使用者指南

AWS 故障注入服務

AWS 故障注入服務: 使用者指南

Table of Contents

什麼是 AWS 故障注入服務？

AWS 故障注入服務 (AWS FIS) 是一項受管服務，可讓您針對 AWS 工作負載執行故障注入實驗。故障注入是基於混亂工程的原理。這些實驗透過建立破壞性事件來 stress 應用程式，以便觀察應用程式的回應方式。然後，您可以使用此資訊來改善應用程式的效能和復原能力，使其行為如預期般。

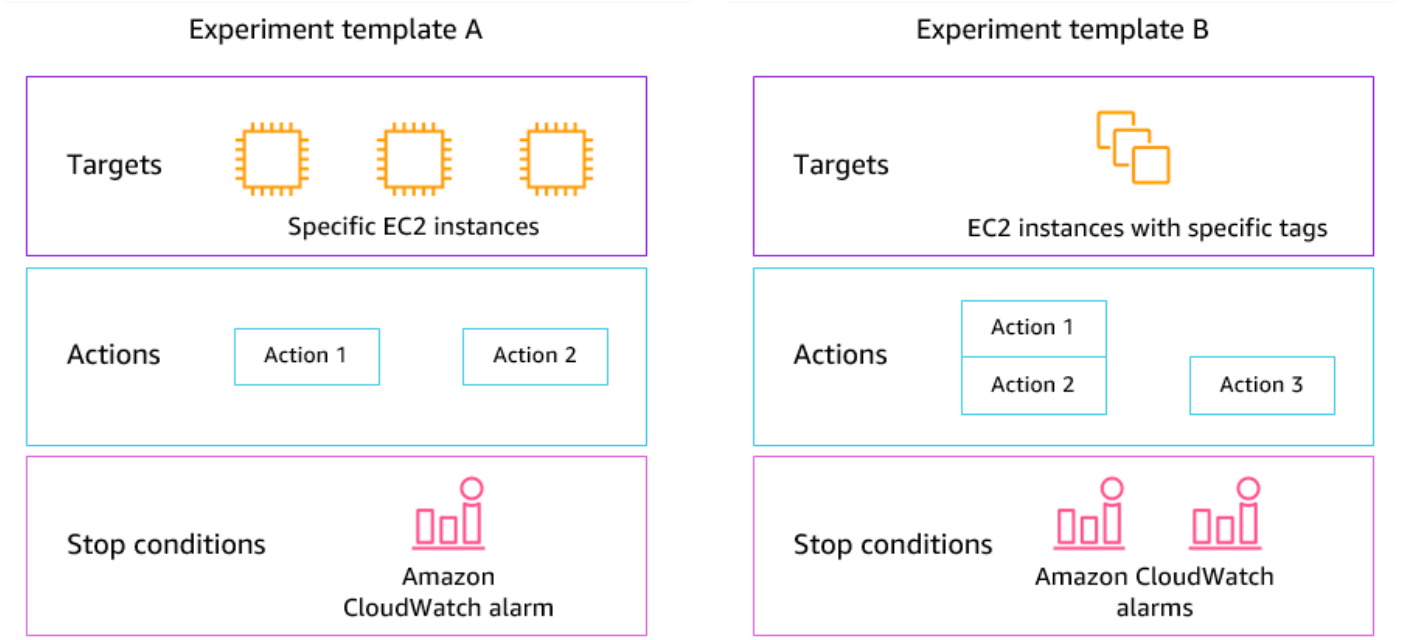
若要使用 AWS FIS，您可以設定並執行實驗，以協助您建立真實世界所需的條件，以發現難以找到的應用程式問題。 AWS FIS 提供可產生中斷的範本，以及在生產環境中執行實驗所需的控制項和護欄，例如在符合特定條件時自動復原或停止實驗。

> **Important**
>
> AWS FIS 執行真正的行動，在您的系統中的實際 AWS 資源。因此，在您使用 AWS FIS 在生產環境中執行實驗之前，我們強烈建議您先完成規劃階段，並在生產前環境中執行實驗。

如需有關規劃實驗的詳細資訊，請參閱測試可靠性和規劃您的 AWS FIS 實驗. 如需 AWS FIS 的詳細資訊，請參閱AWS 故障注入服務。

AWS FIS 概念

若要使用 AWS FIS，您可以對 AWS 資源執行實驗，以測試應用程式或系統在故障條件下執行的理論。若要執行實驗，請先建立實驗範本。實驗模板是實驗的藍圖。它包含了實驗的動作，目標和停止條件。建立實驗範本後，您可以使用它來執行實驗。在實驗運行時，您可以跟踪其進度並查看其狀態。當實驗中的所有動作都運行了實驗就完成了。



動作

動作是 AWS FIS 在實驗期間對 AWS 資源執行的活動。 AWS FIS 會根據資源類型提供一組預先設定的 AWS 動作。在實驗期間，每個動作都會在指定的持續時間內執行，或直到您停止實驗為止。動作可以按順序或同時執行 (parallel)。

目標

目標是 FI AWS S 在實驗期間執行動作的一或多個 AWS 資源。您可以選擇特定資源，也可以根據特定條件 (例如標籤或狀態) 選取資源群組。

停止條件

AWS FIS 提供您在工作負載上安全執行實驗所需的控制項和護欄。 AWS 停止條件是一種在實驗達到您定義為 Amazon CloudWatch 警示的閾值時停止實驗的機制。如果在實驗執行時觸發停止條件，AWS FIS 會停止實驗。

支援 AWS 服務

AWS FIS 會針對跨 AWS 服務的特定類型目標提供預先設定的動作。 AWS FIS 支援針對下列項目的目標資源執行動作： AWS 服務

- Amazon CloudWatch

- Amazon DynamoDB
- Amazon EBS
- Amazon EC2
- Amazon ECS
- Amazon EKS
- Amazon ElastiCache
- Amazon RDS
- Amazon S3
- AWS Systems Manager
- Amazon VPC

對於單帳戶實驗，目標資源必須與實驗 AWS 帳戶 相同。您可以使用 AWS FIS 多帳戶實驗來執行 FIS 實驗，以不同 AWS 帳戶 帳戶中的資源 AWS 為目標。

如需詳細資訊，請參閱 的動作 AWS FIS。

訪問 AWS 金融機構

您可以使用下列任何 AWS 一種方式使用 FIS：

- AWS Management Console— 提供可用來存取 AWS FIS 的 Web 介面。如需詳細資訊，請參閱使用 AWS Management Console。
- AWS Command Line Interface (AWS CLI) — 提供多種 AWS 服務 (包括 AWS FIS) 的指令，並在視窗、macOS 和 Linux 上受到支援。如需詳細資訊，請參閱 AWS Command Line Interface。若要取得有關 AWS FIS 指令的更多資訊，請參閱《指AWS CLI 令參考》中的 fis。
- AWS CloudFormation— 建立描述資 AWS 源的範本。您可以使用範本，佈建並管理這些資源做為單一單位。如需詳細資訊，請參閱AWS 錯誤注入服務資源類型參考。
- AWS SDK — 提供特定語言的 API，並處理許多連線詳細資料，例如計算簽章、處理要求重試和處理錯誤。如需詳細資訊，請參閱 AWS 開發套件。
- HTTPS API — 提供您可以使用 HTTPS 請求呼叫的低階 API 動作。如需詳細資訊，請參閱AWS 錯誤注入服務 API 參考。

