使用者指南

AWS 彈性中樞

AWS 彈性中樞: 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狀態的中心位置 AWS。 AWS Resilience Hub 可讓您定義彈性目標、針對這些目標評估彈性狀態，並根據 AWS Well-Architected Framework 實作改進建議。 AWS Resilience Hub您也可以在其中建立和執行 AWS Fault Injection Service 實驗，模擬應用程式的真實運作中斷，以協助您更了解相依性並發現潛在弱點。 AWS Resilience Hub 提供集中位置，其中包含持續強化復原狀態所需的所有 AWS 服務和工具。 與其他 服務 AWS Resilience Hub 合作，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。

下表提供所有相關彈性服務的文件連結。

相關 AWS 彈性服務和參考

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 Application Recovery Controller (ARC) (ARC)	什麼是 Amazon Application Recovery Controller (ARC)

主題

- AWS Resilience Hub – 彈性管理
- AWS Resilience Hub – 彈性測試
- AWS Resilience Hub 概念
- AWS Resilience Hub 角色
- AWS Resilience Hub 支援的資源
- AWS Resilience Hub 和 myApplications

AWS Resilience Hub – 彈性管理

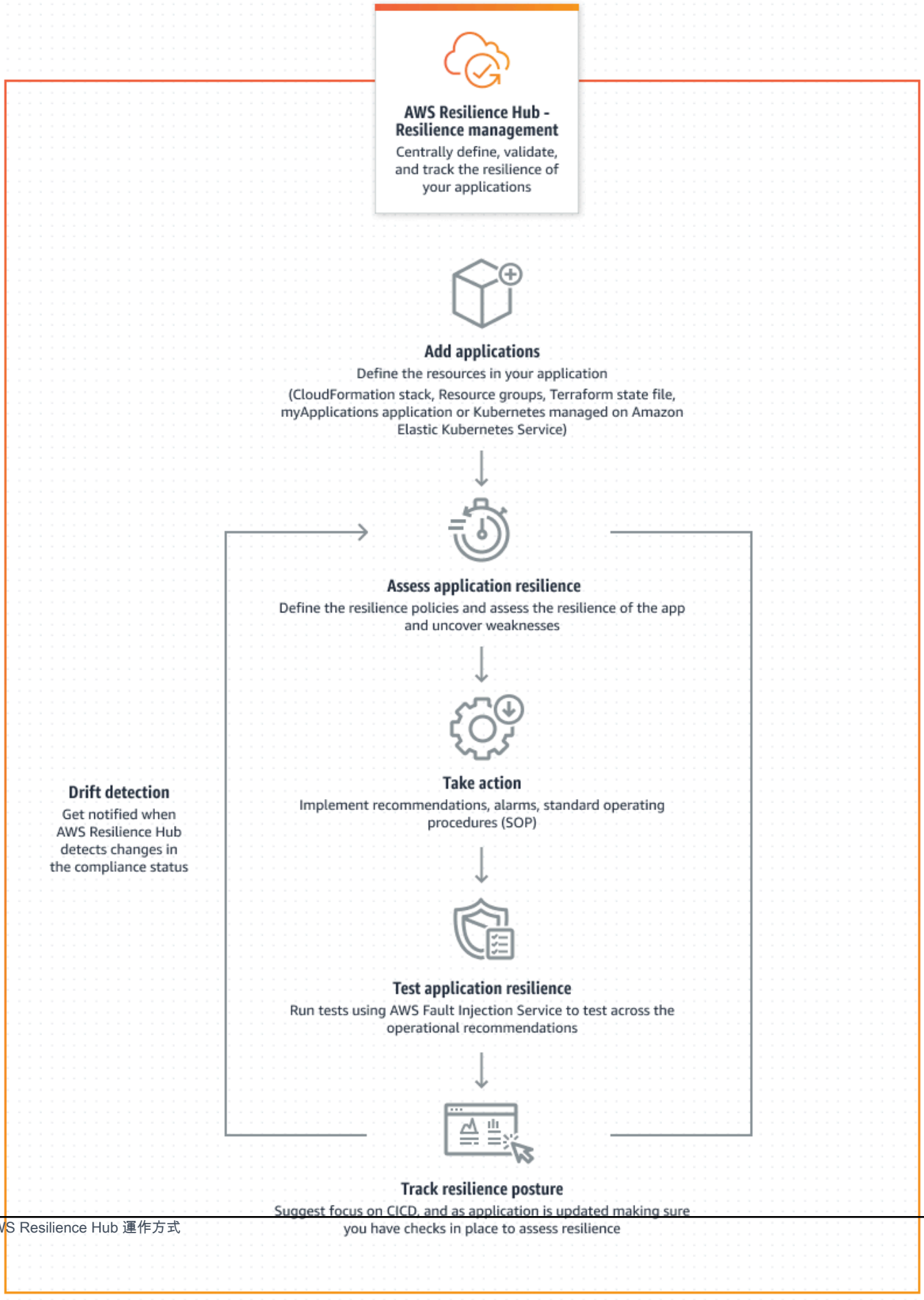
AWS Resilience Hub 可讓您集中定義、驗證和追蹤 AWS 應用程式的彈性。 AWS Resilience Hub 可協助您保護應用程式免受中斷，並降低復原成本，以最佳化業務連續性，以協助符合合規和法規要求。您可以使用 AWS Resilience Hub 執行下列動作：

- 分析您的基礎設施並取得建議，以改善應用程式的彈性。除了改善應用程式彈性的架構指引之外，建議還提供程式碼以符合您的彈性政策、實作測試、警示和標準操作程序 (SOPs)，您可以在整合和交付 (CI/CD) 管道中與應用程式一起部署和執行。
- 在不同條件下評估復原時間目標 (RTO) 和復原點目標 (RPO)。
- 最佳化業務連續性，同時降低復原成本。
- 在問題在生產中發生之前識別並解決問題。

將應用程式部署到生產環境後，您可以將 AWS Resilience Hub 新增至 CI/CD 管道，以便在每個建置發佈到生產環境之前進行驗證。

AWS Resilience Hub 運作方式

下圖提供如何 AWS Resilience Hub 運作的高階大綱。


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, myApplications 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

從 AWS CloudFormation 堆疊、Terraform 狀態檔案 AWS Resource Groups、Amazon Elastic Kubernetes Service 叢集匯入資源，或從已在 myApplications 中定義的應用程式進行選擇，來描述您的應用程式。

定義

為您的應用程式定義彈性政策。這些政策包括應用程式、基礎設施、可用區域和區域中斷的 RTO 和 RPO 目標。這些目標用於估計應用程式是否符合彈性政策。

評估

在您描述應用程式並將彈性政策附加到應用程式之後，請執行彈性評估。 AWS Resilience Hub 評估使用 Well-Architected Framework 的 AWS 最佳實務來分析應用程式的元件，並發現潛在的恢復能力弱點。這些弱點可能是基礎設施設定不完整、組態錯誤或需要額外組態改進的情況所造成。為了改善彈性，請根據評估報告的建議更新您的應用程式和彈性政策。建議包括元件、警示、測試和復原 SOPs組態。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，以查看改善多少彈性。重複此程序，直到您的預估工作負載 RTO 和預估工作負載 RPO 符合您的 RTO 和 RPO 目標。

驗證

執行測試以測量 AWS 資源的彈性，以及從應用程式、基礎設施、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 AWS 資源的中斷。中斷的範例包括網路無法使用錯誤、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

在將 AWS 應用程式部署到生產環境之後，您可以使用 繼續 AWS Resilience Hub 追蹤應用程式的彈性狀態。如果發生中斷，操作員可以在 中檢視中斷， AWS Resilience Hub 並啟動相關聯的復原程序。

AWS Resilience Hub – 彈性測試

AWS Resilience Hub 支援與 的增強型整合 AWS FIS。此整合允許 AWS Resilience Hub 使用 AWS FIS 動作和案例，根據要評估之應用程式的特定內容提供量身打造的建議。執行建議的實驗或使用 AWS FIS 服務執行您自己的測試，將直接有助於改善應用程式的彈性分數。

這些 AWS FIS 動作和案例透過建立破壞性事件來測試應用程式的彈性狀態，以便您可以觀察應用程式回應的方式。 AWS FIS 提供多個預先建置的案例和大量選擇的動作，進而產生中斷。此外，它還包括在生產環境中執行實驗所需的控制項和護欄。控制項和護欄包含選項，可在符合特定條件時執行自動復

原或停止實驗。若要開始使用 從AWS Resilience Hub 主控台 AWS FIS 執行實驗，請完成 the section called “先決條件”章節中定義的先決條件。

下表列出導覽窗格的所有可用 AWS FIS 選項，以及相關文件的連結 AWS FIS ，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 導覽功能表選項	AWS FIS 文件
彈性測試	建立實驗範本
案例程式庫	AWS FIS 程式庫
實驗範本	的實驗範本 AWS FIS

下表列出恢復能力測試區段中下拉式功能表中的所有可用 AWS FIS 選項， AWS FIS 以及相關文件的連結，其中包含從 AWS Resilience Hub 主控台開始使用 AWS FIS 測試的程序。

AWS FIS 下拉式功能表選項和參考

AWS FIS 下拉式選單選項	AWS FIS 文件
建立實驗範本	建立實驗範本
從案例建立實驗	使用案例

AWS Resilience Hub 概念

這些概念可協助您更了解 協助改善應用程式彈性並防止應用程式中斷 AWS Resilience Hub的方法。

彈性

在指定的時間範圍內維持可用性並從軟體和操作中斷中復原的能力。

復原點目標 (RPO)

自上次資料復原點以來可接受的時間上限。這會決定最後一個復原點與服務中斷之間可接受的資料遺失。

復原時間目標 (RTO)

服務中斷和服務還原之間的可接受延遲上限。這會決定可接受的服務無法使用之時間長度。

估計工作負載復原時間目標

估計工作負載復原時間目標 （估計工作負載 RTO) 是應用程式根據匯入的應用程式定義估計符合的 RTO，然後執行評估。

估計工作負載復原點目標

估計工作負載復原點目標 （估計工作負載 RPO) 是應用程式根據匯入的應用程式定義估計符合的 RPO，然後執行評估。

應用程式

AWS Resilience Hub 應用程式是受 AWS 支援資源的集合，這些資源會持續受到監控和評估，以管理其彈性狀態。

應用程式元件

一組運作和失敗的相關 AWS 資源，做為單一單位。例如，如果您有主要資料庫和複本資料庫，則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，`DBInstance`可以屬於 `AWS::ResilienceHub::DatabaseAppComponent`，但不能屬於 `AWS::ResilienceHub::ComputeAppComponent`。

應用程式合規狀態

AWS Resilience Hub 會為您的應用程式報告下列合規狀態類型。

符合政策

應用程式估計符合政策中定義的 RTO 和 RPO 目標。其所有元件都符合定義的政策目標。例如，您針對跨 AWS 區域的中斷選取了 24 小時的 RTO 和 RPO 目標。 AWS Resilience Hub 可以看到您的備份已複製到您的備用區域。您仍然需要從備份標準操作程序 (SOP) 中維護復原，並測試和計時。這是在操作建議中，也是整體恢復能力分數的一部分。

已違反政策

無法估計應用程式是否符合政策中定義的 RTO 和 RPO 目標。其一或多個 AppComponents不符合政策目標。例如，您為跨 AWS 區域的中斷選擇了 24 小時的 RTO 和 RPO 目標，但您的資料庫組態不包含任何跨區域復原方法，例如全域複寫和備份複本。

未評估

應用程式需要評估。目前尚未評估或追蹤。

偵測到變更

有尚未評估的新發佈版本應用程式。

漂移偵測

AWS Resilience Hub 會在執行應用程式評估時執行偏離通知，以檢查 AppComponent 組態中的變更是否影響應用程式的合規狀態。此外，它還會檢查和偵測變更，例如新增或刪除應用程式輸入來源中的資源，並通知相同的 。為了比較， AWS Resilience Hub 使用應用程式元件符合政策的先前評估。AWS Resilience Hub 會偵測下列類型的漂移：

- 應用程式政策偏離 – 此偏離類型可識別在先前評估中符合政策，但在目前評估中未符合政策的所有 AppComponents。
- 應用程式資源偏離 – 此偏離類型可識別目前應用程式版本中的所有偏離資源。

彈性評估

AWS Resilience Hub 使用差距和潛在補救措施的清單來衡量所選政策的有效性，以復原並從災難中繼續。它會使用 政策評估每個應用程式元件或應用程式合規狀態。此報告包含成本最佳化建議和潛在問題的參考。

彈性分數

AWS Resilience Hub 會產生分數，指出您的應用程式遵循我們建議的程度，以符合應用程式的彈性政策、警示、標準操作程序 (SOPs) 和測試。

中斷類型

AWS Resilience Hub 可協助您評估下列中斷類型的彈性：

Application (應用程式)

基礎設施運作狀態良好，但應用程式或軟體堆疊無法視需要運作。這可能發生在部署新的程式碼、組態變更、資料損毀或下游相依性故障之後。

雲端基礎設施

由於中斷，雲端基礎設施無法如預期運作。由於一或多個元件發生本機錯誤，可能會發生中斷。在大多數情況下，這種類型的中斷是透過重新啟動、回收或重新載入故障元件來解決。

雲端基礎設施可用區域中斷

一或多個可用區域無法使用。您可以切換到不同的可用區域來解決這種類型的中斷。

雲端基礎設施區域事件

一或多個區域無法使用。您可以切換到不同的 來解決這類事件 AWS 區域。

AWS FIS 實驗

AWS Resilience Hub 建議使用 AWS FIS 動作來驗證應用程式對不同類型中斷的彈性的實驗。這些中斷包括應用程式、基礎設施、可用區域 (AZ) 或 Application Components AWS 區域 的事件。

這些實驗可讓您執行下列動作：

- 注入失敗。
- 確認警示可以偵測到中斷。
- 確認復原程序或標準操作程序 SOPs) 可正常運作，從中斷中復原應用程式。

SOPs 測試會測量預估工作負載 RTO 和預估工作負載 RPO。您可以測試不同的應用程式組態，並測量輸出 RTO 和 RPO 是否符合政策中定義的目標。

SOP

標準操作程序 (SOP) 是一組規範性步驟，旨在在發生中斷或警示時有效地復原您的應用程式。根據應用程式評估， AWS Resilience Hub 建議一組 SOPs，建議在中斷之前準備、測試和測量 SOPs，以確保及時復原。

AWS Resilience Hub 角色

建置企業應用程式需要來自不同跨職能團隊的協作工作，例如基礎設施、業務連續性、應用程式擁有者和其他負責監控應用程式的利益相關者。來自不同團隊的不同角色有助於在 中建立和管理應用程式

AWS Resilience Hub，每個角色和責任都不同。若要進一步了解如何授予許可給不同的角色，請參閱 the section called “AWS Resilience Hub 角色和 IAM 許可參考”。

若要開始在 中建立應用程式和執行評估 AWS Resilience Hub，我們建議您建立下列角色：

- 基礎設施應用程式管理員 – 具有此角色的使用者負責設定、設定和維護基礎設施和應用程式資源，以確保應用程式的可靠性和安全性。他們的責任包括下列項目：
  - 確保應用程式定期部署和更新
  - 監控系統效能
  - 疑難排解 問題
  - 實作備份和災難復原計劃
- 業務連續性管理員 – 具有此角色的使用者負責指定應用程式政策，並判斷應用程式的業務重要性。他們的責任包括下列項目：
  - 在設定政策時採取關鍵決策
  - 評估業務重要性
  - 為關鍵應用程式配置資源
  - 評估和管理風險
- 應用程式擁有者 – 具有此角色的使用者負責確保高可用性和可靠的應用程式。他們的責任包括下列項目：
  - 定義關鍵效能識別符，以測量和監控應用程式效能並識別瓶頸
  - 為多個利益相關者組織訓練
  - 確保下列文件為up-to-date：
    - 應用程式架構
    - 部署程序
    - 監控組態
    - 效能最佳化技術
- 唯讀存取 – 具有此角色的使用者僅限於唯讀許可。他們的責任包括透過監控彈性分數、操作建議和彈性建議，來維持應用程式效能和運作狀態的可見性和監督。此外，他們還負責識別問題、趨勢和需要改進的領域，以確保應用程式符合組織的目標。

AWS Resilience Hub 支援的資源

在中斷的情況下影響應用程式效能的資源，完全由 AWS Resilience Hub 最上層資源支援，例如 `AWS::RDS::DBInstance`和 `AWS::RDS::DBCluster`。

若要進一步了解 AWS Resilience Hub 包含評估中所有支援服務的資源所需的許可，請參閱 the section called “AWSResilienceHubAsssessmentExecutionPolicy”。

AWS Resilience Hub 支援來自下列 AWS 服務的資源：

- 運算
  - Amazon Elastic Compute Cloud (Amazon EC2)

    > **Note**
    >
    > AWS Resilience Hub 不支援用於存取 Amazon EC2 資源的舊 Amazon Resource Name (ARN) 格式。新的 ARN 格式會使用 AWS 您的帳戶 ID，並啟用增強功能來標記叢集中的資源，以及追蹤叢集中執行之服務和任務的成本。
    >
    > - 舊格式（已棄用）– `arn:aws:ec2:<region>::instance/<instance-id>`
    > - 新格式 – `arn:aws:ec2:<region>:<account-id>:instance/<instance-id>`
    >
    > 如需新 ARN 格式的詳細資訊，請參閱將 Amazon ECS 部署遷移至新的 ARN 和資源 ID 格式。

  - 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
  - Amazon ElastiCache
- 聯網與內容交付
  - Amazon Route 53
  - Elastic Load Balancing

  - 網路地址轉譯 (NAT)
- 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 Application Recovery Controller (ARC) (Amazon 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 可讓您檢視每個資源支援的執行個體，藉此為您的應用程式資源提供額外的透明度。此外， 透過識別每個資源的唯一執行個體，同時在評估過程中探索資源執行個體， AWS Resilience Hub 提供更準確的彈性建議。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 應用程式資源。
> - AWS Resilience Hub 支援 Amazon EKS 和 Amazon ECS on AWS Fargate。
> - AWS Resilience Hub 支援評估 AWS Backup 資源，做為下列服務的一部分：
>   - Amazon EBS
>   - Amazon EFS
>   - Amazon S3
>   - Amazon Aurora 全球資料庫
>   - Amazon DynamoDB
>   - Amazon RDS 服務
>   - Amazon FSx for Windows File Server

- 中的 Amazon ARC 僅 AWS Resilience Hub 評估 Amazon DynamoDB 全域、Elastic Load Balancing、Amazon RDS 和 AWS Auto Scaling 群組。
- 若要 AWS Resilience Hub 讓 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 Application Components 和分組資源所支援資源的詳細資訊，請參閱 應用程式元件中的資源分組。
- 目前，如果 Amazon EKS 叢集位於啟用選擇加入的區域，或如果應用程式是在啟用選擇加入的 AWS 區域中建立， AWS Resilience Hub 則 不支援 Amazon EKS 叢集的跨區域評估。
- 目前， 僅 AWS Resilience Hub 評估下列 Kubernetes 資源類型：
  - 部署
  - ReplicaSets
  - Pod

AWS Resilience Hub 會忽略下列類型的資源：

- 不會影響預估工作負載 RTO 或預估工作負載 RPO 的資源 – 如 `AWS::RDS::DBParameterGroup`等不會影響預估工作負載 RTO 或預估工作負載 RPO 的資源，會被 忽略 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::ApiGatewayV2::Api`Amazon API Gateway 支援 `AWS::ApiGateway::RestApi`和 資源。不過， `AWS::ApiGatewayV2::Stage` 不是頂層資源。因此，它不會由 匯入 AWS Resilience Hub。

> **Note**
>
> 不支援的資源
>
> - 您無法使用 AWS Resource Groups (Amazon Route 53 RecordSets 和 API-GW HTTP) 和 Amazon Aurora Global 資源來識別多個資源。如果您想要在評估中分析這些資源，則必須手動將資源新增至應用程式。不過，當您新增要評估的 Amazon Aurora Global 資源時，它必須與 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 “編輯應用程式資源”。
> - 這些資源可能會影響應用程式復原，但 AWS Resilience Hub 目前並未完全支援。如果應用程式由 AWS CloudFormation 堆疊、Terraform 狀態檔案或 myApplications 應用程式支援 AWS Resource Groups， AWS Resilience Hub 會努力警告使用者不支援的資源。

- 在將應用程式資源匯入 的過程中 AWS Resilience Hub，可能會忽略某些資源。忽略資源時，表示完全無法匯入資源。不過，標示為不支援的資源目前與 不相容， AWS Resilience Hub 但未來可能受到支援，允許將其包含在應用程式中進行評估。此外，如果不支援特定資源， AWS Resilience Hub 則可能會忽略這些資源 AWS Resource Groups。如需 支援資源的詳細資訊 AWS Resource Groups，請參閱可與 AWS Resource Groups 和 標籤編輯器搭配使用的資源類型。

AWS Resilience Hub 和 myApplications

myApplications 儀表板中的彈性小工具可簡化評估和監控應用程式彈性的程序。它可讓您快速評估在 myApplications 中定義的應用程式的彈性，而無需在 AWS Resilience Hub 主控台中手動重新建立應用程式。此整合方法結合了 myApplications 的應用程式管理功能與 的彈性評估功能 AWS Resilience Hub，可讓您利用這兩個平台的優勢。透過結合應用程式定義和彈性評估功能，彈性小工具可簡化工作流程，讓您存取相關資訊並採取動作，從集中位置增強彈性。從彈性小工具評估應用程式時， AWS Resilience Hub 會執行下列動作：

- 在 中建立選取的應用程式 AWS Resilience Hub。
- 自動探索和映射與模型相關聯的資源。
- 建立並指派新的彈性政策，其中包含復原時間目標 (RTO) 和復原點目標 (RPO) 的預先定義值。也就是 RTO 的四小時和 RPO 的一小時。產生評估之後，您可以修改彈性政策，或從 AWS Resilience Hub 主控台指派不同的政策。如需更新彈性政策和連接不同政策的詳細資訊，請參閱管理彈性政策。
- 針對彈性政策中定義的 RTO 和 RPO 評估應用程式的彈性，以識別需要改善應用程式架構的區域。失敗案例包括可用區域故障、區域中斷和其他潛在的中斷。
- 在初始評估之後，持續監控應用程式的資源和組態變更，如果有任何變更影響應用程式的彈性，則提供提醒或更新。

> **Note**
>
> 在開始評估之前，我們建議您評估使用 執行評估時涉及的潛在成本 AWS Resilience Hub。如需詳細的定價資訊，請參閱 AWS Resilience Hub 定價。

評估應用程式後，您可以選擇前往 AWS Resilience Hub 以在 AWS Resilience Hub 主控台中檢視應用程式詳細資訊，以 AWS Resilience Hub 從小工具存取 的完整功能。將應用程式從 myApplications 納入 的程序 AWS Resilience Hub 受下列規則和限制所規範：

- 您只能將一個 myApplications 應用程式與 中的應用程式建立關聯 AWS Resilience Hub。也就是說，您可以透過在 myApplications 儀表板中從彈性小工具執行評估，或在主控台中 AWS Resilience Hub 描述 AWS Resilience Hub 應用程式時完成使用 myApplications 應用程式程序，將 myApplications 應用程式與應用程式建立關聯。
- 您只能包含、評估和檢視位於與 myApplications 環境相同 AWS 區域和 AWS 帳戶邊界內的 myApplications 應用程式。在不同 AWS 區域或在個別 AWS 帳戶下建立的應用程式將無法透過此小工具看見或存取。
- 您只能從 myApplications 儀表板新增、移除和更新資源。當您從 myApplications 儀表板修改應用程式資源時，您必須重新匯入 AWS Resilience Hub 以檢視其中的資源變更 AWS Resilience Hub。

進一步了解

如需在 myApplications 儀表板中管理應用程式和資源的詳細資訊，請參閱 AWS Console Home 文件中的下列主題：

- 什麼是 myApplications AWS？
- 在 myApplications 中建立您的第一個應用程式
- 管理 資源
- 彈性小工具

如需在 中描述應用程式和執行評估的詳細資訊 AWS Resilience Hub，請參閱下列主題：

- 第一次從彈性小工具執行現有 myApplications 應用程式的彈性評估
- 從彈性小工具重新執行現有 myApplications 應用程式的彈性評估
- 在彈性小工具中檢閱評估摘要

開始使用

本節說明如何開始使用 AWS Resilience Hub。這包括為 帳戶建立 AWS Identity and Access Management (IAM) 許可。

主題

先決條件

您必須先完成下列先決條件 AWS Resilience Hub，才能使用 ：

- AWS 帳戶 – AWS 為您要在其中使用的每個帳戶類型 (primary/secondary/resource帳戶) 建立一或多個帳戶 AWS Resilience Hub。如需建立和管理 AWS 帳戶的詳細資訊，請參閱以下內容：
  - 第一次 AWS 使用 - 入門：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，您必須為您建立的每個帳戶設定必要的角色和 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 的必要 IAM 許可 AWS Resilience Hub ，以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 Resilience Hub 如何與 IAM 搭配使用”和 以取得將政策新增至角色的詳細資訊，請參閱 the section called “使用 JSON 檔案定義信任政策”。

  若要快速開始將 IAM 許可新增至使用者、群組和角色，您可以使用我們的 AWS 受管政策 (the section called “AWS 受管政策”)。使用 AWS 受管政策來涵蓋 中可用的常見使用案例， AWS 帳戶比自行撰寫政策更容易。 會將其他許可 AWS Resilience Hub 新增至 AWS 受管政策，以將支援延伸至其他 AWS 服務，並包含新功能。因此：
  - 如果您是現有客戶，而且您希望應用程式在評估中使用最新的增強功能，則必須發佈應用程式的新版本，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 “在 中執行彈性評估 AWS Resilience Hub”
  - 如果您不是使用 AWS 受管政策來指派適當的 IAM 許可給使用者、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 可協助您主動準備和保護您的 AWS 應用程式免受中斷：

- 發現彈性缺點。
- 估算您的目標復原時間目標 (RTO) 和復原點目標 (RPO) 是否可達成。
- 在問題發佈到生產環境之前解決問題。

本節會引導您完成新增應用程式。您可以從現有的 myApplications 應用程式、 AWS CloudFormation 堆疊或 收集資源， AWS Resource Groups 並建立適當的彈性政策。描述應用程式後，您可以在 中發佈應用程式 AWS Resilience Hub，並產生應用程式彈性的評估報告。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，然後反覆運算，直到預估工作負載 RTO 和預估工作負載 RPO 達到 RTO 和 RPO 目標為止。

主題

- 新增應用程式以開始使用
- 選取如何管理此應用程式
- 新增資源集合
- 設定 RTO 和 RPO
- 設定排定的評估和偏離通知
- 設定許可
- 設定應用程式組態參數
- 新增標籤
- 檢閱和發佈您的 AWS Resilience Hub 應用程式
- 執行應用程式 AWS Resilience Hub 評估

新增應用程式以開始使用

描述 AWS 應用程式 AWS Resilience Hub 的詳細資訊並執行報告以評估彈性，以開始使用 。

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。

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

描述 中應用程式的詳細資訊 AWS Resilience Hub

本節說明如何描述 中現有 AWS 應用程式的詳細資訊 AWS Resilience Hub。

描述應用程式的詳細資訊

1. 輸入應用程式的名稱。
2. （選用）輸入應用程式的描述。

下一頁

選取如何管理此應用程式

選取如何管理此應用程式

除了 AWS CloudFormation 堆疊 AWS Resource Groups、myApplications 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 Resilience Hub 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探索資源，請選取此選項。資源集合包括 AWS CloudFormation 堆疊 AWS Resource Groups、myApplications 應用程式和 Terraform 狀態檔案。

  如果您選取此選項，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 叢集內的命名空間探索資源，請選取此選項。

  如果您選取此選項，則必須完成 中的程序 the section called “新增 EKS 叢集”
- 資源集合與 EKS – 如果您想要從 AWS CloudFormation 堆疊 AWS Resource Groups、Terraform 狀態檔案和 Amazon EKS 叢集探索資源，請選取此選項。

  如果您選取此選項，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資訊，請參閱 Service Quotas。

下一頁

新增資源集合

新增資源集合

本節討論下列選項，您可以使用這些選項來構成應用程式結構的基礎：

- 新增資源集合
- 新增 EKS 叢集

新增資源集合

本節討論了以下方法，您用來構成應用程式結構的基礎：

- 使用 AWS CloudFormation 堆疊
- 使用 AWS Resource Groups
- 使用 myApplications 應用程式
- 使用 Terraform 狀態檔案

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。堆疊可以來自您用來描述應用程式的 AWS 帳戶 ，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 堆疊以探索以堆疊為基礎的資源。
2. 從選擇與您 AWS 帳戶 和區域相關聯的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，請選擇與 AWS 區域外新增堆疊相鄰的向右箭頭，然後在輸入堆疊 ARN 方塊中輸入堆疊的 Amazon Resource Name (ARN)，然後選擇新增堆疊 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 AWS Resource Groups

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

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 AWS Resource Groups 包含資源的 。
2. 從選擇資源群組下拉式清單中選擇資源。

   若要使用位於不同 AWS 帳戶、不同區域或兩者的 AWS Resource Groups ，請選擇資源群組 ARN 旁的向右箭頭： ，然後在輸入 AWS Resource Groups 資源群組 ARN 方塊中輸入 的 Amazon Resource Name (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 myApplications 應用程式

選擇您要包含在 中的 myApplications 應用程式 AWS Resilience Hub

在 中包含 myApplications 應用程式 AWS Resilience Hub

1. 選取 myApplications。
2. 從選取應用程式下拉式清單中選擇應用程式。

使用 Terraform 狀態檔案

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

> **Note**
>
> AWS Resilience Hub 支援 Terraform 狀態檔案版本 `0.12`和更新版本。

探索構成應用程式結構基礎的資源

1. 選取 Terraform 狀態檔案以探索 S3 儲存貯體資源。
2. 從選取狀態檔案： : 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 URI 欄位中提供 Terraform 狀態檔案位置的連結，然後選擇新增 S3 URL。

   Terraform 狀態檔案的限制為 4 MB (MB)。

3. 從在 S3 對話方塊中選擇封存，從儲存貯體區段中選取您的 Amazon Simple Storage Service 儲存貯體。
4. 從物件區段中，選取金鑰，然後選擇選擇。

新增 EKS 叢集

本節討論如何使用 Amazon EKS 叢集來構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，才能連線至 Amazon EKS 叢集。如需有關新增單一帳戶和跨帳戶 Amazon EKS 許可，以及要連線至叢集之其他 IAM 角色的詳細資訊，請參閱下列主題：
>
> - AWS Resilience Hub 存取許可參考
> - the section called “啟用對 Amazon EKS 叢集的 AWS Resilience Hub 存取”

選擇包含您要在描述的應用程式中使用的資源的 Amazon EKS 叢集和命名空間。Amazon EKS 叢集可以來自 AWS 帳戶 您用來描述應用程式的 ，也可以來自不同的帳戶或不同的區域。

> **Note**
>
> 若要 AWS Resilience Hub 讓 評估您的 Amazon EKS 叢集，您必須手動將相關的命名空間新增至 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。

新增 Amazon EKS 叢集

1. 在 1. 選取 EKS 叢集區段，從與您的 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，請選擇不同帳戶或區域中新增 EKS 叢集相鄰的向右箭頭，然後在輸入 EKS ARN 方塊中輸入 Amazon EKS 叢集的 Amazon Resource Name (ARN)，然後選擇新增 EKS ARN。如需 ARN 的詳細資訊，請參閱《AWS 一般參考》中的 Amazon Resource Name (ARN)。

如需有關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 “啟用對 Amazon EKS 叢集的 AWS Resilience Hub 存取”。

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 叢集和命名空間資料表中選取位於 Amazon EKS 叢集名稱左側的選項按鈕，然後選擇更新命名空間。

   您可以透過以下方式識別 Amazon EKS 叢集：

   - EKS 叢集名稱 – 指示所選 Amazon EKS 叢集的名稱。
   - 命名空間數目 – 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 包含應用程式中所選 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 – 表示您已包含來自 Amazon EKS 叢集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，選擇新增新的命名空間。

   更新命名空間對話方塊會顯示您已從 Amazon EKS 叢集中選取的所有命名空間，做為可編輯的選項。
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，然後在命名空間方塊中輸入命名空間名稱。

     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，請選擇位於命名空間旁的移除。
   - 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。

     如果您選擇此選項，則您在其他 Amazon EKS 叢集中先前的命名空間選擇，將以目前的命名空間選擇覆寫。
4. 若要在您的應用程式中包含更新的命名空間，請選擇更新。

下一頁

設定 RTO 和 RPO

設定 RTO 和 RPO

您可以使用自己的 RTO/RPO 目標定義新的彈性政策，也可以選擇具有預先定義 RTO/RPO 目標的現有彈性政策。如果您想要使用其中一個現有的彈性政策，請選取選擇現有的政策選項，然後從選項項目下拉式清單中選取現有的目標應用程式。

定義您自己的 RTO/RPO 目標

1. 選取建立新的彈性政策選項。
2. 在輸入政策名稱方塊中（名稱下）輸入彈性政策的名稱。

   我們已使用自動產生的名稱預先填入此欄位。您可以選擇使用相同的 ，或提供不同的名稱。
3. （選用）在描述方塊中輸入彈性政策的描述。
4. 在 RTO/RPO 目標區段中定義您的 RTO/RPO。

   > **Note**
   >
   > - 我們已為您的應用程式預先填入預設 RTO 和 RPO。您可以現在或在評估應用程式之後變更 RTO 和 RPO。
   > - AWS Resilience Hub 可讓您在彈性政策的 RTO 和 RPO 欄位中輸入值零。但是，在評估您的應用程式時，可能的最低評估結果接近零。因此，如果您在 RTO 和 RPO 欄位中輸入值零，估計工作負載 RTO 和估計工作負載 RPO 結果會接近零，且您應用程式的合規狀態會設為違反政策。
5. 若要為您的基礎設施和可用區域定義 RTO/RPO，請選擇向右箭頭以展開基礎設施 RTO 和 RPO 區段。
6. 在 RTO/RPO 目標中，在方塊中輸入數值，然後選擇該值代表 RTO 和 RPO 的時間單位。

