變更	描述	日期
AWSResilienceHubAssessmentExecutionPolicy—AWS Resilience Hub 擴展了對 Amazon FSx for Windows File Server 的支持。	此 AWS Resilience Hub 政策可讓您讀取適用於 Windows 檔案伺服器的 Amazon FSx 組態。	2024年3月26日
AWSResilienceHubAssessmentExecutionPolicy-	此 AWS Resilience Hub 原則可讓您讀取 AWS Step Functions 組態。	2023 年 10 月 30 日

變更	描述	日期
AWS Resilience Hub 擴展支持 AWS Step Functions.		
AWSResilienceHubAssessmentExecutionPolicy—AWS Resilience Hub 改進了對 Amazon Relational Database Service（Amazon RDS）的支持。	此 AWS Resilience Hub 政策可讓您在執行評估時存取 Amazon RDS 上的資源。	2023 年 10 月 5 日
AWSResilienceHubAssessmentExecutionPolicy – 新政策	此 AWS Resilience Hub 原則可讓您存取其他 AWS 服務以執行評估。	2023 年 6 月 26 日
AWS Resilience Hub 開始追蹤變更	AWS Resilience Hub 開始追蹤其 AWS 受管理策略的變更。	2023 年 6 月 15 日

將地形狀態檔案匯入 AWS Resilience Hub

AWS Resilience Hub 支援匯入使用伺服器端加密 (SSE) 與 Amazon 簡單儲存服務受管金鑰 (SSE-S3) 或受管金鑰 (SSE-KMS) 加密的 AWS Key Management Service Terraform 狀態檔案。如果您的 Terraform 狀態檔案使用客戶提供的加密金鑰 (SSE-C) 進行加密，您將無法使用匯入檔案。 AWS Resilience Hub

將 Terraform 狀態檔案匯入至 AWS Resilience Hub 需要下列 IAM 政策，具體取決於您的狀態檔案所在的位置。

從位於主帳戶的 Amazon S3 儲存貯體匯入地形表單狀態檔案

需要下列 Amazon S3 儲存貯體政策和 IAM 政策，才能允許 AWS Resilience Hub 讀取位於主帳戶上 Amazon S3 儲存貯體中的 Terraform 狀態檔案。

- 儲存貯體政策 — 位於主帳戶的目標 Amazon S3 儲存貯體上的儲存貯體政策。如需詳細資訊，請參閱下列範例。

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<s3-bucket-name>/<path-to-state-file>"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::<s3-bucket-name>"
    }
  ]
}
```

- 身分政策 — 為此應用程式定義的 Invoker 角色相關聯的身分政策，或主 AWS 帳戶 AWS Resilience Hub 上 AWS 目前的 IAM 角色。如需詳細資訊，請參閱下列範例。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<s3-bucket-name>/<path-to-state-file>"
    },
    {
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::<s3-bucket-name>"
    }
  ]
}
```

> **Note**
>
> 如果您使用AWSResilienceHubAsssessmentExecutionPolicy受管理的策略，則不需要ListBucket權限。

> **Note**
>
> 如果您的 Terraform 狀態檔案使用 KMS 加密，您必須新增下列kms:Decrypt權限。

```
{
      "Effect": "Allow",
      "Action": [
              "kms:Decrypt",
      ],
      "Resource": "<arn_of_kms_key>"
}
```

從位於次要帳戶的 Amazon S3 儲存貯體匯入地形表單狀態檔案

- 儲存貯體政策 — 目標 Amazon S3 儲存貯體上的儲存貯體政策，該儲存貯體位於其中一個次要帳戶中。如需詳細資訊，請參閱下列範例。

```
 {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>/<path-
to-state-file>"
    },
    {
      "Effect": "Allow",
```

```
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>"
    }
  ]
}
```

- 身份策略 — AWS 帳號角色的關聯身份策略，該角色在主 AWS 帳號 AWS Resilience Hub 上執行。如需詳細資訊，請參閱下列範例。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>/<path-
to-state-file>"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>"
    }
  ]
}
```

> **Note**
>
> 如果您使用AWSResilienceHubAsssessmentExecutionPolicy受管理的策略，則不需要ListBucket權限。

> **Note**
>
> 如果您的 Terraform 狀態檔案使用 KMS 加密，您必須新增下列kms:Decrypt權限。