金融資訊 AWS 系統的定價

系統會根據實驗的目標帳戶數量，從開始到結束執行動作的每分鐘向您收費。如需詳細資訊，請參閱 AWS FIS 定價。

規劃您的 AWS FIS 實驗

錯誤注入是指透過建立破壞性事件 (例如伺服器中斷或 API 節流) 來強調應用程式在測試或生產環境中的程序。通過觀察系統的響應方式，您就可以實施改進。當您在系統上運行實驗時，它可以幫助您以受控的方式識別系統性弱點，然後在這些弱點影響依賴於您的系統的客戶之前。然後，您可以主動解決問題，以幫助防止不可預測的結果。

在開始使用 AWS FIS 執行故障注入實驗之前，我們建議您先熟悉下列原則和指導方針。

> **Important**
>
> AWSFIS 執行真正的行動，在您的系統中的實際AWS資源。因此，在您開始使用 AWS FIS 執行實驗之前，我們強烈建議您先在生產前或測試環境中完成規劃階段和測試。

目錄

基本原則和指引

在開始使用 AWS FIS 進行實驗之前，請執行以下步驟：

1. 識別實驗的目標部署 — 從識別目標部署開始。如果這是您的第一個實驗，我們建議您從生產前或測試環境開始。
2. 檢閱應用程式架構 — 您必須確定已識別每個元件的所有應用程式元件、相依性和復原程序。從檢閱應用程式架構開始。視應用程式而定，請參閱 AWSWell-Architected 的架構。
3. 定義穩定狀態行為 — 根據重要的技術和業務指標來定義系統的穩定狀態行為，例如延遲、CPU 負載、每分鐘登入失敗、重試次數或頁面載入速度。
4. 形成假設 — 形成一個假設，說明您期望系統行為在實驗過程中發生什麼變化。假設的定義遵循以下格式：

   如果執行######，##########不應超過#。

   例如，驗證服務的假設可能如下所示：「如果網路延遲增加 10%，則登入失敗次數增加不到 1%。」 實驗完成後，您可以評估應用程式恢復能力是否符合您的業務和技術期望。

我們也建議您在使用 AWS FIS 時遵循這些準則：

- 永遠開始在測試環境中使AWS用 FIS 進行試驗。永遠不要從生產環境開始。隨著故障注入實驗的進展，您可以在測試環境以外的其他受控環境中進行實驗。
- 從簡單的小型實驗開始，例如在一個目標上執行 aw: ec2: stop- instance 動作，建立團隊對應用程式彈性的信心。
- 故障注入可能會導致真正的問題。謹慎行事，並確保你的第一個故障注射是在測試實例，所以沒有客戶受到影響.
- 測試，測試和測試更多。故障注入旨在通過精心計劃的實驗在受控環境中實施。這使您可以對應用程序和工具的功能建立信心，以承受湍流條件。
- 我們強烈建議您在開始之前擁有出色的監視和警報程序。沒有它，您將無法理解或衡量實驗的影響，這對於可持續的故障注入實踐至關重要。

實驗規劃指南

使用 AWS FIS，您可以對AWS資源執行實驗，以測試應用程式或系統在故障情況下如何執行的理論。

以下是規劃 AWS FIS 實驗的建議準則。

- 檢閱中斷歷史記錄 — 檢閱系統先前的中斷和事件。這可以幫助您建立系統的整體健康狀況和恢復能力的圖片。在您開始在系統上執行實驗之前，您應該解決系統中的已知問題和弱點。
- 識別影響最大的服務 — 檢閱您的服務，並識別對最終使用者或客戶造成最大影響的服務 (如果使用者或客戶發生故障或無法正常運作)。
- 識別目標系統 — 目標系統是您將在其上執行實驗的系統。如果您AWS是 FIS 的新手，或者您以前從未進行過故障注入實驗，我們建議您先在生產前或測試系統上執行實驗。
- 諮詢您的團隊 — 詢問他們擔心什麼。你可以形成一個假設來證明或反駁他們的擔憂。您也可以詢問您的團隊他們不擔心什麼。這個問題可以揭示兩個常見的謬誤：沉沒成本謬誤和確認偏差謬誤。根據團隊的答案形成假設可以幫助您提供有關系統狀態現實情況的更多信息。
- 檢閱您的應用程式架構 — 檢閱您的系統或應用程式，並確定您已識別每個元件的所有應用程式元件、相依性和復原程序。

  我們建議您檢閱 AWS Well-Architected 的架構。此架構可協助您為應用程式和工作負載建置安全、高效能、彈性且有效率的基礎架構。如需詳細資訊，請參閱 AWS Well-Architected。
- 識別適用的指標 — 您可以使用 Amazon 指 CloudWatch標監控實驗對資AWS源的影響。您可以使用這些指標來判斷應用程式執行最佳狀態時的基準線或「穩定狀態」。然後，您可以在實驗期間

或之後監視這些指標，以確定影響。如需詳細資訊，請參閱 使用亞馬遜監控AWS FIS 使用量指標 CloudWatch。

- 為您的系統定義可接受的效能臨界值 — 識別代表系統可接受、穩定狀態的測量結果。您將使用此指標來創建一個或多個代表實驗停止條件的 CloudWatch 警報。如果警報被觸發，實驗將自動停止。如需更多詳細資訊，請參閱 AWS FIS 的停止條件。

AWS 故障注入服務教程

下列教學課程AWS 說明如何使用 AWS 故障注入服務 (FIS) 建立和執行實驗。

教學課程

- 教學課程：測試執行個體停止並開始使用 AWS FIS
- 教學課程：使用 AWS FIS 在執行個體上執行 CPU stress
- 教學課程：使用 FIS 測試 Spot 執行個體中斷 AWS
- 自學課程：模擬連接事件
- 教學課程：排程重複實驗

教學課程：測試執行個體停止並開始使用 AWS FIS

您可以使用AWS故障注入服務 (AWSFIS) 來測試應用程式如何處理執行個體停止和啟動。使用此自學課程建立實驗範本，該範本使用 AWS FIS `aws:ec2:stop-instances` 動作停止一個例證，然後停止第二個例證。

必要條件

若要完成此自學課程，請確定您執行下列動作：

- 在您的帳戶中啟動兩個測試 EC2 執行個體。啟動執行個體後，請記下兩個執行個體的 ID。
- 建立可讓 AWS FIS 服務代表您執行`aws:ec2:stop-instances`動作的 IAM 角色。如需詳細資訊，請參閱 適用於 AWS FIS 實驗的 IAM 角色。
- 請確定您可以存取 AWS FIS。如需詳細資訊，請參閱 AWSFIS 原則範例。

步驟 1：建立實驗範本

使用 AWS FIS 主控台建立實驗範本。在範本中，您可以指定兩個動作，每個動作會依序執行三分鐘。第一個動作會停止 AWS FIS 隨機選擇的其中一個測試執行個體。第二個動作會停止兩個測試執行個體。