   對基礎設施 RTO 和 RPO 區段中的基礎設施和可用區域重複這些項目。
7. （選用）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 - 選用。

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

下一頁

the section called “設定排程評估和偏離通知”

設定排定的評估和偏離通知

AWS Resilience Hub 可讓您設定排程評估和偏離通知，以每天評估您的應用程式，並在偵測到偏離時收到通知。

設定偏離通知

1. 若要每日評估您的應用程式，請開啟每日自動評估。

   如果開啟此選項，則每日評估排程只會在下列情況下開始：

   - 第一次成功手動評估應用程式。
   - 應用程式已設定適當的 IAM 角色。
   - 如果您的應用程式已設定目前的 IAM 使用者許可，您必須建立 `AWSResilienceHubAsssessmentExecutionPolicy`

     角色使用 中的適當程序the section called “AWS Resilience Hub 如何與 IAM 搭配使用”。
2. 若要在 AWS Resilience Hub 偵測到彈性政策的任何偏離時收到通知，或其資源偏離時，請開啟應用程式偏離時的取得通知。

   如果開啟此選項，若要接收偏離通知，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 Amazon SNS SNS 主題。

   > **Note**
   >
   > - 若要讓 AWS Resilience Hub 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。如需設定許可的詳細資訊，請參閱 the section called “啟用 AWS Resilience Hub 以發佈到您的 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，或兩者，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 Resource Name (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

設定許可

設定許可

AWS Resilience Hub 可讓您設定主要帳戶和次要帳戶的必要許可，以探索和評估資源。不過，您必須分別執行程序，以設定每個帳戶的許可。

設定 IAM 角色和 IAM 許可

1. 若要選取用於存取目前帳戶中資源的現有 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 Resource Name (ARNs)， AWS Resilience Hub 將使用您從為所有帳戶選取 IAM 角色下拉式清單中選擇的 IAM 角色。

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

   - AWS IAM 主控台 – 如果您選擇此選項，則必須完成 中的程序才能在 IAM 主控台中建立您的 AWS Resilience Hub 角色。
   - AWS CLI – 如果您選擇此選項，則必須完成 AWS CLI 中的所有步驟。
   - CloudFormation 範本 – 如果選擇此選項，取決於帳戶類型 (主要帳戶或次要帳戶)，您必須使用適當的 AWS CloudFormation 範本建立角色。
2. 選擇向右箭頭，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 ARNs 方塊中輸入 IAM 角色的 ARN。確保您輸入的 IAM 角色ARNs 不屬於目前的帳戶。
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，請選擇向右箭頭以展開 使用目前的 IAM 使用者許可區段，然後選取我了解我必須手動設定許可，才能在其中啟用所需的功能 AWS Resilience Hub。

   如果您選取此選項，有些 AWS Resilience Hub 功能 （ 例如偏離通知 ） 可能無法如預期運作，而且您為建立新應用程式提供的輸入會遭到忽略。

下一頁

設定應用程式組態參數

設定應用程式組態參數

本節可讓您使用 提供跨區域容錯移轉支援的詳細資訊 AWS Elastic Disaster Recovery。 AWS Resilience Hub 將使用此資訊提供彈性建議。

如需應用程式組態參數的詳細資訊，請參閱應用程式組態參數。

新增應用程式組態參數 （選用）

1. 若要展開應用程式組態參數區段，請選擇向右箭頭。
2. 在帳戶 ID 方塊中輸入容錯移轉帳戶 ID。根據預設，我們已使用您用於 的帳戶 ID 預先填入此欄位 AWS Resilience Hub，這可以變更。
3. 從區域下拉式清單中選取容錯移轉區域。

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

下一頁

新增標籤

新增標籤

將標籤或標籤指派給 AWS 資源，以搜尋和篩選您的資源，或追蹤您的 AWS 成本。

（選用）若要將標籤新增至應用程式，如果您想要將一或多個標籤與應用程式建立關聯，請選擇新增標籤。如需標籤的詳細資訊，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您的應用程式。

下一頁

檢閱和發佈您的 AWS Resilience Hub 應用程式

檢閱和發佈您的 AWS Resilience Hub 應用程式

建立應用程式後，您仍然可以檢閱應用程式並編輯其資源。完成後，選擇發佈以發佈應用程式。

> **Note**
>
> AWS Resilience Hub 會在背景中掃描您的應用程式資源，並檢查它們是否可以以更有效率的方式分組，以改善評估的準確性。如果 AWS Resilience Hub 識別可以分組到相關 AppComponents 的資源，它會在應用程式頁面的應用程式結構索引標籤中顯示資源分組建議資訊提醒，您可以選擇檢閱建議來檢閱它們。如需詳細資訊，請參閱the section called “AWS Resilience Hub 資源群組建議”。

如需檢閱應用程式和編輯其資源的詳細資訊，請參閱以下內容：

- the section called “檢視應用程式摘要”
- the section called “編輯應用程式資源”

下一頁

執行應用程式 AWS Resilience Hub 評估

執行應用程式 AWS Resilience Hub 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，您可以在其中執行彈性評估。評估會根據連接到應用程式的彈性政策來評估您的應用程式組態。系統會產生評估報告，顯示您的應用程式如何針對彈性政策中的目標進行測量。

執行彈性評估

1. 在應用程式摘要頁面上，選擇評估彈性。
2. 在執行彈性評估對話方塊中，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，請選擇評估索引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 可協助您改善應用程式在 上的彈性， AWS 並在應用程式中斷時縮短復原時間。

主題：

AWS Resilience Hub 摘要

AWS Resilience Hub 提供具有圖表和圖形的視覺化摘要，可讓您at-a-glance地檢視多個 AWS 服務和資源的應用程式彈性狀態。此全面且簡潔的視覺化摘要可讓您快速識別潛在的彈性差距、排定動作優先順序，以及追蹤進度，以增強應用程式從中斷中復原的能力。當您選擇匯出時，如果您是第一次匯出指標， 會在您存取的區域中 AWS Resilience Hub 建立新的 Amazon S3 儲存貯體 AWS Resilience Hub。此 Amazon S3 儲存貯體只會第一次建立，且會在成功完成時用來儲存匯出的指標。在 Amazon S3 中儲存匯出的資料需要支付額外費用。如需這些費用的詳細資訊，Amazon S3 定價。

小工具中的圖表和圖形可協助您了解下列事項：

- 應用程式的整體彈性分數和目前操作狀態概觀。
- 透過反白顯示不符合已建立政策或偏離建議組態的應用程式，可能違反政策或偏離最佳實務。此外，它還強調了可讓您排定優先順序並解決這些問題的特定區域。
- 需要立即關注的關鍵資源或應用程式。

- 增強彈性實務的建議，例如實作警示、 conduct AWS Fault Injection Service (AWS FIS) 實驗和建立標準操作程序。這些建議會隨著時間進行追蹤，讓您監控實作進度，並測量對應用程式整體彈性狀態的影響。

小工具

- 應用程式狀態
- 依資源類型列出的首要基礎設施建議
- 基礎設施建議
- 未實作的操作建議
- 警示建議
- SOP 建議
- AWS FIS 實驗建議
- 具有漂移的應用程式
- 彈性分數
- 彈性分數的 10 個應用程式
- 政策的應用程式狀態

應用程式狀態

此小工具指出您的應用程式是否符合彈性政策。在彈出視窗中選擇應用程式計數相鄰的數字，以檢視應用程式窗格中所有相關聯的應用程式。若要檢視您建立的所有應用程式，請選擇檢視應用程式。如需在中管理應用程式的詳細資訊 AWS Resilience Hub，請參閱 檢視 AWS Resilience Hub 應用程式摘要。

依資源類型列出的首要基礎設施建議

此小工具會顯示上次成功評估時所提供 AWS 資源的每個資源類型的基礎設施建議數量，以改善其彈性狀態。您可以將滑鼠游標移至詳細資訊上或導覽至詳細資訊，以識別詳細資訊。若要檢視您建立的所有應用程式，請選擇檢視應用程式。如需基礎設施建議的詳細資訊，請參閱檢閱彈性建議。

基礎設施建議

此小工具列出最多 10 個應用程式，這些應用程式在上次成功評估中提供的最大基礎設施建議數量，以改善其彈性狀態。若要檢視您建立的所有應用程式，請選擇檢視應用程式。如需基礎設施建議的詳細資訊，請參閱檢閱彈性建議。

您可以使用下列項目來識別詳細資訊：

- 應用程式名稱 – 您在定義應用程式時所提供的應用程式名稱 AWS Resilience Hub。
- 計數 – 指出上次成功評估 AWS Resilience Hub 中 提供的基礎設施建議數量。選擇數字以檢視評估報告中提供的所有基礎設施建議。
- 上次評估 – 指出應用程式上次成功評估的日期和時間。

未實作的操作建議

此小工具列出最多 10 個應用程式，這些應用程式在上次成功評估中提供的最大未實作操作建議數量，以改善其彈性狀態。若要檢視您建立的所有應用程式，請選擇檢視應用程式。如需操作建議的詳細資訊，請參閱檢閱操作建議。

您可以使用下列項目來識別詳細資訊：

- 應用程式名稱 – 您在定義應用程式時所提供的應用程式名稱 AWS Resilience Hub。
- 計數 – 指出上次成功評估 AWS Resilience Hub 中 提供的操作建議數量。選擇數字以檢視評估報告中所有未實作的操作建議。
- 上次評估時間 – 指出應用程式上次成功評估的日期和時間。

警示建議

此小工具會列出為改善所選期間內的復原狀態而提供的所有 Amazon CloudWatch 警示建議。不同的類別 (已實作、未實作和已排除) 表示其在應用程式中的實作狀態。您可以將滑鼠暫留在每個類別上或瀏覽至每個類別，以檢視其 Amazon CloudWatch 警示建議的數量。若要檢視您建立的所有應用程式，請選擇檢視應用程式。如需警示建議的詳細資訊，請參閱檢閱操作建議。

SOP 建議

此小工具會列出所有標準操作程序 (SOP) 建議，以改善所選期間內的恢復狀態。不同的類別 (已實作、未實作和已排除) 表示其在應用程式中的實作狀態。您可以將滑鼠游標移至每個類別，或瀏覽至它們，以檢視每個類別的 SOP 建議數量。若要檢視您建立的所有應用程式，請選擇檢視應用程式。如需操作建議的詳細資訊，請參閱 檢閱操作建議。

AWS FIS 實驗建議

此小工具會列出在所選期間內提供的所有 AWS FIS 實驗建議，以改善復原狀態。不同的類別 (實作、未實作、部分實作和已排除) 表示其在應用程式中的實作狀態。您可以將滑鼠暫留在每個類別上或

瀏覽至每個類別，以檢視其 AWS FIS 實驗建議的數量。若要檢視您建立的所有應用程式，請選擇檢視應用程式。如需 AWS FIS 實驗建議的詳細資訊，請參閱 管理標準操作程序。

具有漂移的應用程式

此小工具會列出您在上次成功評估時，偏離先前合規狀態的所有應用程式。若要檢視您建立的所有應用程式，請選擇檢視應用程式。如需在 中管理應用程式的詳細資訊 AWS Resilience Hub，請參閱檢視 AWS Resilience Hub 應用程式摘要。

您可以使用下列項目來識別詳細資訊：

- 應用程式名稱 – 您在定義應用程式時所提供的應用程式名稱 AWS Resilience Hub。
- 政策偏離 – 選擇應用程式名稱旁的數字，以檢視在先前評估中符合政策但無法在目前評估中符合的所有應用程式元件。
- 資源漂移 – 選擇以下數字，以檢視在最新匯入中從其組態變更的所有資源。

彈性分數

此小工具會顯示最多五個應用程式在所選時段內應用程式彈性分數的趨勢。您可以將滑鼠游標停留在應用程式名稱相關聯的行上，或瀏覽應用程式名稱，然後選擇應用程式名稱以檢視應用程式摘要，以檢視應用程式的彈性分數。若要檢視您建立的所有應用程式，請選擇檢視應用程式。如需彈性分數的詳細資訊，請參閱了解彈性分數。

彈性分數的 10 個應用程式

此小工具列出最多 10 個應用程式，其最近的評估具有最低的彈性分數，強調需要立即注意以改善其彈性的應用程式。若要檢視您建立的所有應用程式，請選擇檢視應用程式。如需彈性分數的詳細資訊，請參閱了解彈性分數。

您可以使用下列項目來識別詳細資訊：

- 應用程式名稱 – 您在定義應用程式時所提供的應用程式名稱 AWS Resilience Hub。
- 彈性分數 – 執行評估後，由 AWS Resilience Hub 為您的應用程式決定的整體彈性分數。
- 上次評估時間 – 指出應用程式上次成功評估的日期和時間。

政策的應用程式狀態

此小工具會列出您的所有政策，以及已違反、符合或尚未針對這些政策進行評估的應用程式數量。若要檢視您建立的所有政策，請選擇檢視政策。如需彈性分數的詳細資訊，請參閱管理彈性政策。

您可以使用下列項目來識別詳細資訊：

- 政策名稱 – 表示您在定義政策名稱時所提供的政策名稱 AWS Resilience Hub。
- 類型 – 指出連接到應用程式的政策類型 （ 彈性政策)。
- 政策名稱 – 指出違反彈性政策中定義的 RTO 和 RPO 目標的應用程式數量。
- 符合的應用程式 – 指示符合彈性政策的應用程式數量。
- 未評估的應用程式 – 指示尚未根據彈性政策評估的應用程式數量。
- 彈性分數 – 執行評估後，由 AWS Resilience Hub 為您的應用程式決定的整體彈性分數。
- 上次評估時間 – 指出應用程式上次成功評估的日期和時間。

AWS Resilience Hub 儀表板

儀表板提供應用程式產品組合彈性狀態的完整檢視。儀表板會彙總和組織復原能力事件 （ 例如無法使用的資料庫或復原能力驗證失敗）、警示，以及來自 CloudWatch 和 AWS Fault Injection Service () 等服務的洞見AWS FIS。

儀表板也會為每個評估的應用程式產生彈性分數。此分數指出應用程式在評估建議的復原政策、警示、復原標準操作程序 (SOPs) 和測試時，執行效能如何。您可以使用此分數來測量一段時間內的彈性改善。

若要檢視 AWS Resilience Hub 儀表板，請從導覽功能表中選擇儀表板。儀表板頁面會顯示下列區段：

應用程式狀態

應用程式狀態會指出應用程式是否已評估是否符合其連接的彈性政策。此外，評估完成後，狀態也會指出應用程式的輸入來源是否已修改。在下列每個狀態下選擇一個數字，以檢視應用程式頁面中共用相同狀態的所有應用程式：

- 政策中的應用程式 – 指出符合其連接彈性政策的所有應用程式。
- 應用程式違反政策 – 指出不符合其連接彈性政策的所有應用程式。
- 未評估的應用程式 – 指出尚未評估或追蹤其合規的所有應用程式。

- 應用程式漂移 – 指出已從其彈性政策漂移的所有應用程式，或他們的資源是否漂移。

一段時間內的應用程式彈性分數

透過應用程式彈性分數隨時間變化，您可以檢視過去 30 天內應用程式彈性的圖表。雖然下拉式選單可以列出 10 個應用程式， AWS Resilience Hub 但只會顯示一次最多四個應用程式的圖形。如需彈性分數的詳細資訊，請參閱了解彈性分數。

> **Note**
>
> AWS Resilience Hub 不會同時執行排定的評估。因此，您可能需要在稍後時間返回至彈性分數，以檢視應用程式的每日評估。

AWS Resilience Hub 也會使用 Amazon CloudWatch 來產生這些圖形。選擇在 CloudWatch 中檢視指標，即可在 CloudWatch 儀表板中建立和檢視應用程式彈性的更精細資訊。如需 CloudWatch 的詳細資訊，請參閱《Amazon CloudWatch 使用者指南》中的使用儀表板。

實作的警示

本節列出您在 Amazon CloudWatch 中設定的所有警示，以監控所有應用程式。如需更多詳細資訊，請參閱 檢視警示。

實作的實驗

本節列出您已在所有應用程式中實作的所有故障注入實驗。如需詳細資訊，請參閱檢視 AWS FIS 實驗。

描述和管理 AWS Resilience Hub 應用程式

AWS Resilience Hub 應用程式是一組 AWS 資源，其結構是為了防止和復原 AWS 應用程式中斷。

若要描述 AWS Resilience Hub 應用程式，請提供應用程式名稱、一或多個 AWS CloudFormation 堆疊的資源，以及適當的彈性政策。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。

描述應用程式之後，您必須發佈該 AWS Resilience Hub 應用程式，才能對其執行彈性評估。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，然後重複此程序，直到您的預估工作負載 RTO 和預估工作負載 RPO 符合 RTO 和 RPO 目標為止，來改善彈性。

若要檢視應用程式頁面，請從導覽窗格中選擇應用程式。您可以在應用程式頁面中透過下列方式識別您的應用程式：

- 名稱 – 您在定義應用程式時所提供的應用程式名稱 AWS Resilience Hub。
- 描述 – 您在定義應用程式時所提供的應用程式描述 AWS Resilience Hub。
- 合規狀態 – 將應用程式狀態 AWS Resilience Hub 設定為已評估、未評估、違反政策，或偵測到變更。
  - 已評估 - AWS Resilience Hub 已評估您的應用程式。
  - 未評估 - AWS Resilience Hub 未評估您的應用程式。
  - 違反政策 - AWS Resilience Hub 已判斷您的應用程式不符合復原時間目標 (RTO) 和復原點目標 (RPO) 的復原政策目標。在重新評估應用程式彈性 AWS Resilience Hub 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。
  - 偵測到變更 - AWS Resilience Hub 偵測到對與您應用程式相關聯的彈性政策所做的變更。您必須重新評估 的應用程式 AWS Resilience Hub ，以判斷您的應用程式是否符合彈性政策的目標。
- 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 應用程式彈性。
  - 作用中 - 這表示您的應用程式每日都會由 自動評估 AWS Resilience Hub。
  - 已停用 - 這表示您的應用程式不會每日由 自動評估 AWS Resilience Hub ，您必須手動評估您的應用程式。
- 偏離狀態 – 指出您的應用程式是否偏離先前的成功評估，並設定下列其中一種狀態：
  - 偏離 - 表示應用程式在先前成功評估中符合其彈性政策，現在已違反彈性政策，且應用程式面臨風險。此外，它也會指出輸入來源中的資源是否新增或移除，而這些資源包含在目前的應用程式版本中。
  - 未漂移 - 表示應用程式仍估計為符合政策中定義的 RTO 和 RPO 目標。此外，它還指出輸入來源中的資源，包含在目前的應用程式版本中，並未新增或移除。
- 預估工作負載 RTO – 指出應用程式的預估工作負載 RTO 上限。此值是上次成功評估中所有中斷類型的預估工作負載 RTO 上限。
- 預估工作負載 RPO – 指出應用程式的預估工作負載 RPO 上限。此值是上次成功評估中所有中斷類型的預估工作負載 RTO 上限。
- 上次評估時間 – 指出您的應用程式上次成功評估的日期和時間。
- 建立時間 – 建立應用程式的日期和時間。
- ARN – 應用程式的 Amazon Resource Name (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 只有在您將 Amazon ECR 用於映像儲存庫時，才能完整評估跨區域 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，依應用程式的名稱篩選結果。
- 依日期和時間範圍篩選上次評估時間 – 若要套用此篩選條件，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 – 選取其中一個可用的選項，然後選擇套用。

    如果您選擇自訂範圍選項，請在輸入持續時間方塊中輸入持續時間，然後從時間單位下拉式清單中選取適當的時間單位，然後選擇套用。
  - 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 AWS Resilience Hub 應用程式的不同方法，以及如何管理應用程式。

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彈性運作狀態的概觀。

檢視應用程式摘要

1. 從導覽窗格中選擇應用程式。

2. 在應用程式頁面上，選擇您要檢視的應用程式名稱。

應用程式摘要頁面包含下列區段。

主題

評估摘要

本節提供上次成功評估的摘要，並將關鍵建議重點標示為可行的洞見。 AWS Resilience Hub 使用 Amazon Bedrock 生成式 AI 功能，協助使用者專注於 提供的最關鍵彈性建議 AWS Resilience Hub。透過專注於關鍵項目，您可以專注於改善應用程式彈性狀態的最關鍵建議。選擇建議以檢視其摘要，然後選擇檢視詳細資訊，以檢視評估報告相關區段中建議的詳細資訊。如需檢閱評估報告的詳細資訊，請參閱 the section called “檢閱評估報告”。

> **Note**
>
> - 此評估摘要僅適用於美國東部（維吉尼亞北部）區域。
> - Amazon Bedrock 上大型語言模型 (LLMs) 產生的評估摘要只是建議。目前的生成式 AI 技術水準並不完美，LLMs也不是無可取代的。雖然很少有偏差和不正確的答案，但應該預期。使用 LLM 的輸出之前，請先檢閱評估摘要中的每個建議。

Summary

本節提供下列各節中所選應用程式的摘要：

- 應用程式資訊 – 本節提供有關所選應用程式的下列資訊：
  - 應用程式狀態 – 指出應用程式的狀態。
  - 描述 – 應用程式的描述。
  - 版本 – 指出目前評估的應用程式版本。

- 彈性政策 – 指出連接應用程式的彈性政策。如需彈性政策的詳細資訊，請參閱管理彈性政策。
- 應用程式偏離 – 本節重點介紹執行所選應用程式評估時偵測到的偏離，以檢查是否符合其彈性政策。此外，它也會檢查自上次發佈應用程式版本後，是否有任何資源已新增或移除。本節顯示下列資訊：
  - 政策偏離 – 選擇以下數字，以檢視在先前評估中符合政策但未能符合目前評估的所有應用程式元件。
  - 資源漂移 – 選擇以下數字，以檢視最新評估中的所有漂移資源。

應用程式彈性

彈性分數區段中顯示的指標來自應用程式的最新彈性評估。

彈性分數

彈性分數可協助您量化處理潛在中斷的準備程度。此分數反映您的應用程式遵循 AWS Resilience Hub 建議以符合應用程式的彈性政策、警示、標準操作程序 (SOPs) 和測試的程度。

您的應用程式可達到的最大彈性分數為 100%。分數代表在預先定義期間內執行的所有建議測試。這表示測試正在啟動正確的警示，且警示會啟動正確的 SOP。

例如，假設 AWS Resilience Hub 建議使用一個警示和一個 SOP 進行測試。測試執行時，警示會啟動相關聯的 SOP，然後成功執行。如需彈性分數的詳細資訊，請參閱 了解彈性分數。

實作的警示

應用程式摘要實作的警示區段會列出您在 Amazon CloudWatch 中為監控應用程式而設定的警示。如需警示的詳細資訊，請參閱 管理警示。

實作的實驗

應用程式摘要故障注入實驗區段顯示故障注入實驗的清單。如需故障注入實驗的詳細資訊，請參閱 管理 AWS Fault Injection Service 實驗。

編輯 AWS Resilience Hub 應用程式資源

若要接收準確且實用的彈性評估，請確定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、驗證和建議是以列出的資源為基礎。如果您從 AWS 應用程式新增或移除資源，您應該在 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。您可以在應用程式中識別和編輯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。您的實際資源不會進行任何變更。

您可以新增缺少的資源、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的 （ 發行版本 ） 版本，來新增或更新應用程式資源。AWS Resilience Hub 會使用應用程式的發行版本 （ 包括更新的 資源 ） 來執行彈性評估。

評估應用程式的彈性

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，選擇評估彈性。
4. 在執行彈性評估對話方塊中，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，請選擇評估索引標籤和您的評估以檢視報告。
7. 選擇檢閱索引標籤以檢視應用程式的評估報告。

啟用排程評估

1. 在導覽窗格中，選擇 Applications (應用程式)。
2. 在應用程式頁面上，選取您要為其啟用排程評估的應用程式。
3. 開啟 自動評估每日。

停用排程評估

1. 在導覽窗格中，選擇 Applications (應用程式)。
2. 在應用程式頁面上，選取您要為其啟用排程評估的應用程式。
3. 關閉 自動評估每日。

> **Note**
>
> 停用排程評估將停用偏離通知。

4. 選擇關閉。

為您的應用程式啟用偏離通知

1. 在導覽窗格中，選擇 Applications (應用程式)。
2. 在應用程式頁面上，選取要啟用偏離通知的應用程式，或編輯偏離通知設定。
3. 您可以選擇下列其中一個選項來編輯偏離通知：
   - 在動作中，選擇啟用偏離通知。
   - 在應用程式偏離區段中選擇啟用通知。
4. 完成 中的步驟設定排定的評估和偏離通知，然後返回此程序。
5. 選擇 啟用 。

   啟用偏離通知也會啟用排程評估。

編輯應用程式的偏離通知

> **Note**
>
> 如果您已啟用排程評估 (開啟每日自動評估) 和偏離通知，則此程序適用。

1. 在導覽窗格中，選擇 Applications (應用程式)。
2. 在應用程式頁面上，選取要啟用偏離通知的應用程式，或編輯偏離通知設定。
3. 您可以選擇下列其中一個選項來編輯偏離通知：
   - 在動作中，選擇編輯偏離通知。
   - 在應用程式偏離區段中選擇編輯通知。
4. 完成 中的步驟設定排定的評估和偏離通知，然後返回此程序。
5. 選擇 Save (儲存)。

更新應用程式的安全許可

1. 在導覽窗格中，選擇 Applications (應用程式)。
2. 在應用程式頁面上，選取要更新安全許可的應用程式。
3. 從動作中，選擇更新許可。
4. 若要更新安全許可，請完成 中的步驟設定許可，然後返回此程序。
5. 選擇儲存並更新。

將彈性政策連接至您的應用程式

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，選擇連接彈性政策。
4. 在連接政策對話方塊中，從選取彈性政策下拉式清單中選取彈性政策。
5. 選擇 Attach (連接)。

編輯應用程式的輸入來源、資源和 AppComponents

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 + ，然後選擇具有草稿狀態的應用程式版本。
5. 若要編輯應用程式的輸入來源、資源和 AppComponents，請完成下列程序的步驟。

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，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 堆疊匯入的來源名稱，則會將您重新導向至主控台上的 AWS CloudFormation 堆疊詳細資訊頁面。
   - 來源 ARN – 輸入來源的 Amazon Resource Name (ARN)。選擇 ARN，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，則會將您重新導向至 AWS CloudFormation 主控台上的堆疊詳細資訊頁面。

- 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、myApplications 應用程式 AWS Resource Groups、Terraform 狀態檔案，以及手動新增的資源。
- 關聯的資源 – 與輸入來源相關聯的資源數目。在資源索引標籤中選擇數字，以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。如需新增輸入來源的詳細資訊，請參閱the section called “將資源新增至您的 AWS Resilience Hub 應用程式”。
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，它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。

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。

資源區段列出您選擇用作應用程式描述範本的應用程式資源。為了增強您的搜尋體驗， AWS Resilience Hub 已根據多個搜尋條件將資源分組。這些搜尋條件包括 AppComponent 類型、不支援的資源和排除的資源。若要根據資源資料表中的搜尋條件篩選資源，請選擇每個搜尋條件下方的數字。

您可以透過以下方式識別資源：

- 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、myApplications 應用程式或 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之資源的邏輯 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 AWS Resilience Hub 的資源”。

- 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 Amazon EC2 執行個體。如需將 AppComponent 資源分組的詳細資訊，請參閱應用程式元件中的資源分組。
- 來源名稱 – 輸入來源的名稱。選擇來源名稱，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 堆疊匯入的來源名稱，則會將您重新導向至 上的堆疊詳細資訊頁面 AWS CloudFormation。
- 來源類型 – 輸入來源的類型。輸入來源包括 AWS CloudFormation 堆疊、myApplications 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，請完成 中的步驟 編輯應用程式程序的 AWS Resilience Hub 輸入來源。

- 來源堆疊 – 包含 資源的 AWS CloudFormation 堆疊。此欄取決於您選擇的應用程式結構類型。
- 實體 ID – 該資源的實際指派識別符，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 AWS Resilience Hub 在應用程式中包含這些資源。
- 可評估 – 這表示 是否會 AWS Resilience Hub 評估您的資源的彈性。
- AppComponents – 在發現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。
- 帳戶 – 擁有實體資源 AWS 的帳戶。

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，然後選擇從動作中排除資源。
4. 若要解決應用程式上的資源，請選擇重新整理資源。

5. 若要修改現有的應用程式資源，請完成下列步驟：

   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，若要更新您的資源，請完成 中的適當程序新增資源集合，然後返回此程序。

   c. 選擇 Save (儲存)。

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

   a. 從資源類型下拉式清單中選取資源類型。

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

   c. 在資源名稱方塊中輸入資源邏輯 ID。

   d. 在資源識別符方塊中輸入實體資源 ID、資源名稱或資源 ARN。

   e. 選擇新增。

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 Save (儲存)。

8. 若要編輯資源識別符，請選取資源，從動作中選擇編輯資源識別符，然後完成下列步驟：

   a. 在資源識別符方塊中輸入實體資源 ID、資源名稱或資源 ARN。

   b. 選擇 Save (儲存)。

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

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

   b. 選擇新增。

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。

編輯應用程式的 AppComponents

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

> **Note**
>
> 如需將 AppComponent 資源分組的詳細資訊，請參閱應用程式元件中的資源分組。

AppComponents 區段會列出資源分組的所有邏輯元件。您可以透過以下方式識別 AppComponents：

- AppComponent 名稱 – 在發現其應用程式結構時指派給此資源的元件名稱 AWS Resilience Hub 。
- AppComponent 類型 – 元件的 AWS Resilience Hub 類型。
- 來源名稱 – 輸入來源的名稱。選擇來源名稱，以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，則會將您重新導向至 上的堆疊詳細資訊頁面 AWS CloudFormation。
- 資源計數 – 與輸入來源相關聯的資源數量。在資源索引標籤中選擇數字以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建立新的 AppComponent，並完成下列步驟：
   a. 在 AppComponent 名稱方塊中輸入 AppComponent 的名稱。為了參考，我們已使用範例名稱預先填入此欄位。
   b. 從 AppComponent 類型下拉式清單中選取 AppComponent 的類型。
   c. 選擇 Save (儲存)。
3. 若要編輯 AppComponent，請選取 AppComponent，然後從動作中選擇編輯 AppComponent。
4. 若要刪除 AppComponent，請選取 AppComponent，然後從動作中選擇刪除 AppComponent。

變更資源清單後，您會收到提醒，指出已對應用程式的草稿版本進行變更。若要執行準確的彈性評估，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。

管理應用程式元件

應用程式元件 (AppComponent) 是一組相關 AWS 資源，可做為單一單位運作並失敗。例如，如果您有主要資料庫和複本資料庫，這兩個資料庫都屬於相同的 AppComponent. AWS Resilience Hub has 規則，用於管理哪些 AWS 資源可以屬於哪個 AppComponent 類型。例如，`DBInstance`可以屬於 `AWS::ResilienceHub::DatabaseAppComponent` ，而不是屬於 `AWS::ResilienceHub::ComputeAppComponent`。

The AWS Resilience Hub AppComponents 支援下列資源：

- `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::ElastiCache::CacheCluster
  - AWS::ElastiCache::GlobalReplicationGroup
  - AWS::ElastiCache::ReplicationGroup
  - AWS::ElastiCache::ServerlessCache
  - 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 Amazon FSx for Windows File Server。

- `AWS::S3::Bucket`

主題

應用程式元件中的資源分組

當應用程式 AWS Resilience Hub 與其資源匯入至 時， AWS Resilience Hub 會盡最大努力在您匯入應用程式時將相關資源分組至相同的 AppComponent，但分組可能不一定 100% 準確。有些資源會遭到封鎖以進行手動分組，並在適用時自動分組，因為這些服務具有嚴格的相依性，需要特定的分組組態。如需手動分組封鎖的服務完整清單，請參閱the section called “手動分組的封鎖服務”。

AWS Resilience Hub 會在您的應用程式及其資源成功匯入後執行下列活動：

- 掃描您的資源，以檢查是否可以重新分組到新的 AppComponents以提高評估準確性。
- 如果 AWS Resilience Hub 識別可以重新分組為新 AppComponents的資源，則會顯示與建議相同的資源，並允許您接受或拒絕相同資源。在 中 AWS Resilience Hub，指派給分組建議的可信度層級指出資源應根據其屬性和中繼資料分組在一起的確定性程度。高可信度層級表示 AWS Resilience Hub 的可信度層級為 90% 或更高，表示該群組中的資源相關且應分組在一起。中可信度層級表示 AWS Resilience Hub 的可信度層級介於 70% 到 90% 之間，表示該群組中的資源是相關的，且應分組在一起。

> **Note**
>
> AWS Resilience Hub 需要正確的分組，以便可以計算預估工作負載 RTO 和預估工作負載 RPO 來產生建議。

以下是正確分組的範例：

- 在單一 AppComponent 下將主要資料庫和複本分組。
- 在單一 AppComponent 下，將執行相同應用程式的 Amazon EC2 執行個體分組。
- 在單一 AppComponent 下，將某個區域中的 Amazon ECS 服務分組，並將另一個區域中的 Amazon ECS 服務容錯移轉。

如需依 檢閱和包含資源分組建議的詳細資訊 AWS Resilience Hub，請參閱下列主題：

- AWS Resilience Hub 資源群組建議
- 手動將資源分組到 AppComponent

手動分組的封鎖服務

AWS Resilience Hub 會封鎖您手動分組特定 AWS 服務的資源，以防止可能影響應用程式彈性評估和建議的組態錯誤。這些服務會根據其相依性和組態自動分組。當您定義包含這些資源的應用程式時 AWS Resilience Hub，它會分析其關係、相依性和彈性需求，以建立最佳分組，以確保準確的評估結果。

手動分組封鎖 AWS 的服務清單：

- Amazon API Gateway
- Amazon DocumentDB
- Amazon DynamoDB
- Amazon Elastic Block Store
- Amazon Elastic File System
- Amazon Relational Database Service
- Amazon S3
- Amazon Simple Queue Service
- FSx for Windows File Server
- NAT 閘道