```
{
      "Effect": "Allow",
      "Action": [
              "kms:Decrypt",
      ],
      "Resource": "<arn_of_kms_key>"
}
```

啟 AWS Resilience Hub 用對 Amazon Elastic Kubernetes Service 叢集的存取

AWS Resilience Hub 透過分析 Amazon EKS 叢集的基礎設施來評估亞馬遜彈性 Kubernetes 服務 (Amazon EKS) 叢集的復原能力。 AWS Resilience Hub 使用 Kubernetes 角色型存取控制 (RBAC) 組態來評估其他 Kubernetes (K8s) 工作負載，這些工作負載會部署為 Amazon EKS 叢集的一部分。若 AWS Resilience Hub 要查詢 Amazon EKS 叢集以分析和評估工作負載，您必須完成以下操作：

- 在與 Amazon EKS 叢集相同的帳戶中建立或使用現有的 AWS Identity and Access Management (IAM) 角色。
- 啟用 IAM 使用者和角色對 Amazon EKS 叢集的存取權限，並將其他唯讀許可授與 Amazon EKS 叢集內的 K8s 資源。如需啟用 IAM 使用者和角色存取 Amazon EKS 叢集的詳細資訊，請參閱啟用 IAM 使用者和角色存取您叢集的權限-Amazon E KS。

在 Amazon EKS 控制平台上執行的 Kubernetes 的AWS IAM 身份驗證器會啟用使用 IAM 實體存取 Amazon EKS 叢集。驗證器會從中取得組態資訊。aws-auth ConfigMap

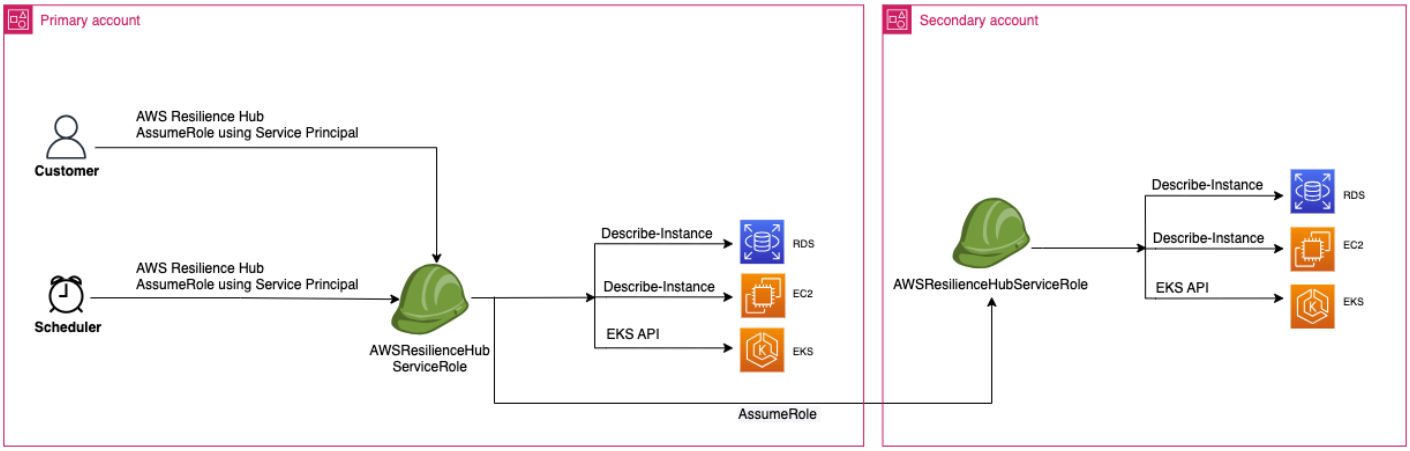
> **Note**
>
> - 如需有關所有`aws-auth ConfigMap`設定的詳細資訊，請參閱（詳見）的完整組態格式 GitHub。
> - 如需有關不同 IAM 身分的詳細資訊，請參閱 IAM 使用者指南中的身分識別 (使用者、群組和角色)。
> - 如需 Kubernetes 角色型存取控制 (RBAC) 組態的相關資訊，請參閱使用 RBAC 授權。

AWS Resilience Hub 使用帳戶中的 IAM 角色查詢 Amazon EKS 叢集中的資源。若 AWS Resilience Hub 要存取 Amazon EKS 叢集內的資源， AWS Resilience Hub 必須將所使用的 IAM 角色對應至具有足夠唯讀許可權的 Kubernetes 群組，才能存取 Amazon EKS 叢集內的資源。

AWS Resilience Hub 可讓您使用下列其中一個 IAM 角色選項存取 Amazon EKS 叢集資源：

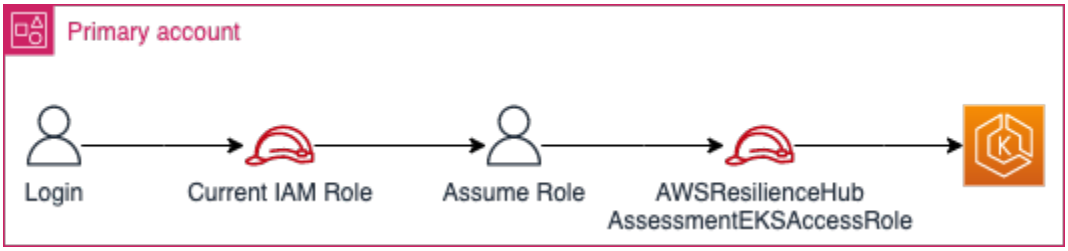
- 如果您的應用程式設定為使用以角色為基礎的存取來存取資源，則在評估期間將使用建立應用程式 AWS Resilience Hub 時傳遞給的呼叫者角色或次要帳戶角色來存取 Amazon EKS 叢集。

  下列概念圖顯示當應用程式設定為以角色為基礎的應用程式時，如何 AWS Resilience Hub 存取 Amazon EKS 叢集。

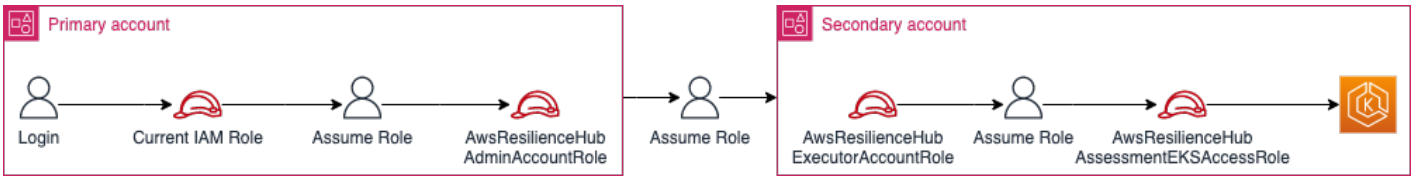


- 如果您的應用程式設定為使用目前的 IAM 使用者存取資源，則必須使用該名稱`AwsResilienceHubAssessmentEKSAccessRole`與 Amazon EKS 叢集相同的帳戶建立新的 IAM 角色。然後，此 IAM 角色將用於存取您的 Amazon EKS 叢集。

  下列概念圖顯示當應用程式設定為使用目前 IAM 使用者許可時，如何 AWS Resilience Hub 存取主要帳戶中部署的 Amazon EKS 叢集。



下列概念圖顯示當應用程式設定為使用目前 IAM 使用者許可時，如何 AWS Resilience Hub 存取次要帳戶上部署的 Amazon EKS 叢集。



AWS Resilience Hub 授與 Amazon EKS 叢集中資源的存取權

AWS Resilience Hub 可讓您存取位於 Amazon EKS 叢集上的資源，前提是您已設定必要的許可。

授與用 AWS Resilience Hub 於探索和評估 Amazon EKS 叢集內資源的必要許可

1. 設定 IAM 角色以存取 Amazon EKS 叢集。

   如果您已使用以角色為基礎的存取來設定應用程式，則可以略過此步驟並繼續執行步驟 2，並使用您用來建立應用程式的角色。如需如何 AWS Resilience Hub 使用 IAM 角色的詳細資訊，請參閱the section called “AWS 彈性中樞如何與 IAM 搭配運作”。

   如果您已使用目前的 IAM 使用者許可設定應用程式，則必須在與 Amazon EKS 叢集相同的帳戶中建立 `AwsResilienceHubAssessmentEKSAccessRole` IAM 角色。然後，存取您的 Amazon EKS 叢集時會使用此 IAM 角色。

   匯入和評估應用程式時， AWS Resilience Hub 會使用 IAM 角色存取 Amazon EKS 叢集中的資源。此角色應建立在與 Amazon EKS 叢集相同的帳戶中，並將與 Kubernetes 群組對應，其中包含評估 Amazon EKS 叢集所 AWS Resilience Hub 需的許可。

   如果您的 Amazon EKS 叢集與 AWS Resilience Hub 呼叫帳戶位於相同的帳戶中，則應使用下列 IAM 信任政策建立角色。在此 IAM 信任政策中，用`caller_IAM_role`於目前帳戶來呼叫 API AWS Resilience Hub。

> **Note**
>
> 這caller_IAM_role是與您的 AWS 使用者帳戶相關聯的角色。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::eks_cluster_account_id:role/caller_IAM_role"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

如果 Amazon EKS 叢集位於跨帳戶 (與 AWS Resilience Hub 呼叫帳戶不同的帳戶)，您必須使用下列 AwsResilienceHubAssessmentEKSAccessRole IAM 信任政策建立 IAM 角色：

> **Note**
>
> 先決條件是，若要存取部署在不同於 AWS Resilience Hub 使用者帳戶的帳戶中的 Amazon EKS 叢集，您必須設定多帳戶存取。如需詳細資訊，請參閱

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::eks_cluster_account_id:role/
AwsResilienceHubExecutorRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
```

```
}
```