建立實驗樣板的步驟

1. 開啟AWS金融資訊系統控制台，網址為 https://console.aws.amazon.com/fis/。
2. 在導覽窗格中，選擇 [實驗範本]。

3. 選擇創建實驗模板。
4. 在「描述」和「名稱」中，輸入範本的描述和名稱。
5. 對於 Actions (動作)，執行下列動作：
   a. 選擇新增動作。
   b. 輸入動作的名稱。例如，輸入 **stopOneInstance**。
   c. 針對「動作類型」，選擇 aw: ec2: 停止執行個體。
   d. 針對目標，請保留 AWS FIS 為您建立的目標。
   e. 對於「動作參數」，請在持續時間後啟動執行個體，指定 3 分鐘 (PT3M)。
   f. 選擇儲存。
6. 對於 Targets (目標)，執行下列動作：
   a. 針對在上一個步驟中為您自動建立 AWS FIS 的目標，選擇 「編輯」。
   b. 以更具描述性的名稱取代預設名稱。例如，輸入 **oneRandomInstance**。
   c. 驗證資源類型是 aw:ec2: 實例。
   d. 對於 Target 方法，請選擇資源 ID，然後選擇兩個測試實例的 ID。
   e. 在選取模式中，選擇「計數」。針對「資源數目」，輸入**1**。
   f. 選擇儲存。
7. 選擇新增目標，然後執行下列動作：
   a. 輸入目標的名稱。例如，輸入 **bothInstances**。
   b. 對於資源類型，請選擇 aw: ec2: 執行個體。
   c. 對於 Target 方法，請選擇資源 ID，然後選擇兩個測試實例的 ID。
   d. 針對「選取」模式，選擇「全部」
   e. 選擇儲存。
8. 在「動作」區段中，選擇「新增動作」。請執行下列操作：
   a. 在「名稱」中，輸入動作的名稱。例如，輸入 **stopBothInstances**。
   b. 針對「動作類型」，選擇 aw: ec2: 停止執行個體。
   c. 在「在之後開始」中，選擇您新增的第一個動作 (**stopOneInstance**)。
   d. 針對「目標」，選擇您新增的第二個目標 (**bothInstances**)。
   e. 對於「動作參數」，請在持續時間後啟動執行個體，指定 3 分鐘 (PT3M)。
   f. 選擇儲存。

9. 對於「服務存取」，請選擇「使用現有的 IAM 角色」，然後按照本教學課程的先決條件中所述選擇您建立的 IAM 角色。如果未顯示您的角色，請確認其具有必要的信任關係。如需詳細資訊，請參閱 the section called “實驗角色”。
10. (選擇性) 對於標籤，請選擇「新增標籤」，然後指定標籤鍵和標籤值。您新增的標籤會套用至您的實驗範本，而不是使用範本執行的實驗。
11. 選擇創建實驗模板。出現確認提示時，請輸入，**create**然後選擇「創建實驗模板」。

(選擇性) 若要檢視實驗範本 JSON

選擇 [匯出] 索引標籤。以下是上述主控台程序所建立的 JSON 範例。

```
{
    "description": "Test instance stop and start",
    "targets": {
        "bothInstances": {
            "resourceType": "aws:ec2:instance",
            "resourceArns": [
                "arn:aws:ec2:region:123456789012:instance/instance_id_1",
                "arn:aws:ec2:region:123456789012:instance/instance_id_2"
            ],
            "selectionMode": "ALL"
        },
        "oneRandomInstance": {
            "resourceType": "aws:ec2:instance",
            "resourceArns": [
                "arn:aws:ec2:region:123456789012:instance/instance_id_1",
                "arn:aws:ec2:region:123456789012:instance/instance_id_2"
            ],
            "selectionMode": "COUNT(1)"
        }
    },
    "actions": {
        "stopBothInstances": {
            "actionId": "aws:ec2:stop-instances",
            "parameters": {
                "startInstancesAfterDuration": "PT3M"
            },
            "targets": {
                "Instances": "bothInstances"
            },
            "startAfter": [
```

```
                "stopOneInstance"
            ]
        },
        "stopOneInstance": {
            "actionId": "aws:ec2:stop-instances",
            "parameters": {
                "startInstancesAfterDuration": "PT3M"
            },
            "targets": {
                "Instances": "oneRandomInstance"
            }
        }
    },
    "stopConditions": [
        {
            "source": "none"
        }
    ],
    "roleArn": "arn:aws:iam::123456789012:role/AllowFISEC2Actions",
    "tags": {}
}
```

步驟 2：開始實驗

完成實驗模板的創建後，您可以使用它來開始實驗。

開始實驗的步驟

1. 您應該在剛剛創建的實驗模板的詳細信息頁面上。否則，請選擇實驗模板，然後選擇實驗模板的 ID 以打開詳細信息頁面。
2. 選擇 Start experiment (開始實驗)。
3. （可選）要在實驗中添加標籤，請選擇「添加新標籤」，然後輸入標籤鍵和標籤值。
4. 選擇 Start experiment (開始實驗)。出現確認提示時，輸入**start**並選擇「開始實驗」。

步驟 3：追蹤實驗進度

您可以追蹤執行中實驗的進度，直到實驗完成、停止或失敗為止。

追蹤實驗的進度

1. 您應該在剛開始實驗的詳細信息頁面上。否則，請選擇實驗，然後選擇實驗的 ID 以打開詳細信息頁面。
2. 要查看實驗的狀態，請檢查詳細信息窗格中的狀態。如需詳細資訊，請參閱實驗狀態。
3. 當實驗的狀態為「運行」時，請轉到下一個步驟。

步驟 4：驗證實驗結果

您可以驗證實例是否已按預期停止和啟動實驗。

驗證實驗結果

1. 在新的瀏覽器索引標籤或視窗中開啟 Amazon EC2 主控台，網址為 https://console.aws.amazon.com/ec2/。這可讓您在 AWS FIS 主控台中繼續追蹤實驗進度，同時在 Amazon EC2 主控台中檢視實驗結果。
2. 在導覽窗格中，選擇執行個體。
3. 當第一個動作的狀態從「擱置中」變更為「執行中」(AWSFIS 主控台) 時，其中一個目標執行個體的狀態會從「執行中」變更為「已停止」(Amazon EC2 主控台)。
4. 三分鐘後，第一個動作的狀態會變更為「已完成」，第二個動作的狀態會變更為「執行中」，而其他目標執行處理的狀態則變更為「已停止」。
5. 三分鐘後，第二個動作的狀態會變更為「已完成」，目標執行個體的狀態會變更為「執行中」，且實驗的狀態會變更為「已完成」。

步驟 5：清除

如果您不再需要為此實驗建立的測試 EC2 執行個體，可以終止它們。

終止執行個體

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導覽窗格中，選擇執行個體。
3. 選取兩個測試執行個體，然後選取 Instance state (執行個體狀態)、Terminate instance (終止執行個體)。
4. 出現確認提示時，請選擇終止。

如果您不再需要實驗範本，可以將其刪除。

使用 AWS FIS 控制台刪除實驗範本

1. 開啟AWS金融資訊系統控制台，網址為 https://console.aws.amazon.com/fis/。
2. 在導覽窗格中，選擇 [實驗範本]。
3. 選取實驗範本，然後選擇 [動作] > [刪除實驗範本]。
4. 當系統提示您進行確認時，請輸入，**delete**然後選擇刪除實驗模板。

教學課程：使用 AWS FIS 在執行個體上執行 CPU stress

您可以使用AWS故障注入服務 (AWSFIS) 來測試應用程式如何處理 CPU stress。使用此教學課程建立實驗範本，該範本使用 AWS FIS 執行預先設定的 SSM 文件，該文件會在執行個體上執行 CPU stress。當執行個體的 CPU 使用率超過設定的臨界值時，教學課程會使用停止條件來中止實驗。

如需詳細資訊，請參閱 the section called “預先設定 AWS 的金融資訊系統 SSM 文件”。

必要條件

在您可以使用 AWS FIS 執行 CPU stress 之前，請先完成下列先決條件。

建立 IAM 角色

建立角色並附加原則，讓 AWS FIS 代表您使用`aws:ssm:send-command`動作。如需詳細資訊，請參閱 適用於 AWS FIS 實驗的 IAM 角色。