AWS Resilience Hub 資源群組建議

本節說明如何在 中產生和檢閱資源分組建議 AWS Resilience Hub。

> **Note**
>
> 您可以使用 `AWSResilienceHubAsssessmentExecutionPolicy` AWS 受管政策 AWS Resilience Hub ，授予使用 所需的必要 IAM 許可。如需 AWS 受管政策的詳細資訊，請參閱 AWSResilienceHubAsssessmentExecutionPolicy。

檢視資源分組建議

1. 在導覽窗格中，選擇 Applications (應用程式)。
2. 選擇新增應用程式頁面，選擇您要檢閱資源群組建議的應用程式名稱。
3. 選擇應用程式結構索引標籤。
4. 如果 AWS Resilience Hub 顯示資訊提醒，請選擇檢閱建議以檢視所有資源群組建議。否則請完成下列步驟，以手動產生資源分組建議：

   a. 選擇資源。

   b. 從動作功能表中選擇取得分組建議。

      AWS Resilience Hub 會掃描您的 資源，以檢查如何以最佳方式分組到相關的 AppComponents以改善評估的準確性。如果 AWS Resilience Hub 得知您的資源可以分組在一起，則會顯示相同的資訊提醒。

   c. 如果顯示資訊提醒，請選擇檢閱建議以檢視所有資源群組建議。

   您可以使用下列方式，在檢閱資源群組建議區段中識別 AppComponents：

   - AppComponent 名稱 – 將分組資源的 AppComponent 名稱。
   - 可信度層級 – 在分組建議中指出 AWS Resilience Hub 的可信度層級。
   - 資源計數 – 指示要在 AppComponent 中分組的資源數量。
   - AppComponent 類型 – 指示 AppComponent 的類型。

檢視將在 AppComponents 中分組的資源

1. 完成檢視資源分組建議程序中的步驟，然後返回此程序。
2. 在檢閱資源分組建議區段中，選取核取方塊 (AppComponent 名稱旁 ），以檢視將在所選 AppComponent 內分組的所有資源。如果您選取多個核取方塊，則 AWS Resilience Hub 會顯示

動態產生的建議已選取區段，將選取的 AppComponents分組至其個別的 AppComponent 類型。選擇每個 AppComponent 類型下方的數字，以檢視將在所選 AppComponent 內分組的所有資源。

您可以使用下列各項，在資源區段的所選 AppComponent 中識別要分組的資源：

- 邏輯 ID – 指示資源的邏輯 ID。邏輯 ID 是用來識別 AWS CloudFormation 堆疊、Terraform 狀態檔案、myApplications 應用程式或 中資源的名稱 AWS Resource Groups。
- 實體 ID – 資源的實際指派識別符，例如 Amazon EC2 執行個體 ID 或 Amazon S3 儲存貯體名稱。
- 類型 – 指出資源的類型。
- 區域 – 資源所在的 AWS 區域。

接受資源分組建議

1. 完成檢視資源分組建議程序中的步驟，然後返回此程序。
2. 在檢閱資源群組建議區段中，選取 AppComponent 名稱旁的所有核取方塊。若要尋找特定的 AppComponent，請在尋找 AppComponent AppComponents 名稱。

> **Note**
>
> 根據預設， AWS Resilience Hub 會顯示所有資源群組建議。若要使用先前拒絕的資源群組建議來篩選資料表，請從尋找 AppComponents 方塊旁邊的下拉式功能表中選擇先前拒絕。

3. 選擇 Accept (接受)。
4. 在接受資源群組建議對話方塊中選擇接受。

AWS Resilience Hub 如果資源群組成功， 會顯示資訊提醒。如果您只接受一部分的資源群組建議，檢閱資源群組建議區段會顯示您尚未接受的所有資源群組建議。

拒絕資源群組建議

1. 完成檢視資源分組建議程序中的步驟，然後返回此程序。
2. 在檢閱資源群組建議區段中，選取 AppComponent 名稱旁的所有核取方塊。若要尋找特定的 AppComponent，請在尋找 AppComponent AppComponents 名稱。

> **Note**
>
> 根據預設，AWS Resilience Hub 會顯示所有資源群組建議。若要使用先前拒絕的資源群組建議篩選資料表，請從尋找 AppComponents 方塊旁的下拉式功能表中選取先前拒絕。

3. 選擇 Reject (拒絕)。
4. 選取拒絕資源群組建議的原因之一，然後在拒絕資源群組建議對話方塊中選擇拒絕。

   AWS Resilience Hub 會顯示確認相同的資訊提醒。如果您只拒絕資源群組建議的子集，檢閱資源群組建議區段會顯示所有您尚未接受的資源群組建議。

手動將資源分組到 AppComponent

本節說明如何將資源手動分組到 AppComponent，並將不同的 AppComponent 指派給其中的資源 AWS Resilience Hub。

將資源分組

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，選取具有草稿狀態的應用程式版本。
5. 選擇 Resources (資源) 標籤。
6. 選取與邏輯 ID 相鄰的核取方塊，以選取要分組的所有資源。

> **Note**
>
> 您無法選擇手動新增的資源。

7. 選擇動作，然後選擇群組資源。
8. 從選擇AppComponent將資源分組的 AppComponent 下拉式清單中選擇 AppComponent。
9. 選擇 Save (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，請完成下列步驟：

a. 在版本索引標籤下，選取目前版本狀態的應用程式版本。

b. 選擇 Resources (資源) 標籤。

將資源指派給 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. 在版本下，選取具有草稿狀態的應用程式版本。
5. 選擇 Resources (資源) 標籤。
6. 選取邏輯 ID 旁邊的核取方塊，以選取資源。
7. 從動作功能表中選擇變更 AppComponent。
8. 若要從 AppComponent 區段刪除目前的 AppComponent，請在顯示您目前 AppComponent 名稱的標籤右上角選擇 X。
9. 若要將資源分組到不同的 AppComponent，請從選擇 AppComponent 下拉式清單中選擇不同的 AppComponent。
10. 選擇新增。
11. 從 AppComponents 索引標籤中刪除任何空白的 AppComponents。
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，請完成下列步驟：

    a. 在版本索引標籤下，選取目前版本狀態的應用程式版本。

    b. 選擇 Resources (資源) 標籤。

發佈新的 AWS Resilience Hub 應用程式版本

如 中所述變更 AWS Resilience Hub 應用程式資源後[編輯 AWS Resilience Hub 應用程式資源](#)，您必須發佈應用程式的新版本，才能執行準確的彈性評估。此外，如果您將新的建議警示、SOPs 和測試新增至應用程式，您可能需要發佈應用程式的新版本。

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中的名稱方塊中，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 (發布)。

   當您發佈應用程式的新版本時，這會成為執行彈性評估時評估的版本。此外，在您進行任何變更之前，草稿版本將與發行版本相同。

在您發佈應用程式的新版本後，我們建議您執行新的彈性評估報告，以確認您的應用程式仍符合您的彈性政策。如需有關執行評估的資訊，請參閱 在 中執行和管理彈性評估 AWS Resilience Hub。

檢視所有 AWS Resilience Hub 應用程式版本

為了協助追蹤應用程式變更， AWS Resilience Hub 會顯示從建立應用程式時開始的先前版本 AWS Resilience Hub。

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 (+)。 分別使用草稿和目前版本狀態 AWS Resilience Hub 來表示應用程式的草稿版本和最近發行版本。您可以選擇應用程式的任何版本，以檢視其資源、AppComponent、輸入來源和其他相關資訊。

   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，依應用程式版本名稱篩選結果。
   - 依日期和時間範圍篩選 – 若要套用此篩選條件，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 – 選取其中一個可用的選項，然後選擇套用。

       如果您選擇自訂範圍選項，請在輸入持續時間方塊中輸入持續時間，然後從時間單位下拉式清單中選取適當的時間單位，然後選擇套用。

- 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

檢視您應用程式的資源

1. 在導覽窗格中，選擇 Applications (應用程式)。
2. 在應用程式頁面上，選取要更新安全許可的應用程式。
3. 在動作中，選擇檢視資源。

   在資源索引標籤中，您可以透過下列方式識別資源資料表中的資源：

   - 邏輯 ID – 邏輯 ID 是用來識別 AWS CloudFormation 堆疊、Terraform 狀態檔案、myApplications 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之資源的邏輯 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 AWS Resilience Hub 的資源”。

   - 狀態 – 這表示 是否會 AWS Resilience Hub 評估您的 資源的彈性。
   - 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 Amazon EC2 執行個體。如需將 AppComponent 資源分組的詳細資訊，請參閱應用程式元件中的資源分組。
   - 來源名稱 – 輸入來源的名稱。選擇來源名稱，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 堆疊匯入的來源名稱，則會將您重新導向至 上的堆疊詳細資訊頁面 AWS CloudFormation。
   - 來源類型 – 輸入來源的類型。
   - AppComponent 類型 – 輸入來源的類型。輸入來源包括 AWS CloudFormation 堆疊、myApplications 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，請完成 中的步驟 編輯應用程式程序的 AWS Resilience Hub 輸入來源。

- 實體 ID – 該資源的實際指派識別符，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 – 在發現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。
- 帳戶 – 擁有實體資源 AWS 的帳戶。

4. 選擇儲存並更新。

刪除 AWS Resilience Hub 應用程式

達到 50 個應用程式的上限後，您必須先刪除一或多個應用程式，才能新增更多應用程式。

如欲刪除應用程式

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刪除，然後選擇刪除。

應用程式組態參數

AWS Resilience Hub 提供輸入機制，以收集與應用程式相關聯資源的其他資訊。透過此資訊， AWS Resilience Hub 將更深入了解您的資源，並提供更好的彈性建議。

應用程式組態參數區段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 – 指出您應用程式已設定的區域。例如，容錯移轉組態。
- 目的 – 指出 AWS Resilience Hub 請求資訊的原因。
- 參數 – 指出應用程式區域特有的詳細資訊，這些區域 AWS Resilience Hub 將用於為您的應用程式提供建議。目前，此參數只會使用一個容錯移轉區域的金鑰值，以及一個相關聯的帳戶。

更新應用程式組態參數

本節可讓您更新 的組態參數， AWS Elastic Disaster Recovery 並發佈應用程式，以包含更新後的彈性評估參數。

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**
>
> 如果您想要停用此功能，請從下拉式清單中選取「–」。

7. 選擇更新並發佈。

管理彈性政策

本節說明如何為您的應用程式建立彈性政策。正確設定彈性政策可讓您了解應用程式的彈性狀態。彈性政策包含您用來評估應用程式是否預估會從中斷類型復原的資訊和目標，例如軟體、硬體、可用區域或 AWS 區域。這些政策不會變更或影響實際的應用程式。多個應用程式可以有相同的彈性政策。

建立彈性政策時，您可以定義目標目標：復原時間目標 (RTO) 和復原點目標 (RPO)。這些目標決定應用程式是否符合彈性政策。將政策連接至您的應用程式並執行彈性評估。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，即時交易應用程式與每月報告應用程式會有不同的彈性政策。

> **Note**
>
> AWS Resilience Hub 可讓您在彈性政策的 RTO 和 RPO 欄位中輸入值零。但是，在評估您的應用程式時，最低的評估結果接近零。因此，如果您在 RTO 和 RPO 欄位中輸入值零，估計工作負載 RTO 和估計工作負載 RPO 結果會接近零，而您應用程式的合規狀態會設為違反政策。

評估會根據連接的彈性政策評估您的應用程式組態。在程序結束時， AWS Resilience Hub 會提供評估，評估您的應用程式如何針對復原政策中的復原目標進行測量。

您可以在應用程式和彈性政策中建立彈性政策。您可以存取政策的相關詳細資訊，也可以修改和刪除它們。

AWS Resilience Hub 使用您的 RTO 和 RPO 目標來測量這些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。
- 雲端基礎設施 – 硬體遺失，例如 EC2 執行個體。
- 雲端基礎設施可用區域 (AZ) – 一或多個可用區域無法使用。
- 雲端基礎設施區域 – 一或多個區域無法使用。

AWS Resilience Hub 可讓您建立自訂彈性政策，或使用我們建議的開放標準彈性政策。當您建立自訂政策時，請命名並描述您的政策，然後選擇定義政策的適當層級或層。這些層包括：基礎 IT 核心服務、關鍵任務、關鍵、重要和非關鍵任務。

選擇適合您應用程式類別的方案。例如，您可以將即時交易系統分類為關鍵，而您可以將每月報告應用程式分類為非關鍵。當您使用我們的標準政策時，您可以根據中斷類型，為 RTO 和 RPO 目標選擇具有預先設定層和值的彈性政策。如有必要，您可以變更層、RTO 和 RPO 目標。

您可以在彈性政策中建立彈性政策，或在描述新應用程式時建立彈性政策。

建立彈性政策

在 中 AWS Resilience Hub，您可以建立彈性政策。彈性政策包含您用來評估應用程式是否可以從中斷類型復原的資訊和目標，例如軟體、硬體、可用區域或 AWS 區域。這些政策不會變更或影響實際的應用程式。多個應用程式可以有相同的彈性政策。

建立彈性政策時，您可以定義復原時間目標 (RTO) 和復原點目標 (RPO) 目標。當您執行評估時， AWS Resilience Hub 會判斷應用程式是否估計為符合彈性政策中定義的目標。

評估會根據連接的彈性政策評估您的應用程式組態。在程序結束時， AWS Resilience Hub 會提供評估，評估您的應用程式如何針對彈性政策中的目標進行測量。

> **Note**
>
> AWS Resilience Hub 可讓您在彈性政策的 RTO 和 RPO 欄位中輸入值零。但是，在評估您的應用程式時，最低的評估結果接近零。因此，如果您在 RTO 和 RPO 欄位中輸入值零，估計工作負載 RTO 和估計工作負載 RPO 結果將接近零，且應用程式的合規狀態將設定為違反政策。

您可以在應用程式和彈性政策中建立彈性政策。您可以存取政策的相關詳細資訊，也可以修改和刪除它們。

在應用程式中建立彈性政策

1. 在左側導覽功能表中，選擇應用程式。
2. 完成從 the section called “新增應用程式以開始使用”到 的程序the section called “將標籤新增至您的應用程式 ”。
3. 在彈性政策區段中，選擇建立彈性政策。

   隨即顯示建立彈性政策頁面。
4. 在選擇建立方法區段中，選取建立政策。
5. 輸入政策的名稱。
6. (選用) 輸入政策的描述。
7. 從層級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)
   - 非關鍵
8. 對於 RTO 和 RPO 目標，在 Customer Application RTO 和 RPO 下，在方塊中輸入數值，然後選擇值代表的時間單位。

   在基礎設施 RTO 和 RPO for Infrastructure and Availability Zone 下重複這些項目。
9. （選用）如果您有多區域應用程式，您可能想要定義區域的 RTO 和 RPO 目標。

   開啟區域。對於區域 RTO 和 RPO 目標，在客戶應用程式 RTO 和 RPO 下，在方塊中輸入數值，然後選擇值代表的時間單位。

10. （選用）如果您想要新增標籤，您可以在稍後繼續建立政策時執行此操作。如需標籤的詳細資訊，請參閱 AWS 一般參考中的標記資源。
11. 若要建立政策，請選擇建立。

在彈性政策中建立彈性政策

1. 在左側導覽功能表中，選擇政策。
2. 在彈性政策區段中，選擇建立彈性政策。

   隨即顯示建立彈性政策頁面。
3. 輸入政策的名稱。
4. (選用) 輸入政策的描述。
5. 從 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)
   - 非關鍵
6. 對於 RTO 和 RPO 目標，在 Customer Application RTO 和 RPO 下，在方塊中輸入數值，然後選擇值代表的時間單位。

   在基礎設施 RTO 和 RPO for Infrastructure and Availability Zone 下重複這些項目。
7. （選用）如果您有多區域應用程式，您可能想要定義區域的 RTO 和 RPO 目標。

   開啟區域。對於 RTO 和 RPO 目標，在 Customer Application RTO 和 RPO 下，在方塊中輸入數值，然後選擇值代表的時間單位。
8. （選用）如果您想要新增標籤，您可以在稍後繼續建立政策時執行此操作。如需標籤的詳細資訊，請參閱 AWS 一般參考中的標記資源。
9. 若要建立政策，請選擇建立。

根據建議的政策建立彈性政策

1. 在左側導覽功能表中，選擇政策。
2. 在選擇建立方法區段中，選取根據建議政策選取政策。

3. 在彈性政策區段中，選擇建立彈性政策。

   隨即顯示建立彈性政策頁面。
4. 輸入彈性政策的名稱。
5. (選用) 輸入政策的描述。
6. 在建議的彈性政策區段下，檢視並選擇下列其中一個預先決定的彈性政策層：

   - 非關鍵應用程式
   - 重要應用程式
   - 關鍵應用程式
   - 全域關鍵應用程式
   - 任務關鍵應用程式
   - 全域任務關鍵應用程式
   - 基礎核心服務
7. 若要建立彈性政策，請選擇建立政策。

存取彈性政策詳細資訊

當您開啟彈性政策時，您會看到政策的重要詳細資訊。您也可以編輯或刪除彈性。

彈性政策詳細資訊包含兩個主要檢視：摘要和標籤。

摘要

基本資訊

提供有關彈性政策的下列資訊：名稱、描述、層、成本層和建立日期。

預估工作負載 RTO 和預估工作負載 RPO

顯示與此彈性政策相關聯的預估工作負載 RTO 和預估工作負載 RPO 中斷類型。

Tags (標籤)

使用此檢視來管理、新增和刪除此應用程式內部的標籤。

在彈性政策詳細資訊中編輯彈性政策

1. 在左側導覽功能表中，選擇政策。

2. 在彈性政策中，開啟彈性政策。
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)。

在彈性政策中編輯彈性政策

1. 在左側導覽功能表中，選擇政策。
2. 在彈性政策中，選擇彈性政策。
3. 選擇動作，然後選擇編輯。
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)。

在彈性政策詳細資訊中刪除彈性政策

1. 在左側導覽功能表中，選擇政策。
2. 在彈性政策中，開啟彈性政策。
3. 選擇 刪除 。確認您的刪除，然後選擇刪除。

在彈性政策中刪除彈性政策

1. 在左側導覽功能表中，選擇政策。
2. 在彈性政策中，選擇彈性政策。
3. 選擇動作，然後選擇刪除。
4. 確認您的刪除，然後選擇刪除。

在 中執行和管理彈性評估 AWS Resilience Hub

當您的應用程式變更時，您應該執行彈性評估。評估會將每個應用程式元件組態與政策進行比較，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 建議提供的指令碼可管理常見的復原程序，例如從備份復原。測試建議提供建議，以驗證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，例如因網路問題而自動擴展或負載平衡。您可以測試當資源達到其限制時是否觸發應用程式警示。您也可以測試 SOPs 在您指定的條件下的運作狀態。

主題：

在 中執行彈性評估 AWS Resilience Hub

您可以從 中的多個位置執行彈性評估 AWS Resilience Hub。如需應用程式的詳細資訊，請參閱 the section called “管理應用程式”。

從動作功能表執行彈性評估

1. 在左側導覽功能表中，選擇應用程式。
2. 從應用程式資料表中選擇應用程式。
3. 從動作功能表中選擇評估彈性。
4. 在執行彈性評估對話方塊中，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”。

從評估索引標籤執行彈性評估

您可以在應用程式或彈性政策變更時執行新的彈性評估。

1. 在左側導覽功能表中，選擇應用程式。
2. 從應用程式資料表中選擇應用程式。
3. 選擇評估索引標籤。
4. 選擇執行彈性評估。
5. 在執行彈性評估對話方塊中，您可以輸入唯一名稱，或使用為評估產生的名稱。
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估檢視中找到評估報告。

尋找評估報告

1. 在左側導覽功能表中，選擇應用程式。
2. 在應用程式中，開啟應用程式。
3. 在評估索引標籤中，從彈性評估區段中選擇評估報告。

當您開啟報告時，您會看到以下內容：

- 評估報告的整體概觀
- 改善彈性的建議。
- 設定警示、SOPs 和測試的建議
- 如何建立和管理標籤，以搜尋和篩選您的 AWS 資源

評估報告

本節提供評估 report. AWS Resilience Hub lists 每種中斷類型和相關聯應用程式元件的概觀。它也會列出您的實際 RTO 和 RPO 政策，並判斷應用程式元件是否可以實現政策目標。

概觀

顯示應用程式的名稱、彈性政策的名稱，以及報告的建立日期。

偵測到的資源偏離

本節列出在已發佈應用程式最新版本中包含之後新增或移除的所有資源。選擇重新匯入輸入來源，以在輸入來源索引標籤中重新匯入所有輸入來源（其中包含漂移的資源）。選擇發佈和評估，以將更新的資源包含在應用程式中，並接收準確的彈性評估。

您可以使用下列方法識別漂移的輸入來源：

- 邏輯 ID – 指示資源的邏輯 ID。邏輯 ID 是用來識別 AWS CloudFormation 堆疊、Terraform 狀態檔案、myApplications 應用程式或 中資源的名稱 AWS Resource Groups。
- 變更 – 指示輸入資源是否已新增或移除。

- 來源名稱 – 指示資源名稱。選擇來源名稱，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 堆疊匯入的來源名稱，則會將您重新導向至 上的堆疊詳細資訊頁面 AWS CloudFormation。
- 資源類型 – 指出資源類型。
- 帳戶 – 指出擁有實體資源 AWS 的帳戶。
- 區域 – 指出 AWS 資源所在的區域。

RTO

顯示應用程式估計是否符合彈性政策目標的圖形表示。這是根據應用程式可以停機的時間量，而不會對組織造成重大損害。評估提供預估的工作負載 RTO。

RPO

顯示應用程式估計是否符合彈性政策目標的圖形表示。這是根據在對業務造成重大損害之前，資料可能遺失的時間量。評估提供預估的工作負載 RPO。

詳細資訊

使用所有結果和應用程式合規偏離索引標籤，提供每種中斷類型的詳細說明。所有結果索引標籤會顯示所有中斷，包括合規偏離，而應用程式合規偏離索引標籤只會顯示合規偏離。中斷類型包括應用程式、雲端基礎設施 （基礎設施和可用區域) 和區域，並提供其相關資訊：

- 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。

- 預估 RTO

  指出您的政策組態是否符合您的政策需求。我們提供兩個值：我們的預估 RTO 和您的目標 RTO。例如，如果您在目標 RTO 下看到 2 小時值，在預估工作負載 RTO 下看到 40 公尺值，則表示我們提供的預估工作負載 RTO 為 40 分鐘，而您應用程式的目前 RTO 為 2 小時。我們根據組態而非政策來計算預估工作負載 RTO。因此，無論您選取哪個政策，多可用區域資料庫都會有相同預估的可用區域故障工作負載 RTO。
- RTO 偏離

  指出您的應用程式已從先前成功評估的估計工作負載 RTO 偏離的持續時間。我們提供兩個值：預估 RTO 和 RTO 偏離。例如，如果您在預估 RTO 下看到 2 小時值，在 RTO 偏離下看到 40 公尺，則表示您的應用程式偏離先前成功評估的預估工作負載 RTO 達 40 分鐘。

- 預估 RPO

  顯示根據您為每個應用程式元件設定的目標 RPO 政策所預估的實際預估工作負載 RPO 政策。 AWS Resilience Hub 例如，您可能已將可用區域故障的彈性政策中的 RPO 目標設定為一小時。估計結果的計算可能接近零。這假設我們遞交每筆交易的 Amazon Aurora 在六個節點中，有四個節點成功，橫跨多個可用區域。point-in-time還原可能需要五分鐘的時間。

  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，當對 AWS 服務有關鍵相依性時，規劃復原非常有用，這可能會在整個區域中無法使用。

  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操作建議。

- RPO 偏離

  指出您的應用程式已從先前成功評估的預估工作負載 RPO 漂移的持續時間。我們提供兩個值：預估 RPO 和 RPO 偏離。例如，如果您在預估 RPO 下看到 2 小時值，在 RPO 偏離下看到 40 公尺值，則表示您的應用程式偏離先前成功評估的預估工作負載 RPO 達 40 分鐘。

檢閱彈性建議

彈性建議會評估 Application Components，並建議如何透過預估工作負載 RTO 和預估工作負載 RPO、成本和最少的變更進行最佳化。

使用 時 AWS Resilience Hub，您可以在為什麼應該選擇此選項中，使用以下其中一個建議選項來最佳化彈性：

> **Note**
>
> - AWS Resilience Hub 提供最多三個 AWS Resilience Hub 建議的選項。
> - 如果您設定區域性 RTO 和 RPO 目標， 會在建議的選項中 AWS Resilience Hub 顯示區域性 RTO/RPO 最佳化。如果未設定區域 RTO 和 RPO 目標，則會顯示可用區域最佳化 (AZ) RTO/RPO。如需在建立彈性政策時設定區域 RTO/RPO 目標的詳細資訊，請參閱 建立彈性政策 。
> - 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，取決於資料量和個別 AppComponents 不過，這些值只是估計值。您應該使用自己的測試 （ 例如 AWS Fault Injection Service) 來測試應用程式的實際復原時間。

針對可用區域 RTO/RPO 最佳化

在可用區域 (AZ) 中斷期間，最低的估計工作負載復原時間 (RTO/RPO)。如果您的組態無法充分變更以符合 RTO 和 RPO 目標，則會通知您預估最低工作負載 AZ 復原時間，讓您的組態接近符合政策的可能性。

針對區域 RTO/RPO 最佳化

區域中斷期間最低的估計工作負載復原時間 (RTO/RPO)。如果您的組態無法充分變更以符合 RTO 和 RPO 目標，則會通知您最低的估計工作負載區域復原時間，讓您的組態接近符合政策的可能性。

成本最佳化

您可以產生的最低成本，但仍符合您的彈性政策。如果您的組態無法充分變更以符合最佳化目標，則會通知您可產生的最低成本，讓您的組態接近符合政策的可能性。

針對最少的變更進行最佳化

實現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，則會通知您建議的變更，讓您的組態接近符合政策的可能性。

最佳化類別明細中包含下列項目：

- Description

  描述 建議的組態 AWS Resilience Hub。
- 變更

  文字變更的清單，說明切換到建議組態的必要任務。
- 基本成本

  與建議變更相關聯的預估成本。

  > **Note**
  >
  > 基本成本會根據用量而有所不同，且不包含企業折扣計劃 (EDP) 的任何折扣或優惠。
- 預估工作負載 RTO 和 RPO

  變更後的預估工作負載 RTO 和預估工作負載 RPO。

AWS Resilience Hub 會評估應用程式元件 (AppComponent) 是否可符合彈性政策。如果 AppComponent 不符合彈性政策，且 AWS Resilience Hub 無法提出任何建議以促進合規，可能是因為在 AppComponent 限制範圍內，無法滿足所選 AppComponent 的復原時間。AppComponent 限制條件的範例包括資源類型、儲存體大小或資源組態。

為了促進 AppComponent 符合彈性政策，請變更 AppComponent 的資源類型，或更新彈性政策以符合資源可以提供的內容。

檢閱操作建議

操作建議包含透過 AWS CloudFormation 範本設定警示、SOPs 和 AWS FIS 實驗的建議。

AWS Resilience Hub 提供 AWS CloudFormation 範本檔案，供您下載和管理應用程式的基礎設施做為程式碼。因此，我們在 中提供建議 AWS CloudFormation ，以便您可以將它們新增至您的應用程式程式碼。如果 AWS CloudFormation 範本檔案的大小超過一個 MB 且包含超過 500 個資源， AWS Resilience Hub 會產生多個 AWS CloudFormation 範本檔案，其中每個檔案的大小不超過一個 MB，且包含最多 500 個資源。如果 AWS CloudFormation 範本檔案分割成多個檔案， AWS CloudFormation 範本檔案名稱會附加 `partXofY`，其中 `X` 表示序列中的檔案編號，並`Y`表示範本檔案分割的檔案總數 AWS CloudFormation 。例如，如果範本檔案`big-app-template5-Alarm-104849185070-us-west-2.yaml`分為四個檔案，檔案名稱如下：

- `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`

不過，如果 AWS CloudFormation 範本較大，系統會要求您提供 Amazon Simple Storage Service URI，而不是使用 CLI/API 搭配本機檔案做為輸入。

在 中 AWS Resilience Hub，您可以執行下列動作：

- 您可以佈建選取的警示、SOPs 和 AWS FIS 實驗。若要佈建警示、SOPs 和 AWS FIS 實驗，請選取適當的建議並輸入唯一的名稱。 會根據您選擇的建議 AWS Resilience Hub 建立範本。在範本中，您可以透過 Amazon Simple Storage Service (Amazon S3) URL 存取您建立的範本。
- 您可以隨時包含或排除應用程式建議的所選警示、SOPs 和 AWS FIS 實驗。如需詳細資訊，請參閱 the section called “包含或排除操作建議”。
- 您也可以搜尋、建立、新增、移除和管理應用程式的標籤，並查看與其相關聯的所有標籤。

包含或排除操作建議

AWS Resilience Hub 提供選項，以包含或排除建議在任何時間點改善應用程式彈性分數的警示、SOPs 和 AWS FIS 實驗（測試）。只有在您執行新的評估後，包含和排除操作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，並了解其對應用程式的影響。

如需限制許可以包含或排除每個應用程式的建議的詳細資訊，請參閱the section called “限制納入或排除 AWS Resilience Hub 建議的許可”。

從應用程式納入或排除操作建議

1. 在左側導覽功能表中，選擇應用程式。
2. 在應用程式中，開啟應用程式。
3. 選擇評估，然後從彈性評估資料表中選取評估。如果您沒有評估，請完成 中的程序，the section called “在 中執行彈性評估 AWS Resilience Hub”然後返回此步驟。
4. 選取操作建議索引標籤。
5. 若要從您的應用程式包含或排除操作建議，請完成下列程序：

從您的應用程式中包含或排除建議的警示

1. 若要排除警示，請完成下列步驟：
   a. 在警示索引標籤下，從警示資料表中選取您要排除的所有警示 (未實作狀態）。您可以從狀態欄識別警示的目前實作狀態。
   b. 從動作中，選擇排除已選取。
   c. 從排除建議對話方塊中，選取下列其中一個原因（選用），然後選擇排除選取的項目，以從應用程式排除選取的警示。
      - 已實作 – 如果您已在 Amazon CloudWatch 或任何其他第三方服務提供者等 AWS 服務中實作這些警示，請選擇此選項。
      - 不相關 – 如果警示不符合您的業務需求，請選擇此選項。
      - 實作過於複雜 – 如果您認為這些警示過於複雜而無法實作，請選擇此選項。
      - 其他 – 選擇此選項，以指定排除建議的任何其他原因。
2. 若要包含警示，請完成下列步驟：
   a. 在警示索引標籤下，從警示資料表中選取您要包含的所有警示（具有排除狀態）。您可以從狀態欄識別警示的目前實作狀態。

b. 從動作中，選擇包含已選取項目。

c. 從包含建議對話方塊中，選擇包含選取的 ，以將所有選取的警示包含在應用程式中。

在您的應用程式中包含或排除建議的標準操作程序 SOPs)

1. 若要排除建議的 SOPs，請完成下列步驟：

   a. 在標準操作程序索引標籤下，從 SOPs資料表中選取您要排除的所有 SOPs （具有已實作或未實作狀態）。您可以從狀態欄識別 SOP 的目前實作狀態。

   b. 從動作中，選擇排除選取的 ，從您的應用程式中排除選取的 SOPs。

   c. 從排除建議對話方塊中，選取下列其中一個原因 （選用），然後選擇排除選取的項目，以從應用程式排除選取的 SOPs。

      - 已實作 – 如果您已在 AWS 服務或任何其他第三方服務提供者中實作這些 SOPs，請選擇此選項。
      - 不相關 – 如果 SOPs 不符合您的業務需求，請選擇此選項。
      - 實作過於複雜 – 如果您認為這些 SOPs 太複雜而無法實作，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 SOPs，請完成下列步驟：

   a. 在標準操作程序索引標籤下，從 SOPs資料表中選取您要包含的所有警示 （具有排除狀態）。您可以從狀態欄識別警示的目前實作狀態。

   b. 從動作中，選擇包含已選取項目。

   c. 從包含建議對話方塊中，選擇包含選取的項目，以包含應用程式中所有選取的 SOPs。

在您的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，請完成下列步驟：

   a. 在錯誤注入實驗範本索引標籤下，從錯誤注入實驗範本資料表中選取您要排除的所有測試（具有已實作或未實作狀態）。您可以從狀態欄識別測試的目前實作狀態。

   b. 在動作中，選擇排除已選取。

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

- 已實作 – 如果您已在 AWS 服務或任何其他第三方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。
- 實作過於複雜 – 如果您認為這些測試過於複雜而無法實作，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，請完成下列步驟：

   a. 在錯誤注入實驗範本索引標籤下，從錯誤注入實驗範本資料表中選取您要包含的所有測試（具有排除狀態）。您可以從狀態欄識別測試的目前實作狀態。
   b. 從動作中，選擇包含已選取項目。
   c. 從包含建議對話方塊中，選擇包含選取的項目，以包含應用程式中所有選取的測試。

刪除彈性評估

您可以在應用程式的評估檢視中刪除彈性評估。

刪除彈性評估

1. 在左側導覽功能表中，選擇應用程式。
2. 在應用程式中，開啟應用程式。
3. 在評估中，選擇彈性評估表中的評估報告。
4. 如要確認刪除，請選擇 Delete (刪除)。

   報告不會再出現在彈性評估表中。

從彈性小工具執行和管理彈性評估

AWS Resilience Hub 可讓您針對在彈性小工具 myApplications 中建立和管理的應用程式執行評估。每當您修改應用程式時，建議您從彈性小工具或 AWS Resilience Hub 主控台執行彈性評估。在此評估期間，會根據已建立的政策和最佳實務來評估每個應用程式元件的組態。根據此評估，評估會產生設定警示、建立標準操作程序 SOPs) 和實作測試策略的建議。實作這些組態建議可以提高復原程序的速度和效率，確保更快的事件回應，並將潛在的停機時間降至最低。

警示建議可協助您設定偵測中斷的警示。SOP 建議提供的指令碼可管理常見的復原程序，例如從備份復原。測試建議提供建議，以驗證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，例如因網路問題而自動擴展或負載平衡。您可以測試在資源達到其限制時是否觸發應用程式警示。您也可以測試 SOPs 在您指定的條件下的運作狀態。