2. 為 AWS Resilience Hub 應用程式建立`ClusterRole`和 `ClusterRoleBinding` (或`RoleBinding`) 角色。

   建立`ClusterRole`並`ClusterRoleBinding`將授與必要的唯讀許可， AWS Resilience Hub 以便分析和評估屬於 Amazon EKS 叢集中特定命名空間一部分的資源。

   AWS Resilience Hub 可讓您透過完成下列其中一項，來限制其對命名空間的存取，以產生復原能力評估：

   a. 將所有命名空間的讀取權限授與 AWS Resilience Hub 應用程式。

      若 AWS Resilience Hub 要評估 Amazon EKS 叢集內所有命名空間之資源的彈性，您必須建立下列項目和。`ClusterRole` `ClusterRoleBinding`

      - `resilience-hub-eks-access-cluster-role`(`ClusterRole`) — 定義評估 Amazon EKS 叢集所需的許可。 AWS Resilience Hub
      - `resilience-hub-eks-access-cluster-role-binding`(`ClusterRoleBinding`) — 定義 Amazon EKS 叢集`resilience-hub-eks-access-group`中命名的群組授與其使用者，以及在中執行彈性評估所需的許可。 AWS Resilience Hub

      將所有命名空間讀取訪問權限授予 AWS Resilience Hub 應用程序的模板如下：

```
cat << EOF | kubectl apply -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: resilience-hub-eks-access-cluster-role
rules:
- apiGroups:
    - ""
  resources:
    - pods
    - replicationcontrollers
    - nodes
  verbs:
    - get
    - list
- apiGroups:
```

```
    - apps
  resources:
    - deployments
    - replicasets
  verbs:
    - get
    - list
- apiGroups:
    - policy
  resources:
    - poddisruptionbudgets
  verbs:
    - get
    - list
- apiGroups:
    - autoscaling.k8s.io
  resources:
    - verticalpodautoscalers
  verbs:
    - get
    - list
- apiGroups:
    - autoscaling
  resources:
    - horizontalpodautoscalers
  verbs:
    - get
    - list
- apiGroups:
    - karpenter.sh
  resources:
    - provisioners
  verbs:
    - get
    - list
- apiGroups:
    - karpenter.k8s.aws
  resources:
    - awsnodetemplates
  verbs:
    - get
    - list
---
apiVersion: rbac.authorization.k8s.io/v1
```

```
kind: ClusterRoleBinding
metadata:
  name: resilience-hub-eks-access-cluster-role-binding
subjects:
  - kind: Group
    name: resilience-hub-eks-access-group
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: resilience-hub-eks-access-cluster-role
  apiGroup: rbac.authorization.k8s.io
---
EOF
```

b. 授與讀 AWS Resilience Hub 取特定命名空間的存取權。

您可以使 AWS Resilience Hub RoleBinding用限制訪問一組特定命名空間內的資源。若要達成此目的，您必須建立下列角色：

- ClusterRole— 若 AWS Resilience Hub 要存取 Amazon EKS 叢集內特定命名空間中的資源並評估其彈性，您必須建立以下角色。ClusterRole
  - resilience-hub-eks-access-cluster-role— 指定評估特定命名空間內資源的必要權限。
  - resilience-hub-eks-access-global-cluster-role— 指定必要的許可，以評估 Amazon EKS 叢集內的叢集範圍資源，這些資源與特定命名空間無關聯。 AWS Resilience Hub 需要權限才能存取 Amazon EKS 叢集上叢集範圍的資源 (例如節點)，以評估應用程式的彈性。

  創建ClusterRole角色的模板如下：

```
cat << EOF | kubectl apply -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: resilience-hub-eks-access-cluster-role
rules:
  - apiGroups:
      - ""
    resources:
      - pods
      - replicationcontrollers
```

```
    verbs:
      - get
      - list
  - apiGroups:
      - apps
    resources:
      - deployments
      - replicasets
    verbs:
      - get
      - list
  - apiGroups:
      - policy
    resources:
      - poddisruptionbudgets
    verbs:
      - get
      - list
  - apiGroups:
      - autoscaling.k8s.io
    resources:
      - verticalpodautoscalers
    verbs:
      - get
      - list
  - apiGroups:
      - autoscaling
    resources:
      - horizontalpodautoscalers
    verbs:
      - get
      - list

---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: resilience-hub-eks-access-global-cluster-role
rules:
  - apiGroups:
      - ""
    resources:
      - nodes
    verbs:
```

```
      - get
      - list
  - apiGroups:
      - karpenter.sh
    resources:
      - provisioners
    verbs:
      - get
      - list
  - apiGroups:
      - karpenter.k8s.aws
    resources:
      - awsnodetemplates
    verbs:
      - get
      - list

---
EOF
```

- RoleBindingrole — 此角色授與存取特定命名空間內資源的必要權限。 AWS Resilience Hub 也就是說，您必須在每個命名空間中建立RoleBinding角色， AWS Resilience Hub 才能存取指定命名空間內的資源。