驗證對 AWS FIS 的存取

請確定您可以存取 AWS FIS。如需詳細資訊，請參閱 AWSFIS 原則範例。

準備一個測試 EC2 實例

- 根據預先設定的 SSM 文件的要求，使用 Amazon Linux 2 或 Ubuntu 啟動 EC2 執行個體。
- 執行個體必須由 SSM 管理。若要確認執行個體是否由 SSM 管理，請開啟叢集管理員主控台。如果執行個體不是由 SSM 管理，請確認 SSM 代理程式已安裝，並且執行個體具有附加的 IAM 角色與 Amazon ManagedInstanceCore SSM 政策。若要驗證已安裝的 SSM 代理程式，請連線至您的執行個體並執行下列命令。

  Amazon Linux 2

```
yum info amazon-ssm-agent
```

Ubuntu

```
apt list amazon-ssm-agent
```

- 啟用執行個體的詳細監控。這會在 1 分鐘內提供資料，但需額外付費。選取執行個體，然後選擇 [動作]、[監視和疑難排解]、[管理詳細

步驟 1：建立停止狀態的 CloudWatch 警示

設定 CloudWatch 警示，以便在 CPU 使用率超過您指定的閾值時停止實驗。下列程序會將目標執行個體的臨界值設定為 50% CPU 使用率。如需詳細資訊，請參閱 停止條件。

建立警示以指出 CPU 使用率何時超過臨界值

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導覽窗格中，選擇執行個體。
3. 選取目標執行個體，然後選擇 [動作]、[監視及疑難排解]、 CloudWatch [管理
4. 對於警示通知，請使用開關關閉 Amazon SNS 通知。
5. 對於警示臨界值，請使用下列設定：
   - 樣本分組依據：最大
   - 要取樣的資料類型：CPU 使用率
   - 百分比:**50**
   - 期間：**1 Minute**
6. 設定完鬧鐘後，請選擇 [建立]。

步驟 2：建立實驗範本

使用 AWS FIS 主控台建立實驗範本。在範本中，您可以指定下列要執行的動作：aw: ssm: AWSFIS 傳送命令/-Run CPU 應力。

建立實驗樣板的步驟

1. 開啟AWS金融資訊系統控制台，網址為 https://console.aws.amazon.com/fis/。

2. 在導覽窗格中，選擇 [實驗範本]。
3. 選擇創建實驗模板。
4. 在「描述」和「名稱」中，輸入範本的描述和名稱。
5. 對於 Actions (動作)，執行下列動作：
   a. 選擇新增動作。
   b. 輸入動作的名稱。例如，輸入 **runCpuStress**。
   c. 針對「動作類型」，選擇 aw: SSM: AWSFIS 傳送指令/-執行 CPU 應力。這會自動將 SSM 文件的 ARN 新增至文件 ARN。
   d. 針對目標，請保留 AWS FIS 為您建立的目標。
   e. 針對「作業」參數的「文件」參數，輸入下列內容：

      ```
      {"DurationSeconds":"120"}
      ```

   f. 對於「動作參數」 的「持續時間」，指定 5 分鐘 (PT5M)。
   g. 選擇儲存。
6. 對於 Targets (目標)，執行下列動作：
   a. 針對在上一個步驟中為您自動建立 AWS FIS 的目標，選擇 「編輯」。
   b. 以更具描述性的名稱取代預設名稱。例如，輸入 **testInstance**。
   c. 驗證資源類型是 aw:ec2: 實例。
   d. 對於 Target 方法，請選擇資源 ID，然後選擇測試實例的 ID。
   e. 針對「選取」模式，選擇「全部」
   f. 選擇儲存。
7. 對於「服務存取」，請選擇「使用現有的 IAM 角色」，然後按照本教學課程的先決條件中所述選擇您建立的 IAM 角色。如果未顯示您的角色，請確認其具有必要的信任關係。如需詳細資訊，請參閱 the section called “實驗角色”。
8. 針對停止條件，選取您在步驟 1 中建立的 CloudWatch 警示。
9. (選擇性) 對於標籤，請選擇「新增標籤」，然後指定標籤鍵和標籤值。您新增的標籤會套用至您的實驗範本，而不是使用範本執行的實驗。
10. 選擇創建實驗模板。

(選擇性) 若要檢視實驗範本 JSON

選擇 [匯出] 索引標籤。以下是上述主控台程序所建立的 JSON 範例。

```
{
    "description": "Test CPU stress predefined SSM document",
    "targets": {
        "testInstance": {
            "resourceType": "aws:ec2:instance",
            "resourceArns": [
                "arn:aws:ec2:region:123456789012:instance/instance_id"
            ],
            "selectionMode": "ALL"
        }
    },
    "actions": {
        "runCpuStress": {
            "actionId": "aws:ssm:send-command",
            "parameters": {
                "documentArn": "arn:aws:ssm:region::document/AWSFIS-Run-CPU-Stress",
                "documentParameters": "{\"DurationSeconds\":\"120\"}",
                "duration": "PT5M"
            },
            "targets": {
                "Instances": "testInstance"
            }
        }
    },
    "stopConditions": [
        {
            "source": "aws:cloudwatch:alarm",
            "value": "arn:aws:cloudwatch:region:123456789012:alarm:awsec2-instance_id-
GreaterThanOrEqualToThreshold-CPUUtilization"
        }
    ],
    "roleArn": "arn:aws:iam::123456789012:role/AllowFISSSMActions",
    "tags": {}
}
```

步驟 3：開始實驗

完成實驗模板的創建後，您可以使用它來開始實驗。

開始實驗的步驟

1. 您應該在剛剛創建的實驗模板的詳細信息頁面上。否則，請選擇實驗模板，然後選擇實驗模板的 ID 以打開詳細信息頁面。
2. 選擇 Start experiment (開始實驗)。
3. （可選）要在實驗中添加標籤，請選擇「添加新標籤」，然後輸入標籤鍵和標籤值。
4. 選擇 Start experiment (開始實驗)。出現確認提示時，請按一下 **`start`**。選擇 Start experiment (開始實驗)。

步驟 4：追蹤實驗進度

您可以跟踪正在運行的實驗的進度，直到實驗完成，停止或失敗。

追蹤實驗進度

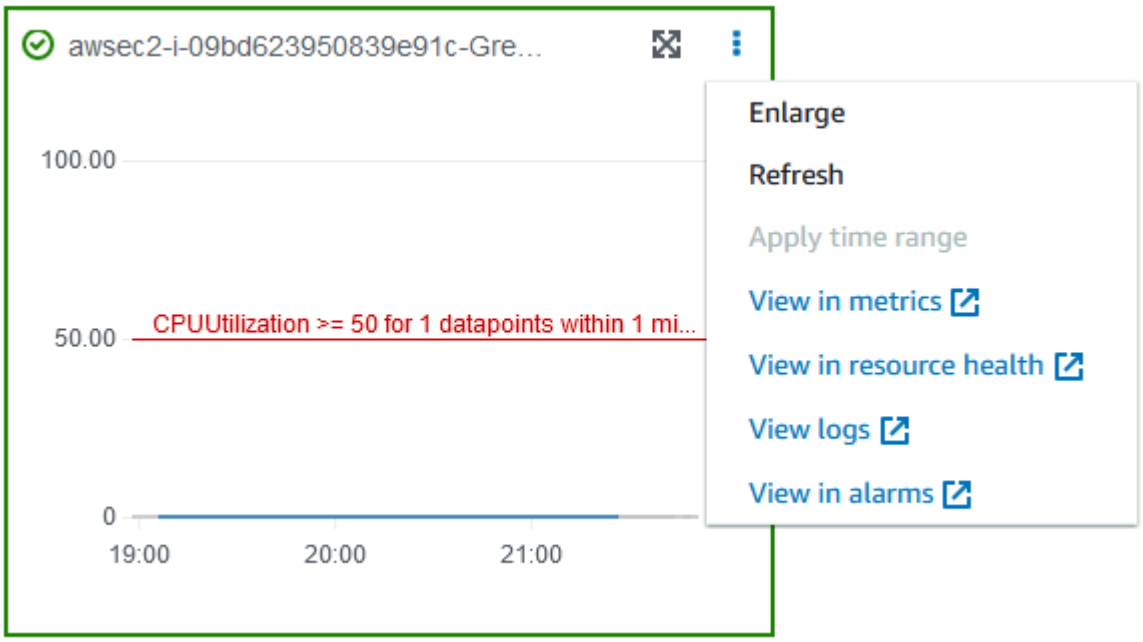
1. 您應該在剛開始實驗的詳細信息頁面上。否則，請選擇實驗，然後選擇實驗的 ID 以打開實驗的詳細信息頁面。
2. 要查看實驗的狀態，請檢查詳細信息窗格中的狀態。如需詳細資訊，請參閱實驗狀態。
3. 當實驗狀態為「執行中」時，請前往下一個步驟。