主題：

從彈性小工具執行彈性評估

對於在 myApplications widget 中建立的應用程式，您現在可以從彈性小工具和 AWS Resilience Hub 主控台執行彈性評估。如需從 AWS Resilience Hub 主控台執行彈性評估的詳細資訊，請參閱 在 中執行彈性評估 AWS Resilience Hub。

第一次從彈性小工具執行現有 myApplications 應用程式的彈性評估

1. 登入 AWS 管理主控台。
2. 展開左側邊欄，然後選擇 myApplications。
3. 選取您要為其執行評估的應用程式。

   作為先決條件，請確定您已在 AWS 主控台中新增彈性小工具。若要新增此小工具，請完成下列步驟。

   a. 在主控台首頁儀表板的右上角或右下角，選擇 + 新增小工具。

   b. 選擇由小工具標題列左上角六個垂直點表示的拖曳指標，然後將其拖曳至主控台首頁儀表板。
4. 選擇評估應用程式。
5. 若要選取用於存取目前帳戶中資源的現有 IAM 角色，請選取使用 IAM 角色，然後從選取 IAM 角色下拉式清單中選取 IAM 角色。

   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，請選擇使用目前的 IAM 使用者許可，然後選取我了解，我必須在 中使用目前的 IAM 使用者探索應用程式資源區段中手動設定許可，以啟用 中所需的功能 AWS Resilience Hub。
6. 選擇評估。

   或者，開啟自動評估每日，讓 AWS Resilience Hub 每天評估您的應用程式，而不需要任何額外費用。

   AWS Resilience Hub 會執行下列動作：

- 在 中建立應用程式 AWS Resilience Hub ，並自動探索和映射相關聯的資源。
- 建立和指派具有復原時間目標 (RTO) 和復原點目標 (RPO) 預先定義值的新彈性政策。也就是說，RTO 為 4 小時，RPO 為 1 小時。產生評估之後，您可以修改彈性政策，或從 AWS Resilience Hub 主控台指派不同的政策。如需更新彈性政策並連接不同政策的詳細資訊，請參閱管理彈性政策。
- 評估應用程式對 RTO 和 RPO 的彈性，並持續監控資源和組態變更，並發佈結果。

> **Note**
>
> 在開始評估之前，建議您評估使用 執行評估時涉及的潛在成本 AWS Resilience Hub。如需詳細的定價資訊，請參閱 AWS Resilience Hub 定價。

從彈性小工具重新執行現有 myApplications 應用程式的彈性評估

1. 登入 AWS 管理主控台。
2. 展開左側邊欄，然後選擇 myApplications。
3. 選取您要重新評估的應用程式。

   作為先決條件，請確定您已在 AWS 主控台中新增彈性小工具。若要新增此小工具，請完成下列步驟。

   a. 在主控台首頁儀表板的右上角或右下角，選擇 + 新增小工具。

   b. 選擇由小工具標題列左上角六個垂直點表示的拖曳指標，然後將其拖曳至主控台首頁儀表板。
4. 從彈性小工具中選擇重新評估。

   或者，開啟自動評估每日，讓 AWS Resilience Hub 每天評估您的應用程式，無需任何額外費用。

在彈性小工具中檢閱評估摘要

彈性小工具會顯示評估結果的快照，為您提供有關 myApplications 應用程式彈性、潛在漏洞、關鍵效能指標 (KPIs) 和改善建議動作最重要且可行的洞見。您可以使用下列各項，從最近的評估中進一步了解應用程式的彈性狀態：

- 彈性分數歷史記錄 – 此圖表會顯示應用程式彈性分數長達一年的趨勢。

- 彈性分數 – 指出在最新評估中評估的應用程式彈性分數。此分數反映您的應用程式遵循我們建議的程度，以符合應用程式的彈性政策，以及實作警示、標準操作程序 (SOPs) 和 AWS Fault Injection Service (AWS FIS) 實驗。在 AWS Resilience Hub 主控台的摘要索引標籤下，選擇檢視彈性分數區段中其他資訊的數字。如需詳細資訊，請參閱評估報告。
- 政策違規 – 選擇以下數字，以檢視在 AWS Resilience Hub 主控台的評估報告窗格中違反附加至應用程式之所有應用程式元件 (AppComponents)。如需詳細資訊，請參閱評估報告。
- 政策偏離 – 指出在先前評估中符合政策，但在目前評估中未符合政策的 AppComponents。選擇以下數字，在 AWS Resilience Hub 主控台的評估報告窗格中檢視 AppComponents。如需詳細資訊，請參閱評估報告。
- 資源偏離 – 選擇以下數字，以檢視主控台中評估報告窗格中最新評估偏離的所有資源 AWS Resilience Hub 。如需詳細資訊，請參閱評估報告。
- 前往彈性中心 – 選擇此選項，以在 AWS Resilience Hub 主控台中開啟您的應用程式。

管理警示

當您執行彈性評估時， AWS Resilience Hub 建議設定 Amazon CloudWatch 警示以監控您的應用程式彈性。我們建議您根據目前應用程式組態的資源和元件來發出這些警示。如果應用程式中的資源和元件變更，您應該執行彈性評估，以確保您有更新應用程式的正確 Amazon CloudWatch 警示。

此外， AWS Resilience Hub 現在會自動偵測任何已設定的 Amazon CloudWatch 警示並將其整合到其彈性評估中，提供應用程式彈性狀態的更全面檢視。這項新功能結合了 AWS Resilience Hub 建議與您目前的監控設定、簡化警示管理，以及提升評估準確性。如果您已實作 Amazon CloudWatch 警示， AWS Resilience Hub 但未自動偵測到，您可以排除警示，然後選取已實作的原因。如需排除建議的詳細資訊，請參閱 包含或排除操作建議。

AWS Resilience Hub 提供範本檔案 (`README.md`)，可讓您建立 AWS （例如 Amazon CloudWatch) AWS Resilience Hub 內或外建議的警示 AWS。警示中提供的預設值，是以用來建立這些警示的最佳實務為基礎。

主題

- 從操作建議建立警示
- 檢視警示

從操作建議建立警示

AWS Resilience Hub 會建立範本 AWS CloudFormation ，其中包含在 Amazon CloudWatch 中建立所選警示的詳細資訊。產生範本後，您可以透過 Amazon S3 URL 存取範本、下載相同 URL，並將其放在程式碼管道中，或透過 AWS CloudFormation 主控台建立堆疊。

若要根據 AWS Resilience Hub 建議建立警示，您必須為 AWS CloudFormation 建議的警示建立範本，並將其包含在程式碼基礎中。

在操作建議中建立警示

1. 在左側導覽功能表中，選擇應用程式。
2. 在應用程式中，選擇您的應用程式。
3. 選擇評估索引標籤。

   在彈性評估表中，您可以使用以下資訊來識別您的評估：

   - 名稱 – 您在建立時提供的評估名稱。
   - 狀態 – 指示評估的執行狀態。
   - 合規狀態 – 指出評估是否符合彈性政策。
   - 彈性偏離狀態 – 指出您的應用程式是否偏離先前的成功評估。
   - 應用程式版本 – 應用程式的版本。
   - 叫用者 – 指示叫用評估的角色。
   - 開始時間 – 表示評估的開始時間。
   - 結束時間 – 表示評估的結束時間。
   - ARN – 評估的 Amazon Resource Name (ARN)。
4. 從彈性評估資料表中選取評估。如果您沒有評估，請完成 中的程序，the section called “在 中執行彈性評估 AWS Resilience Hub”然後返回此步驟。
5. 選擇操作建議。
6. 如果預設未選取，請選擇警示索引標籤。

   在警示資料表中，您可以使用下列項目來識別建議的警示：

   - 名稱 – 您已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 警示的目前實作狀態。

此欄會顯示下列其中一個值：

- 已實作 – 表示 建議的警示 AWS Resilience Hub 已實作在您的應用程式中。選擇以下數字會篩選警示資料表，以顯示應用程式中所實作的所有建議警示。
- 未實作 – 表示 建議的警示 AWS Resilience Hub 已包含在應用程式中，但未實作。選擇以下數字將篩選警示資料表，以顯示未在應用程式中實作的所有建議警示。
- 已排除 – 表示您的應用程式 AWS Resilience Hub 已排除 建議的警示。選擇以下數字會篩選警示資料表，以顯示應用程式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 – 表示警示已部署至 Amazon CloudWatch，但在 Amazon CloudWatch 中狀態設定為 INSUFFICIENT_DATA。選擇以下數字將篩選警示資料表，以顯示所有已實作和非作用中的警示。

- 組態 – 指出是否有任何需要解決的待處理組態相依性。
- 類型 – 指出警示的類型。
- AppComponent – 指出與此警示相關聯的應用程式元件 (AppComponents)。
- 參考 ID – 指出堆疊 AWS CloudFormation 事件的邏輯識別符 AWS CloudFormation。
- 建議 ID – 指示 AWS CloudFormation 堆疊資源的邏輯識別符 AWS CloudFormation。

7. 在警示索引標籤中，若要根據特定狀態篩選警示資料表中的警示建議，請選取相同狀態下方的數字。
8. 選取您要為應用程式設定的警示建議，然後選擇建立 CloudFormation 範本。
9. 在建立 CloudFormation 範本對話方塊中，您可以使用自動產生的名稱，也可以在 CloudFormation AWS CloudFormation 範本名稱方塊中輸入範本的名稱。 CloudFormation
10. 選擇 Create (建立)。這可能需要幾分鐘的時間來建立 AWS CloudFormation 範本。

    完成下列程序，將建議納入您的程式碼庫。

包含您的程式碼庫 AWS Resilience Hub 建議

1. 選擇範本索引標籤以檢視您剛建立的範本。您可以使用下列各項來識別您的範本：

   - 名稱 – 您在建立時提供的評估名稱。
   - 狀態 – 指示評估的執行狀態。
   - 類型 – 指示操作建議的類型。
   - 格式 – 指示範本建立的格式 (JSON/文字）。

- 開始時間 – 表示評估的開始時間。
- 結束時間 – 表示評估的結束時間。
- ARN – 範本的 ARN

2. 在範本詳細資訊下，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 主控台的物件資料表中，選擇警示資料夾連結。
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，您必須提供從上一個步驟複製的 Amazon S3 路徑。

檢視警示

您可以檢視已設定的所有作用中警示，以監控應用程式的彈性。 AWS Resilience Hub 會使用 AWS CloudFormation 範本來存放警示詳細資訊，這些詳細資訊會依序用於在 Amazon CloudWatch 中建立警示。您可以使用 Amazon S3 URL 存取 AWS CloudFormation 範本，並下載範本並將其放入程式碼管道，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。在實作的警示表中，您可以使用下列資訊來識別實作的警示：

- 應用程式受影響 – 已實作此警示的應用程式名稱。
- 作用中警示 – 指出從應用程式觸發的作用中警示數目。
- FIS 進行中 – 指出目前為您的應用程式執行的 AWS FIS 實驗。

檢視在您的應用程式中實作的警示

1. 在左側導覽功能表中，選擇應用程式。
2. 從應用程式資料表中選取應用程式。
3. 在應用程式摘要頁面中，實作的警示表會顯示應用程式內實作的所有建議警示。

   若要在實作的警示資料表中尋找特定警示，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、選擇操作，然後輸入值。

   - 警示名稱 – 您已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 警示的目前實作狀態。

  此欄會顯示下列其中一個值：

  - 已實作 – 表示 建議的警示 AWS Resilience Hub 已實作在您的應用程式中。選擇以下數字，在操作建議索引標籤中檢視所有建議和實作的警示。
  - 未實作 – 表示 建議的警示 AWS Resilience Hub 已包含在應用程式中，但未實作。選擇以下數字，在操作建議索引標籤中檢視所有建議和非實作的警示。
  - 已排除 – 表示您的應用程式 AWS Resilience Hub 已排除 建議的警示。選擇以下數字，在操作建議索引標籤中檢視所有建議和排除的警示。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 – 表示警示已部署至 Amazon CloudWatch，但在 Amazon CloudWatch 中狀態設定為 INSUFFICIENT_DATA。選擇以下數字，在操作建議索引標籤中檢視所有已實作和非作用中的警示。
- 來源範本 – 提供包含警示詳細資訊之 AWS CloudFormation 堆疊的 Amazon Resource Name (ARN)。
- 資源 – 顯示此警示所連接並實作的資源。
- 指標 – 顯示為警示指派的 Amazon CloudWatch 指標。如需 Amazon CloudWatch 指標的詳細資訊，請參閱 Amazon CloudWatch 指標。
- 上次變更 – 顯示上次修改警示的日期和時間。

從評估檢視建議的警示

1. 在左側導覽功能表中，選擇應用程式。
2. 從應用程式資料表中選取應用程式。

   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. 選擇評估索引標籤。

   在彈性評估表中，您可以使用以下資訊來識別您的評估：

   - 名稱 – 您在建立時提供的評估名稱。
   - 狀態 – 指示評估的執行狀態。
   - 合規狀態 – 指出評估是否符合彈性政策。
   - 彈性偏離狀態 – 指出您的應用程式是否偏離先前的成功評估。

- 應用程式版本 – 應用程式的版本。
- 叫用者 – 指示叫用評估的角色。
- 開始時間 – 表示評估的開始時間。
- 結束時間 – 表示評估的結束時間。
- ARN – 評估的 Amazon Resource Name (ARN)。

4. 從彈性評估資料表中選取評估。
5. 選擇操作建議索引標籤。
6. 如果預設未選取，請選擇警示索引標籤。

   在警示資料表中，您可以使用下列項目來識別建議的警示：

   - 名稱 – 您已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 警示的目前實作狀態。

     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示資料表，以顯示應用程式中所實作的所有建議警示。
     - 未實作 – 表示警示未實作或包含在應用程式中。選擇以下數字會篩選警示資料表，以顯示未在應用程式中實作的所有建議警示。
     - 已排除 – 表示警示已從應用程式排除。選擇以下數字會篩選警示資料表，以顯示應用程式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 “包含或排除操作建議”。
     - 非作用中 – 表示警示已部署至 Amazon CloudWatch，但在 Amazon CloudWatch 中狀態設定為 INSUFFICIENT_DATA。選擇以下數字會篩選警示資料表，以顯示所有已實作和非作用中的警示。
   - 組態 – 指出是否有任何需要解決的待處理組態相依性。
   - 類型 – 表示警示的類型。
   - AppComponent – 指出與此警示相關聯的應用程式元件 (AppComponents)。
   - 參考 ID – 指示堆疊 AWS CloudFormation 事件的邏輯識別符 AWS CloudFormation。
   - 建議 ID – 指示 AWS CloudFormation 堆疊資源的邏輯識別符 AWS CloudFormation。

管理標準操作程序

標準操作程序 (SOP) 是一組規範性步驟，旨在在發生停機或警示時有效地復原您的應用程式。事先準備、測試和測量您的 SOPs，以確保在操作中斷時及時復原。

根據您的應用程式元件， AWS Resilience Hub 建議您應準備SOPs。 與 Systems Manager AWS Resilience Hub 合作，透過提供許多 SSM 文件來自動化 SOPs 的步驟，您可以將這些文件做為這些 SOPs 的基礎。

例如， AWS Resilience Hub 可能會建議根據現有 SSM Automation 文件新增磁碟空間的 SOP。若要執行此 SSM 文件，您需要具有正確許可的特定 IAM 角色。 會在應用程式中 AWS Resilience Hub 建立中繼資料，指出在磁碟不足的情況下要執行哪些 SSM 自動化文件，以及執行該 SSM 文件需要哪些 IAM 角色。此中繼資料接著會儲存在 SSM 參數中。

除了設定 SSM 自動化之外，最佳實務是使用 AWS FIS 實驗進行測試。因此， AWS Resilience Hub 也提供可呼叫 SSM 自動化文件的 AWS FIS 實驗 - 如此一來，您可以主動測試應用程式，以確保您建立的 SOP 執行預期任務。

AWS Resilience Hub 以您可以新增至應用程式程式碼庫的 AWS CloudFormation 範本形式提供其建議。此範本提供：

- 具有執行 SOP 所需許可的 IAM 角色。
- 您可以使用 測試 SOP 的 AWS FIS 實驗。
- 包含應用程式中繼資料的 SSM 參數，指出要執行哪些 SSM 文件和哪個 IAM 角色做為 SOP，以及在哪個資源上執行。例如：`$(DocumentName) for SOP $(HandleCrisisA) on $(ResourceA)`。

建立 SOP 可能需要一些試驗和錯誤。針對您的應用程式執行彈性評估，並從 AWS Resilience Hub 建議產生 AWS CloudFormation 範本是很好的開始。使用 AWS CloudFormation 範本產生 AWS CloudFormation 堆疊，然後使用 SSM 參數和 SOP 中的預設值。執行 SOP 並查看您需要進行哪些改進。

由於所有應用程式都有不同的需求， AWS Resilience Hub 因此提供的預設 SSM 文件清單將不足以滿足您的所有需求。不過，您可以複製預設的 SSM 文件，並將其做為建立應用程式自訂文件的基礎。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 參數建立關聯，以便在 SOP 執行時呼叫正確的 SSM 文件。

當您建立必要的 SSM 文件並在必要時更新參數和文件關聯，完成您的 SOP 之後，請直接將 SSM 文件新增至您的程式碼基礎，並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up-to-date SOP。

主題

根據 AWS Resilience Hub 建議建置 SOP

若要根據 AWS Resilience Hub 建議建置 SOP，您需要一個附加彈性政策 AWS Resilience Hub 的應用程式，而且必須對該應用程式執行彈性評估。彈性評估會為您的 SOP 產生建議。

若要根據 AWS Resilience Hub 建議建置 SOP，您必須為建議的 SOPs 建立 AWS CloudFormation 範本，並將其包含在程式碼基礎中。

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. 選擇評估索引標籤。
5. 從彈性評估資料表中選取評估。如果您沒有評估，請完成 中的程序，the section called “在 中執行彈性評估 AWS Resilience Hub”然後返回此步驟。
6. 在操作建議下，選擇標準操作程序。
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。

   完成下列程序，將 SOP 建議納入您的程式碼庫。

在您的程式碼庫中包含 AWS Resilience Hub 建議

1. 在操作建議中，選擇範本。

2. 在範本清單中，選擇您剛建立的 SOP 範本名稱。

   您可以使用以下資訊來識別在應用程式中實作SOPs：

   - SOP 名稱 – 您已為應用程式定義的 SOP 名稱。
   - 描述 – 描述 SOP 的目標。
   - SSM 文件 – 包含 SOP 定義的 SSM 文件的 Amazon S3 URL。
   - 測試執行 – 文件的 Amazon S3 URL，其中包含最新測試的結果。
   - 來源範本 – 提供包含 SOP 詳細資訊之 AWS CloudFormation 堆疊的 Amazon Resource Name (ARN)。
3. 在範本詳細資訊下，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 主控台的物件資料表中，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，您必須提供從上一個步驟複製的 Amazon S3 路徑。

建立自訂 SSM 文件

若要完全自動化應用程式的復原，您可能需要在 Systems Manager 主控台中為您的 SOP 建立自訂 SSM 文件。您可以修改現有的 SSM 文件做為基礎，也可以建立新的 SSM 文件。

如需使用 Systems Manager 建立 SSM 文件的詳細資訊，請參閱逐步解說：使用文件建置器建立自訂 Runbook。

如需 SSM 文件語法的相關資訊，請參閱 SSM 文件語法。

如需自動化 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 文件而非預設值

若要將 SOP AWS Resilience Hub 建議的 SSM 文件取代為您建立的自訂文件，請直接在程式碼基礎中運作。除了新增新的自訂 SSM 自動化文件之外，您還將：

1. 新增執行自動化所需的 IAM 許可。
2. 新增 AWS FIS 實驗以測試您的 SSM 文件。

3. 新增指向您要用作 SOP 的自動化文件的 SSM 參數。

一般而言，在 中使用建議的預設值最有效率， AWS Resilience Hub 並視需要加以自訂。例如，視需要新增或移除 IAM 角色的許可、變更 AWS FIS 實驗設定以指向新的 SSM 文件，或變更 SSM 參數以指向新的 SSM 文件。

測試 SOPs

如前所述，最佳實務是將 AWS FIS 實驗新增至您的 CI/CD 管道，以定期測試您的 SOPs；這可確保在發生中斷時隨時可以開始。

測試 AWS Resilience Hub提供的 和自訂 SOPs。

檢視標準操作程序

從應用程式檢視實作SOPs

1. 在左側導覽功能表中，選擇應用程式。
2. 在應用程式中，開啟應用程式。
3. 選擇標準操作程序索引標籤。

   在標準操作程序摘要區段中，實作的標準操作程序資料表會顯示從 SOPs 建議產生的 SOP 清單。

   您可以透過下列方式識別您的 SOPs：

   - SOP 名稱 – 您已為應用程式定義的 SOP 名稱。
   - SSM 文件 – Amazon EC2 Systems Manager 文件的 S3 URL，其中包含 SOP 定義。
   - 描述 – 描述 SOP 的目標。
   - 測試執行 – 包含最新測試結果的文件 S3 URL。
   - 參考 ID – 參考 SOP 建議的識別符。
   - 資源 ID – 實作 SOP 建議的資源識別符。

檢視評估中建議的 SOPs

1. 在左側導覽功能表中，選擇應用程式。
2. 從應用程式資料表中選取應用程式。

   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. 選擇評估索引標籤。

   在彈性評估表中，您可以使用下列資訊來識別您的評估：

   - 名稱 – 您在建立時提供的評估名稱。
   - 狀態 – 指出評估的執行狀態。
   - 合規狀態 – 指出評估是否符合彈性政策。
   - 彈性偏離狀態 – 指出您的應用程式是否偏離先前的成功評估。
   - 應用程式版本 – 應用程式的版本。
   - 調用 – 指示調用評估的角色。
   - 開始時間 – 表示評估的開始時間。
   - 結束時間 – 指示評估的結束時間。
   - ARN – 評估的 Amazon Resource Name (ARN)。
4. 從彈性評估資料表中選取評估。
5. 選擇操作建議索引標籤。
6. 選擇標準操作程序索引標籤。

   在標準操作程序資料表中，您可以使用下列資訊進一步了解建議的 SOPs：

   - 名稱 – 建議的 SOP 名稱。
   - 描述 – 描述 SOP 的目標。
   - 狀態 – 指出 SOP 目前的實作狀態。也就是說，已實作、未實作和已排除。
   - 組態 – 指出是否有任何需要解決的待處理組態相依性。
   - 類型 – 指出 SOP 的類型。
   - AppComponent – 指出與此 SOP 相關聯的應用程式元件 (AppComponents)。如需支援的 AppComponents 的詳細資訊，請參閱在 AppComponent 中分組資源。
   - 參考 ID – 指出堆疊 AWS CloudFormation 事件的邏輯識別符 AWS CloudFormation。
   - 建議 ID – 指示 AWS CloudFormation 堆疊資源的邏輯識別符 AWS CloudFormation。

管理 AWS Fault Injection Service 實驗

本節說明如何在 中管理 AWS Fault Injection Service (AWS FIS) 實驗 AWS Resilience Hub。您可以執行 AWS FIS 實驗來測量 AWS 資源的彈性，以及從應用程式、基礎設施、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 AWS FIS 實驗會模擬資源 AWS 的中斷。中斷的範例包括網路無法使用錯誤、容錯移轉、在 Amazon EC2 或 AWS ASG 上停止的程序、在 Amazon RDS 中開機復原，以及可用區域的問題。當 AWS FIS 實驗結束時，您可以估計應用程式是否可以從彈性政策的 RTO 目標中定義的中斷類型中復原。

中所有實驗 AWS Resilience Hub 都是使用 建置 AWS FIS 的，且會執行 AWS FIS 動作。 AWS FIS 實驗只會使用針對特定 AWS 服務（例如 Amazon EKS 動作） 自訂的 AWS FIS 自動化動作。如需 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，或根據您的需求自訂實驗。如需從 AWS Resilience Hub 主控台和 AWS FIS 主控台管理 AWS FIS 實驗的詳細資訊，請參閱下列主題：

- AWS Resilience Hub 主控台
  - 檢視 AWS FIS 實驗
    - 從應用程式檢視實作 AWS FIS 實驗的清單
    - 從評估檢視建議的 AWS FIS 實驗
  - the section called “執行 AWS FIS 實驗”
  - the section called “AWS Fault Injection Service 實驗失敗/狀態檢查”
- AWS FIS 主控台
  - 管理您的 AWS FIS 實驗
  - 使用 AWS FIS 案例程式庫
  - 管理 AWS FIS 實驗範本

啟動、建立和執行 AWS FIS 實驗

AWS Resilience Hub 透過整合 AWS FIS 實驗來簡化 AWS FIS 實驗。它提供量身打造的建議，並允許使用映射至您 Application Components (AppComponents) 的預先填入範本啟動 AWS FIS 實驗，從而實現高效的彈性測試。

從操作建議啟動 AWS FIS 實驗

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，選擇您要為其建立測試的應用程式。
4. 選擇評估索引標籤。

5. 從彈性評估資料表中選取評估。如果您沒有評估，請完成 中的程序，the section called “在 中執行彈性評估 AWS Resilience Hub”然後返回此步驟。
6. 選擇操作建議索引標籤。
7. 在故障注入實驗之前，選擇向右箭頭。

   本節列出應用程式 AWS Resilience Hub 建議的所有 AWS FIS 實驗，以測試壓力並提高其彈性。根據您的實作， AWS FIS 實驗會分類為下列狀態：

   - 已實作 – 表示 建議的實驗 AWS Resilience Hub 已實作在您的應用程式中。選擇以下數字，以檢視實驗資料表中的所有實作實驗。
   - 已部分實作 – 表示 建議的實驗 AWS Resilience Hub 已部分實作於您的應用程式中。選擇以下數字，以檢視實驗資料表中所有部分實作的實驗。
   - 未實作 – 表示您的應用程式中 AWS Resilience Hub 未實作 建議的實驗。選擇以下數字，以檢視實驗資料表中的所有未實作實驗。
   - 已排除 – 表示您的應用程式 AWS Resilience Hub 已排除 建議的實驗。選擇以下數字，以檢視實驗資料表中所有排除的實驗。如需包含和排除建議實驗的詳細資訊，請參閱包含或排除操作建議。

   實驗資料表列出所有實作 AWS FIS 的實驗，這些實驗會影響應用程式的彈性分數。您可以使用下列資訊來識別 AWS FIS 實驗：

   - 動作名稱 – 指出為您的應用程式建議 AWS FIS 的動作。選擇動作名稱，以在AWS FIS 實驗詳細資訊頁面上檢視所有建議的 AppComponents 當狀態設定為不可追蹤時，表示 AWS FIS 實驗是案例。選擇案例名稱，在 主控台的 AWS FIS 案例庫頁面上檢視其詳細資訊。
   - 狀態 – 指出 AWS FIS 實驗目前的實作狀態。也就是說，已實作、部分實作、未實作和已排除。

     > **Note**
     >
     > AWS FIS 案例是具有多個預先定義動作的主控台限定功能。因此， AWS Resilience Hub 無法追蹤它，它會將狀態設定為無法追蹤。

   - 描述 – 描述 AWS FIS 動作的目標。
8. 選取您要為其啟動實驗 AWS FIS 的動作。

   在 AWS FIS 實驗建議區段中，您可以使用下列資訊，進一步了解在 AppComponents 上實作所需的實驗：

- 名稱 – 資源分組所在的 AppComponent 名稱。
- 狀態 – 指出 AWS FIS 動作目前的實作狀態。也就是說，已實作、部分實作、未實作和已排除。

> **Note**
>
> AWS FIS 案例是具有多個預先定義動作的主控台限定功能。因此， AWS Resilience Hub 無法追蹤它，它會將狀態設定為無法追蹤。

- 目標選擇 – 指出當您選擇啟動實驗時，資源將如何包含在實驗中。如果 AWS Resilience Hub 未自動判斷目標資源，請將滑鼠游標移至個別的目標選取欄位，以取得新增這些資源的指引。
- 資源 – 指示 AppComponent 下分組的資源數量。在資源對話方塊中選擇檢視這些資源的號碼。您可以使用下列項目來識別資源：
  - 邏輯 ID – 指示資源的邏輯 ID。邏輯 ID 是用來識別您 AWS CloudFormation、Terraform 狀態檔案、myApplications 應用程式、 AWS Resource Groups resource 或 Amazon Elastic Kubernetes Service 叢集中資源的名稱。
  - 實體 ID – 指示資源的實際指派識別符，例如 Amazon EC2 執行個體 ID 或 Amazon S3 儲存貯體名稱。
  - 類型 – 指出資源的類型。
  - 區域 – 指出 AWS 資源所在的區域。

9. 選取 AppComponent，然後選擇包含或排除，分別在 AWS FIS 實驗中包含或排除 AppComponent。
10. 選擇啟動實驗。

    AWS Resilience Hub 會將您重新導向至 AWS FIS 主控台中的指定範本詳細資訊頁面，並在新索引標籤中開啟。
11. 若要建立實驗範本，請完成 中的步驟 使用主控台建立實驗範本。

    此外，在您輸入範本詳細資訊，並依照 中的步驟在 AWS FIS 主控台的指定範本詳細資訊頁面中選擇下一步 若要使用主控台建立實驗範本， AWS Resilience Hub 會自動嘗試在動作和目標頁面中映射資源類型的動作和目標。不過，若要改善涵蓋範圍，您可以分別選擇新增動作和新增目標，然後完成其他程序來建立實驗，以手動新增動作和目標。

執行 AWS FIS 實驗

在 AWS FIS 主控台中建立實驗後，請遵循從範本開始實驗中的步驟，在主控台中 AWS FIS 執行實驗。如果您想要 AWS Resilience Hub 偵測在 中執行的最新實驗 AWS FIS，您必須執行新的評估。如需執行評估的詳細資訊，請參閱 在 中執行彈性評估 AWS Resilience Hub。

檢視 AWS FIS 實驗

在 中 AWS Resilience Hub，檢視您設定以測量 AWS 資源彈性的 AWS FIS 實驗，以及從應用程式、基礎設施、可用區域和 AWS 區域 事件復原所需的時間。

若要從儀表板檢視作用中 AWS FIS 實驗的清單，請從左側導覽功能表中選擇儀表板。

在實作實驗表中，您可以使用以下資訊來識別 AWS FIS 實驗：

- 實驗 ID – 實驗的 AWS FIS 識別符。
- 動作 – 指出與 AWS FIS 實驗相關聯的 AWS FIS 動作。此外，如果有多個動作，則會反白顯示與 AWS FIS 實驗相關聯的 AWS FIS 動作數目。您可以將滑鼠游標移至詳細資訊上或瀏覽詳細資訊，藉此識別詳細資訊。
- 實驗範本 ID – 用來建立 AWS FIS 實驗的 AWS FIS 實驗範本識別符。

從應用程式檢視實作 AWS FIS 實驗的清單

1. 在左側導覽功能表中，選擇應用程式。
2. 從應用程式資料表中選取應用程式。

   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. 選擇故障注入實驗。

   在實作的實驗表中，您可以使用以下資訊來識別應用程式中實作的 AWS FIS 實驗：

   - 實驗 ID – 實驗的 AWS FIS 識別符。
   - 動作 – 指出與 AWS FIS 實驗相關聯的 AWS FIS 動作。此外，如果有多個動作，則會反白顯示與 AWS FIS 實驗相關聯的 AWS FIS 動作數目。您可以將滑鼠游標移至詳細資訊上或導覽至詳細資訊，以識別詳細資訊。
   - 實驗範本 ID – 用來建立 AWS FIS 實驗的 AWS FIS 實驗範本識別符。

從評估檢視建議的 AWS FIS 實驗

1. 在左側導覽功能表中，選擇應用程式。
2. 從應用程式資料表中選取應用程式。

   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. 選擇評估索引標籤。

   在評估表中，您可以使用下列資訊來識別您的評估：

   - 名稱 – 您在建立時提供的評估名稱。
   - 狀態 – 指出評估的執行狀態。
   - 合規狀態 – 指出評估是否符合彈性政策。
   - 彈性 – 指出您的應用程式是否偏離附加彈性政策中定義的 RTO 和 RPO 目標，或偏離先前的成功評估。
   - 應用程式版本 – 評估的應用程式版本。
   - 調用 – 指示調用評估的角色。
   - 開始時間 – 表示評估的開始時間。
   - 結束時間 – 表示評估的結束時間。
   - ARN – 評估的 Amazon Resource Name (ARN)。
4. 從評估資料表中選取評估。
5. 選擇操作建議。
6. 選擇故障注入實驗之前的向右箭頭。

   本節列出應用程式 AWS Resilience Hub 建議的所有 AWS FIS 實驗，以測試壓力並提高其彈性。根據您的實作， AWS FIS 實驗會分類為下列狀態：

   - 已實作 – 表示 建議的實驗 AWS Resilience Hub 已實作在您的應用程式中。選擇以下數字，以檢視實驗資料表中的所有實作實驗。
   - 已部分實作 – 表示 建議的實驗 AWS Resilience Hub 已部分實作於您的應用程式中。選擇以下數字，以檢視實驗資料表中所有部分實作的實驗。
   - 未實作 – 表示 建議的實驗 AWS Resilience Hub 未在您的應用程式中實作。選擇以下數字，以檢視實驗資料表中的所有未實作實驗。

- 已排除 – 表示您的應用程式 AWS Resilience Hub 已排除 建議的實驗。選擇以下數字，以檢視實驗資料表中所有排除的實驗。如需包含和排除建議實驗的詳細資訊，請參閱包含或排除操作建議。

實驗資料表列出所有實作 AWS FIS 的實驗，這些實驗會影響應用程式的彈性分數。您可以使用下列資訊來識別 AWS FIS 實驗：

- 動作名稱 – 指出為您的應用程式建議 AWS FIS 的動作。當狀態設定為不可追蹤時，表示 AWS FIS 實驗是案例。選擇案例名稱，在 主控台的 AWS FIS 案例庫頁面上檢視其詳細資訊。
- 狀態 – 指出 AWS FIS 實驗目前的實作狀態。也就是說，已實作、部分實作、未實作和已排除。