  > **Note**
  >
  > 如果您使用自動調度ClusterAutoscaler資源，則必須RoleBinding在中另外建立。kube-system這對於評估您的ClusterAutoscaler，這是kube-system命名空間的一部分是必要的。
  > 這樣，您將授予 AWS Resilience Hub 評估 Amazon EKS 叢集時所需的權限，以評估kube-system命名空間內的資源。

  創建RoleBinding角色的模板如下：

```
cat << EOF | kubectl apply -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: resilience-hub-eks-access-cluster-role-binding
```

```
  namespace: <namespace>
subjects:
  - kind: Group
    name: resilience-hub-eks-access-group
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: resilience-hub-eks-access-cluster-role
  apiGroup: rbac.authorization.k8s.io

---
EOF
```

- `ClusterRoleBinding`role — 此角色授與存取叢集範圍資 AWS Resilience Hub 源的必要權限。

  創建`ClusterRoleBinding`角色的模板如下：

```
cat << EOF | kubectl apply -f -
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: resilience-hub-eks-access-global-cluster-role-binding
subjects:
  - kind: Group
    name: resilience-hub-eks-access-group
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: resilience-hub-eks-access-global-cluster-role
  apiGroup: rbac.authorization.k8s.io

---
EOF
```

3. 更新`aws-auth ConfigMap`以使用用於存取 Amazon EKS 叢集的 IAM 角色對應。`resilience-hub-eks-access-group`

   此步驟會在步驟 1 中使用的 IAM 角色與步驟 2 中建立的 Kubernetes 群組之間建立對應。此對應授予存取權管理角色的許可，以存取 Amazon EKS 叢集內的資源。

> **Note**
>
> - ROLE-NAME是指用於存取 Amazon EKS 叢集的 IAM 角色。
>   - 如果您的應用程式設定為使用以角色為基礎的存取，則該角色應該是建立應用程式 AWS Resilience Hub 時傳送給的呼叫者角色或次要帳戶角色。
>   - 如果您的應用程式設定為使用目前的 IAM 使用者存取資源，則該應用程式必須是AwsResilienceHubAssessmentEKSAccessRole.
> - ACCOUNT-ID應該是 Amazon EKS 叢集的 AWS 帳戶識別碼。

您可以使aws-authConfigMap用下列其中一種方式建立：

- 使用 eksctl

  使用下列指令來更新 aws-authConfigMap：

  ```
  eksctl create iamidentitymapping \
   --cluster <cluster-name> \
   --region=<region-code> \
   --arn arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>\
   --group resilience-hub-eks-access-group \
   --username AwsResilienceHubAssessmentEKSAccessRole
  ```

- 您可以aws-authConfigMap通過將 IAM 角色詳細信息添加到ConfigMap下面數據的mapRoles部分來手動編輯。使用下列指令來編輯aws-authConfigMap。

  ```
  kubectl edit -n kube-system configmap/aws-auth
  ```

  mapRoles部分由以下參數組成：

  - rolearn— 要新增的 IAM 角色的 Amazon 資源名稱 (ARN)。
    - ARN 語法 —arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>.
  - username— 要對應至 IAM 角色的 Kubernetes 中的使用者名稱 ()。AwsResilienceHubAssessmentEKSAccessRole
  - groups— 群組名稱應與步驟 2 (resilience-hub-eks-access-group) 中建立的群組名稱相符。

> **Note**
>
> 如果mapRoles區段不存在，您必須手動新增此區段。

使用以下範本將 IAM 角色詳細資料新增至ConfigMap下方資料的mapRoles部分。

```
    - groups:
      - resilience-hub-eks-access-group
      rolearn: arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>
      username: AwsResilienceHubAssessmentEKSAccessRole
```

啟用發佈 AWS Resilience Hub 到您的 Amazon 簡易通知服務主題

本節說明如何啟用將應 AWS Resilience Hub 用程式相關通知發佈到 Amazon Simple Notification Service (Amazon SNS) 主題。若要將通知推送至 Amazon SNS 主題，請確保您具備下列各項：

- 作用中的 AWS Resilience Hub 應用程式。
- AWS Resilience Hub 必須向其傳送通知的現有 Amazon SNS 主題。如需有關建立 Amazon SNS 主題的詳細資訊，請參閱建立 Amazon SNS 主題。

若 AWS Resilience Hub 要啟用將通知發佈到您的 Amazon SNS 主題，您必須使用下列步驟更新 Amazon SNS 主題的存取政策：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowResilienceHubPublish",
      "Effect": "Allow",
      "Principal": {
        "Service": "resiliencehub.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account-id:topic-name"
    }
  ]
}
```

> **Note**
>
> 當您使用 AWS Resilience Hub 將訊息從選擇加入的區域發佈到位於預設啟用的區域中的主題時，您必須修改為 Amazon SNS 主題建立的資源政策。將主體的值從變更`resiliencehub.amazonaws.com`為`resiliencehub.<opt-in-region>.amazonaws.com`。

如果您使用的是伺服器端加密 (SSE) Amazon SNS 主題，則必須確保 AWS Resilience Hub 擁有 Amazon SNS 加密金鑰的`Decrypt`和 `GenerateDataKey` * 存取權。

若要提供`Decrypt`和`GenerateDataKey*`存取 AWS Resilience Hub，您必須包含下列權限才能 AWS Key Management Service 存取原則。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowResilienceHubDecrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "resiliencehub.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:region:account-id:key/key-id"
    }
  ]
}
```

限制權限以包含或排除 AWS Resilience Hub 建議

AWS Resilience Hub 可讓您限制每個應用程式包含或排除建議的權限。您可以使用下列 IAM 信任政策來限制許可，以包含或排除每個應用程式的建議。在此 IAM 信任政策中，目前帳 AWS 戶會使用 `caller_IAM_role` (與您的使用者帳戶相關聯) 來呼叫 API AWS Resilience Hub。