步驟 5：驗證實驗結果

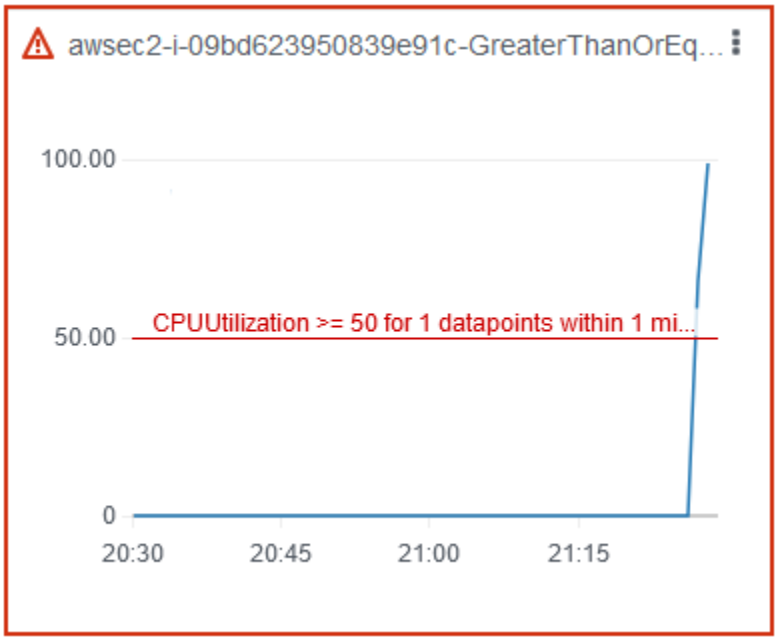
您可以在實驗執行時監控執行個體的 CPU 使用率。當 CPU 使用率達到閾值時，會觸發警報，並由停止條件停止實驗。

驗證實驗結果

1. 選擇「停止條件」標籤。綠色邊框和綠色核取記號圖示表示警示的初始狀態為0K。紅線表示警示臨界值。如果您偏好更詳細的圖表，請從 Widget 選單中選擇「放大」。



2. 當 CPU 使用率超過臨界值時，[停止條件] 索引標籤中的紅色邊框和紅色驚嘆號圖示表示警示狀態已變更為ALARM。在「詳細資料」窗格中，實驗的狀態為「已停止」。如果選擇狀態，則顯示的消息是「實驗停止條件中止」。



3. 當 CPU 使用率降低到臨界值以下時，綠色邊框和綠色核取記號圖示表示警示狀態已變更為0K。
4. (選擇性) 從小工具選單中選擇在鬧鐘中檢視。這會開啟 CloudWatch 主控台中的警示詳細資訊頁面，您可以在其中取得有關鬧鐘的詳細資訊或編輯鬧鐘設定。

步驟 6：清除

如果您不再需要為此實驗建立的測試 EC2 執行個體，可以終止它。

若要終止執行個體

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導覽窗格中，選擇執行個體。
3. 選擇測試實例，然後選擇實例狀態，終止實例。
4. 出現確認提示時，請選擇終止。

如果您不再需要實驗範本，可以將其刪除。

使用 AWS FIS 控制台刪除實驗範本

1. 開啟AWS金融資訊系統控制台，網址為 https://console.aws.amazon.com/fis/。
2. 在導覽窗格中，選擇 [實驗範本]。
3. 選取實驗範本，然後選擇 [動作] > [刪除實驗範本]。
4. 當系統提示您進行確認時，請輸入，**delete**然後選擇刪除實驗模板。

教學課程：使用 FIS 測試 Spot 執行個體中斷 AWS

競價型執行個體使用可用的備用 EC2 容量，與隨需定價相比，discount 高達 90%。但是，Amazon EC2 可以在需要容量恢復時中斷您的競價型執行個體。使用 Spot 執行個體時，您必須為潛在中斷做好準備。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的競價型執行個體中斷。

您可以使用AWS故障注入服務 (AWSFIS) 來測試應用程式如何處理 Spot 執行個體中斷。使用本教學課程建立使用 AWS FIS `aws:ec2:send-spot-instance-interruptions` 動作中斷其中一個 Spot 執行個體的實驗範本。

或者，若要使用 Amazon EC2 主控台啟動實驗，請參閱 Amazon EC2 使用者指南中的啟動競價型執行個體中斷。

必要條件

在您可以使用 AWS FIS 中斷 Spot 執行個體之前，請先完成下列先決條件。

1. 建立 IAM 角色

建立角色並附加原則，讓 AWS FIS 代表您執行aws:ec2:send-spot-instance-interruptions動作。如需詳細資訊，請參閱 適用於 AWS FIS 實驗的 IAM 角色。

2. 驗證對 AWS FIS 的存取

請確定您可以存取 AWS FIS。如需詳細資訊，請參閱 AWSFIS 原則範例。

3. (選擇性) 建立競價型執行個體請求

如果您想要新的 Spot 執行個體用於此實驗，請使用執行個體命令來請求 Spot 執行個體。預設值是終止中斷的 Spot 執行個體。如果您將中斷行為設定為stop，您也必須將類型設定為persistent。在本教學課程中，請勿將中斷行為設定為hibernate，因為休眠程序會立即開始。

```
aws ec2 run-instances \
    --image-id ami-0ab193018fEXAMPLE \
    --instance-type "t2.micro" \
    --count 1 \
    --subnet-id subnet-1234567890abcdef0 \
    --security-group-ids sg-111222333444aaab \
    --instance-market-options file://spot-options.json \
    --query Instances[*].InstanceId
```

以下是 spot-options.json 檔案的範例。

```
{
    "MarketType": "spot",
    "SpotOptions": {
        "SpotInstanceType": "persistent",
        "InstanceInterruptionBehavior": "stop"
    }
}
```

範例指令中的--query選項可讓指令僅傳回 Spot 執行個體的執行個體 ID。下列為範例輸出。

```
[
    "i-0abcdef1234567890"
]
```

4. 加入標籤，以便 AWS FIS 可以識別目標 Spot 例項

使用「建立標籤」指令將標籤新增至目標競價型執Name=interruptMe行個體。

```
aws ec2 create-tags \
    --resources i-0abcdef1234567890 \
    --tags Key=Name,Value=interruptMe
```

步驟 1：建立實驗範本

使用 AWS FIS 主控台建立實驗範本。在範本中，您可以指定要執行的動作。此動作會使用指定的標籤中斷 Spot 執行個體。如果有多個具有標籤的競價型例證，AWSFIS 會隨機選擇其中一個。