> **Note**
>
> AWS FIS 案例是具有多個預先定義動作的主控台限定功能。因此， AWS Resilience Hub 無法追蹤它，它會將狀態設定為無法追蹤。

- 描述 – 描述 AWS FIS 動作的目標。

AWS Fault Injection Service 實驗失敗/狀態檢查

AWS Resilience Hub 可讓您追蹤您已開始的實驗狀態。如需詳細資訊，請參閱 從評估檢視建議的 AWS FIS 實驗 程序。

主題

- 使用 AWS Systems Manager 分析 AWS FIS 實驗執行
- AWS FIS 測試在 Amazon Elastic Kubernetes Service 叢集中執行的 Kubernetes Pod 時，實驗失敗

使用 AWS Systems Manager 分析 AWS FIS 實驗執行

執行 AWS FIS 實驗後，您可以在 Systems Manager AWS 中檢視執行詳細資訊。

1. 前往 CloudTrail > 事件歷史記錄。
2. 使用實驗 ID 依使用者名稱篩選事件。
3. 檢視 StartAutomationExecution 項目。請求 ID 是 SSM 自動化 ID。
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訊。

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。執行輸入參數會出現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。

您可以在執行步驟中向下切入特定步驟，以尋找步驟狀態和其他步驟詳細資訊的相關資訊。

常見故障

以下是執行評估報告時遇到的常見故障：

- 在執行 Test/SOP 實驗之前，未部署警示範本。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：確保在重新執行故障注入實驗之前，轉譯相關警示並部署產生的範本。
- 執行角色中缺少許可。如果提供的執行角色缺少許可並出現在步驟詳細資訊中，則會發生此錯誤訊息。
  - 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.`
  - 修復：確認您提供了正確的執行角色。如果已完成，請新增必要的許可並重新執行評估。
- 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的結果。
  - 失敗訊息：執行成功，因此不會顯示錯誤訊息。
  - 修復：檢查輸入參數並查看分析 AWS FIS 實驗執行中說明的執行步驟，然後再檢查預期輸入和輸出的個別步驟。

AWS FIS 測試在 Amazon Elastic Kubernetes Service 叢集中執行的 Kubernetes Pod 時，實驗失敗

以下是在測試 Amazon EKS 叢集中執行的 Kubernetes Pod 時遇到的常見 Amazon Elastic Kubernetes Service (Amazon EKS) 故障：

- AWS FIS 實驗或 Kubernetes 服務帳戶的 IAM 角色組態不正確。

- 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.`
- 修復：驗證下列項目。
  - 請確定您已遵循使用 AWS FISaws:eks:pod 動作中的說明。
  - 請確定您已使用必要的 RBAC 許可和正確的命名空間建立並設定 Kubernetes Service 帳戶。
  - 請確定您已將提供的 IAM 角色（請參閱測試 AWS CloudFormation 堆疊的輸出）映射至 Kubernetes 使用者。
- 無法啟動 AWS FIS Pod：已達到故障的附屬容器上限。這通常發生在記憶體不足以執行 AWS FIS 附屬容器時。
  - 失敗訊息：`Unable to heartbeat FIS Pod: Max failed sidecar containers reached`。
  - 修復：避免此錯誤的其中一個選項是減少目標負載百分比，以與可用的記憶體或 CPU 保持一致。
- 警示聲明在實驗開始時失敗。發生此錯誤是因為相關警示沒有資料點。
  - 失敗訊息：`Assertion failed for the following alarms`。列出宣告失敗的所有警示。
  - 修復：確保已正確為警示安裝 Container Insights，且警示未開啟（處於 ALARM 狀態）。

了解彈性分數

本節說明如何 AWS Resilience Hub 量化來自不同中斷案例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。此分數反映應用程式遵循我們建議的程度，以符合應用程式的彈性政策、警示、標準操作程序 (SOPs) 和測試。根據應用程式使用的資源類型， AWS Resilience Hub 建議每個中斷類型的警示、SOPs 和一組測試。

最高彈性分數為 100 分。若要獲得最佳分數或最高分數，您必須在應用程式中實作所有建議的警示、SOPs 和測試。例如， AWS Resilience Hub 建議使用一個警示和一個 SOP 來建議測試。測試會執行和觸發警示，並啟動相關聯的 SOP。如果成功執行，且應用程式符合彈性政策，則會收到接近或等於 100 分的彈性分數。

執行第一次評估後， AWS Resilience Hub 會提供選項，從您的應用程式排除操作建議。若要了解排除的建議對彈性分數的影響，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 “包含或排除操作建議”。

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，以檢視應用程式的彈性分數。

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. 在應用程式彈性分數隨時間變化中，在選擇最多 4 個應用程式下拉式清單中選擇一或多個應用程式。
3. 彈性分數圖表會顯示所有所選應用程式的彈性分數。

從應用程式存取彈性分數

1. 在左側導覽功能表中，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您應用程式彈性分數長達一年的趨勢。 AWS Resilience Hub 會顯示動作項目、違反彈性政策的情況，以及需要解決的操作建議，以改善和達到可能的彈性分數上限：

   - 若要檢視需要完成的動作項目，以改善和達到可能的彈性分數上限，請選擇動作項目索引標籤。選取後， AWS Resilience Hub 會顯示下列項目：
     - RTO/RPO – 指出需要修正的復原時間 (RTO/RPOs)，以解決應用程式彈性政策中的違規。選擇 值，以在應用程式的評估報告中檢視 RTO/RPO 詳細資訊。
     - 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，以檢視應用程式評估報告中需要修正的 Amazon CloudWatch 警示。
     - SOPs – 指出需要在應用程式中實作的建議 SOPs 數目。選擇 值，以檢視應用程式評估報告中需要修正的 SOPs。
     - 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。
   - 若要檢視每個影響彈性分數的元件分數，請選擇分數明細。選取後， AWS Resilience Hub 會顯示下列項目：

- RTO/RPO 合規 – 指出應用程式元件 (AppComponents) 與估計工作負載復原時間，以及應用程式彈性政策中定義的目標復原時間的合規程度。選擇 值，以在應用程式的評估報告中檢視 RTO/RPO 估算。
- 實作的警示 – 指出實作的 Amazon CloudWatch 警示相較於其對應用程式彈性分數可能做出的最大貢獻的實際貢獻。選擇 值，在應用程式的評估報告中檢視實作的 Amazon CloudWatch 警示。
- 實作SOPs – 指出實作SOPs 實際貢獻，相較於其對應用程式彈性分數的可能貢獻上限。選擇值，以檢視應用程式評估報告中實作的 SOPs。
- 實作的 FIS 實驗 – 指出實作測試相較於其對應用程式彈性分數可能做出的最大貢獻的實際貢獻。選擇 值，在應用程式的評估報告中檢視實作的測試。

- 若要檢視彈性政策違規和操作建議，請選擇向右箭頭以展開政策違規和操作建議明細區段。展開時， AWS Resilience Hub 會顯示下列項目：
  - 違反彈性政策 – 指出違反應用程式彈性政策的應用程式元件數量。選擇 RTO/RPO 旁的值，以檢視應用程式評估報告之彈性建議索引標籤中的詳細資訊。
  - 操作建議 – 指出尚未實作或執行的操作建議，以使用未處理和排除索引標籤來增強應用程式的彈性。操作建議包括所有非作用中的建議，以及尚未實作的建議。

    若要檢視需要實作的操作建議，請選擇未完成索引標籤。選取後， AWS Resilience Hub 會顯示下列項目：

    - 警示 – 指出需要實作的建議 Amazon CloudWatch 警示數量。
    - SOPs – 指出需要實作的建議 SOPs 數目。
    - FIS – 指出需要實作的建議測試數目。

    若要檢視應用程式排除的操作建議，請選擇排除索引標籤。選取時 AWS Resilience Hub 會顯示下列項目：

    - 警示 – 指出應用程式排除的建議 Amazon CloudWatch 警示數量。
    - SOPs – 指出應用程式排除的建議 SOPs 數量。
    - FIS – 指出應用程式排除的建議測試數量。

計算彈性分數

本節中的表格說明 AWS Resilience Hub 用來判斷每個建議類型的評分元件的公式，以及應用程式的彈性分數。 AWS Resilience Hub 為每種建議類型的計分元件決定的所有結果值，以及您應用程式的彈性分數，都會四捨五入到最接近的點。例如，如果三個警示中有兩個已實作，則分數為 13.33 ((2/3) * 20)

點。此值將四捨五入至 13 點。如需資料表中公式中使用的權重詳細資訊，請參閱the section called "AppComponents的權重和中斷類型"一節。

某些評分元件只能透過 ScoringComponentResiliencyScore API 取得。如需此 API 的詳細資訊，請參閱 ScoringComponentResiliencyScore。

資料表

- 用於計算每個建議類型的分數元件的公式
- 計算彈性分數的公式
- 計算 AppComponents 和中斷類型的彈性分數的公式

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

用於計算每個建議類型的分數元件的公式

評分元件	描述	公式	範例
測試涵蓋範圍 (T)	標準化分數 (0 - 100 分），根據 AWS Resilience Hub 建議測試總數中成功實作和排除的測試數量。 **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， AWS Resilience Hub 才會將其視為已實作。	`T = ((Total number of tests implemented) + (Total number of tests excluded)) / (Total number of tests recommended)` 公式的部分如下所示： • 設定的測試總數 – 指示在 AWS CloudFormation 主控台中建立和上傳 AWS CloudFormation 範本時設定的測試總數。 • 建議的測試總數 – 指示 AWS Resilience Hub 基於應用程式資源建議的測試。	如果您已在 20 個建議測試中實作 10 AWS Resilience Hub 項並排除 5 項測試，則測試涵蓋範圍的計算方式如下： `T = (10 + 5) / 20` 也就是說 `T = .75 or 75 points`

評分元件	描述	公式	範例
		• 排除的測試總數 – 指出您已從應用程式排除的建議測試數量。	
警示涵蓋範圍 (A)	標準化分數 (0 - 100 分），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 AWS Resilience Hub ，讓 將其視為已實作。	`A = ((Total number of alarms implemented) + (Total number of alarms excluded)) / (Total number of alarms recommended)` 公式的部分如下所示： • 設定的警示總數 – 指示在 AWS CloudFormation 主控台中建立和上傳 AWS CloudFormation 範本時設定的 Amazon CloudWatch 警示總數。 • 建議的警示總數 – 指出 AWS Resilience Hub 基於應用程式資源建議的 Amazon CloudWatch 警示。 • 排除的警示總數 – 指出您已從應用程式排除的建議 Amazon CloudWatch 警示數量。	如果您已實作 10 個，並在 20 個 AWS Resilience Hub 建議的 Amazon CloudWatch 警示中排除 5 個 Amazon CloudWatch 警示，Amazon CloudWatch 警示涵蓋範圍的計算方式如下： `A = (10 + 5) / 20` 也就是說 `A = .75 or 75 points`

評分元件	描述	公式	範例
SOP 涵蓋範圍 (S)	標準化分數 (0 - 100 分），根據 AWS Resilience Hub 建議 SOPs 總數中成功實作和排除SOPs 數量。	`S = ((Total number of SOPs implemented) + (Total number of SOPs excluded)) / (Total number of SOPs recommended)` 公式的部分如下所示： • 設定的 SOPs總數 – 指示在 AWS CloudFormation 主控台中建立和上傳 AWS CloudFormation 範本時設定的 SOPs 總數。 • 建議的 SOPs總數 – 指出 AWS Resilience Hub 基於應用程式資源建議的 SOPs。 • 排除SOPs 總數 – 表示您已從應用程式排除的建議 SOPs 數目。	如果您已實作 10 個，並在 20 AWS Resilience Hub 個建議的 SOPs 中排除 5 SOPs，則 SOP 涵蓋範圍的計算方式如下： `S = (10 + 5) / 20` 也就是說 `S = .75 or 75 points`

評分元件	描述	公式	範例

RTO/RPO 合規 (P)	標準化分數 (0 - 100 分），以應用程式符合其彈性政策為基礎。	`P = Total weights of disruption types meeting the application's resiliency policy / Total weights of all disruption types .`	如果您應用程式彈性政策僅符合可用區域 (AZ) 和基礎設施中斷類型，則彈性政策分數 (P) 的計算方式如下：
			• 如果您已設定區域性 RTO 和 RPO 目標，P 的計算方式如下：
			`P = (20 + 30)/ 100`
			也就是說 `P = .5 or 50 points`
			• 如果您尚未設定區域性 RTO 和 RPO 目標，P 的計算方式如下：
			`P = (22.22 + 33.33)/ 99.9`
			也就是說 `P = .55 or 55 points`

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

計算彈性分數的公式

評分元件	描述	公式	範例
應用程式彈性分數 (RS)	根據您的應用程式符合其彈性政策的標準化彈性分數 (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。也就是說： RS = Weighted Average (T, A, S, P)	每個應用程式的彈性分數是使用以下公式計算： RS = (T * Weight(T) + A * Weight(A) + S * Weight(S) + P * Weight(P)) / (Weight(T) + Weight(A) + Weight(S) + Weight(P))	計算每個建議類型資料表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) 也就是說 RS = .65 or 65 points

下表說明 AWS Resilience Hub 用來計算 Application Components (AppComponents) 和中斷類型的彈性分數的公式。不過，您只能透過下列 AWS Resilience Hub APIs 取得 AppComponents 和中斷類型的彈性分數：

- 要取得的 DescribeAppAssessment RSo
- ListAppComponentCompliances 以取得 RSao 和 RSA

計算 AppComponents 和中斷類型的彈性分數的公式

評分元件	描述	公式	範例
每個 AppComponent 和每個中斷類型的彈性分數 (RSao)	標準化分數 (0 - 100 分），根據 AppComponent 符合每個中斷類型的彈性政策。每個 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。 也就是說：RSao = Weighted Average (T, A, S, P) 的值T, A, S, P會針對 AppComponent 和中斷類型的所有建議測試、警示、SO	每個 AppComponent 和每個中斷類型的復原能力分數是使用以下公式計算： 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) 也就是說 RSao = .65 or 65 points

評分元件	描述	公式	範例
	Ps 和會議彈性政策計算。		
每個 AppComponent 的彈性分數 (RSa)	標準化分數 (0 - 100 分），以符合其彈性政策為基礎。每個 AppComponent 的彈性分數是所有建議類型的加權平均值。也就是說：RSa = Weighted Average (T, A, S, P) 的值T, A, S, P會針對 AppComponent 的所有建議測試、警示、SOPs 和會議彈性政策計算。	每個 AppComponent 的彈性分數是使用以下公式計算： 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 AppComponent 的彈性分數計算方式如下： RSa = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) / (.2 + .2 + .2 + .4) 也就是說 RSa = .65 or 65 points

評分元件	描述	公式	範例
每種中斷類型的彈性分數 (RSo)	標準化分數 (0 - 100 分），以符合其彈性政策為基礎。每個中斷類型的彈性分數是所有建議類型的加權平均值。也就是說：RSo = Weighted Average (T, A, S, P) 的值T, A, S, P會針對所有建議的中斷類型測試、警示、SOPs 和會議彈性政策計算。	每個中斷類型的彈性分數是使用以下公式計算： 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) 也就是說 RSo = .65 or 65 points

權重

AWS Resilience Hub 會將權重指派給總彈性分數的每個建議類型。

下表顯示警示、SOPs、測試、會議彈性政策和中斷類型的權重。中斷類型包括應用程式、基礎設施、AZ 和區域。

> **Note**
>
> 如果您選擇不為政策定義區域 RTO 或 RPO 目標，則當區域未定義時，其他中斷類型的權重會相應地增加，如權重所示。

警示的權重、SOPs、測試、政策目標

建議類型	Weight
警示	20 點
SOPs	20 點
測試	20 點
會議彈性政策	40 點

中斷類型的權重

中斷類型	定義區域時的權重	區域未定義時的權重
應用程式	40 點	44.44 點
基礎設施	30 點	33.33 點
可用區域	20 點	22.22 點
區域	10 點	N/A

將操作建議與 整合到您的應用程式中 AWS CloudFormation

在操作建議頁面中選擇建立 CloudFormation 範本後， AWS Resilience Hub 會建立 AWS CloudFormation 範本，說明應用程式的特定警示、標準操作程序 (SOP) 或 AWS FIS 實驗。 AWS CloudFormation 範本存放在 Amazon S3 儲存貯體中，您可以在操作建議頁面上的範本詳細資訊索引標籤中檢查範本的 S3 路徑。

例如，以下清單顯示 JSON 格式的 AWS CloudFormation 範本，說明 所轉譯的警示建議 AWS Resilience Hub。這是名為 之 DynamoDB 資料表的讀取調節警示`Employees`。

範本的 Resources區段說明當 DynamoDB 資料表的讀取限流事件數目超過 1 時所啟動的AWS::CloudWatch::Alarm警示。這兩個AWS::SSM::Parameter資源定義中繼資料，允許 AWS Resilience Hub 識別已安裝的資源，而無需掃描實際的應用程式。

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",
  "Parameters" : {
    "SNSTopicARN" : {
      "Type" : "String",
      "Description" : "The ARN of the Amazon 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 資源整合到主要應用程式最簡單的方式，就是在描述應用程式範本的範本中將其新增為另一個資源。以下提供的 JSON 格式檔案提供 AWS CloudFormation 範本中如何描述 DynamoDB 資料表的基本大綱。真正的應用程式可能會包含更多資源，例如額外的資料表。

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

```
}
```

若要允許使用應用程式部署警示資源，您現在需要將硬式編碼資源取代為應用程式堆疊中的動態參考。

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

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

至下列：

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

在AWS::SSM::Parameter資源定義的 下，變更下列項目：

```
"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\"]}"
```

至下列：

```
"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 SOPs 和 AWS FIS 實驗的 AWS CloudFormation 範本時，您將採用相同的方法，以動態參考取代硬式編碼的參考 IDs，即使在硬體變更後仍然有效。

透過使用 DynamoDB 資料表的參考，您可以 AWS CloudFormation 允許 執行下列動作：

- 首先建立資料庫資料表。
- 一律使用警示中產生資源的實際 ID，如果 AWS CloudFormation 需要取代資源，則動態更新警示。

> **Note**
>
> 您可以選擇更進階的方法來使用 AWS CloudFormation 管理應用程式資源，例如巢狀堆疊或參考個別 AWS CloudFormation 堆疊中的資源輸出。（但如果您想要將建議堆疊與主要堆疊分開，則需要設定在兩個堆疊之間傳遞資訊的方式。）
> 此外，第三方工具，例如 HashiCorp 的 Terraform，也可以用來將基礎設施佈建為程式碼 (IaC)。

使用 AWS Resilience Hub APIs來描述和管理應用程式

作為使用 AWS Resilience Hub 主控台描述和管理應用程式的替代方案， AWS Resilience Hub 可讓您使用 AWS Resilience Hub APIs描述和管理應用程式。本章說明如何使用 AWS Resilience Hub APIs建立應用程式。它還定義了您需要執行 APIs的序列，以及您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 “準備應用程式”
- the section called “執行和分析應用程式”
- the section called “修改您的應用程式”

準備應用程式

若要準備應用程式，您必須先建立應用程式、指派彈性政策，然後從輸入來源匯入應用程式資源。如需用於準備應用程式之 AWS Resilience Hub APIs的詳細資訊，請參閱下列主題：

- the section called “建立應用程式”
- the section called “建立彈性政策”
- the section called “匯入應用程式資源並監控匯入狀態”
- the section called “發佈您的應用程式並指派彈性政策”

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。

下列範例示範如何使用 AWS Resilience Hub `CreateApp` API 在 `newApp`中建立新的應用程式。

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"
    }
}
```

建立彈性政策

建立應用程式之後，您必須建立彈性政策，讓您使用 `CreateResiliencyPolicy` API 了解應用程式的彈性狀態。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。

下列範例示範如何使用 AWS Resilience Hub `CreateResiliencyPolicy` API 在 中`newPolicy`為您的應用程式建立 。

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控匯入狀態

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

- `ImportResourcesToDraftAppVersion` – 此 API 可讓您從不同的輸入來源將資源匯入到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 會發佈應用程式的新版本，以及更新的 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 資源匯入應用程式版本的狀態。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。

下列範例示範如何使用 AWS Resilience Hub `ImportResourcesToDraftAppVersion` API 將資源匯入至 中的應用程式。

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>
        }
    ]
}
```

下列範例示範如何使用 CreateAppVersionResource API AWS Resilience Hub 將資源手動新增至中的應用程式。

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"
            }
        ]
    }
}
```

下列範例示範如何使用 AWS Resilience Hub `DescribeDraftAppVersionResourcesImportStatus` API 在 中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彈性政策

在執行評估之前，您必須先發佈應用程式的草稿版本，並將彈性政策指派給應用程式的發行版本。

發佈應用程式的草稿版本並指派彈性政策

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。

   下列範例示範如何使用 AWS Resilience Hub `PublishAppVersion` API 在 中發佈應用程式的草稿版本。

請求

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

回應

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

2. 使用 UpdateApp API 將彈性政策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。

下列範例示範如何使用 AWS Resilience Hub UpdateApp API 將彈性政策套用至 中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"
    }
}
```

執行和管理 AWS Resilience Hub 彈性評估

發佈應用程式的新版本後，您必須執行新的彈性評估並分析結果，以確保您的應用程式符合彈性政策中定義的預估工作負載 RTO 和預估 RPO。評估會將每個應用程式元件組態與政策進行比較，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 “執行和監控彈性評估”
- the section called “建立彈性政策”

執行和監控 AWS Resilience Hub 彈性評估

若要在 中執行彈性評估 AWS Resilience Hub 並監控其狀態，您必須使用下列 APIs：

- `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 說明應用程式的評估，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。

下列範例示範如何使用 `StartAppAssessment` API 在 中 AWS Resilience Hub 開始執行新的評估。

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": {}
    }
}
```

下列範例示範如何使用 AWS Resilience Hub `DescribeAppAssessment` API 在 中監控評估的狀態。您可以從 `assessmentStatus`變數擷取評估的狀態。

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，您可以使用下列 APIs來檢查評估結果。

- `DescribeAppAssessment` – 此 API 可讓您根據彈性政策追蹤應用程式的目前狀態。此外，您也可以從`complianceStatus`變數擷取合規狀態，以及從`resiliencyScore`結構中擷取每個中斷類型的彈性分數。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 Resource Name (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。 APIs

下列範例示範如何使用 `ListAlarmRecommendations` API 評估的 Amazon Resource Name (ARN) 取得警示建議。

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

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 Amazon 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": "An alarm by AWS Resilience Hub that reports when Amazon 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": "An alarm by AWS Resilience Hub 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": "An alarm by AWS Resilience Hub 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": "An alarm by AWS Resilience Hub 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": "An alarm by AWS Resilience Hub 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": "An 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（如何改善目前彈性的建議）。

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
Amazon 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
Amazon 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 Amazon ECS service with launch type Amazon
EC2 and Amazon EFS storage, deployed in multiple AZs. AWS Backup is used to backup
Amazon EFS and copy snapshots in-Region.",
                    "suggestedChanges": [
                        "Add AWS Auto Scaling Groups and Capacity Providers in multiple
AZs",
                        "Change desired count of the setup",
                        "Remove Amazon 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 Amazon EFS from
backup. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
```

```
                        "expectedRpoDescription": "Recovery Point Objective for
Amazon EFS from backups, derived from backup frequency"
                    }
                },
                "optimizationType": "BestAZRecovery",
                "description": "Amazon 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 Amazon EFS from
backup. (Estimate is based on averages, real time restore may vary).",
                        "expectedRpoInSecs": 86400,
                        "expectedRpoDescription": "Recovery Point Objective for
Amazon EFS from backups, derived from backup frequency"
                    }
                },
```

```
                    "optimizationType": "BestAttainable",
                    "description": "Amazon EFS with backups configured",
                    "suggestedChanges": [
                        "Add additional availability zone"
                    ],
                    "haArchitecture": "MultiSite",
                    "referenceId": "efs:config:with_backups:2020-04-01"
                }
            ]
        }
    ]
}
```

修改您的應用程式

AWS Resilience Hub 可讓您透過編輯應用程式的草稿版本，並將變更發佈至新的 （已發佈） 版本，來修改應用程式資源。 AWS Resilience Hub 會使用您應用程式的已發佈版本，其中包含更新的 資源，來執行彈性評估。

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 “從 AppComponent 排除資源”

手動將資源新增至您的應用程式

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 將資源手動新增至應用程式。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。

您必須提供下列參數給此 API：

- 應用程式 Amazon Resource Name (ARN)
- 資源的邏輯 ID
- 資源的實體 ID
- AWS CloudFormation 類型

下列範例示範如何使用 CreateAppVersionResource API AWS Resilience Hub 將資源手動新增至中的應用程式。

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

應用程式元件 (AppComponent) 是一組相關 AWS 資源，可做為單一單位運作並失敗。例如，當您有用作待命部署的跨區域工作負載時。 AWS Resilience Hub 規則會管理哪些 AWS 資源可以屬於哪

種類型的 AppComponent。 AWS Resilience Hub 可讓您使用下列資源管理 APIs 將資源分組到單一 AppComponent。

- `UpdateAppVersionResource` – 此 API 會更新應用程式的資源詳細資訊。如需此 API 的詳細資訊，請參閱 UpdateAppVersionResource。
- `DeleteAppVersionAppComponent` – 此 API 會從應用程式刪除 AppComponent。如需此 API 的詳細資訊，請參閱 DeleteAppVersionAppComponent。

下列範例示範如何使用 AWS Resilience Hub `DeleteAppVersionAppComponent` API 在 中更新應用程式的資源詳細資訊。

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"
    }
}
```

下列範例顯示如何使用 AWS Resilience Hub `UpdateAppVersionResource` API 刪除在先前範例中建立的空白 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"
    }
}
```

從 AppComponent 排除資源

AWS Resilience Hub 可讓您使用 UpdateAppVersionResource API 從評估中排除資源。運算應用程式的彈性時，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資源。

下列範例示範如何使用 AWS Resilience Hub UpdateAppVersionResource API 在 中排除應用程式的資源。

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

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

安全性是 AWS 和 之間的共同責任。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 Cloud 中執行 AWS 服務的基礎設施。 AWS 也提供您可以安全使用的服務。第三方稽核人員會定期測試和驗證我們的安全有效性，做為AWS 合規計畫的一部分。若要了解適用的合規計劃 AWS Resilience Hub，請參閱AWS 合規計劃範圍內的服務。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。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。

本文件可協助您了解如何在使用 時套用共同的責任模型 AWS Resilience Hub。下列主題說明如何設定 AWS Resilience Hub 以符合您的安全和合規目標。您也會了解如何使用其他 AWS 服務來協助您監控和保護 AWS Resilience Hub 資源。

目錄

中的資料保護 AWS Resilience Hub

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

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

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。

- 使用 設定 API 和使用者活動記錄 AWS CloudTrail。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《 使用者指南》中的使用 CloudTrail 追蹤。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-3 驗證的密碼編譯模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-3。

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

靜態加密

AWS Resilience Hub 會加密靜態資料。中的資料 AWS Resilience Hub 是使用透明的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 AWS 服務之間傳輸的資料。所有在 AWS Resilience Hub 和 整合服務之間傳遞的資料都會使用 Transport Layer Security (TLS) 進行加密。 為跨 AWS 服務的特定類型目標 AWS Resilience Hub 提供預先設定的動作，並支援目標資源的動作。

AWS 復原力中樞的身分和存取管理

AWS Identity and Access Management (IAM) 是一種 AWS 服務 ，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行身分驗證 （ 登入 ） 和授權 （ 具有許可 ），以使用 AWS Resilience Hub 資源。IAM 是您可以免費使用 AWS 服務 的 。

主題

- 目標對象
- 使用身分驗證
- 使用政策管理存取權
- AWS Resilience Hub 如何與 IAM 搭配使用

- 設定 IAM 角色和許可
- 對 AWS 復原中心身分和存取權進行故障診斷
- AWS Resilience Hub 存取許可參考
- AWS 的 受管政策 AWS Resilience Hub
- AWS Resilience Hub 角色和 IAM 許可參考
- 將 Terraform 狀態檔案匯入至 AWS Resilience Hub
- 啟用對 Amazon Elastic Kubernetes Service 叢集的 AWS Resilience Hub 存取
- 啟用 AWS Resilience Hub 以發佈到您的 Amazon Simple Notification Service 主題
- 限制納入或排除 AWS Resilience Hub 建議的許可

目標對象

使用方式 AWS Identity and Access Management (IAM) 會有所不同，取決於您在 AWS Resilience Hub 中執行的工作。

服務使用者 – 如果您使用 AWS Resilience Hub 服務來執行您的任務，則您的管理員會為您提供所需的登入資料和許可。當您使用更多 AWS 彈性中樞功能來執行工作時，您可能需要額外的許可。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 Resilience Hub 中的功能，請參閱 對 AWS 復原中心身分和存取權進行故障診斷。

服務管理員 – 如果您在公司負責 AWS Resilience Hub 資源，您可能可以完整存取 AWS Resilience Hub。您的任務是判斷您的服務使用者應存取的 AWS Resilience Hub 功能和資源。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 Resilience Hub 使用 IAM，請參閱AWS Resilience Hub 如何與 IAM 搭配使用。

IAM 管理員 – 如果您是 IAM 管理員，建議您了解如何撰寫政策以管理 AWS 對 Resilience Hub 的存取的詳細資訊。若要檢視您可以在 IAM 中使用的 AWS Resilience Hub 身分型政策範例，請參閱 AWS Resilience Hub 的身分型政策範例。

使用身分驗證

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

您可以使用透過身分來源提供的憑證，以聯合身分 AWS 身分身分身分登入 。 AWS IAM Identity Center (IAM Identity Center) 使用者、您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。當您使用聯合 AWS 身分存取 時，您會間接擔任角色。

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

如果您以 AWS 程式設計方式存取 ， AWS 會提供軟體開發套件 (SDK) 和命令列界面 (CLI)，以使用您的登入資料以密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，則必須自行簽署請求。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》中的適用於 API 請求的AWS Signature 第 4 版。

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) 來提高帳戶的安全性。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 IAM 中的AWS 多重要素驗證。

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 帳戶中的所有 AWS 服務 和資源。此身分稱為 AWS 帳戶 Theroot 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

最佳實務是， 要求人類使用者，包括需要管理員存取權的使用者，使用臨時登入資料 AWS 服務 與身分提供者聯合來存取 。

聯合身分是來自您的企業使用者目錄、Web 身分提供者、 AWS Directory Service、身分中心目錄，或是使用透過身分來源提供的憑證 AWS 服務 存取的任何使用者。當聯合身分存取時 AWS 帳戶，它們會擔任角色，而角色會提供臨時憑證。

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，或者您可以連接並同步到您自己的身分來源中的一組使用者 AWS 帳戶 和群組，以便在所有 和應用程式中使用。如需 IAM Identity Center 的詳細資訊，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 中具有單一人員或應用程式特定許可 AWS 帳戶 的身分。建議您盡可能依賴臨時憑證，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，但角色僅提供臨時憑證。如需更多資訊，請參閱《IAM 使用者指南》中的 IAM 使用者的使用案例。

IAM 角色

IAM 角色是 中具有特定許可 AWS 帳戶 的身分。它類似 IAM 使用者，但不與特定的人員相關聯。若要暫時在 中擔任 IAM 角色 AWS Management Console，您可以從使用者切換至 IAM 角色（主控台）。您可以透過呼叫 AWS CLI 或 AWS API 操作或使用自訂 URL 來擔任角色。如需使用角色的方法詳細資訊，請參閱《IAM 使用者指南》中的擔任角色的方法。

使用臨時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 — 如需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 (聯合) 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 (信任的主體) 存取您帳戶的資源。角色是授予跨帳戶存取權的主要方式。不過，對於某些 AWS 服務，您可以直接將政策連接到資源（而不是使用角色做為代理）。如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取。
- 跨服務存取 – 有些 AWS 服務 使用其他 中的功能 AWS 服務。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。
  - 轉送存取工作階段 (FAS) – 當您使用 IAM 使用者或角色在 中執行動作時 AWS，您會被視為委託人。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 使用呼叫 的委託人許可 AWS 服務，並結合 AWS 服務 請求向下游服務提出請求。只有當服務收到需要

與其他 AWS 服務 或 資源互動才能完成的請求時，才會提出 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。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可權給 AWS 服務。
- 服務連結角色 – 服務連結角色是連結至 的服務角色類型 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶 ，並由服務擁有。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 執行個體上執行之應用程式的臨時登入資料，以及提出 AWS CLI 或 AWS API 請求。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，並將其提供給其所有應用程式，您可以建立連接至執行個體的執行個體描述檔。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臨時憑證。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM 角色來授予許可權給 Amazon EC2 執行個體上執行的應用程式。

使用政策管理存取權

您可以透過建立政策並將其連接到身分或資源 AWS 來控制 AWS 中的存取。政策是 中的物件， AWS 當與身分或資源建立關聯時， 會定義其許可。當委託人（使用者、根使用者或角色工作階段）發出請求時， 會 AWS 評估這些政策。政策中的許可決定是否允許或拒絕請求。大多數政策會以 JSON 文件 AWS 的形式存放在 中。如需 JSON 政策文件結構和內容的詳細資訊，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。具有該政策的使用者可以從 AWS Management Console AWS CLI、 或 API AWS 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。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

身分型政策可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。受管政策是獨立的政策，您可以連接到 中的多個使用者、群組和角色 AWS 帳戶。受管政策包括 AWS 受管政策和客戶受管政策。如需了解如何在受管政策及內嵌政策之間選擇，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。委託人可以包含帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

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

存取控制清單 (ACL)

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

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

其他政策類型

AWS 支援其他較不常見的政策類型。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。如需許可界限的詳細資訊，請參閱 IAM 使用者指南中的 IAM 實體許可界限。
- 服務控制政策 SCPs) – SCPs是 JSON 政策，可指定 in. 中組織或組織單位 (OU) 的最大許可 AWS Organizations。 AWS Organizations 是一種用於分組和集中管理您企業擁有 AWS 帳戶 的多個的服務。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 會限制成員帳戶中實體的許可，包括每個實體 AWS 帳戶根使用者。如需 Organizations 和 SCP 的詳細資訊，請參閱《AWS Organizations 使用者指南》中的服務控制政策。
- 資源控制政策 (RCP) - RCP 是 JSON 政策，可用來設定您帳戶中資源的可用許可上限，採取這種方式就不需要更新附加至您所擁有的每個資源的 IAM 政策。RCP 會限制成員帳戶中資源的

許可，並可能影響身分的有效許可，包括 AWS 帳戶根使用者，無論它們是否屬於您的組織。如需 Organizations 和 RCPs的詳細資訊，包括支援 RCPs AWS 服務 的 清單，請參閱AWS Organizations 《 使用者指南》中的資源控制政策 RCPs)。

- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過撰寫程式的方式建立角色或聯合使用者的暫時工作階段時，做為參數傳遞。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。如需詳細資訊，請參閱 IAM 使用者指南中的工作階段政策。

多種政策類型

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。若要了解如何 AWS 在涉及多種政策類型時決定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

AWS Resilience Hub 如何與 IAM 搭配使用

在您使用 IAM 管理 AWS 對 Resilience Hub 的存取之前，請先了解哪些 IAM 功能可與 AWS Resilience Hub 搭配使用。

您可以搭配 AWS Resilience Hub 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

IAM 功能	AWS 彈性中樞支援
服務角色	是

若要深入了解 AWS Resilience Hub 和其他 AWS 服務如何與大多數 IAM 功能搭配使用，請參閱《IAM 使用者指南》中的AWS 與 IAM 搭配使用的 服務。

AWS 彈性中樞的身分型政策

支援身分型政策：是

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。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

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。

AWS Resilience Hub 的身分型政策範例

若要檢視 AWS Resilience Hub 身分型政策的範例，請參閱 AWS Resilience Hub 的身分型政策範例。

AWS Resilience Hub 中的資源型政策

支援資源型政策：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。委託人可以包含帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

如需啟用跨帳戶存取權，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，做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。當主體和資源位於不同的位置時 AWS 帳戶，信任帳戶中的 IAM 管理員也必須授予主體實體 （使用者或角色） 存取資源的許可。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 中的快帳戶資源存取。

AWS Resilience Hub 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。政策動作通常具有與相關聯 AWS API 操作相同的名稱。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 復原中心動作的清單，請參閱服務授權參考中的AWS 復原中心定義的動作。

AWS Resilience Hub 中的政策動作在動作之前使用下列字首：