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "resiliencehub:BatchUpdateRecommendationStatus",
      "Resource": "arn:aws:resiliencehub:us-west-2:12345678900:app/0e6237b7-23ba-4103-
adb2-91811326b703"
    }
  ]
}
```

基礎結構安全 AWS Resilience Hub

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

您可以使用 AWS 已發佈的 API 呼叫透 AWS Resilience Hub 過網路進行存取。用戶端必須支援 Transport Layer Security (TLS) 1.2 或更新版本。建議使用 TLS 1.3 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，您可以使用 AWS Security Token Service (AWS STS) 以產生暫時安全憑證以簽署請求。

使用其他 服務

本節說明與之互動的 AWS 服務 AWS Resilience Hub。

主題

- AWS CloudFormation
- AWS CloudTrail
- AWS Systems Manager
- AWS Trusted Advisor

AWS CloudFormation

AWS Resilience Hub 已與 AWS CloudFormation 整合，這項服務可協助您建立 AWS 資源的模型和設定，以減少建立和管理資源和基礎設施的時間。您可以建立描述您想要的所有AWS資源 (例如 AWS::ResilienceHub:::ResiliencyPolicy 和 AWS::ResilienceHub:::App) 的範本，並為您AWS CloudFormation佈建和設定這些資源。

當您使用 AWS CloudFormation 時，您可以重複使用您的範本，重複、一致的設定您的 AWS Resilience Hub 資源。一次描述您的資源，然後在多個AWS帳戶和區域中重複佈建相同的資源。

AWS Resilience Hub 和 AWS CloudFormation 範本

若要佈建和配置 AWS Resilience Hub 與相關服務的資源，您必須了解 AWS CloudFormation 範本。範本是以 JSON 或 YAML 格式化的文本檔案。而您亦可以透過這些範本的說明，了解欲在 AWS CloudFormation 堆疊中佈建的資源。如果您不熟悉 JSON 或 YAML，您可以使用 AWS CloudFormation 設計器協助您開始使用 AWS CloudFormation 範本。如需更多詳細資訊，請參閱 AWS CloudFormation 使用者指南 中的 什麼是 AWS CloudFormation 設計器？。

AWS Resilience Hub支援建立 AWS::ResilienceHub:::ResiliencyPolicy 和 AWS::ResilienceHub:::App 在中AWS CloudFormation。如需詳細資訊，包括和的 JSON 和 YAML 範本範本範例 AWS::ResilienceHub:::ResiliencyPolicy AWS::ResilienceHub:::App，請參閱AWS CloudFormation使用者指南中的AWS Resilience Hub資源類型參考。

您可以使用AWS CloudFormation堆疊來定義AWS Resilience Hub應用程式。堆疊可讓您以單一單元的形式管理相關資源。堆疊可以包含執行 Web 應用程式所需的所有資源，例如 Web 伺服器或網路規則。

進一步了解 AWS CloudFormation

如需 AWS CloudFormation 的詳細資訊，請參閱以下資源：

- AWS CloudFormation
- AWS CloudFormation使用者指南
- AWS CloudFormation API 參考
- AWS CloudFormation 命令列介面使用者指南

AWS CloudTrail

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

若要取得有關的更多資訊 CloudTrail，請參閱AWS CloudTrail 使用者指南。

AWS Systems Manager

AWS Resilience Hub 與 Systems Manager 合作，通過提供一些 SSM 文檔，您可以用作這些 SOP 的基礎來自動執行 SOP 的步驟。

AWS Resilience Hub 提供 AWS CloudFormation 範本，其中包含執行不同 Systems Manager 文件所需的 IAM 角色，每份文件都有一個角色，其中包含特定文件所需的權限。使用 AWS CloudFormation 範本建立堆疊之後，它會設定 IAM 角色，並將中繼資料儲存在系統管理員參數中，供系統管理員自動化文件執行，以便針對不同的復原程序執行。

如需使用 SOP 的詳細資訊，請參閱標準作業程序。

AWS Trusted Advisor

AWS Trusted Advisor 是 AWS 最佳實務建議的集中式首頁，可協助您識別、排定優先順序，以及最佳化您的部署 AWS。 AWS Trusted Advisor 檢查您的 AWS 環境，然後透過檢查提出建議，以節省成

本、改善系統可用性和效能，或協助縮小安全性漏洞。這些檢查會根據其用途分為多個品類。若要取得有關不同入庫納管品類的更多資訊 AWS Trusted Advisor，請參閱《AWS Support使用指南》。

AWS Trusted Advisor 透過針對容錯能力類別 AWS Resilience Hub 下的每個應用程式進行復原檢查，提供多個高階復原建議。容錯類別會列出測試應用程式以判斷其彈性和可靠性的所有檢查。這些檢查會在發 AppComponent 生故障和原則違規時提醒您，這些檢查可能會導致復原風險並影響應用程式的可用性以實現業務連續性。它還提供了彈性建議，這些建議將提高降低這些風險的機會，在「建議的動作」部分中 AWS Resilience Hub需要解決。如需有關中每個應用程式之建議的詳細資訊 AWS Trusted Advisor，建議您檢視中提供的詳細建議 AWS Resilience Hub。

AWS Trusted Advisor 針對中的每個應用程式提供下列檢查 AWS Resilience Hub：

- AWS Resilience Hub 應用程式彈性分數 — 從應用程式的最新評估中檢查應用程式的備援分數，AWS Resilience Hub 並在彈性分數低於特定值時向您發出警示。

  警示條件

  - 綠色 — 表示您的應用程式的復原分數為 70 及以上。
  - 黃色 — 表示您的應用程式的復原分數介於 40 到 69 之間。
  - 紅色 — 表示您的應用程式的復原分數低於 40。

  建議的動作

  若要改善彈性狀態並取得應用程式的最佳彈性分數，請使用應用程式資源的最新更新版本執行評估，如果適用，請實作建議的作業建議。如需執行、檢閱和實作評量、檢閱與包含/排除作業建議，以及實作相同建議的詳細資訊，請參閱下列主題：

  - the section called “執行復原能力評估”
  - the section called “檢閱評估報告”
  - the section called “複查復原建議”
  - the section called “包括或排除操作建議”
- AWS Resilience Hub 違反應用程式原則 — 檢查 AWS Resilience Hub 應用程式是否符合您為應用程式設定的 RTO 和 RPO 目標，並在應用程式不符合 RTO 和 RPO 目標時警示您。