建立實驗樣板的步驟

1. 開啟AWS金融資訊系統控制台，網址為 https://console.aws.amazon.com/fis/。
2. 在導覽窗格中，選擇 [實驗範本]。
3. 選擇創建實驗模板。
4. 在「描述」和「名稱」中，輸入範本的描述和名稱。
5. 對於 Actions (動作)，執行下列動作：
    a. 選擇新增動作。
    b. 輸入動作的名稱。例如，輸入 **interruptSpotInstance**。
    c. 針對「動作類型」，選擇 aw: ec2:。send-spot-instance-interruptions
    d. 針對目標，請保留 AWS FIS 為您建立的目標。
    e. 對於動作參數，中斷前的持續時間，指定 2 分鐘 (PT2M)。
    f. 選擇儲存。
6. 對於 Targets (目標)，執行下列動作：
    a. 針對在上一個步驟中為您自動建立 AWS FIS 的目標，選擇 「編輯」。
    b. 以更具描述性的名稱取代預設名稱。例如，輸入 **oneSpotInstance**。
    c. 驗證資源類型是 aw:ec2: 現場實例。
    d. 對於 Target 方法，請選擇資源標籤、篩選器和參數。
    e. 對於資源標籤，請選擇新增標籤，然後輸入標籤鍵和標籤值。使用您新增至 Spot 執行個體的標籤來中斷，如本教學課程的先決條件中所述。
    f. 對於資源過濾器，選擇添加新的過濾器，然後輸入**State.Namerunning**作為路徑和值。
    g. 在選取模式中，選擇「計數」。針對「資源數目」，輸入**1**。

h. 選擇儲存。

7. 對於「服務存取」，請選擇「使用現有的 IAM 角色」，然後按照本教學課程的先決條件中所述選擇您建立的 IAM 角色。如果未顯示您的角色，請確認其具有必要的信任關係。如需詳細資訊，請參閱 the section called “實驗角色”。
8. (選擇性) 對於標籤，請選擇「新增標籤」，然後指定標籤鍵和標籤值。您新增的標籤會套用至您的實驗範本，而不是使用範本執行的實驗。
9. 選擇創建實驗模板。出現確認提示時，請輸入，**create**然後選擇「創建實驗模板」。

(選擇性) 若要檢視實驗範本 JSON

選擇 [匯出] 索引標籤。以下是上述主控台程序所建立的 JSON 範例。

```
{
    "description": "Test Spot Instance interruptions",
    "targets": {
        "oneSpotInstance": {
            "resourceType": "aws:ec2:spot-instance",
            "resourceTags": {
                "Name": "interruptMe"
            },
            "filters": [
                {
                    "path": "State.Name",
                    "values": [
                        "running"
                    ]
                }
            ],
            "selectionMode": "COUNT(1)"
        }
    },
    "actions": {
        "interruptSpotInstance": {
            "actionId": "aws:ec2:send-spot-instance-interruptions",
            "parameters": {
                "durationBeforeInterruption": "PT2M"
            },
            "targets": {
                "SpotInstances": "oneSpotInstance"
            }
        }
```

```
    },
    "stopConditions": [
        {
            "source": "none"
        }
    ],
    "roleArn": "arn:aws:iam::123456789012:role/AllowFISSpotInterruptionActions",
    "tags": {
        "Name": "my-template"
    }
}
```

步驟 2：開始實驗

完成實驗模板的創建後，您可以使用它來開始實驗。

開始實驗的步驟

1. 您應該在剛剛創建的實驗模板的詳細信息頁面上。否則，請選擇實驗模板，然後選擇實驗模板的 ID 以打開詳細信息頁面。
2. 選擇 Start experiment (開始實驗)。
3. （可選）要在實驗中添加標籤，請選擇「添加新標籤」，然後輸入標籤鍵和標籤值。
4. 選擇 Start experiment (開始實驗)。出現確認提示時，輸入**start**並選擇「開始實驗」。

步驟 3：追蹤實驗進度

您可以追蹤執行中實驗的進度，直到實驗完成、停止或失敗為止。

追蹤實驗進度

1. 您應該在剛開始實驗的詳細信息頁面上。否則，請選擇實驗，然後選擇實驗的 ID 以打開詳細信息頁面。
2. 要查看實驗的狀態，請檢查詳細信息窗格中的狀態。如需詳細資訊，請參閱實驗狀態。
3. 當實驗的狀態為「運行」時，請轉到下一個步驟。

步驟 4：驗證實驗結果

完成此實驗的動作後，會發生下列情況：

- 目標 Spot 執行個體會收到執行個體重新平衡建議。
- Amazon EC2 終止或停止執行個體前兩分鐘會發出 Spot 執行個體中斷通知。
- 兩分鐘後，Spot 執行個體就會終止或停止。
- 由 AWS FIS 停止的 Spot 執行個體會保持停止狀態，直到您重新啟動為止。

驗證實例是否被實驗中斷

1. 前往 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 從導覽窗格中，在單獨的瀏覽器索引標籤或視窗中開啟 Spot Requests (Spot 請求) 和 Instances (執行個體)。
3. 對於 Spot Requests (Spot 請求)，選取 Spot 執行個體請求。起始狀態為 `fulfilled`。實驗完成後，狀態會變更如下：
   - `terminate`-狀態變更為`instance-terminated-by-experiment`。
   - `stop`-狀態變更為，`marked-for-stop-by-experiment`然後`instance-stopped-by-experiment`。
4. 對於 Instances (執行個體)，選取 Spot 執行個體。起始狀態為 `Running`。收到 Spot 執行個體中斷通知後兩分鐘，狀態會變更如下：
   - `stop`-狀態變更為，`Stopping`然後`Stopped`。
   - `terminate`-狀態變更為，`Shutting-down`然後`Terminated`。

步驟 5：清除

如果您為此實驗建立了測試 Spot 執行個體的中斷行為，`stop`而您不再需要它，則可以取消競價型執行個體請求並終止 Spot 執行個體。

若要使用取消要求並終止執行個體 AWS CLI

1. 使用命cancel-spot-instance-requests令取消 Spot 執行個體請求。

```
aws ec2 cancel-spot-instance-requests --spot-instance-request-ids sir-ksie869j
```

2. 使用終止實例命令終止實例。

```
aws ec2 terminate-instances --instance-ids i-0abcdef1234567890
```

如果您不再需要實驗範本，可以將其刪除。

使用 AWS FIS 控制台刪除實驗範本

1. 開啟AWS金融資訊系統控制台，網址為 https://console.aws.amazon.com/fis/。
2. 在導覽窗格中，選擇 [實驗範本]。
3. 選取實驗範本，然後選擇 [動作] > [刪除實驗範本]。
4. 出現確認提示時，請輸入，**delete**然後選擇刪除實驗模板。

自學課程：模擬連接事件

您可以使用 AWS 故障注入服務 (AWS FIS) 來模擬各種連線事件。 AWS FIS 會以下列其中一種方式封鎖網路連線，以模擬連線事件：

- `all`— 拒絕所有進入和離開子網路的流量。請注意，此選項允許子網路內部流量，包括進出子網路介面的流量。
- `availability-zone`— 拒絕進出其他可用區域中子網路的 VPC 內部流量。
- `dynamodb`— 拒絕進出目前區域中 DynamoDB 區域端點的流量。
- `prefix-list`— 拒絕往返於指定前置詞清單的流量。
- `s3`— 拒絕目前區域中 Amazon S3 區域端點進出的流量。
- `vpc`— 拒絕流量進入和離開 VPC。