```
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 Resilience Hub 身分型政策的範例，請參閱 AWS Resilience Hub 的身分型政策範例。

AWS Resilience Hub 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 Resilience Hub 資源類型及其 ARNs 的清單，請參閱服務授權參考中的 AWS Resilience Hub 定義的資源。若要了解您可以使用哪些動作來指定每個資源的 ARN，請參閱 Resilience Hub AWS 定義的動作。

若要檢視 AWS Resilience Hub 身分型政策的範例，請參閱 AWS Resilience Hub 的身分型政策範例。

AWS Resilience Hub 的政策條件索引鍵

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， 會使用邏輯OR操作 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的條件金鑰。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的AWS 全域條件內容索引鍵。

若要查看 Resilience Hub AWS 條件索引鍵的清單，請參閱服務授權參考中的 AWS Resilience Hub 條件索引鍵。若要了解您可以使用條件金鑰的動作和資源，請參閱 Resilience Hub AWS 定義的動作。

若要檢視 AWS Resilience Hub 身分型政策的範例，請參閱 AWS Resilience Hub 的身分型政策範例。

AWS 彈性中樞中的 ACLs

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 彈性中心

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。您可以將標籤連接至 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。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，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》中的使用 ABAC 授權定義許可。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 Resilience Hub 使用臨時憑證

支援臨時憑證：是

當您使用臨時憑證登入時，有些 AWS 服務 無法使用。如需詳細資訊，包括 AWS 服務 使用哪些臨時登入資料，請參閱《AWS 服務 IAM 使用者指南》中的使用 IAM 的 。

如果您 AWS Management Console 使用使用者名稱和密碼以外的任何方法登入 ，則會使用臨時登入資料。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取 時，該程序會自動建立臨時登入資料。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》中的從使用者切換至 IAM 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。

轉送 AWS 彈性中樞的存取工作階段

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，您會被視為委託人。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 使用呼叫 的委託人許可 AWS 服務，並結合

AWS 服務 請求向下游服務提出請求。只有當服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會提出 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 Resilience Hub 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。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可權給 AWS 服務。

> **Warning**
>
> 變更服務角色的許可可能會中斷 AWS Resilience Hub 功能。只有在 AWS 彈性中心提供指引時，才能編輯服務角色。

AWS Resilience Hub 的身分型政策範例

根據預設，使用者和角色沒有建立或修改 AWS Resilience Hub 資源的許可。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行任務。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。

如需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 (主控台)。

如需 AWS Resilience Hub 定義的動作和資源類型的詳細資訊，包括每種資源類型的 ARNs 格式，請參閱服務授權參考中的 AWS Resilience Hub 的動作、資源和條件索引鍵。

主題

- 政策最佳實務
- 使用 AWS Resilience Hub 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 應用程式
- 啟動應用程式評估
- 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
- 更新具有特定彈性政策的應用程式

政策最佳實務

以身分為基礎的政策會判斷是否有人可以在您的帳戶中建立、存取或刪除 AWS Resilience 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 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用 AWS 受管政策來授予許多常見使用案例的許可。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，進一步減少許可。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。如果透過特定 使用服務動作，您也可以使用條件來授予存取服務動作的權限 AWS 服務，例如 AWS CloudFormation。如需詳細資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM Access Analyzer 驗證政策。
- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以增加安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_configure-api-require.html中的透過 MFA 的安全 API 存取。

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

使用 AWS Resilience Hub 主控台

若要存取 AWS Resilience Hub 主控台，您必須擁有一組最低許可。這些許可必須允許您列出和檢視中 AWS 有關 Resilience Hub 資源的詳細資訊 AWS 帳戶。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。

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

為了確保使用者和角色仍然可以使用 AWS Resilience Hub 主控台，也請將 AWS Resilience Hub *ConsoleAccess*或*ReadOnly* AWS 受管政策連接到實體。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。

下列政策授予使用者許可，以列出和檢視 AWS Resilience Hub 主控台中的所有資源，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。此政策包含在主控台上完成此動作的許可，或使用 AWS CLI 或 AWS API 以程式設計方式完成此動作的許可。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
```

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

列出可用的 AWS Resilience Hub 應用程式

下列政策授予使用者列出可用 AWS Resilience Hub 應用程式的許可。

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

啟動應用程式評估

下列政策授予使用者啟動特定 AWS Resilience Hub 應用程式評估的許可。

```
{
  "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

下列政策授予使用者許可，以刪除特定 AWS Resilience Hub 應用程式的評估。

```
{
  "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

下列政策授予使用者為特定 AWS Resilience Hub 應用程式建立建議範本的許可。

```
{
  "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

下列政策授予使用者刪除特定 AWS Resilience Hub 應用程式建議範本的許可。

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

更新具有特定彈性政策的應用程式

下列政策授予使用者使用特定彈性政策更新 AWS Resilience Hub 應用程式的許可。

```
{
  "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 可讓您設定要在應用程式執行評估時使用的 IAM 角色。有多種方式可設定 AWS Resilience Hub 來取得應用程式的唯讀存取權。不過， AWS Resilience Hub 建議下列方式：

- 角色型存取 – 此角色已定義並在目前帳戶中使用。 AWS Resilience Hub 將擔任此角色來存取您應用程式的資源。

  若要提供角色型存取，角色必須包含下列項目：

  - 唯讀許可，以讀取您的 資源 (AWS Resilience Hub 建議您使用 `AWSResilienceHubAsssessmentExecutionPolicy`受管政策）。
  - 信任政策以擔任此角色，這可讓 AWS Resilience Hub Service Principal 擔任此角色。如果您沒有在帳戶中設定這類角色， AWS Resilience Hub 會顯示建立該角色的指示。如需詳細資訊，請參閱the section called “設定許可”。

  > **Note**
  >
  > 如果您只提供叫用者角色名稱，而且您的資源位於另一個 帳戶中，則 AWS Resilience Hub 會在其他帳戶中使用此角色名稱來存取跨帳戶資源。或者，您可以為其他 帳戶設定角色 ARNs，這將用來取代叫用者角色名稱。

- 目前的 IAM 使用者存取權 – AWS Resilience Hub 將使用目前的 IAM 使用者來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 將擔任下列 IAM 角色來存取資源：

- AwsResilienceHubAdminAccountRole 在目前帳戶中
- AwsResilienceHubExecutorAccountRole 在其他帳戶中

此外，當您設定排定的評估時， AWS Resilience Hub 將擔任該AwsResilienceHubPeriodicAssessmentRole角色。不過，AwsResilienceHubPeriodicAssessmentRole不建議使用 ，因為您必須手動設定角色和許可，而且某些功能 （ 例如偏離通知) 可能無法如預期般運作。

對 AWS 復原中心身分和存取權進行故障診斷

使用下列資訊來協助您診斷和修正使用 AWS Resilience Hub 和 IAM 時可能遇到的常見問題。

主題

- 我無權在 AWS Resilience Hub 中執行 動作
- 我未獲得執行 iam:PassRole 的授權
- 我想要允許 以外的人員 AWS 帳戶 存取我的 AWS Resilience Hub 資源

我無權在 AWS Resilience Hub 中執行 動作

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 管理員。您的管理員提供您的簽署憑證。

我未獲得執行 iam:PassRole 的授權

如果您收到錯誤，表示您未獲授權執行iam:PassRole動作，則必須更新您的政策，以允許您將角色傳遞給 AWS Resilience Hub。

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

當名為 的 IAM `marymajor` 使用者嘗試使用主控台在 AWS Resilience Hub 中執行動作時，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 管理員。您的管理員提供您的簽署憑證。

我想要允許 以外的人員 AWS 帳戶 存取我的 AWS Resilience Hub 資源

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

如需進一步了解，請參閱以下內容：

- 若要了解 AWS Resilience Hub 是否支援這些功能，請參閱 AWS Resilience Hub 如何與 IAM 搭配使用。
- 若要了解如何 AWS 帳戶 在您擁有的 資源間提供存取權，請參閱《IAM 使用者指南》中的在您擁有 AWS 帳戶 的另一個 IAM 使用者中提供存取權。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的提供存取權給第三方 AWS 帳戶 擁有。
- 如需了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取。

AWS Resilience Hub 存取許可參考

您可以使用 AWS Identity and Access Management (IAM) 來管理應用程式資源的存取，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 “叫用者角色”(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

可以連接政策，定義 AWS Resilience Hub 存取其他 AWS 資源或應用程式資源所需的許可。呼叫者角色必須具有新增至 AWS Resilience Hub Service Principal 的信任政策。

若要管理應用程式的許可，建議使用 the section called “AWS 受管政策”。您可以使用這些受管政策，而不需進行任何修改，也可以使用它們做為撰寫自我限制政策的起點。政策可以使用其他選用條件，限制不同動作的資源層級使用者許可。

如果您的應用程式資源位於不同的帳戶（次要/資源帳戶），您必須在包含應用程式資源的每個帳戶中設定新的角色。

> **Note**
>
> 如果您為工作負載資源定義 VPC 端點，請確定 VPC 端點政策提供存取資源 AWS Resilience Hub 的唯讀存取權。如需詳細資訊，請參閱使用端點政策控制對 VPC 端點的存取。

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 資源的建議許可選項。

主題

- the section called “叫用者角色”
- the section called “不同 AWS 帳戶中跨帳戶存取的角色”

叫用者角色

AWS Resilience Hub 叫用者角色是 AWS Identity and Access Management (IAM) 角色， AWS Resilience Hub 擔任 存取 AWS 服務和資源。例如，您可以建立叫用者角色，該角色具有存取 CFN 範本及其建立的資源的許可。此頁面提供如何建立、檢視和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，您會提供叫用者角色。 AWS Resilience Hub 會擔任此角色，以便在您匯入資源或開始評估時存取您的資源。若要 AWS Resilience Hub 讓 正確擔任您的叫用者角色，角色的信任政策必須將 AWS Resilience Hub 服務主體 (resiliencehub.amazonaws.com) 指定為信任的服務。

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選單中選擇更新許可。

您可以隨時從應用程式調用者角色新增或移除許可，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 主控台中建立調用者角色”
- the section called “使用 IAM API 管理角色”
- the section called “使用 JSON 檔案定義信任政策”

在 IAM 主控台中建立調用者角色

若要讓 AWS Resilience Hub 能夠存取 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 服務的角色（主控台）。

使用 IAM 主控台在主要帳戶中建立調用者角色

1. 在 `https://console.aws.amazon.com/iam/` 開啟 IAM 主控台。
2. 從導覽窗格中，選擇角色，然後選擇建立角色。
3. 選取自訂信任政策，在自訂信任政策視窗中複製下列政策，然後選擇下一步。

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

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

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

4. 在新增許可頁面的許可政策區段AWSResilienceHubAsssessmentExecutionPolicy中，輸入依屬性或政策名稱篩選政策，然後按 Enter 方塊。
5. 選取政策，然後選擇下一步。
6. 在角色詳細資訊區段中，在角色名稱方塊中輸入唯一的角色名稱（例如AWSResilienceHubAssessmentRole)。

   此欄位只接受英數字元和「+=,.@-_/」字元。
7. （選用）在描述方塊中輸入角色的描述。
8. 選擇建立角色。

   若要編輯使用案例和許可，請在步驟 6 中，選擇步驟 1：選取信任實體或步驟 2：新增許可區段右側的編輯按鈕。

建立叫用者角色和資源角色（如適用）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/角色中擁有呼叫者角色的iam:passRole許可。不過，您不需要此許可即可執行評估。

使用 IAM API 管理角色

角色的信任政策提供指定主體擔任角色的許可。若要使用 AWS Command Line Interface (AWS CLI) 建立角色，請使用 create-role命令。使用此命令時，您可以內嵌指定信任政策。下列範例示範如何授予 AWS Resilience Hub 服務主體擔任您的角色的許可。

> **Note**
>
> 逸出 JSON 字串中引號 (' ') 的需求可能會根據您的 Shell 版本而有所不同。

範例 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 檔案定義信任政策

您可以使用單獨的 JSON 檔案來定義角色的信任政策，然後執行 create-role命令。在下列範例中，**trust-policy.json** 是在目前目錄中包含信任政策的檔案。此政策會透過執行 **create-role**命令連接至角色。**create-role** 命令的輸出會顯示在範例輸出中。若要將許可新增至角色，請使用 attach-policy-to-role 命令，而且您可以從新增AWSResilienceHubAsssessmentExecutionPolicy受管政策開始。如需此受管政策的詳細資訊，請參閱 the section called “AWSResilienceHubAsssessmentExecutionPolicy”。

範例 trust-policy.json

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

範例 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"
            }]
        }
    }
}
```

範例 **attach-policy-to-role**

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

不同 AWS 帳戶中跨帳戶存取的角色 - 選用

當您的資源位於次要/資源帳戶中時，您必須在每個帳戶中建立角色，才能讓 AWS Resilience Hub 成功評估您的應用程式。角色建立程序類似於叫用者角色建立程序，但信任政策組態除外。

> **Note**
>
> 您必須在資源所在的次要帳戶中建立角色。

主題

- the section called “在次要/資源帳戶的 IAM 主控台中建立角色”
- the section called “使用 IAM API 管理角色”
- the section called “使用 JSON 檔案定義信任政策”

在次要/資源帳戶的 IAM 主控台中建立角色

若要讓 AWS Resilience Hub 能夠存取其他 AWS 帳戶中 AWS 的服務和資源，您必須在每個帳戶中建立角色。

使用 IAM 主控台在 IAM 主控台中為次要/資源帳戶建立角色

1. 在 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 從導覽窗格中，選擇角色，然後選擇建立角色。
3. 選取自訂信任政策，在自訂信任政策視窗中複製下列政策，然後選擇下一步。

> **Note**
>
> 如果您的資源位於不同的帳戶中，您必須在每個帳戶中建立角色，並為其他帳戶使用次要帳戶信任政策。

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

4. 在新增許可頁面的許可政策區段AWSResilienceHubAsssessmentExecutionPolicy中，輸入依屬性或政策名稱篩選政策，然後按 Enter 方塊。
5. 選取政策，然後選擇下一步。
6. 在角色詳細資訊區段中，在角色名稱方塊中輸入唯一的角色名稱（例如AWSResilienceHubAssessmentRole)。
7. （選用）在描述方塊中輸入角色的描述。
8. 選擇建立角色。

若要編輯使用案例和許可，請在步驟 6 中，選擇步驟 1：選取信任實體或步驟 2：新增許可區段右側的編輯按鈕。

此外，您也需要將 `sts:assumeRole` 許可新增至叫用者角色，讓它能夠擔任次要帳戶中的角色。

針對您建立的每個次要角色，將下列政策新增至您的呼叫者角色：

```
{
    "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

角色的信任政策提供指定主體擔任角色的許可。若要使用 AWS Command Line Interface (AWS CLI) 建立角色，請使用 `create-role`命令。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予 AWS Resilience Hub 服務主體擔任您角色的許可。

> **Note**
>
> 逸出 JSON 字串中引號 (' ') 的需求可能會根據您的 Shell 版本而有所不同。

範例 **`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 檔案定義信任政策

您可以使用單獨的 JSON 檔案來定義角色的信任政策，然後執行 `create-role`命令。在下列範例中，**`trust-policy.json`** 是在目前目錄中包含信任政策的檔案。此政策會透過執行 **`create-role`**命令連接至角色。**`create-role`** 命令的輸出會顯示在範例輸出中。若要將許可新增至角色，請使用 attach-policy-to-role 命令，您可以先新增`AWSResilienceHubAsssessmentExecutionPolicy`受管政策。如需此受管政策的詳細資訊，請參閱 the section called “AWSResilienceHubAsssessmentExecutionPolicy”。

範例 `trust-policy.json`

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

範例 `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"
                }
            ]
        }
    }
}
```

範例 **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 使用者許可來建立和執行評估，請使用此方法。您可以將 `AWSResilienceHubAsssessmentExecutionPolicy` 受管政策連接至您的 IAM 使用者或與使用者相關聯的角色。

單一帳戶設定

使用上述的受管政策，就足以對應用程式執行評估，而該應用程式是在與 IAM 使用者相同的帳戶中受管。

排定的評估設定

您必須建立新的角色`AwsResilienceHubPeriodicAssessmentRole`，才能讓 AWS Resilience Hub 執行排定的評估相關任務。

> **Note**
>
> - 使用角色型存取（使用上述叫用者角色）時，不需要此步驟。

- 角色名稱必須是 AwsResilienceHubPeriodicAssessmentRole。

啟用 AWS Resilience Hub 以執行排定的評估相關任務

1. 將 AWSResilienceHubAsssessmentExecutionPolicy 受管政策連接至角色。
2. 新增下列政策，其中 primary_account_id是定義應用程式並將執行評估 AWS 的帳戶。此外，您必須新增排程評估角色的關聯信任政策 (AwsResilienceHubPeriodicAssessmentRole)，以授予 AWS Resilience Hub 服務擔任排程評估角色的許可。

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

排程評估角色的信任政策 (**AwsResilienceHubPeriodicAssessmentRole**)

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

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

跨帳戶設定

如果您將 AWS Resilience Hub 與多個帳戶搭配使用，則需要下列 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許可。設定 AWS Resilience Hub 跨帳戶存取時，會考慮下列帳戶和角色：

- 主要帳戶 – AWS 您要在其中建立應用程式和執行評估的帳戶。
- 次要/資源帳戶 (s) – 資源所在的 AWS 帳戶 (s)。

> **Note**
>
> - 使用角色型存取（使用上述叫用者角色）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 “啟用對 Amazon EKS 叢集的 AWS Resilience Hub 存取”。

主要帳戶設定

您必須在主要帳戶中建立新的角色`AwsResilienceHubAdminAccountRole`，並啟用 AWS Resilience Hub 存取以擔任該角色。此角色將用於存取您 AWS 帳戶中包含您資源的另一個角色。它不應具有讀取資源的許可。

> **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`許可。

- secondary_account_id_1/2/... 將 取代為相關的次要帳戶識別符。

下列政策為您的角色提供執行器許可，以存取您 AWS 帳戶中另一個角色中的資源：

```
{
  {
  "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) 的信任政策如下所示：

```
{
  "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/資源帳戶 (s) 設定

在每個次要帳戶中，您必須建立新的 ，AwsResilienceHubExecutorAccountRole並啟用上述建立的管理員角色，才能擔任此角色。由於 會使用此角色 AWS Resilience Hub 來掃描和評估您的應用程式資源，因此也需要適當的許可。

不過，您必須將AWSResilienceHubAsssessmentExecutionPolicy受管政策連接至角色，並連接執行器角色政策。

執行器角色信任政策如下所示：

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

AWS 的 受管政策 AWS Resilience Hub

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

請記住， AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為這些許可可供所有 AWS 客戶使用。我們建議您定義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 AWS 受管政策中定義的許可。如果 AWS 更新受管政策中 AWS 定義的許可，則更新會影響政策連接的所有主體身分 （使用者、群組和角色）。當新的 AWS 服務 啟動或新的 API 操作可用於現有 服務時， AWS 最有可能更新受 AWS 管政策。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

AWSResilienceHubAsssessmentExecutionPolicy

您可以將 AWSResilienceHubAsssessmentExecutionPolicy 連接至您的 IAM 身分。執行評估時，此政策會授予其他 AWS 服務的存取許可，以執行評估。

許可詳細資訊

此政策提供足夠的許可，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 儲存貯體名稱必須以 開頭aws-resilience-hub-artifacts-。如果您想要發佈到另一個 Amazon S3 儲存貯體，您可以在呼叫 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) – 取得您在 Amazon CloudWatch 中設定的所有實作警示，以監控應用程式。此外，我們使用 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 AWS 您的帳戶相關聯的 Amazon Data Lifecycle Manager 資源並提供其Describe許可。
- Amazon DevOpsGuru – 列出與 AWS 您的帳戶相關聯的 Amazon DevOpsGuru 資源並提供其Describe許可。
- Amazon DocumentDB – 列出與您的帳戶 AWS 相關聯的 Amazon DocumentDB 資源並提供Describe其許可。
- Amazon DynamoDB (DynamoDB) – 列出與您的帳戶 AWS 相關聯的 Amazon DynamoDB 資源並提供Describe其許可。
- Amazon ElastiCache (ElastiCache) – 為與您 AWS 帳戶相關聯的 ElastiCache 資源提供Describe許可。
- Amazon ElastiCache (Redis OSS) Serverless (ElastiCache (Redis OSS) Serverless) – 為與您 AWS 帳戶相關聯的 ElastiCache (Redis OSS) Serverless 組態提供Describe許可。

- Amazon Elastic Compute Cloud (Amazon EC2) – 列出與您的帳戶 AWS 相關聯的 Amazon EC2 資源並提供其Describe許可。
- Amazon Elastic Container Registry (Amazon ECR) – 為與您 AWS 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 帳戶相關聯的 Amazon ECS 資源提供Describe許可。
- Amazon Elastic File System (Amazon EFS) – 為與您 AWS 帳戶相關聯的 Amazon EFS 資源提供Describe許可。
- Amazon Elastic Kubernetes Service (Amazon EKS) – 列出與您的帳戶 AWS 相關聯的 Amazon EKS 資源並提供Describe其許可。
- Amazon EC2 Auto Scaling – 列出與 AWS 您的帳戶相關聯的 Amazon EC2 Auto Scaling 資源並提供其Describe許可。
- Amazon EC2 Systems Manager (SSM) – 為與您 AWS 帳戶相關聯的 SSM 資源提供Describe許可。
- AWS Fault Injection Service (AWS FIS) – 列出和提供與 AWS 您的帳戶相關聯的 AWS FIS 實驗和實驗範本的Describe許可。
- Amazon FSx for Windows File Server (Amazon FSx) – 列出與您的帳戶 AWS 相關聯的 Amazon FSx 資源並提供Describe其許可。
- Amazon RDS – 列出與 AWS 您的帳戶相關聯的 Amazon RDS 資源並提供Describe許可。
- Amazon Route 53 (Route 53) – 列出與您的帳戶 AWS 相關聯的 Route 53 資源並提供Describe許可。
- Amazon Route 53 Resolver – 列出與 AWS 您的帳戶相關聯的 Amazon Route 53 Resolver 資源並提供Describe許可。
- Amazon Simple Notification Service (Amazon SNS) – 列出與您的帳戶 AWS 相關聯的 Amazon SNS 資源並提供Describe其許可。
- Amazon Simple Queue Service (Amazon SQS) – 列出與您的帳戶 AWS 相關聯的 Amazon SQS 資源並提供Describe其許可。
- Amazon Simple Storage Service (Amazon S3) – 列出與您的帳戶 AWS 相關聯的 Amazon S3 資源並提供Describe其許可。

> **Note**
>
> 執行評估時，如果有任何缺少的許可需要從受管政策更新， AWS Resilience Hub 將使用 s3：GetBucketLogging 許可成功完成評估。不過， AWS Resilience Hub 會顯示警告訊息，

列出缺少的許可，並提供寬限期來新增相同許可。如果您未在指定的寬限期內新增缺少的許可，評估將會失敗。

- AWS Backup – 列出並取得與您 AWS 帳戶相關聯的 Amazon EC2 Auto Scaling 資源`Describe`許可。
- AWS CloudFormation – 列出並取得與您 AWS 帳戶相關聯之 AWS CloudFormation 堆疊上資源的`Describe`許可。
- AWS DataSync – 列出與 AWS 您的帳戶相關聯的 AWS DataSync 資源並提供`Describe`許可。
- AWS Directory Service – 列出與 AWS 您的帳戶相關聯的 AWS Directory Service 資源並提供`Describe`許可。
- AWS Elastic Disaster Recovery （彈性災難復原） – 為與您 AWS 帳戶相關聯的彈性災難復原資源提供`Describe`許可。
- AWS Lambda (Lambda) – 列出與您的帳戶 AWS 相關聯的 Lambda 資源並提供`Describe`其許可。
- AWS Resource Groups （資源群組） – 列出與您的帳戶 AWS 相關聯的資源群組資源並提供`Describe`其許可。
- AWS Service Catalog （服務目錄） – 列出與您的帳戶 AWS 相關聯的 Service Catalog 資源並提供`Describe`其許可。
- AWS Step Functions – 列出與 AWS 您的帳戶相關聯的 AWS Step Functions 資源並提供`Describe`許可。
- Elastic Load Balancing – 列出與 AWS 您的帳戶相關聯的 Elastic Load Balancing 資源並提供其`Describe`許可。
- `ssm:GetParametersByPath` – 我們使用此許可來管理針對您的應用程式設定的 CloudWatch 警示、測試或 SOPs。

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，這些使用者、使用者群組和角色提供必要的許可，讓您的團隊在執行評估時存取 AWS 服務。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSResilienceHubFullResourceStatement",
            "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",
                "docdb-elastic:GetCluster",
                "docdb-elastic:GetClusterSnapshot",
                "docdb-elastic:ListClusterSnapshots",
                "docdb-elastic:ListTagsForResource",
                "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:DescribeServerlessCaches",
                "elasticahce:DescribeServerlessCacheSnapshots",
                "elasticache:DescribeSnapshots",
                "elasticfilesystem:DescribeFileSystems",
                "elasticfilesystem:DescribeLifecycleConfiguration",
                "elasticfilesystem:DescribeMountTargets",
                "elasticfilesystem:DescribeReplicationConfigurations",
                "elasticloadbalancing:DescribeListeners",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "fis:GetExperiment",
                "fis:GetExperimentTemplate",
                "fis:ListExperiments",
                "fis:ListExperimentResolvedTargets",
                "fis:ListExperimentTemplates",
                "fsx:DescribeFileSystems",
                "lambda:GetFunctionConcurrency",
                "lambda:GetFunctionConfiguration",
                "lambda:ListAliases",
                "lambda:ListEventSourceMappings",
                "lambda:ListFunctionEventInvokeConfigs",
                "lambda:ListVersionsByFunction",
                "rds:DescribeDBClusterSnapshots",
                "rds:DescribeDBClusters",
                "rds:DescribeDBInstanceAutomatedBackups",
                "rds:DescribeDBInstances",
                "rds:DescribeDBProxies",
```

```
                "rds:DescribeDBProxyTargets",
                "rds:DescribeDBSnapshots",
                "rds:DescribeGlobalClusters",
                "rds:ListTagsForResource",
                "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:ListBucket",
                "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": "*"
        },
        {
            "Sid": "AWSResilienceHubApiGatewayStatement",
            "Effect": "Allow",
            "Action": [
                "apigateway:GET"
            ],
            "Resource": [
                "arn:aws:apigateway:*::/apis/*",
                "arn:aws:apigateway:*::/restapis/*",
                "arn:aws:apigateway:*::/usageplans"
```

```
            ]
        },
        {
            "Sid": "AWSResilienceHubS3ArtifactStatement",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:PutObject",
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::aws-resilience-hub-artifacts-*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "AWSResilienceHubS3AccessStatement",
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
                "s3:GetBucketLogging",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketTagging",
                "s3:GetBucketVersioning",
                "s3:GetMultiRegionAccessPointRoutes",
                "s3:GetReplicationConfiguration",
                "s3:ListAllMyBuckets",
                "s3:ListMultiRegionAccessPoints"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "AWSResilienceHubCloudWatchStatement",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
```

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

AWS Resilience Hub 受 AWS 管政策的更新

檢視自此服務開始追蹤這些變更 AWS Resilience Hub 以來， AWS 受管政策更新的詳細資訊。如需此頁面變更的自動提醒，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 – 變更	AWS Resilience Hub 已更新 `AWSResilienceHubAssessmentExecutionPolicy` 以授予 `List`和 `Get`許可，讓您可在執行評估 AWS FIS 時從 存取實驗。	2024 年 12 月 17 日
AWSResilienceHubAssessmentExecutionPolicy – 變更	AWS Resilience Hub 已更新 `AWSResilienceHubAssessmentExecutionPolicy` 以授予`Describe`許可，讓您在執行評估時存取 Amazon ElastiCache (Redis	2024 年 9 月 25 日

變更	描述	日期
	OSS) Serverless 上的資源和組態。	
AWSResilienceHubAssessmentExecutionPolicy – 變更	AWS Resilience Hub 已更新 `AWSResilienceHubAssessmentExecutionPolicy` 以授予`Describe`許可，讓您存取 Amazon DocumentDB、Elastic Load Balancing 和執行評估 AWS Lambda 時的資源和組態。	2024 年 8 月 1 日
AWSResilienceHubAssessmentExecutionPolicy – 變更	AWS Resilience Hub 已更新 `AWSResilienceHubAssessmentExecutionPolicy` 以授予`Describe`許可，讓您在執行評估時讀取 Amazon FSx for Windows File Server 組態。	2024 年 3 月 26 日
AWSResilienceHubAssessmentExecutionPolicy – 變更	AWS Resilience Hub 已更新 `AWSResilienceHubAssessmentExecutionPolicy` 以授予`Describe`許可，讓您在執行評估時讀取 AWS Step Functions 組態。	2023 年 10 月 30 日
AWSResilienceHubAssessmentExecutionPolicy – 變更	AWS Resilience Hub 已更新 `AWSResilienceHubAssessmentExecutionPolicy` 以授予`Describe`許可，讓您在執行評估時存取 Amazon RDS 上的資源。	2023 年 10 月 5 日

變更	描述	日期
AWSResilienceHubAssessmentExecutionPolicy – 新的	此 AWS Resilience Hub 政策提供其他 AWS 服務的存取權，以執行評估。	2023 年 6 月 26 日
AWS Resilience Hub 已開始追蹤變更	AWS Resilience Hub 已開始追蹤其 AWS 受管政策的變更。	2023 年 6 月 15 日

AWS Resilience Hub 角色和 IAM 許可參考

您可以使用 AWS Resilience Hub `AWSResilienceHubAsssessmentExecutionPolicy` AWS 受管政策和下列其中一個角色特定政策，將 IAM 許可授予使用 所需的角色。如需 AWS 受管政策的詳細資訊，請參閱 the section called “AWSResilienceHubAsssessmentExecutionPolicy”。

以下建議的角色政策 AWS Resilience Hub：

- 基礎設施應用程式管理員角色的 IAM 許可
- Business continuity Manager 角色的 IAM 許可
- 應用程式擁有者角色的 IAM 許可
- 授予唯讀存取權的 IAM 許可

基礎設施應用程式管理員角色的 IAM 許可

下列政策授予基礎設施應用程式管理員角色所需的必要許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "InfrastructureApplicationManager",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:AddDraftAppVersionResourceMappings",
        "resiliencehub:CreateAppVersionAppComponent",
        "resiliencehub:CreateAppVersionResource",
        "resiliencehub:CreateRecommendationTemplate",
        "resiliencehub:DeleteAppAssessment",
        "resiliencehub:DeleteAppInputSource",
```

```
        "resiliencehub:DeleteAppVersionAppComponent",
        "resiliencehub:DeleteAppVersionResource",
        "resiliencehub:DeleteRecommendationTemplate",
        "resiliencehub:Describe*",
        "resiliencehub:List*",
        "resiliencehub:PublishAppVersion",
        "resiliencehub:PutDraftAppVersionTemplate",
        "resiliencehub:RemoveDraftAppVersionResourceMappings",
        "resiliencehub:ResolveAppVersionResources",
        "resiliencehub:StartAppAssessment",
        "resiliencehub:TagResource",
        "resiliencehub:UntagResource",
        "resiliencehub:UpdateAppVersion",
        "resiliencehub:UpdateAppVersionAppComponent",
        "resiliencehub:UpdateAppVersionResource"
      ],
      "Resource": "*"
    }
  ]
}
```