  警示條件

  - 綠色 — 表示應用程式具有原則，且預估的工作負載 RTO 和預估的工作負載 RPO 符合 RTO 和 RPO 目標。
  - 黃色 — 表示應用程式具有策略且尚未經過評估。

- 紅色 — 表示應用程式具有原則，且預估的工作負載 RTO 和預估的工作負載 RPO 不符合 RTO 和 RPO 目標。

  建議的動作

  若要確保應用程式的預估工作負載 RTO 和預估的工作負載 RPO 仍符合定義的 RTO 和 RPO 目標，請定期使用應用程式資源的最新更新版本執行評估。此外，如果您想確保應用程式的恢復原則不會違反，建議您檢閱評估報告並實作建議的恢復能力建議。如需啟用 AWS Resilience Hub 代表您每天執行評量、執行評量、檢閱復原建議以及實作相同的詳細資訊，請參閱下列主題：

  - the section called “編輯應用資源”(若 AWS Resilience Hub 要啟用代表您每天執行評估，請完成若要更新應用程式程序的復原性漂移偵測以選取每日自動評估此應用程式核取方塊中的步驟。)
  - the section called “執行復原能力評估”
  - the section called “檢閱評估報告”
  - the section called “複查復原建議”
  - the section called “包括或排除操作建議”
- AWS Resilience Hub 應用程式評估年齡 — 檢查自從您對中的每個應用程式執行評估以來的最後一次時間 AWS Resilience Hub。如果您尚未在指定天數內執行評估，它會提醒您。

  警示條件

  - 綠色 — 表示您在過去 30 天內已針對應用程式執行評估。
  - 黃色 — 表示您在過去 30 天內未針對應用程式執行評估。

  建議的動作

  定期執行評估，以管理和改善應用程式的彈性狀態 AWS。如果您想 AWS Resilience Hub 要代表您每天評估您的應用程式，可以透過選取 AWS Resilience Hub 復原性漂移偵測中的每日自動評估此應用程式核取方塊來啟用此應用程式。若要選取每日自動評估此應用程式核取方塊，請完成中的若要更新應用程式程序的恢復性漂移偵測。???

  > **Note**
  >
  > 此檢查只會決定在 AWS Resilience Hub中評估過至少一次之應用程式的評估年齡。

- AWS Resilience Hub 應用程式元件檢查 — 檢查應用程式中的應用程式元件 (AppComponent) 是否無法復原。也就是說，如果 AppComponent 在發生中斷事件時無法復原，您可能會遇到未知的資料遺失和系統停機時間。如果警示條件設定為「紅色」，則表示無 AppComponent 法復原。

建議的動作

若要確保您 AppComponent 可復原，請檢閱並實作復原建議，然後執行新的評估。如需檢閱復原建議的詳細資訊，請參閱the section called “複查復原建議”。

若要取得有關使用的更多資訊 AWS Trusted Advisor，請參閱AWS Support使用指南。

AWS Resilience Hub 使用者指南的文件歷史記錄

下表說明此版本的文件 AWS Resilience Hub。

- API 版本：最新
- 最新文件更新：2024 年 3 月 28 日

變更	描述	日期
AWS Trusted Advisor 增強	AWS Resilience Hub AWS Trusted Advisor 透過新增檢查以識別無法復原的應用程式元件 (AppComponents) 來擴展對的支援。 如需詳細資訊，請參閱 the section called “AWS Trusted Advisor”。	2024年3月28日
AWS Resilience Hub 擴展對建議警報的支持	AWS Resilience Hub 已更新`README.md` 範本檔案的值，可讓您建立由 AWS Resilience Hub 內部 AWS (例如 Amazon CloudWatch) 或外部建議的警示 AWS。 如需詳細資訊，請參閱 the section called “管理警示”。	2024年3月26日
AWS Resilience Hub 擴展了對 Amazon FSx for Windows File Server 支持	AWS Resilience Hub 延伸適用於 Windows 檔案伺服器資源的 Amazon FSx 評估支援，同時評估應用程式的彈性。對於使用適用於 Windows 檔案伺服器的 Amazon FSx 的應用程式， AWS Resilience Hub 提供一組新的彈性建議，包括可	2024年3月26日

	用區域 (AZ) 和異地同步備份部署，以及備份計劃以及資料複寫。 AWS Resilience Hub 支援適用於 Windows 檔案伺服器的 Amazon FSx，包括對 Microsoft 活動目錄的檔案系統依賴性，適用於區域內部署和跨區域部署。 如需詳細資訊，請參閱下列主題： • the section called “支援的 AWS Resilience Hub 資源” • the section called “AWSResilienceHubAsssessmentExecutionPolicy” • the section called “對資源進行分組 AppComponent”	
AWS Resilience Hub 提供有關復原分數的其他資訊	AWS Resilience Hub 已更新彈性評分使用者體驗，以協助您輕鬆瀏覽並瞭解改善應用程式彈性狀態所需的動作。 如需詳細資訊，請參閱 the section called “了解彈性分數”。	2023 年 11 月 9 日

AWS Resilience Hub 擴展對包括 Amazon Elastic Kubernetes Service (Amazon EKS) 資源的應用程式的支援	AWS Resilience Hub 擴展對包含 Amazon EKS 資源之應用程式的支援，以納入新的操作建議。在執行包含 Amazon EKS 叢集資源的評估時，我們現在會建議要執行的測試和警示，以協助改善應用程式的彈性狀態。 如需詳細資訊，請參閱 the section called “Amazon 故障注入服務實驗”。	2023 年 11 月 9 日
AWS Resilience Hub 提供應用程式層級的其他資訊	AWS Resilience Hub 在應用程式層級提供有關預估工作負載 RTO 和估計工作負載 RPO 的其他資訊。此額外資訊指出最新成功評估後，應用程式可能的最大估計工作負載 RTO 和預估工作負載 RPO。此值是所有中斷類型的最大估計工作負載 RTO 和預估工作負載 RPO。 如需詳細資訊，請參閱 the section called “應用程式”。	2023 年 10 月 30 日

AWS Resilience Hub 擴展對資源的評估支 AWS Step Functions 援	AWS Resilience Hub 延伸 AWS Step Functions 資源評估支援，同時評估應用程式的彈性。 AWS Resilience Hub 分析 AWS Step Functions 組態，包括狀態機器類型 (標準或快速工作流程)。此外，也 AWS Resilience Hub 會提供建議，協助您符合預估的工作負載復原時間目標 (RTO) 和估計的工作負載復原點目標 (RPO)。若要評估包括 AWS Step Functions 資源在內的應用程式，您必須設定必要的權限，方法是使用 AWS 受管理的策略或手動新增允許讀 AWS Resilience Hub 取 AWS Step Functions 組態的特定權限。 如需關聯權限的詳細資訊，請參閱the section called “AWSResilienceHubAsssessmentExecutionPolicy”。	2023 年 10 月 30 日