使用此教學建立實驗範本，該範本使用 AWS FIS `aws:network:disrupt-connectivity` 動作導致目標子網路中 Amazon S3 的連線中斷。

主題

必要條件

在開始本教學之前，您需要具有適當許可的角色 AWS 帳戶，並測試 Amazon EC2 執行個體：

具有權限的角色 AWS 帳戶

建立角色並附加原則，讓 AWS FIS 代表您執行`aws:network:disrupt-connectivity`動作。

您的 IAM 角色需要下列政策：

- AWSFaultInjectionSimulatorNetworkAccess— 授予 Amazon EC2 聯網和其他必要服務中的 AWS FIS 服務許可，以執行與網路基礎設施相關的 AWS FIS 動作。

> **Note**
>
> 為了簡單起見，本教學課程使用 AWS 受管理的策略。對於生產環境使用，我們建議您改為僅授與使用案例所需的最低權限。
> 如需有關如何建立 IAM 角色的詳細資訊，請參閱《IAM 使用者指南》中的適用 AWS 於 FIS 實驗的 IAM 角色 (AWS CLI) 或建立 IAM 角色 (主控台)。

測試 Amazon EC2 實例

啟動並連線到測試的 Amazon EC2 執行個體。您可以使用下列教學啟動並連接到 Amazon EC2 執行個體：教學課程：在 Amazon EC2 使用者指南中開始使用 Amazon EC2 Linux 執行個體。

步驟 1：建立 AWS FIS 實驗範本

使用 AWS FI AWS Management Console S 建立實驗範本。 AWS FIS 範本是由動作、目標、停止條件和實驗角色組成。如需有關範本如何運作的詳細資訊，請參閱 AWS FIS 的實驗範本。

在開始之前，請確保您已準備好以下內容：

- 具有正確許可的 IAM 角色。
- Amazon EC2 執行個體。
- 您的亞馬遜 EC2 執行個體的子網路識別碼。

建立實驗樣板的步驟

1. 開啟 AWS 金融資訊系統控制台，網址為 https://console.aws.amazon.com/fis/。

2. 在左側導覽窗格中，選擇 [實驗範本]。
3. 選擇創建實驗模板。
4. 輸入範本的描述，例如Amazon S3 Network Disrupt Connectivity。
5. 在「動作」 下選擇「新增動作」。
   a. 對於「名稱」，輸入disruptConnectivity。
   b. 針對「動作類型」，選取「aw: 網路:中斷連線」。
   c. 在動作參數之下，將持續時間設定為2 minutes。
   d. 在「範圍」下，選取 s3。
   e. 選擇畫面頂端的 [儲存]。
6. 在「目標」下，您應該會看到已自動建立的目標。選擇編輯。
   a. 確認資源類型為aws:ec2:subnet。
   b. 在目標方法下，選取資源 ID，然後在先決條件步驟中選擇您在建立 Amazon EC2 執行個體時使用的子網路。
   c. 確認 「選取」模式為「全部」。
   d. 選擇儲存。
7. 在「服務存取」下，選取您建立的 IAM 角色，如本教學課程的先決條件中所述。如果未顯示您的角色，請確認其具有必要的信任關係。如需詳細資訊，請參閱 the section called “實驗角色”。
8. （可選）在停止條件下，您可以選擇 CloudWatch警報以在條件發生時停止實驗。如需詳細資訊，請參閱 AWS FIS 的停止條件。
9. (選擇性) 在「日誌」下，您可以選取 Amazon S3 儲存貯體，或將日誌傳送到您 CloudWatch 的實驗。
10. 選擇創建實驗模板，並在提示確認時輸入create。然後選擇創建實驗模板。

步驟 2：平安 Amazon S3 端點

確認您的 Amazon EC2 執行個體能夠連接到 Amazon S3 端點。

1. Connect 到您在先決條件步驟中建立的 Amazon EC2 執行個體。

   如需疑難排解，請參閱 Amazon EC2 使用者指南中的疑難排解連線至執行個體。
2. 檢查以查看執行 AWS 區域 個體所在的位置。您可以在 Amazon EC2 主控台或執行下列命令來執行此操作。

```
hostname
```

例如，如果您在中啟動 Amazon EC2 執行個體us-west-2，您會看到下列輸出。

```
[ec2-user@ip-172.16.0.0 ~]$ hostname
ip-172.16.0.0.us-west-2.compute.internal
```

3. Amazon S3 的 AWS 區域. 將 *AWS ##* 取代為您的區域。

```
ping -c 1 s3.AWS ##.amazonaws.com
```

對於輸出，您應該會看到成功的 ping，其中包含 0% 封包遺失，如下列範例所示。

```
PING s3.us-west-2.amazonaws.com (x.x.x.x) 56(84) bytes of data.
64 bytes from s3-us-west-2.amazonaws.com (x.x.x.x: icmp_seq=1 ttl=249 time=1.30 ms

--- s3.us-west-2.amazonaws.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.306/1.306/1.306/0.000 ms
```

步驟 3：開始您的 AWS FIS 實驗

使用剛建立的實驗範本開始實驗。

1. 開啟 AWS 金融資訊系統控制台，網址為 https://console.aws.amazon.com/fis/。
2. 在左側導覽窗格中，選擇 [實驗範本]。
3. 選取您建立的實驗範本 ID，以開啟其詳細資訊頁面。
4. 選擇 Start experiment (開始實驗)。
5. （可選）在確認頁面中，為實驗添加標籤。
6. 在確認頁面中，選擇 [開始實驗]。

步驟 4：追蹤 AWS FIS 實驗進度

您可以追蹤執行中實驗的進度，直到實驗完成、停止或失敗為止。

1. 您應該在剛開始實驗的詳細信息頁面上。如果不是，請選擇實驗，然後選擇實驗的 ID 以打開其詳細信息頁面。
2. 要查看實驗的狀態，請檢查詳細信息窗格中的狀態。如需詳細資訊，請參閱實驗狀態。
3. 當實驗狀態為「執行中」時，請移至下一個步驟。

步驟 5：確認 Amazon S3 網路中斷

您可以透過對 Amazon S3 端點執行偵測來驗證實驗進度。

- 從您的 Amazon EC2 實例中 Amazon S3 在您的 AWS 區域. 將 *AWS ##* 取代為您的區域。

```
ping -c 1 s3.AWS ##.amazonaws.com
```

對於輸出，您應該會看到 100% 封包遺失失敗的 Ping，如下列範例所示。

```
ping -c 1 s3.us-west-2.amazonaws.com
PING s3.us-west-2.amazonaws.com (x.x.x.x) 56(84) bytes of data.

--- s3.us-west-2.amazonaws.com ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms
```

步驟 5：清除

如果您不再需要為此實驗建立的 Amazon EC2 執行個體或 AWS FIS 範本，可以將其移除。

若要移除亞馬遜 EC2 執行個體

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導覽窗格中，選擇執行個體。
3. 選取測試執行個體，選擇執行個體狀態，然後選擇 [終止執行個體]。
4. 出現確認提示時，請選擇終止。

使用 AWS FIS 控制台刪除實驗範本

1. 開啟 AWS 金融資訊系統控制台，網址為 https://console.aws.amazon.com/fis/。
2. 在導覽窗格中，選擇 [實驗範本]。

3. 選取實驗範本，然後選擇 [動作] > [刪除實驗範本]。
4. 當系統提示您進行確認時delete，請輸入，然後選擇刪除實驗範本。

教學課程：排程重複實驗

使用AWS故障注入服務 (AWSFIS)，您可以對AWS工作負載執行故障注入實驗。這些實驗在包含要在指定目標上執行的一或多個動作的範本上執行。當您還使用時Amazon EventBridge，您可以將實驗安排為一次性任務或重複性任務。