Business continuity Manager 角色的 IAM 許可

下列政策會授予業務持續性管理員角色所需的必要許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "BusinessContinuityManager",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:CreateResiliencyPolicy",
        "resiliencehub:DeleteResiliencyPolicy",
        "resiliencehub:Describe*",
        "resiliencehub:List*",
        "resiliencehub:ResolveAppVersionResources",
        "resiliencehub:TagResource",
        "resiliencehub:UntagResource",
        "resiliencehub:UpdateAppVersion",
        "resiliencehub:UpdateAppVersionAppComponent",
        "resiliencehub:UpdateAppVersionResource",
        "resiliencehub:UpdateResiliencyPolicy"
```

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

應用程式擁有者角色的 IAM 許可

下列政策會授予應用程式擁有者角色所需的必要許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ApplicationOwner",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:AddDraftAppVersionResourceMappings",
        "resiliencehub:BatchUpdateRecommendationStatus",
        "resiliencehub:CreateApp",
        "resiliencehub:CreateAppVersionAppComponent",
        "resiliencehub:CreateAppVersionResource",
        "resiliencehub:CreateRecommendationTemplate",
        "resiliencehub:CreateResiliencyPolicy",
        "resiliencehub:DeleteApp",
        "resiliencehub:DeleteAppAssessment",
        "resiliencehub:DeleteAppInputSource",
        "resiliencehub:DeleteAppVersionAppComponent",
        "resiliencehub:DeleteAppVersionResource",
        "resiliencehub:DeleteRecommendationTemplate",
        "resiliencehub:DeleteResiliencyPolicy",
        "resiliencehub:Describe*",
        "resiliencehub:ImportResourcesToDraftAppVersion",
        "resiliencehub:List*",
        "resiliencehub:PublishAppVersion",
        "resiliencehub:PutDraftAppVersionTemplate",
        "resiliencehub:RemoveDraftAppVersionResourceMappings",
        "resiliencehub:ResolveAppVersionResources",
        "resiliencehub:StartAppAssessment",
        "resiliencehub:TagResource",
        "resiliencehub:UntagResource",
        "resiliencehub:UpdateApp",
        "resiliencehub:UpdateAppVersion",
```

```
        "resiliencehub:UpdateAppVersionAppComponent",
        "resiliencehub:UpdateAppVersionResource",
        "resiliencehub:UpdateResiliencyPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

授予唯讀存取權的 IAM 許可

下列政策會授予唯讀存取所需的必要許可。

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

將 Terraform 狀態檔案匯入至 AWS Resilience Hub

AWS Resilience Hub 支援匯入使用伺服器端加密 (SSE) 搭配 Amazon Simple Storage Service 受管金鑰 (SSE-S3) 或使用受管金鑰 (SSE-KMS) 加密的 AWS Key Management Service Terraform 狀態檔案。如果您的 Terraform 狀態檔案是使用客戶提供的加密金鑰 (SSE-C) 進行加密，您將無法使用 匯入它們 AWS Resilience Hub。

匯入 Terraform 狀態檔案到 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。

從主要帳戶中的 Amazon S3 儲存貯體匯入 Terraform 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 讀取位於主要帳戶 Amazon S3 儲存貯體中的 Terraform 狀態檔案。

- 儲存貯體政策 – 位於主要帳戶中的目標 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，或主要 AWS 帳戶 AWS Resilience Hub 上 AWS 目前 IAM 角色的關聯身分政策。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**
>
> 如果您使用的是 AWSResilienceHubAsssessmentExecutionPolicy 受管政策，則不需要 ListBucket 許可。

> **Note**
>
> 如果您的 Terraform 狀態檔案使用 KMS 加密，您必須新增下列kms:Decrypt許可。
>
> ```
> {
>       "Effect": "Allow",
>       "Action": [
>               "kms:Decrypt",
>       ],
>       "Resource": "<arn_of_kms_key>"
> }
> ```

從次要帳戶中的 Amazon S3 儲存貯體匯入 Terraform 狀態檔案

- 儲存貯體政策 – 位於目標 Amazon S3 儲存貯體上的儲存貯體政策，位於其中一個次要帳戶。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>"
    }
  ]
}
```

- 身分政策 – 帳戶角色的 AWS 關聯身分政策，在主要 AWS 帳戶 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**
>
> 如果您使用的是 AWSResilienceHubAsssessmentExecutionPolicy 受管政策，則不需要 ListBucket 許可。

> **Note**
>
> 如果您的 Terraform 狀態檔案使用 KMS 加密，您必須新增下列kms:Decrypt許可。
>
> ```
> {
>       "Effect": "Allow",
>       "Action": [
>               "kms:Decrypt",
>       ],
>       "Resource": "<arn_of_kms_key>"
> }
> ```

啟用對 Amazon Elastic Kubernetes Service 叢集的 AWS Resilience Hub 存取

AWS Resilience Hub 透過分析 Amazon EKS 叢集的基礎設施來評估 Amazon Elastic Kubernetes Service (Amazon EKS) 叢集的彈性。 AWS Resilience Hub 使用 Kubernetes 角色型存取控制 (RBAC) 組態來評估其他 Kubernetes (K8) 工作負載，這些工作負載會部署為 Amazon EKS 叢集的一部分。若要 AWS Resilience Hub 讓 查詢您的 Amazon EKS 叢集以分析和評估工作負載，您必須完成下列操作：

- 在與 Amazon EKS 叢集相同的帳戶中建立或使用現有 AWS Identity and Access Management (IAM) 角色。
- 啟用 IAM 使用者和角色存取 Amazon EKS 叢集，並授予其他唯讀許可給 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的叢集 - Amazon EKS。

使用 IAM 實體存取 Amazon EKS 叢集是由 AWS IAM Authenticator for Kubernetes 啟用，該 Kubernetes 會在 Amazon EKS 控制平面上執行。驗證器會從 取得組態資訊`aws-auth ConfigMap`。

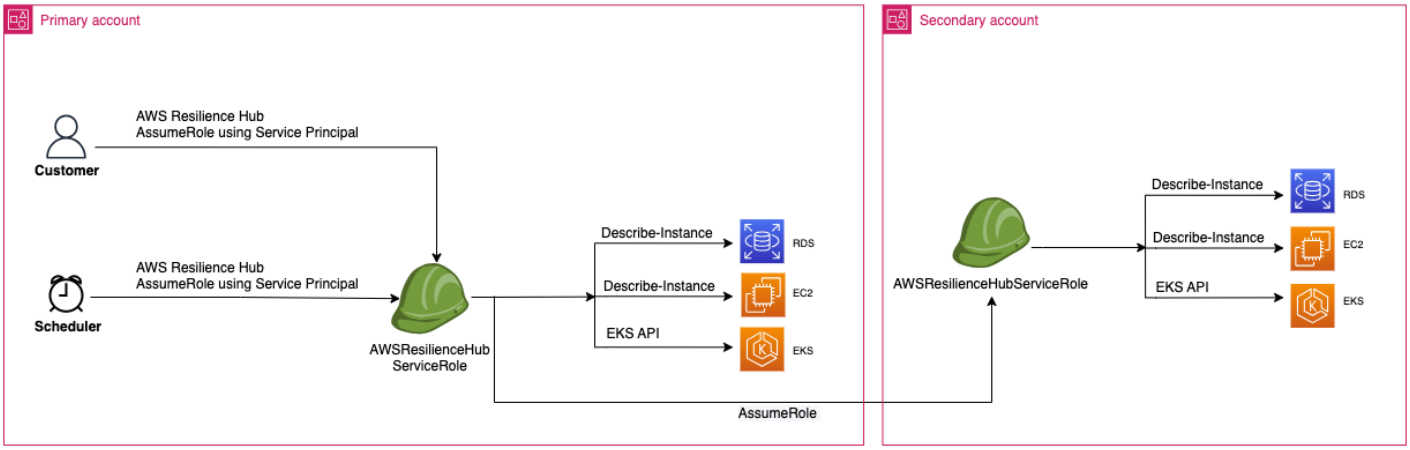
> **Note**
>
> - 如需所有`aws-auth ConfigMap`設定的詳細資訊，請參閱 GitHub 上的完整組態格式。
> - 如需不同 IAM 身分的詳細資訊，請參閱《IAM 使用者指南》中的身分（使用者、群組和角色）。
> - 如需 Kubernetes 角色型存取控制 (RBAC) 組態的詳細資訊，請參閱使用 RBAC 授權。

AWS Resilience Hub 會使用帳戶中的 IAM 角色查詢 Amazon EKS 叢集內的資源。若要 AWS Resilience Hub 讓 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的 Kubernetes 群組，以存取 Amazon EKS 叢集內的資源。

AWS Resilience Hub 允許 使用下列其中一個 IAM 角色選項來存取您的 Amazon EKS 叢集資源：

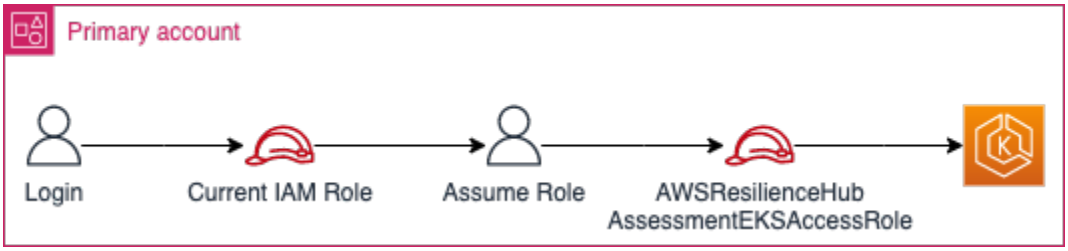
- 如果您的應用程式設定為使用角色型存取來存取資源，則在建立應用程式時傳遞給 AWS Resilience Hub 的叫用者角色或次要帳戶角色，將用於在評估期間存取您的 Amazon EKS 叢集。

  下列概念圖顯示應用程式設定為角色型應用程式時，如何 AWS Resilience Hub 存取 Amazon EKS 叢集。

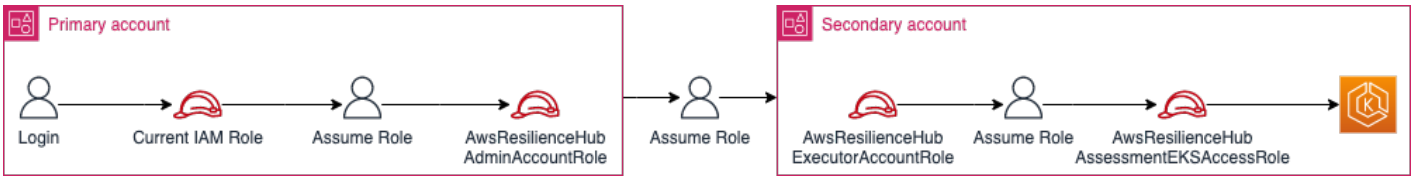


- 如果您的應用程式設定為使用目前的 IAM 使用者存取資源，則必須在`AwsResilienceHubAssessmentEKSAccessRole`與 Amazon EKS 叢集相同的帳戶中建立名稱為 的新 IAM 角色。然後，此 IAM 角色將用於存取您的 Amazon EKS 叢集。

  下列概念圖顯示當應用程式設定為使用目前的 IAM 使用者許可時， 如何 AWS Resilience Hub 存取部署在您主要帳戶中的 Amazon EKS 叢集。



下列概念圖顯示當應用程式設定為使用目前的 IAM 使用者許可時， 如何 AWS Resilience Hub 存取部署在次要帳戶上的 Amazon EKS 叢集。



授予 Amazon EKS 叢集中資源的 AWS Resilience Hub 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。

將探索和評估 AWS Resilience Hub Amazon EKS 叢集內資源所需的許可授予

1. 設定 IAM 角色以存取 Amazon EKS 叢集。

   如果您已使用角色型存取來設定應用程式，您可以略過此步驟並繼續步驟 2，並使用您用來建立應用程式的角色。如需如何使用 AWS Resilience Hub IAM 角色的詳細資訊，請參閱the section called “AWS Resilience Hub 如何與 IAM 搭配使用”。

   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 `AwsResilienceHubAssessmentEKSAccessRole` Amazon EKS 叢集相同的帳戶中建立 IAM 角色。存取 Amazon EKS 叢集時，將會使用此 IAM 角色。

   在匯入和評估應用程式時， AWS Resilience Hub 會使用 IAM 角色來存取 Amazon EKS 叢集中的資源。此角色應與 Amazon EKS 叢集在相同的帳戶中建立，並將與包含 AWS Resilience Hub 評估 Amazon EKS 叢集所需許可的 Kubernetes 群組對應。

   如果您的 Amazon EKS 叢集與 AWS Resilience Hub 呼叫帳戶位於同一個帳戶中，應使用下列 IAM 信任政策來建立角色。在此 IAM 信任政策中， `caller_IAM_role` 會用於目前 帳戶中以呼叫 APIs AWS Resilience Hub。

> **Note**
>
> 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"
    }
  ]
}
```

如果您的 Amazon EKS 叢集位於跨帳戶 （與 AWS Resilience Hub 呼叫帳戶不同的帳戶），您必須使用以下 AwsResilienceHubAssessmentEKSAccessRole IAM 信任政策建立 IAM 角色：

> **Note**
>
> 作為先決條件，若要存取部署在 AWS Resilience Hub 與使用者帳戶不同的帳戶中的 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`並將`ClusterRoleBinding`授予 所需的唯讀許可， AWS Resilience Hub 以分析和評估屬於 Amazon EKS 叢集中特定命名空間一部分的資源。

   AWS Resilience Hub 可讓您完成下列其中一項，以限制對命名空間的存取，以產生彈性評估：

   a. 授予應用程式所有命名空間的 AWS Resilience Hub 讀取存取權。

      若要 AWS Resilience Hub 讓 評估 Amazon EKS 叢集內所有命名空間的資源彈性，您必須建立下列 `ClusterRole`和 `ClusterRoleBinding`。

      - `resilience-hub-eks-access-cluster-role` (`ClusterRole`) – 定義 AWS Resilience Hub 評估 Amazon EKS 叢集所需的許可。
      - `resilience-hub-eks-access-cluster-role-binding` (`ClusterRoleBinding`) – 定義 Amazon EKS 叢集`resilience-hub-eks-access-group`中名為 的群組，授予其使用者在 中執行彈性評估所需的許可 AWS Resilience Hub。

      授予 AWS Resilience Hub 應用程式所有命名空間讀取存取權的範本如下：

```
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
    - nodepools
  verbs:
    - get
    - list
- apiGroups:
    - karpenter.k8s.aws
  resources:
    - awsnodetemplates
    - ec2nodeclasses
  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. 授予讀取特定命名空間的 AWS Resilience Hub 存取權。

您可以使用 限制 AWS Resilience Hub 存取特定命名空間集中的資源RoleBinding。若要達成此目的，您必須建立下列角色：

- ClusterRole – 若要 AWS Resilience Hub 讓 存取 Amazon EKS 叢集中特定命名空間中的資源並評估其彈性，您必須建立下列ClusterRole角色。
  - resilience-hub-eks-access-cluster-role – 指定評估特定命名空間內資源的必要許可。
  - resilience-hub-eks-access-global-cluster-role – 指定在 Amazon EKS 叢集中評估叢集範圍資源的必要許可，這些資源不會與特定命名空間相關聯。 AWS Resilience Hub 需要存取 Amazon EKS 叢集上叢集範圍資源 （例如節點） 的許可，才能評估應用程式的彈性。

建立ClusterRole角色的範本如下所示：

```
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
      - nodepools
    verbs:
      - get
      - list
  - apiGroups:
      - karpenter.k8s.aws
    resources:
      - awsnodetemplates
      - ec2nodeclasses
    verbs:
      - get
      - list

---
EOF
```

- RoleBinding 角色 – 此角色授予 所需的許可 AWS Resilience Hub ，以存取特定命名空間內的資源。也就是說，您必須在每個命名空間中建立RoleBinding角色，讓 AWS Resilience Hub 存取指定命名空間內的資源。

> **Note**
>
> 如果您使用 ClusterAutoscaler進行自動擴展，則必須在 RoleBinding中另外建立 kube-system。這是評估 的必要項目ClusterAutoscaler，這是 kube-system 命名空間的一部分。
> 透過這樣做，您將授予 AWS Resilience Hub 必要的許可，以評估kube-system命名空間內的資源，同時評估 Amazon EKS 叢集。

建立RoleBinding角色的範本如下所示：

```
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 角色 – 此角色授予 AWS Resilience Hub 存取叢集範圍資源所需的許可。

  建立ClusterRoleBinding角色的範本如下所示：

```
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，將 resilience-hub-eks-access-group 對應至用於存取 Amazon EKS 叢集的 IAM 角色。

此步驟會在步驟 1 中使用的 IAM 角色與步驟 2 中建立的 Kubernetes 群組之間建立映射。此映射會將許可授予 IAM 角色，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角色型存取，該角色應該是叫用者角色，或在建立應用程式 AWS Resilience Hub 時傳遞給 的次要帳戶角色。
>   - 如果您的應用程式設定為使用目前的 IAM 使用者來存取資源，則它必須是 AwsResilienceHubAssessmentEKSAccessRole。
> - ACCOUNT-ID 應為 Amazon EKS 叢集 AWS 的帳戶 ID。

您可以使用下列aws-authConfigMap其中一種方式建立 ：

- 使用 eksctl

  使用下列命令來更新 aws-auth ConfigMap：

  ```
  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
  ```

- 您可以手動編輯aws-authConfigMap，方法是將 IAM 角色詳細資訊新增至資料ConfigMap下的 mapRoles區段。使用下列命令來編輯 aws-auth ConfigMap。

  ```
  kubectl edit -n kube-system configmap/aws-auth
  ```

  mapRoles 區段包含下列參數：

  - rolearn – 要新增之 IAM 角色的 Amazon Resource Name (ARN)。
    - ARN 語法 – arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>。
  - username – 要映射至 IAM 角色的 Kubernetes 內使用者名稱 (AwsResilienceHubAssessmentEKSAccessRole)。

- groups – 群組名稱應與步驟 2 () 中建立的群組名稱相符resilience-hub-eks-access-group。

> **Note**
>
> 如果mapRoles區段不存在，您必須手動新增此區段。

使用下列範本，將 IAM 角色詳細資訊新增至資料ConfigMap下的 mapRoles區段。

```
- groups:
  - resilience-hub-eks-access-group
  rolearn: arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>
  username: AwsResilienceHubAssessmentEKSAccessRole
```

啟用 AWS Resilience Hub 以發佈到您的 Amazon Simple Notification Service 主題

本節說明如何啟用 AWS Resilience Hub ，將應用程式的相關通知發佈至您的 Amazon Simple Notification Service (Amazon SNS) 主題。若要將通知推送至 Amazon SNS 主題，請確定您有下列項目：

- 作用中 AWS Resilience Hub 的應用程式。
- 必須 AWS Resilience Hub 傳送通知的現有 Amazon SNS 主題。如需建立 Amazon SNS 主題的詳細資訊，請參閱建立 Amazon SNS 主題。

若要讓 AWS Resilience Hub 將通知發佈到您的 Amazon SNS 主題，您必須使用下列內容更新 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 將訊息從選擇加入區域發佈到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 `resiliencehub.amazonaws.com`變更為 `resiliencehub.<opt-in-region>.amazonaws.com`。

如果您使用的是伺服器端加密 (SSE) Amazon SNS 主題，您必須確保 AWS Resilience Hub 具有 `Decrypt`和 `GenerateDataKey*` 對 Amazon SNS 加密金鑰的存取權。

若要提供 `Decrypt`和 的`GenerateDataKey*`存取權 AWS Resilience Hub，您必須包含下列 AWS Key Management Service 存取政策的許可。