AWS Resilience Hub 允許排除操作建議	AWS Resilience Hub 新增排除操作建議的功能，包括警示、標準作業程序 (SOP) 和 Amazon 故障注入服務 (AWS FIS) 測試。在上執行評估時 AWS Resilience Hub，系統會為您提供估計的復原時間，以及如何提高評估之應用程式復原能力的建議。使用排除建議工作流程，您現在可以排除與它們無關的建議警示、SOP 和 AWS FIS 測試。如果您使用的是建議的平台以外的平台，或者已經以替代方法實作建議，則排除工作流程會很有幫助。 如需詳細資訊，請參閱下列主題： • the section called “包括或排除操作建議” • the section called “限制權限以包含或排除 AWS Resilience Hub 建議”	2023 年 8 月 9 日

改善的權限設計 AWS Resilience Hub	AWS Resilience Hub 引入了新的權限設計，以便在設定 AWS Identity and Access Management (IAM) 角色時提供彈性 AWS Resilience Hub。它還將權限合併為單一角色，並能夠建立對您和您的團隊有意義的自訂角色名稱。中的新受管理策略可 AWS Resilience Hub 讓您擁有支援服務的適當權限。如果您對當前設置權限的方法感到滿意，我們將繼續支持手動配置。 如需有關 AWS 受管理原則的詳細資訊，請參閱the section called “AWSResilienceHubAsssessmentExecutionPolicy”。	2023 年 8 月 2 日

應用程式彈性漂移偵測 AWS Resilience Hub	AWS Resilience Hub 可讓您主動偵測並瞭解解決應用程式彈性的必要動作。當預估的工作負載復原時間目標 (RTO) 或預估工作負載復原點目標 (RPO) 已從達到目標移至不再滿足組織的業務目標時，啟用 Amazon SNS 收到通知。從手動執行評估的同時以反應方式尋找彈性問題，以透過 Amazon SNS 主題主動接收通知，讓您能夠更早預測潛在的中斷情況，並提供額外的信心，確保能夠達成復原目標。 如需詳細資訊，請參閱下列主題： • the section called “步驟 5：設定彈性漂移偵測” • the section called “編輯應用資源”	2023 年 8 月 2 日

AWS Resilience Hub 改善了對 Amazon Relational Database Service 和 Amazon Aurora 的	AWS Resilience Hub 擴展對 Amazon Relational Database Service 代理以及無周邊和 Amazon Aurora 資料庫組態的評估支援。此外，在評估包含 Amazon RDS 的應用程式時，我們現在將區分不同的資料庫引擎，以提供更精確的估計工作負載復原時間目標 (RTO)。AWS Resilience Hub 也會提供其他動作，以在您的 AWS 環境中實作彈性最佳做法。最佳實務可以包括對 DevOps Guru for Amazon RDS 的效能洞察、增強型監控，以及支援的資料庫引擎上的藍/綠部署自動化。 若要進一步瞭解在評估中包含所有支援服務的資源所需的權限，請參閱the section called “AWSResilienceHubAsssessmentExecutionPolicy”。AWS Resilience Hub	2023 年 8 月 2 日

AWS Resilience Hub 擴展對 Amazon 彈性區塊存放區快照的支援	AWS Resilience Hub 擴展對亞馬遜彈性區塊存放區 (Amazon EBS) 的評估支援，以辨識 Amazon EBS 快照，這些快照是使用直接 API 在同一個 Amazon EBS 區域內拍攝的。除了目前使用 Amazon 資料生命週期管理員 (Amazon Data Lifecycle Manager) 或 AWS Backup 的客戶提供的擴充支援。 如需詳細資訊，請參閱 Amazon Elastic Block Store (Amazon EBS)。	2023 年 8 月 2 日

Amazon 彈性運算雲端增強功能	AWS Resilience Hub 擴大了對 Amazon Elastic Compute Cloud (Amazon EC2) 的支持。對於不同大小的應用程式，AWS 可讓使用 Amazon EC2 的客戶選擇適合其使用案例的組態。 AWS Resilience Hub 支援下列 Amazon EC2 組態的評估： • 隨需執行個體。 • 執行個體由 AWS Backup 和備份 AWS Elastic Disaster Recovery。 • Support 使用 Amazon Route 53 應用程式復原控制器 (Route 53 ARC) 的 auto-scaling 群組 未來，評估支援將擴展到包括競價型執行個體、專用主機、專用執行個體、置放群組和叢集。 如需詳細資訊，請參閱 the section called “AWS Resilience Hub 存取權限參考”。	2023 年 6 月 27 日
AWS 受管理策略更新	已新增可存取其他 AWS 服務以執行評估的新原則。 如需詳細資訊，請參閱 the section called “AWSResilienceHubAsssessmentExecutionPolicy”。	2023 年 6 月 26 日

新的 Amazon DynamoDB 建議警示	對於使用 Amazon DynamoDB 的應用程式， AWS Resilience Hub 現在會提供一組新警示，提醒您隨需和佈建容量模式和全域表的彈性風險。若要存取新警示，您可能需要更新所使用角色的 AWS Identity and Access Management (IAM) 政策。 如需詳細資訊，請參閱 the section called “AWS Resilience Hub 存取權限參考”。	2023 年 5 月 2 日
AWS Trusted Advisor 增強	AWS Resilience Hub 已擴大對使用 Amazon DynamoDB 應用程式的支援 AWS Trusted Advisor 和應用程式。當您 AWS Trusted Advisor 搭配使用時 AWS Resilience Hub，您現在可以在過去 30 天內未評估應用程式時收到通知。此通知會提示您重新評估應用程式，以瞭解是否有任何會影響其恢復能力的變更。 如需AWS Resilience Hub 評估年齡檢查的詳細資訊，請參閱the section called “AWS Trusted Advisor”。	2023 年 5 月 2 日

對 Amazon 簡單存儲服務的其他支持	除了目前支援 Amazon Simple Storage Service (Amazon S3) 跨區域複寫 (Amazon S3 CRR)/Amazon S3 同區域複寫 (SRR)、版本控制和 AWS Backup 的目前支援之外，現在還 AWS Resilience Hub 會針對 Amazon S3 多區域存取點、Amazon S3 複寫時間控制 (Amazon S3 RTC) 和 AWS Backup point-in-time 復原 (PITR) 設定進行評估。 如需詳細資訊，請參閱下列主題： • the section called “AWS Resilience Hub 存取權限參考” • 管理您的 Amazon S3 儲存	2023 年 3 月 21 日

Amazon Elastic Kubernetes Service 的其他支持	AWS Resilience Hub 已新增 Amazon EKS 叢集作為支援的資源，用於定義、驗證和追蹤應用程式彈性。客戶可以將 Amazon EKS 叢集新增至新的或現有的應用程式，並獲得改善彈性的評估和建議。客戶可以使用 AWS CloudFormation、地形、和新增應用程式資源。 AWS Resource Groups AppRegistry此外，客戶可以直接在一個或多個區域中新增一或多個 Amazon EKS 叢集，每個叢集中有一或多個命名空間。這可 AWS Resilience Hub 以提供單一和跨區域的評估和建議。除了檢查部署、複本和 Pod 之外 ReplicationControllers，還 AWS Resilience Hub 將分析整體叢集恢復能力。AWS Resilience Hub 支援無狀態的 Amazon EKS 叢集工作負載。新功能可在所有受支援的 AWS 區域中使 AWS Resilience Hub 用。 如需詳細資訊，請參閱下列主題： • the section called “步驟 2：管理您的應用程式資源” • the section called “新增 EKS 叢集” • the section called “AWS Resilience Hub 存取權限參考”	2023 年 3 月 21 日

	• AWS 區域服務	
對 Amazon Elastic File System 的其他支援	除了目前對亞馬遜彈性檔案系統 (Amazon EFS) 備份的支援外，現在還 AWS Resilience Hub 將評估 Amazon EFS 以進行 Amazon EFS 複寫和 AZ 組態。 如需詳細資訊，請參閱下列主題： • the section called “支援的 AWS Resilience Hub 資源” • 什麼是 Amazon Elastic File System？	2023 年 3 月 21 日
Support 應用程式輸入來源	AWS Resilience Hub 現在提供有關應用程式來源的透明度。它可協助您新增、刪除和重新匯入應用程式的輸入來源，以及發佈新的應用程式版本。 如需詳細資訊，請參閱 the section called “編輯應用資源”。	2023 年 2 月 21 日

Support 應用程式組態參數	AWS Resilience Hub 現在提供輸入機制，以收集與應用程式相關聯之資源的其他資訊。有了這些資訊， AWS Resilience Hub 就能更深入地瞭解您的資源，並提供更好的彈性建議。 如需詳細資訊，請參閱下列主題： • the section called “應用組態參數” • the section called “步驟 7：設定應用程式組態參數” • the section called “更新應用程式組態參”	2023 年 2 月 21 日
Amazon 彈性塊商店的其他支持	除了目前對亞馬遜彈性區塊存放區 (Amazon EBS) 磁碟區的支援外，現在還 AWS Resilience Hub 將透過亞馬遜資料生命週期管理器和 Amazon EBS 快速快照還原 (FSR) 來評估 Amazon EBS 快照。 如需詳細資訊，請參閱下列主題： • the section called “AWS Resilience Hub 存取權限參考” • Amazon Elastic Block Store (Amazon EBS)	2023 年 2 月 21 日

與整合 AWS Trusted Advisor	AWS Trusted Advisor 使用者將能夠檢視與其帳戶相關聯且經過評估的應用程式 AWS Resilience Hub。 AWS Trusted Advisor 顯示最新的恢復分數，並提供狀態，指出是否符合目標恢復原則 (RTO 和 RPO)。每次執行評估時，都 AWS Resilience Hub 會 AWS Trusted Advisor 以最新的結果進行更新。 AWS Trusted Advisor 是一項不斷分析您的 AWS 帳戶並提供建議的服務，以協助您遵循 AWS 最佳實務和 AWS Well-Architected 的準則。 如需詳細資訊，請參閱 the section called “AWS Trusted Advisor”。	2022 年 11 月 18 日

Support Amazon Simple Notification Service (Amazon SNS)	AWS Resilience Hub 現在透過分析 Amazon SNS 組態 (包括訂閱者) 來評估使用 Amazon SNS 的應用程式，並提供符合組織應用程式預估工作負載復原目標 (估計工作負載 RTO 和估計工作負載 RPO) 的建議。Amazon SNS 是一種受管服務，可將來自發佈者 (生產者) 的訊息傳遞給訂閱者 (消費者)。 如需詳細資訊，請參閱下列主題： • the section called “支援的 AWS Resilience Hub 資源” • the section called “身分和存取權管理” • the section called “對資源進行分組 AppComponent”	2022 年 11 月 16 日

Amazon 路線 53 應用程序恢復控制器的其他 Support（亞馬遜路線 53 ARC）	AWS Resilience Hub 現在評估 Amazon Route 53 ARC Elastic Load Balancing 和 Amazon Relational Database Service（Amazon RDS），其中包括什麼時候 Amazon Route 53 ARC 將是有益的建議。將 Amazon Route 53 ARC 評估支援擴展 AWS Resilience Hub到 AWS Auto Scaling 展群組 (AWS ASG) 和 Amazon DynamoDB 之外。Amazon Route 53 ARC 為您的應用程式提供高可用性，可讓您快速將整個應用程式容錯移轉至容錯移轉區域。 如需詳細資訊，請參閱下列主題： • the section called “支援的 AWS Resilience Hub 資源” • the section called “身分和存取權管理”	2022 年 11 月 16 日

AWS Backup 的其他 Support	AWS Resilience Hub 現在評估 Amazon Route 53 ARC Elastic Load Balancing 和 Amazon Relational Database Service（Amazon RDS），其中包括什麼時候 Amazon Route 53 ARC 將是有益的建議。將 Amazon Route 53 ARC 評估支援擴展 AWS Resilience Hub到 AWS Auto Scaling 展群組 (AWS ASG) 和 Amazon DynamoDB 之外。Amazon Route 53 ARC 為您的應用程式提供高可用性，可讓您快速將整個應用程式容錯移轉至容錯移轉區域。 如需詳細資訊，請參閱下列主題： • the section called “支援的 AWS Resilience Hub 資源” • the section called “身分和存取權管理”	2022 年 11 月 16 日
更新內容：新增應用程式元件資源	在 AppComponent 分組區段中將 Route53 和 AWS Backup 新增到支援的應用程式元件資源清單中。	2022 年 7 月 1 日
新內容：應用程式合規狀態概念	添加了檢測到的變更狀態類型。	2022 年 6 月 2 日

介紹 AWS Resilience Hub	AWS Resilience Hub 現在可用。本指南說明如何使用 AWS Resilience Hub 來分析基礎結構、取得改善 AWS 應用程式復原能力的建議、檢閱彈性分數等等。	2021 年 11 月 10 日

AWS 詞彙表

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

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。