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

限制納入或排除 AWS Resilience Hub 建議的許可

AWS Resilience Hub 可讓您限制許可，以包含或排除每個應用程式的建議。您可以使用下列 IAM 信任政策，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， `caller_IAM_role`（與您的 AWS 使用者帳戶相關聯） 會用於目前 帳戶，以呼叫 APIs 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"
    }
  ]
}
```

中的基礎設施安全性 AWS Resilience Hub

作為受管服務， AWS Resilience Hub 受到 Amazon Web Services：安全程序概觀白皮書中所述 AWS 的全球網路安全程序的保護。

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

AWS 服務的彈性檢查

本章提供 AWS Resilience Hub 為支援 AWS 的服務執行的各種彈性檢查的詳細資訊，以確保應用程式的彈性狀態不受影響。這些檢查會根據每個應用程式元件 (AppComponent) 彈性政策中定義的值，預估復原時間目標 (RTO) 和復原點目標 (RPO)。評估包含不同類型的中斷，即應用程式、基礎設施故障、可用區域中斷和區域故障。不過，若要執行這些檢查，您必須提供相關的 IAM 許可給 AWS Resilience Hub ，以允許其存取您的 資源。若要進一步了解允許 AWS Resilience Hub 存取您的資源並執行本章中的復原能力檢查所需的 IAM 許可，請參閱 AWS 的 受管政策 AWS Resilience Hub。

AWS 服務

- Amazon Elastic File System
- Amazon Relational Database Service 和 Amazon Aurora
- Amazon Simple Storage Service
- Amazon DynamoDB
- Amazon Elastic Compute Cloud
- Amazon EBS
- AWS Lambda
- Amazon Elastic Kubernetes Service
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- Amazon Elastic Container Service
- Elastic Load Balancing
- Amazon API Gateway
- Amazon DocumentDB
- NAT 閘道
- Amazon Route 53
- Amazon Application Recovery Controller (ARC)
- Amazon FSx for Windows File Server
- AWS Step Functions
- Amazon ElastiCache (Redis OSS)

Amazon Elastic File System

本節列出 Amazon Elastic File System 特有的所有彈性檢查和建議。如需 Amazon Elastic File System 的詳細資訊，請參閱 Amazon Elastic File System 文件。

檔案系統類型

AWS Resilience Hub 會檢查檔案系統類型：區域或單區域。檔案系統類型會影響其在基礎設施或可用區域中斷時的彈性。如需檔案系統類型的詳細資訊，請參閱 Amazon EFS 檔案系統的可用性和耐久性。

檔案系統備份

AWS Resilience Hub 會檢查是否已為部署的檔案系統定義 AWS Backup 計劃。此外，它會驗證`Cross-Region`備份選項是否已啟用，確保政策需要時涵蓋區域層級中斷。

資料複寫

AWS Resilience Hub 會檢查是否已為部署的檔案系統定義區域內或跨區域 Amazon EFS 資料複寫。Amazon EFS 資料複寫有助於改善應用程式、基礎設施、AZ 和區域層級的預估 RTO 和預估 RPO。此外， 會 AWS Resilience Hub 檢查它是否與區域內的 結合 AWS Backup ，以便在應用程式中斷時啟用檔案系統彈性。

Amazon Relational Database Service 和 Amazon Aurora

本節列出 Amazon Relational Database Service 和 Amazon Aurora 特有的所有彈性檢查和建議。如需 Amazon Relational Database Service 和 Amazon Aurora 的詳細資訊，請參閱 Amazon Relational Database Service 文件。

單一可用區部署

AWS Resilience Hub 會檢查資料庫是否部署為單一執行個體，如果確定，則表示資料庫不支援次要執行個體和僅供讀取複本。

Multi-AZ deployment (異地同步備份部署)

AWS Resilience Hub 會檢查資料庫是否與次要執行個體或僅供讀取複本一起部署。如果使用僅供讀取複本部署資料庫， 會 AWS Resilience Hub 驗證其是否部署在不同 AZ 中，以便在 AZ 中斷時允許容錯移轉。

備份

AWS Resilience Hub 會檢查下列備份功能是否套用至部署的資料庫執行個體。

- AWS Backup 具有自動備份選項的計劃
- AWS Backup 如果您的政策要求，則使用跨區域備份複本進行規劃
- 第三方備份系統的手動快照

跨區域容錯移轉

AWS Resilience Hub 會檢查彈性政策中定義的 RTO 和 RPO 目標，以從區域中斷中復原。此外，AWS Resilience Hub 可以識別下列跨區域架構，以涵蓋區域中斷：

- 具有跨區域快照副本的區域內備份
- 另一個區域中的僅供讀取複本
- 在另一個區域中具有次要叢集的 Amazon Aurora 全域資料庫
- Amazon Aurora 全域資料庫，在另一個區域中具有無周邊次要叢集

更快速的區域內容錯移轉

AWS Resilience Hub 在基礎設施或 AZ 中斷期間， 會檢查彈性政策中定義的 RTO 和 RPO 目標。此外， AWS Resilience Hub 可以識別下列區域內架構，以涵蓋應用程式、基礎設施和可用區域中斷：

- 區域備份
- 不同 AZ 中的僅供讀取複本
- 在另一個 AZ 中具有僅供讀取複本的 Aurora 叢集
- Amazon Relational Database Service (Amazon RDS) 的異地同步備份執行個體
- Amazon RDS 多可用區域叢集
- 在另一個 AZ 中具有僅供讀取複本的 Amazon RDS 單一執行個體

Amazon Simple Storage Service

本節列出 Amazon Simple Storage Service (Amazon S3) 特有的所有彈性檢查和建議。如需 Amazon S3 的詳細資訊，請參閱 Amazon S3 文件。

版本控制

AWS Resilience Hub 驗證 Amazon S3 儲存貯體是否已設定已啟用版本控制。

排程備份

AWS Resilience Hub 會檢查是否已為部署的 Amazon Simple Storage Service (Amazon S3) 儲存貯體定義 AWS Backup 計劃。此外，它也會檢查您的政策是否需要涵蓋區域層級中斷，是否已啟用跨區域備份選項。

時間點復原

AWS Resilience Hub 會檢查彈性政策的 RPO 目標是否需要point-in-time復原 (PITR)。不過，PITR 不支援跨區域備份。因此，您可以使用已啟用跨區域備份選項的現有排程 AWS Backup 計劃，或建立新的排程計劃。

資料複寫

AWS Resilience Hub 會檢查是否已為部署的 Amazon S3 儲存貯體定義相同的區域複寫 (SRR) 和跨區域複寫 (CRR)。Amazon S3 資料複寫可在應用程式、基礎設施、可用區域和區域層級改善預估工作負載 RTO 和預估工作負載 RPO。此外，它還可以保護物件免於實體刪除，因為刪除物件版本不會複寫到目標 Amazon S3 儲存貯體。此外，根據彈性政策中定義的 RTO 目標， 會 AWS Resilience Hub 檢查是否應啟用 Amazon S3 複寫時間控制 (S3 RTC)。此計費功能會在 15 分鐘內複寫 99.99% 的來源儲存貯體物件。

- AWS Backup 具有自動備份選項的計劃
- AWS Backup 如果您的政策要求，則使用跨區域備份複本進行規劃
- 第三方備份系統的手動快照

Amazon DynamoDB

本節列出 Amazon DynamoDB 特有的所有彈性檢查和建議。如需 Amazon DynamoDB 的詳細資訊，請參閱 Amazon DynamoDB 文件。

排程備份

AWS Resilience Hub 會檢查是否已為部署的資料表定義備份。此外，它也會檢查是否需要為您的政策設定跨區域備份，以涵蓋區域層級中斷。

時間點復原

AWS Resilience Hub 會根據彈性政策的 RPO 目標，檢查是否需要point-in-time復原 (PITR)。不過，PITR 不支援跨區域備份。因此，您可以使用已啟用跨區域備份選項的現有排程 AWS Backup 計劃，或建立新的排程計劃。

全域資料表

AWS Resilience Hub 會檢查部署的 Amazon DynamoDB 資料表是否定義為在其他區域中具有一或多個複本的全域資料表。設定全域資料表可改善區域層級的預估工作負載 RTO 和預估工作負載 RPO，也提供在主動主動主動或主動被動多區域模式中運作的功能。 AWS Backup 或 Amazon DynamoDB PITR 可用於其中一個區域來處理應用程式中斷。

Amazon Elastic Compute Cloud

本節列出 Amazon Elastic Compute Cloud 特有的所有彈性檢查和建議。如需 Amazon Elastic Compute Cloud 的詳細資訊，請參閱 Amazon Elastic Compute Cloud 文件。

狀態執行個體

AWS Resilience Hub 如果符合下列其中一項條件， 會將 Amazon EC2 執行個體識別為具狀態執行個體：

- 如果`DeleteOnTermination`至少有一個連接至此執行個體的 Amazon Elastic Block Store (Amazon EBS) 磁碟區屬性設定為 false。
- 如果 Amazon Data Lifecycle Manager 或 AWS Backup 計劃連接到 Amazon EC2 執行個體或至少一個 Amazon EBS 磁碟區。
- 如果 AWS Elastic Disaster Recovery 用於複寫 Amazon EC2 執行個體儲存磁碟區。

> **Note**
>
> 如果 Amazon EC2 執行個體不符合上述任何條件， 會 AWS Resilience Hub 將其視為無狀態 Amazon EC2 執行個體。

Auto Scaling 群組

AWS Resilience Hub 會檢查無狀態 Amazon EC2 執行個體群組。如果發現，建議使用具有多可用區域組態的 Auto Scaling 群組 (ASG) 來協調相同的 。如果已識別現有的 ASG，ARH 將驗證是否已跨多個可用區域設定它。如果 ASG 也只使用 Spot Amazon EC2 執行個體定義，建議您使用隨需 Amazon EC2 執行個體增加其容量，以在 Spot Amazon EC2 執行個體無法使用時改善彈性。

Amazon EC2 機群

AWS Resilience Hub 可識別 Amazon EC2 機群，並驗證其是否定義為異地同步備份部署，以及是否僅使用 Spot Amazon EC2 執行個體。將 Amazon EC2 機群定義為異地同步備份部署，可改善異地同步備份中斷時的彈性。當 Spot 執行個體無法使用時，使用隨需執行個體增強 Amazon EC2 機群可改善其彈性。

Amazon EBS

本節列出 Amazon EBS 特有的所有彈性檢查和建議。如需 Amazon EBS 的詳細資訊，請參閱 Amazon EBS 文件。

排程備份

AWS Resilience Hub 會檢查是否已為您的 Amazon EBS 磁碟區定義下列其中一項或兩項。

- 連接至 Amazon EC2 執行個體之特定 Amazon EBS 磁碟區的備份規則。
- 將 Amazon EBS 後端 AMI 建立至 Amazon EC2 執行個體的備份規則。
- 第三方備份系統的手動快照。

此外，如果您的政策需要涵蓋區域層級中斷， 會 AWS Resilience Hub 檢查您的備份規則是否已啟用跨區域備份選項。

資料備份和複寫

AWS Resilience Hub 如果符合下列其中一項條件，則 Amazon EBS 磁碟區會被視為具狀態磁碟區：

- 如果此 Amazon EBS 磁碟區的`DeleteOnTermination`屬性設定為 false。
- 如果 Amazon Data Lifecycle Manager 或 AWS Backup 計劃與此 Amazon EBS 磁碟區或 Amazon EC2 執行個體相關聯，則會連接至該磁碟區或 Amazon EC2 執行個體。
- 如果 AWS Elastic Disaster Recovery 用於複寫 Amazon EC2 執行個體儲存磁碟區。

AWS Lambda

本節列出特定的所有彈性檢查和建議 AWS Lambda。如需詳細資訊 AWS Lambda，請參閱 AWS Lambda 文件。

客戶 Amazon VPC 存取

AWS Resilience Hub 識別連線至 VPC 的 AWS Lambda 函數。 AWS Lambda 連線至 Amazon VPC 不同AZs子網路，可在發生可用區域中斷時允許函數彈性。

無效字母佇列

AWS Resilience Hub 會檢查 AWS Lambda 函數是否連接無效字母佇列 (DLQ)，以儲存失敗的請求。將 DLQ 連接至 AWS Lambda 函數可讓 防止請求的資料遺失，並重試在稍後階段處理失敗的請求。

Amazon Elastic Kubernetes Service

本節列出 Amazon Elastic Kubernetes Service (Amazon EKS) 特有的所有彈性檢查和建議。如需 Amazon EKS 的詳細資訊，請參閱 Amazon EKS 文件。

Multi-AZ deployment (異地同步備份部署)

AWS Resilience Hub 識別 Pod 部署是否在多個 AZs 中的多個工作者節點上執行。如果您的彈性政策在區域中斷時需要涵蓋範圍，則需要在另一個區域中使用額外的 Amazon EKS 叢集。此額外的 Amazon EKS 叢集也會針對分佈在多個 AZs 中多個工作者節點之間的 Pod 部署進行驗證。

部署與 ReplicaSet

AWS Resilience Hub 會檢查您是否使用 ReplicaSets 或 Pod 物件，而非部署。將 ReplicaSets 或 Pod 物件取代為部署，可簡化新版本軟體的 Pod 更新，並包含其他實用功能。

部署維護

AWS Resilience Hub 會檢查下列最佳實務是否用於部署：

- 使用 Pod 中斷預算 (PDB) – 使用 PDB 可透過設定工作負載中 Pod 數量的限制，在任何指定時間中斷，來改善可用性。
- 將自我管理節點群組取代為 Amazon EKS 受管節點群組 – 此取代可簡化維護期間的工作者節點映像更新。

- 支援每個部署的動態 CPU 和記憶體請求 – 這些請求可協助 Kubernetes 選擇符合 Pod 需求的節點。
- 為所有容器設定即時性和準備度探查 – 設定即時性探查有助於透過重新啟動非功能 Pod 來改善復原能力。設定準備程度探查可讓您將流量從忙碌的 Pod 中轉移來改善可用性。
- 設定 Karpenter、Cluster Autoscaler 或 AWS Fargate – 這些組態可讓 Amazon EKS 叢集的基礎設施成長並滿足工作負載需求。
- 設定水平 Pod Autoscaler – 此組態可協助 Amazon EKS 叢集自動擴展工作負載，以滿足請求處理需求。

Amazon Simple Notification Service

本節列出 Amazon Simple Notification Service (Amazon SNS) 特有的所有彈性檢查和建議。如需 Amazon SNS 的詳細資訊，請參閱 Amazon SNS 文件。

主題訂閱

AWS Resilience Hub 會檢查 Amazon SNS 主題是否至少連接 1 個訂閱，以確保傳入的訊息不會遺失。

Amazon Simple Queue Service

本節列出 Amazon Simple Queue Service (Amazon SQS) 特有的所有彈性檢查和建議。如需 Amazon SQS 的詳細資訊，請參閱 Amazon SQS 文件。

無效字母佇列

AWS Resilience Hub 會檢查 Amazon SQS 佇列是否有與其相關聯的 DLQ，以處理無法成功交付給訂閱用戶的訊息。

Amazon Elastic Container Service

本節列出 Amazon Elastic Container Service (Amazon ECS) 特有的所有彈性檢查和建議。如需 Amazon ECS 的詳細資訊，請參閱 Amazon ECS 文件。

Multi-AZ deployment (異地同步備份部署)

AWS Resilience Hub 根據 Amazon EC2 或啟動類型，檢查 Amazon ECS 任務或服務是否在多個 AZs 中執行。 AWS Fargate 如果您的政策需要區域中斷的涵蓋範圍，則需要在另一個區域中使用額外的 Amazon ECS 叢集。其他叢集也會經過驗證，以便在多個 AZs 中執行任務或服務。

Elastic Load Balancing

本節列出 Elastic Load Balancing 特有的所有彈性檢查和建議。如需 Elastic Load Balancing 的詳細資訊，請參閱 Elastic Load Balancing 文件。

Multi-AZ deployment (異地同步備份部署)

AWS Resilience Hub 會檢查 Elastic Load Balancing 是否在多個 AZs 中執行。

如果您的政策需要區域中斷的涵蓋範圍，則需要在不同的區域中使用額外的 Elastic Load Balancing。其他 Elastic Load Balancing 位於不同區域，也會針對其在多個 AZs 中的部署進行驗證。

Amazon API Gateway

本節列出 Amazon API Gateway 特有的所有彈性檢查和建議。如需 Amazon API Gateway 的詳細資訊，請參閱 Amazon API Gateway 文件。

跨區域部署

如果您的政策需要考慮區域中斷， AWS Resilience Hub 將檢查不同區域中是否有額外的 Amazon API Gateway API 資源部署。

私有 API 多可用區部署

AWS Resilience Hub 會檢查您的 API 是否在 Amazon API Gateway 中定義為私有。私有 APIs應透過部署到多個 AZs 的 Amazon VPC 介面端點接收流量。

Amazon DocumentDB

本節列出 Amazon DocumentDB 特有的所有檢查和建議。如需 Amazon DocumentDB 的詳細資訊，請參閱 Amazon DocumentDB 文件。

Multi-AZ deployment (異地同步備份部署)

AWS Resilience Hub 會檢查 Amazon DocumentDB 叢集是否部署在多個 AZs 中。如果您的政策需要涵蓋區域中斷，則不同區域需要額外的次要 Amazon DocumentDB 叢集。位於不同區域的 Amazon DocumentDB 叢集也會驗證其在多個 AZs 中的執行。

彈性叢集和多可用區域部署

AWS Resilience Hub 檢查 Amazon DocumentDB Elastic 叢集碎片是否使用部署在不同 AZs僅供讀取複本。

彈性叢集和手動快照

AWS Resilience Hub 會檢查是否定期為 Amazon DocumentDB Elastic 叢集建立手動快照。手動快照允許更長的持久性，並提供設定快照頻率的彈性，以滿足您的業務需求。

NAT 閘道

本節列出 NAT Gateway 特有的所有檢查和建議。如需 NAT Gateways 的詳細資訊，請參閱 NAT Gateways。

Multi-AZ deployment (異地同步備份部署)

AWS Resilience Hub 會檢查 NAT Gateway 是否部署在多個 AZs 中。如果您的政策需要涵蓋區域中斷，則不同區域需要額外的 NAT Gateway 部署。其他 NAT Gateway 位於不同區域，也會針對其在多個 AZs 中的部署進行驗證。

Amazon Route 53

本節列出 Amazon Route 53 特有的所有檢查和建議。如需 Amazon Route 53 的詳細資訊，請參閱 Amazon Route 53 文件。

Multi-AZ deployment (異地同步備份部署)

AWS Resilience Hub 會檢查 Amazon Route 53 託管區域記錄是否在相同區域中定義多個目標，以及這些目標是否部署在多個 AZs 中。如果您的政策需要區域中斷的涵蓋範圍， AWS Resilience Hub 會檢查 Amazon Route 53 託管區域記錄是否在多個區域中定義，每個區域具有多個目標，以及這些目標是否部署在多個 AZs 中。

Amazon Application Recovery Controller (ARC)

本節列出 Amazon Application Recovery Controller (ARC) (ARC) 特有的所有檢查和建議。如需 ARC 的詳細資訊，請參閱 ARC 文件。

Multi-AZ deployment (異地同步備份部署)

AWS Resilience Hub 會檢查類似資源是否部署在多個區域中，並建議作為最佳實務，以定義 ARC 整備檢查，以在區域中斷時提高其可用性和整備程度。您將會收到通知，告知您將產生額外的每小時費用。

Amazon FSx for Windows File Server

本節列出 Amazon FSx for Windows File Server 特有的所有檢查和建議。如需 Amazon FSx for Windows File Server 的詳細資訊，請參閱 Amazon FSx for Windows File Server 文件。

檔案系統類型

AWS Resilience Hub 會檢查檔案系統類型： `Regional`或 `One Zone`。檔案系統類型會影響其在基礎設施或可用區域中斷時的彈性。如需檔案系統類型的詳細資訊，請參閱 Amazon EFS。

檔案系統備份

AWS Resilience Hub AWS Backup 會檢查是否已為部署的檔案系統定義 。此外，它也會檢查您的政策是否需要涵蓋區域層級中斷，是否已啟用`cross-Region backup`選項。

資料複寫

AWS Resilience Hub 會檢查是否已為部署的檔案系統定義區域內或跨區域排程 AWS DataSync 資料複寫任務。

AWS DataSync 排程資料複寫任務可以改善基礎設施、AZ 和區域層級的預估工作負載 RTO 和預估工作負載 RPO。此外，它可以與 區域內的 結合， AWS Backup 以便在應用程式中斷時復原。

AWS Step Functions

本節列出特定的所有檢查和建議 AWS Step Functions。如需詳細資訊 AWS Step Functions，請參閱 AWS Step Functions 文件。

版本控制和別名

AWS Resilience Hub 會檢查 AWS Step Functions 工作流程是否使用版本控制和別名來改善重新部署時間。

跨區域部署

AWS Resilience Hub 會檢查是否在不同區域中部署相同 AWS Step Functions 工作流程類型的工作流程，以便在區域中斷時復原。

Amazon ElastiCache (Redis OSS)

本節列出 Amazon ElastiCache (Redis OSS) 特有的所有檢查和建議。

如需 Amazon ElastiCache (Redis OSS) 的詳細資訊，請參閱 Amazon ElastiCache 文件。

單一可用區部署

AWS Resilience Hub 會檢查 Amazon ElastiCache (Redis OSS) 叢集是否部署為單一節點，或是否將其所有節點部署在單一可用區域中。

單一可用區部署

AWS Resilience Hub 驗證 Amazon ElastiCache (Redis OSS) 叢集是否部署為跨多個可用區域的複寫群組（啟用叢集模式和停用叢集模式的叢集），以便在可用區域中斷時允許容錯移轉。

跨區域容錯移轉

AWS Resilience Hub 會檢查彈性政策中定義的 RTO 和 RPO 目標，以從區域中斷中復原。此外，AWS Resilience Hub 可以識別部署在多個區域中的 Amazon ElastiCache (Redis OSS) 全域資料存放區叢集。

備份

AWS Resilience Hub 會檢查下列備份功能是否套用至部署的 Amazon ElastiCache (Redis OSS) 或自行設計的叢集：

- 自動備份
- 第三方備份系統的手動備份

AWS Resilience Hub 如果您不使用備份， 不會建議備份做為復原方法。不過，您可以在資料不一致時重設快取層，並從主要儲存體重新建立資料。

更快速的區域內容錯移轉

AWS Resilience Hub 在基礎設施或 AZ 中斷期間， 會檢查彈性政策中定義的 RTO 和 RPO 目標。此外， AWS Resilience Hub 可以識別下列區域內架構，從基礎設施和可用區域中斷中復原：

- 叢集模式停用類型 Amazon ElastiCache (Redis OSS) 叢集的不同可用區域中的次要待命節點執行個體。
- 叢集模式啟用類型 Amazon ElastiCache (Redis OSS) 叢集的每個碎片中，位於不同可用區域的次要待命節點執行個體。

使用其他 服務

本節說明與 互動 AWS 的服務 AWS Resilience Hub。

主題

AWS CloudFormation

AWS Resilience Hub 已與 整合 AWS CloudFormation，此服務可協助您建立和設定 AWS 資源的模型，以便減少建立和管理資源和基礎設施的時間。您可以建立範本來描述您想要的所有 AWS 資源 （例如 AWS::ResilienceHub:::ResiliencyPolicy 和 AWS::ResilienceHub:::App)，並為您 AWS CloudFormation 佈建和設定這些資源。

使用 時 AWS CloudFormation，您可以重複使用範本，以一致且重複地設定 AWS Resilience Hub 資源。描述您的資源一次，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

若要佈建和設定 AWS Resilience Hub 及相關 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。這些範本說明您想要在 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 設計工具來協助您開始使用 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 支援在 中建立 AWS::ResilienceHub:::ResiliencyPolicy 和 AWS::ResilienceHub:::App AWS CloudFormation。如需詳細資訊，包括 AWS::ResilienceHub:::ResiliencyPolicy 和 AWS::ResilienceHub:::App 的 JSON 和 YAML 範本範例，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位管理相關資源。堆疊可以包含執行 Web 應用程式所需的所有資源，例如 Web 伺服器或聯網規則。

進一步了解 AWS CloudFormation

如需詳細資訊 AWS CloudFormation，請參閱下列資源：

- 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 已與 整合 AWS CloudTrail，此服務提供使用者、角色或服務在 AWS 中採取動作的記錄 AWS Resilience Hub。CloudTrail 會將 的所有 API 呼叫擷取 AWS Resilience Hub 為事件。擷取的呼叫包括從 AWS Resilience Hub 主控台呼叫，以及對 AWS Resilience Hub API 操作的程式碼呼叫。如果您建立線索，您可以啟用 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 的事件 AWS Resilience Hub。即使您未設定追蹤，依然可以透過 CloudTrail 主控台中的事件歷史記錄檢視最新事件。使用 CloudTrail 所收集的資訊，您可以判斷提出的請求 AWS Resilience Hub、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。

如需有關 CloudTrail 的相關資訊，請參閱 AWS CloudTrail 使用者指南。

AWS Systems Manager

AWS Resilience Hub 與 Systems Manager 搭配使用，藉由提供許多 SSM 文件來自動化 SOPs 的步驟，您可以將這些文件做為這些 SOPs 的基礎。

AWS Resilience Hub 為您提供 AWS CloudFormation 範本，其中包含執行不同 Systems Manager 文件所需的 IAM 角色，每個文件一個角色，具有特定文件所需的許可。使用 AWS CloudFormation 範本建立堆疊後，它會設定 IAM 角色，並將中繼資料儲存在 Systems Manager 參數中，供 Systems Manager 自動化文件針對不同的復原程序執行。

如需使用 SOPs的詳細資訊，請參閱 管理標準操作程序。

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、排定優先順序和最佳化部署 AWS。 會 AWS Trusted Advisor 檢查您的 AWS 環境，然後在有節省成本的機會、改善系統可用性

和效能時，透過檢查提出建議，或協助解決安全漏洞。這些檢查會根據其用途分為多個類別。如需不同類別的簽入詳細資訊 AWS Trusted Advisor，請參閱 AWS 支援 使用者指南。

AWS Trusted Advisor 透過容錯能力類別 AWS Resilience Hub 下每個應用程式的彈性檢查，提供多個高階彈性建議。容錯能力類別會列出測試應用程式的所有檢查，以判斷其彈性和可靠性。這些檢查會在 AppComponent 失敗和政策違規時提醒您，這些故障和政策違規可能會導致復原風險，並影響應用程式可用性以實現業務連續性。它也提供彈性建議，以改善在需要解決的建議動作區段中降低這些風險的機會 AWS Resilience Hub。如需 中每個應用程式建議的詳細資訊 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 中的最新評估檢查應用程式的彈性分數， AWS Resilience Hub 並在其彈性分數低於特定值時提醒您。

  警示條件

  - 綠色 – 表示您的應用程式彈性分數為 70 分及以上。
  - 黃色：表示您的應用程式彈性分數介於 40 到 69 之間。
  - 紅色 – 表示您的應用程式彈性分數低於 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，請實作建議的操作建議。如需執行、檢閱和實作評估、檢閱和包含/排除操作建議，以及實作相同建議的詳細資訊，請參閱下列主題：

  - the section called “在 中執行彈性評估 AWS Resilience Hub”
  - the section called “檢閱評估報告”
  - the section called “檢閱彈性建議”
  - the section called “包含或排除操作建議”
- AWS Resilience Hub 違反應用程式政策 – 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 目標時提醒您。

  警示條件

  - 綠色 – 表示應用程式具有政策，且預估工作負載 RTO 和預估工作負載 RPO 符合 RTO 和 RPO 目標。
  - 黃色 – 表示應用程式具有政策且尚未評估。

- 紅色 – 表示應用程式具有政策，且預估工作負載 RTO 和預估工作負載 RPO 不符合 RTO 和 RPO 目標。

  建議的動作

  為了確保應用程式的預估工作負載 RTO 和預估工作負載 RPO 仍符合定義的 RTO 和 RPO 目標，請使用應用程式資源的最新更新版本定期執行評估。此外，如果您想要確保應用程式的彈性政策未遭到違反，我們建議您檢閱評估報告並實作建議的彈性建議。如需有關啟用 代表您每天 AWS Resilience Hub 執行評估、執行評估、檢閱彈性建議和實作相同項目的詳細資訊，請參閱下列主題：

  - the section called “編輯應用程式資源”（若要 AWS Resilience Hub 讓 代表您每日執行評估，請完成 中的步驟 編輯應用程式程序的偏離通知設定，以選取自動評估每日核取方塊。）
  - the section called “在 中執行彈性評估 AWS Resilience Hub”
  - the section called “檢閱評估報告”
  - the section called “檢閱彈性建議”
  - the section called “包含或排除操作建議”

- AWS Resilience Hub 應用程式評估使用期 – 檢查自上次您為其中的每個應用程式執行評估以來的時間點 AWS Resilience Hub。如果您未在指定的天數內執行評估，它會提醒您。

  警示條件

  - 綠色 – 表示您在過去 30 天內已執行應用程式的評估。
  - 黃色 – 表示您在過去 30 天內尚未執行應用程式的評估。

  建議的動作

  定期執行評估，以管理和改善應用程式上的復原狀態 AWS。如果您想要代表您每天 AWS Resilience Hub 評估應用程式，您可以在 AWS Resilience Hub 偏離通知中選取自動評估此應用程式的每日核取方塊來啟用相同功能。若要選取自動評估此應用程式的每日核取方塊，請完成在 中編輯應用程式程序的偏離通知???。

  > **Note**
  >
  > 此檢查只會決定至少一次評估的應用程式評估期 AWS Resilience Hub。

- 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，如果此 AppComponent 在發生中斷事件時未復原，您可能會遇到未知的資料遺失和系統停機時間。如果警示條件設為紅色，則表示 AppComponent 無法復原。

建議的動作

若要確保您的 AppComponent 可復原，請檢閱並實作彈性建議，然後執行新的評估。如需檢閱彈性建議的詳細資訊，請參閱 the section called “檢閱彈性建議”。

如需使用 的詳細資訊 AWS Trusted Advisor，請參閱 AWS 支援 使用者指南。

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
- 文件最近更新時間：2024 年 12 月 17 日

變更	描述	日期
AWS Resilience Hub 整合已實作的 Amazon CloudWatch 警示	AWS Resilience Hub 現在會自動偵測已設定的 Amazon CloudWatch 警示並將其整合到其彈性評估中，提供應用程式彈性狀態的更全面檢視。這項新功能結合了 AWS Resilience Hub 建議與您目前的監控設定，以簡化警示管理並增強評估準確性。 如需詳細資訊，請參閱管理警示。	2024 年 12 月 17 日
AWS Resilience Hub 已啟用其他功能，以量身打造的 AWS Fault Injection Service 實驗提供簡化的彈性測試	AWS Resilience Hub 現在支援與 AWS Fault Injection Service (AWS FIS) 的增強型整合，以根據特定應用程式內容使用 AWS FIS 動作和案例來提供量身打造的建議，以改善彈性狀態。執行建議的實驗或您自己的測試將改善您的復原能力分數，讓您追蹤一段時間內的變更。 如需詳細資訊，請參閱下列主題：	2024 年 12 月 17 日

	• AWSResilienceHubAssessmentExecutionPolicy • 管理 AWS Fault Injection Service 實驗 • AWS Resilience Hub – 彈性測試	
AWS Resilience Hub 引入摘要檢視	AWS Resilience Hub的新摘要檢視透過清晰的圖表和圖形提供應用程式彈性的高階視覺化呈現，可讓您視覺化應用程式產品組合的狀態，並有效率地管理和改善應用程式承受中斷並從中斷中復原的能力。除了新的摘要檢視之外，您還可以匯出支援摘要檢視的資料，以建立利益相關者通訊的自訂報告。 如需詳細資訊，請參閱the section called “AWS Resilience Hub 摘要”。	2024 年 11 月 21 日

AWS Resilience Hub 在 myApplications 儀表板中引入彈性小工具	myApplications 儀表板中的新彈性小工具可簡化評估和監控應用程式的彈性狀態。它可讓您快速評估 myApplications 中定義的應用程式的彈性，而不必在 中手動複寫 AWS Resilience Hub。 如需詳細資訊，請參閱下列主題： • the section called “AWS Resilience Hub 和 myApplications” • the section called “從彈性小工具管理彈性評估”	2024 年 10 月 22 日

AWS Resilience Hub 擴充對 Amazon ElastiCache (Redis OSS) Serverless 的支援	AWS Resilience Hub 現在會評估使用 Amazon ElastiCache (Redis OSS) 的應用程式，包括 Amazon ElastiCache (Redis OSS) Serverless 和 Global Datastores，並提供增強的彈性建議。這些包括區域和多區域設定的準則，以及多可用區域部署、資源分組和備份的策略。此外，為了改善對應用程式彈性狀態的控制，AWS Resilience Hub 提供專為 Amazon ElastiCache (Redis OSS) 量身打造的 Amazon CloudWatch 警示。 Amazon ElastiCache 如需詳細資訊，請參閱下列主題： • the section called “管理應用程式元件” • the section called “支援 AWS Resilience Hub 的資源” • the section called “AWSResilienceHubAsssessmentExecutionPolicy”	2024 年 9 月 25 日

AWS Resilience Hub 推出分組建議	AWS Resilience Hub 引入新的智慧分組選項，以在加入應用程式時將資源分組到 Application Components (AppComponents)。當您在 上執行彈性評估時 AWS Resilience Hub，請務必將資源準確分組為適當的 AppComponents以接收最佳化且可採取動作的建議。此選項非常適合複雜或跨區域應用程式，以減少加入應用程式所需的時間，並且補充了目前可用的現有應用程式加入工作流程。 如需詳細資訊，請參閱下列主題： • the section called “管理應用程式元件” • the section called “AWS Resilience Hub 資源群組建議”	2024 年 8 月 1 日

AWS Resilience Hub 推出新的評估摘要小工具	AWS Resilience Hub 推出新的評估摘要小工具，使用 Amazon Bedrock 生成式 AI 功能，將複雜的彈性資料轉換為高度可行的洞見。這些評估摘要會擷取關鍵調查結果、排定風險優先順序，並建議改善復原能力的步驟。透過專注於最有影響力的元素，您可以更輕鬆地了解評估，這可協助您提供高影響力的資訊，以專注於復原狀態最關鍵的元素。 如需詳細資訊，請參閱the section called “評估摘要”。	2024 年 8 月 1 日
AWS Resilience Hub 擴充對 Amazon DocumentDB 的支援	此 AWS Resilience Hub 政策可讓您授予`Describe`許可，讓您在執行評估 AWS Lambda 時存取 Amazon DocumentDB、Elastic Load Balancing 上的資源和組態。 如需 AWS 受管政策的詳細資訊，請參閱 the section called “AWSResilienceHubAsssessmentExecutionPolicy”。	2024 年 8 月 1 日

AWS Resilience Hub 擴展應用程式彈性漂移偵測功能	AWS Resilience Hub 已推出一種新的偏離偵測類型 – 應用程式資源偏離，以擴展其偏離偵測功能。此增強功能會偵測變更，例如新增或刪除應用程式輸入來源中的資源。您可以啟用 AWS Resilience Hub 排定的評估和偏離通知服務，並在發生偏離時收到通知。最新的彈性評估會識別漂移，並呈現修補動作，讓應用程式恢復符合您的彈性政策。 如需詳細資訊，請參閱下列主題： • the section called “漂移偵測” • the section called “設定排程評估和偏離通知”	2024 年 5 月 8 日
AWS Trusted Advisor 增強功能	AWS Resilience Hub 已透過新增檢查以識別無法復原的應用程式元件 (AppComponents) AWS Trusted Advisor 來擴充對 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 延伸對建議警示的支援	AWS Resilience Hub 已使用值更新README.md 範本檔案，可讓您建立 AWS （例如 Amazon CloudWatch) AWS Resilience Hub 內或外建議的警示 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 擴充對 Amazon FSx for Windows File Server 的支援	AWS Resilience Hub 擴展對 Amazon FSx for Windows File Server 資源的評估支援，同時評估應用程式的彈性。對於使用 Amazon FSx for Windows File Server 的應用程式， AWS Resilience Hub 提供一組新的彈性建議，涵蓋可用區域 (AZ) 和多可用區域部署，以及備份計劃，以及資料複寫。 AWS Resilience Hub 支援 Amazon FSx for Windows File Server，包括區域內和跨區域部署的 Microsoft Active Directory 上的檔案系統相依性。 如需詳細資訊，請參閱下列主題： • the section called “支援 AWS Resilience Hub 的資源” • the section called “AWSResilienceHubAsssessmentExecutionPolicy” • the section called “應用程式元件中的資源分組”	2024 年 3 月 26 日

AWS Resilience Hub 提供有關彈性分數的其他資訊	AWS Resilience Hub 已更新彈性分數使用者體驗，協助您輕鬆導覽和了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 擴展對包含 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 資源的應用程式的支援，以納入新的操作建議。執行包含來自 Amazon EKS 叢集資源的評估時，我們現在建議執行測試和警示，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 “管理 AWS Fault Injection Service 實驗”。	2023 年 11 月 9 日
AWS Resilience Hub 在應用程式層級提供其他資訊	AWS Resilience Hub 在應用程式層級提供有關預估工作負載 RTO 和預估工作負載 RPO 的其他資訊。此額外資訊指出最新成功評估中應用程式的最大可能估計工作負載 RTO 和估計工作負載 RPO。此值是所有中斷類型的最大估計工作負載 RTO 和估計工作負載 RPO。 如需詳細資訊，請參閱the section called “管理應用程式”。	2023 年 10 月 30 日

AWS Resilience Hub 擴展 AWS Step Functions 資源的評估支援	AWS Resilience Hub 擴展對 AWS Step Functions 資源的評估支援，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，AWS Resilience Hub 也將提供建議，協助您達成估計工作負載復原時間目標 (RTO) 和估計工作負載復原點目標 (RPO)。若要評估應用程式，包括 AWS Step Functions 資源，您必須使用 AWS 受管政策或手動新增特定許可來設定必要的許可， AWS Resilience Hub 以允許 讀取 AWS Step Functions 組態。 如需相關許可的詳細資訊，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、標準操作程序 SOPs) 和 AWS Fault Injection Service (AWS FIS) 測試。在 上執行評估時 AWS Resilience Hub，系統會提供您預估的復原時間，以及提高評估應用程式彈性的建議。使用排除建議工作流程，您現在可以排除與其無關的建議警示、SOPs 和 AWS FIS 測試。如果您使用的平台不是建議的平台，或已在替代方法中實作建議，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 “包含或排除操作建議” • the section called “限制納入或排除 AWS Resilience Hub 建議的許可”	2023 年 8 月 9 日

改善 的許可設計 AWS Resilience Hub	AWS Resilience Hub 引進新的許可設計，以在設定 AWS Identity and Access Management (IAM) 角色時提供彈性 AWS Resilience Hub。它還將許可合併為單一角色，能夠建立對您和團隊有意義的自訂角色名稱。中的新受管政策 AWS Resilience Hub 可讓您擁有支援服務的適當許可。如果您對於目前的許可設定方法感到滿意，我們將繼續支援手動組態。 如需 AWS 受管政策的詳細資訊，請參閱 the section called “AWSResilienceHubAsssessmentExecutionPolicy”。	2023 年 8 月 2 日

使用 偵測應用程式彈性偏離 AWS Resilience Hub	AWS Resilience Hub 可讓您主動偵測並了解必要的動作，以解決應用程式彈性問題。讓 Amazon Simple Notification Service (Amazon SNS) 在估計工作負載復原時間目標 (RTO) 或估計工作負載復原點目標 (RPO) 從達到目標移至不再滿足組織的業務目標時收到通知。從被動地尋找彈性問題，同時手動執行評估，以透過 Amazon SNS 主題主動收到通知，將可讓您提早預測潛在的中斷，並讓您對實現復原目標有額外的信心。 如需詳細資訊，請參閱下列主題： • the section called “設定排程評估和偏離通知” • the section called “編輯應用程式資源”	2023 年 8 月 2 日

AWS Resilience Hub 改善對 Amazon Relational Database Service 和 Amazon Aurora 的支援	AWS Resilience Hub 擴展了對 Amazon Relational Database Service 代理以及無周邊和 Amazon Aurora 資料庫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 (RTOs)。 AWS Resilience Hub 也將提供額外的動作，以在 AWS 環境中實作彈性最佳實務。最佳實務可以包括 DevOps Guru for Amazon RDS 的效能洞察、增強型監控，以及在支援的資料庫引擎上實現藍/綠部署自動化。 若要進一步了解在評估中 AWS Resilience Hub 包含來自所有支援服務的資源所需的許可，請參閱 the section called “AWSResilienceHubAsssessmentExecutionPolicy”。	2023 年 8 月 2 日

AWS Resilience Hub 擴展對 Amazon Elastic Block Store 快照的支援	AWS Resilience Hub 擴展對 Amazon Elastic Block Store (Amazon EBS) 的評估支援，以識別使用直接 APIs 在同一 Amazon EBS 區域內拍攝的 Amazon EBS 快照。延伸支援是使用 Amazon Data Lifecycle Manager (Amazon Data Lifecycle Manager) 或 AWS Backup 的客戶目前支援之外的額外支援。 如需詳細資訊，請參閱 Amazon Elastic Block Store (Amazon EBS)。	2023 年 8 月 2 日

Amazon Elastic Compute Cloud 增強功能	AWS Resilience Hub 已擴展對 Amazon Elastic Compute Cloud (Amazon EC2) 的支援。對於大小不同的應用程式，AWS 允許其客戶使用 Amazon EC2 選取適合其使用案例的組態。 AWS Resilience Hub 支援對下列 Amazon EC2 組態進行評估： • 隨需執行個體。 • 執行個體由 AWS Backup 和備份 AWS Elastic Disaster Recovery。 • 支援使用 Amazon Application Recovery Controller (ARC) (ARC) 的自動擴展群組 接下來，評估支援將擴展到包含 Spot 執行個體、專用主機、專用執行個體、置放群組和機群。 如需詳細資訊，請參閱the section called “AWS Resilience Hub 存取許可參考”。	2023 年 6 月 27 日
AWS 受管政策更新	已新增新政策，提供其他 AWS 服務的存取權，以執行評估。 如需詳細資訊，請參閱the section called “AWSResilienceHubAsssessmentExecutionPolicy”。	2023 年 6 月 26 日

新的 Amazon DynamoDB 操作建議警示	對於使用 Amazon DynamoDB 的應用程式， AWS Resilience Hub 現在提供一組新的警示，提醒您隨需和佈建容量模式和全域資料表的彈性風險。若要存取新警示，您可能需要更新您正在使用的角色的 AWS Identity and Access Management (IAM) 政策。 如需詳細資訊，請參閱the section called “AWS Resilience Hub 存取許可參考”。	2023 年 5 月 2 日
AWS Trusted Advisor 增強功能	AWS Resilience Hub 已擴展對 AWS Trusted Advisor 和使用 Amazon DynamoDB 的應用程式的支援。當您 AWS Trusted Advisor 搭配 使用 時 AWS Resilience Hub，您現在可以在應用程式在過去 30 天內尚未評估時收到通知。此通知會提示您重新評估應用程式，以了解是否有任何變更會影響其彈性。 如需AWS Resilience Hub 評估存留期檢查的詳細資訊，請參閱 the section called “AWS Trusted Advisor”。	2023 年 5 月 2 日

Amazon Simple Storage Service 的其他支援	除了目前對 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 備份的支援之外， 現在 AWS Resilience Hub 還將評估 Amazon S3 多區域存取點、Amazon S3 複寫時間控制 (Amazon S3 RTC) 和 AWS 備份point-in-time(PITR) 組態。 如需詳細資訊，請參閱下列主題： • the section called “AWS Resilience Hub 存取許可參考” • 管理您的 Amazon S3 儲存體	2023 年 3 月 21 日

Amazon Elastic Kubernetes Service 的其他支援	AWS Resilience Hub 已新增 Amazon EKS 叢集做為定義、驗證和追蹤應用程式彈性的支援資源。客戶可以將 Amazon EKS 叢集新增至新的或現有的應用程式，並接收評估和改善彈性的建議。客戶可以使用 AWS CloudFormation、Terraform AWS Resource Groups 和 myApplications 新增應用程式資源。此外，客戶可以在一或多個區域中直接新增一或多個 Amazon EKS 叢集，每個叢集中具有一或多個命名空間。這允許 AWS Resilience Hub 提供單一和跨區域評估和建議。除了檢查部署之外，Replicas、ReplicationControllers 和 Pod AWS Resilience Hub 也會分析整體叢集彈性。AWS Resilience Hub 支援無狀態 Amazon EKS 叢集工作負載。 AWS Resilience Hub 支援 的所有 AWS 區域都提供新功能。 如需詳細資訊，請參閱下列主題： • the section called “管理您的應用程式資源” • the section called “新增 EKS 叢集” • the section called “AWS Resilience Hub 存取許可參考”	2023 年 3 月 21 日

	• AWS 區域服務	
Amazon Elastic File System 的其他支援	除了目前對 Amazon Elastic File System (Amazon EFS) 備份的支援之外，現在 AWS Resilience Hub 還將評估 Amazon EFS 用於 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 AWS Resilience Hub 的資源” • 什麼是 Amazon Elastic File System？	2023 年 3 月 21 日
支援應用程式輸入來源	AWS Resilience Hub 現在提供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 “編輯應用程式資源”。	2023 年 2 月 21 日

支援應用程式組態參數	AWS Resilience Hub 現在提供輸入機制，以收集與應用程式相關聯資源的其他資訊。透過此資訊， AWS Resilience Hub 將更深入了解您的資源，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 “應用程式組態參數” • the section called “設定應用程式組態參數” • the section called “更新應用程式組態參數”	2023 年 2 月 21 日
Amazon Elastic Block Store 的其他支援	除了目前對 Amazon Elastic Block Store (Amazon EBS) 磁碟區的支援之外， 現在 AWS Resilience Hub 將由 Amazon Data Lifecycle Manager 和 Amazon EBS 快速快照還原 (FSR) 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 存取許可參考” • 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 帳戶相關聯的應用程式，這些應用程式已由 評估 AWS Resilience Hub。 AWS Trusted Advisor 顯示最新的彈性分數，並提供狀態，指出是否已符合目標彈性政策 (RTO 和 RPO)。每次執行評估時， 都會 AWS Resilience Hub 更新 AWS Trusted Advisor 最新結果。AWS Trusted Advisor 是一種服務，可持續分析 AWS 您的帳戶，並提供建議，協助您遵循 AWS 最佳實務和 AWS Well-Architected 準則。 如需詳細資訊，請參閱the section called “AWS Trusted Advisor”。	2022 年 11 月 18 日

支援 Amazon Simple Notification Service (Amazon SNS)	AWS Resilience Hub 現在透過分析 Amazon SNS 組態來評估使用 Amazon SNS 的應用程式，包括訂閱者，並提供建議以滿足組織的預估工作負載復原目標（預估工作負載 RTO 和預估工作負載 RPO)。Amazon SNS 是一種受管服務，可將訊息從發佈者（生產者）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 AWS Resilience Hub 的資源” • the section called “身分和存取權管理” • the section called “應用程式元件中的資源分組”	2022 年 11 月 16 日

Amazon Application Recovery Controller (ARC) (Amazon ARC) 的其他支援	AWS Resilience Hub 現在會評估 Amazon ARC for Elastic Load Balancing 和 Amazon Relational Database Service (Amazon RDS)，其中包括建議 Amazon ARC 何時會有幫助。延伸 AWS Resilience Hub，Amazon ARC 評估支援 AWS Auto Scaling Group (AWS ASG) 和 Amazon DynamoDB 以外的功能。Amazon 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 AWS Resilience Hub 的資源” • the section called “身分和存取權管理”	2022 年 11 月 16 日

AWS 備份的其他支援	AWS Resilience Hub 現在會評估 Amazon ARC for Elastic Load Balancing 和 Amazon Relational Database Service (Amazon RDS)，其中包括建議 Amazon ARC 何時會有幫助。延伸 AWS Resilience Hub，Amazon ARC 評估支援 AWS Auto Scaling Group (AWS ASG) 和 Amazon DynamoDB 以外的功能。Amazon 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 AWS Resilience Hub 的資源” • the section called “身分和存取權管理”	2022 年 11 月 16 日
已更新內容：新增了新的應用程式元件資源	在 AppComponent 分組區段中，將 Route53 和 AWS Backup 新增至支援的 Application Component 資源清單。	2022 年 7 月 1 日
新內容：應用程式合規狀態概念	新增變更偵測到的狀態類型。	2022 年 6 月 2 日

簡介 AWS Resilience Hub	AWS Resilience Hub 現已推出。本指南說明如何使用 AWS Resilience Hub 來分析您的基礎設施、取得改善 AWS 應用程式彈性的建議、檢閱彈性分數等。	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。