使用此自學課程建立每 5 分鐘執行 AWS FIS 實驗範本的 EventBridge 排程。

任務

- 必要條件
- 步驟 1：建立 IAM 角色和政策
- 步驟 2：建立Amazon EventBridge排程器
- 步驟 3：驗證您的實驗
- 步驟 4：清理

必要條件

在開始此自學課程之前，必須具有要按明細表執行的 AWS FIS 實驗樣板。如果您已經擁有可用的實驗範本，請記下範本 ID 和AWS 區域。否則，您可以依照中的指示建立範本the section called “測試實例停止和啟動”，然後返回本自學課程。

步驟 1：建立 IAM 角色和政策

若要建立 IAM 角色和政策

1. 開啟位於 https://console.aws.amazon.com/iam/ 的 IAM 主控台。
2. 在左側導覽窗格中，選擇 [角色]，然後選取 [建立角色]。
3. 選擇 [自訂信任原則]，然後插入下列程式碼片段，讓Amazon EventBridge排程器代表您擔任該角色。

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

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

選擇下一步。

4. 在 [新增權限] 下，選擇 [建立原則]
5. 選擇 [JSON]，然後插入下列原則。將*your-experiment-template-id*值替換為先決條件步驟中實驗的模板 ID。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "fis:StartExperiment",
            "Resource": [
                "arn:aws:fis:*:*:experiment-template/your-experiment-template-id",
                "arn:aws:fis:*:*:experiment/*"
            ]
        }
    ]
}
```

您可以限制排程器僅執行具有特定標籤值的 AWS FIS 實驗。例如，下列政策授予所有 AWS FIS 實驗範本的`StartExperiment`權限，但限制排程器僅執行已標記的實驗。`Purpose=Schedule`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "fis:StartExperiment",
            "Resource": "arn:aws:fis:*:*:experiment/*"
        },
```

```
        {
            "Effect": "Allow",
            "Action": "fis:StartExperiment",
            "Resource": "arn:aws:fis:*:*:experiment-template/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Purpose": "Schedule"
                }
            }
        }
    ]
}
```

選擇下一步：標籤。

6. 選擇下一步：檢閱。
7. 在 [檢閱原則] 底下，命名您的原則`FIS_RecurringExperiment`，然後選擇 [建立原則]。
8. 在 [新增權限] 底下，將新`FIS_RecurringExperiment`原則新增至您的角色，然後選擇 [下一步]。
9. 在 [名稱] 下檢閱和建立角色命名`FIS_RecurringExperiment_role`，然後選擇 [建立角色]。

步驟 2：建立Amazon EventBridge排程器

建立Amazon EventBridge排程器

1. 在以下位置打開 Amazon EventBridge 控制台 https://console.aws.amazon.com/events/。
2. 在左側導覽窗格中，選擇「排程」。
3. 請確認您與 AWS FIS 實驗範本相同AWS 區域。
4. 選擇 [建立排程]，然後填入下列項目：

   - 在「明細表名稱」下，插入`FIS_recurring_experiment_tutorial`。
   - 在排程模式下，選取週期性排程。
   - 在「排程類型」下，選取「以比率為基礎的
   - 在「比率運算式」下，選擇 5 分鐘。
   - 在彈性時間範圍下，選擇關閉。
   - (選擇性) 在時間範圍下，選取您的時區。
   - 選擇下一步。

5. 在 [選取目標] 下，選擇 [所有 API]，然後搜尋 AWSFIS。
6. 選擇 AWSFIS，然後選取StartExperiment。
7. 在「輸入」下，插入下列 JSON 承載。用實驗的模板 ID 替換該*your-experiment-template-id*值。ClientToken是排程器的唯一識別碼。在本教程中，我們使用Amazon EventBridge調度程序允許的上下文關鍵字。如需詳細資訊，請參閱 Amazon EventBridge 使用者指南中的新增內容屬性。

```
{
    "ClientToken": "<aws.scheduler.execution-id>",
    "ExperimentTemplateId": "your-experiment-template-id"
}
```

   選擇下一步。
8. (選擇性) 在 [設定] 下，您可以設定 [重試] 原則、無效字母佇列 (DLQ) 和 [加密] 設定。或者，您可以保留預設值。
9. 在 [權限] 下，選取 [使用現有角色]，然後搜尋FIS_RecurringExperiment_role。
10. 選擇下一步。
11. 在 [檢閱並建立排程] 底下，檢閱排程器詳細資料，然後選擇 [建立排程]。

步驟 3：驗證您的實驗

確認 AWS FIS 實驗是否按排程執行

1. 開啟AWS金融資訊系統控制台，網址為 https://console.aws.amazon.com/fis/。
2. 在左側導覽窗格中，選擇 [實驗]。
3. 建立排程五分鐘後，您應該會看到您的實驗正在執行。

步驟 4：清理

若要停用您的Amazon EventBridge排程器

1. 在以下位置打開 Amazon EventBridge 控制台 https://console.aws.amazon.com/events/。
2. 在左側導覽窗格中，選擇「排程」。
3. 選取新建立的排程器，然後選擇 [停用]。

的動作 AWS FIS

動作是您使用 AWS Fault Injection Service (AWS FIS) 在目標上執行的錯誤注入活動。 AWS FIS 針對跨 AWS 服務的特定類型目標提供預先設定的動作。您可以將動作新增至實驗範本，然後用來執行實驗。

目錄

動作識別碼

每個 AWS FIS 動作都具有下列格式的識別碼：

```
aws:service-name:action-type
```

例如，下列動作會停止目標 Amazon EC2 執行個體：

```
aws:ec2:stop-instances
```

如需動作的完整清單，請參閱AWS FIS 動作參考。若要使用取得清單 AWS CLI，請參閱列出動作。

動作參數

某些 AWS FIS 動作具有動作特定的其他參數。這些參數用於在執行動作 AWS FIS 時將資訊傳遞給。

AWS FIS 使用動作支援自訂錯誤類型，該aws:ssm:send-command動作會使用 SSM 代理程式和 SSM 命令文件在目標執行個體上建立錯誤狀況。該aws:ssm:send-command動作包括一

個documentArn參數，該參數將 SSM 文檔的 Amazon 資源名稱（ARN）作為值。將動作加入至實驗範本時，您可以指定參數的值。

如需有關為aws:ssm:send-command動作指定參數的詳細資訊，請參閱使用動aws:ssm:send-command作。

如果可能的話，您可以在動作參數中輸入復原組態 (也稱為 post 動作)。後置動作會將目標回復為動作執行前所處的狀態。後置動作會在動作持續時間中指定的時間後執行。並非所有動作都支援貼文動作。例如，如果動作終止了 Amazon EC2 執行個體，您就無法在執行個體終止後復原該執行個體。

行動目標

動作會在您指定的目標資源上執行。定義目標之後，您可以在定義動作時指定其名稱。

```
"targets": {
    "resource_type": "resource_name"
}
```

AWS FIS 動作支援動作目標的下列資源類型：

- Auto Scaling 群組 — Amazon EC2 Auto Scaling 群組
- 桶-Amazon S3 桶
- 群集 — Amazon EKS 集群
- 叢集 — Amazon ECS 叢集或 Amazon Aurora 資料庫叢集
- 數據庫執行個體 — Amazon RDS 數據庫
- 加密的全域表 — Amazon DynamoDB；使用客戶受管金鑰加密的全域表
- 全域表 — Amazon DynamoDB；全域表
- 執行個體 — Amazon EC2 執行個體
- 節點群組 — Amazon EKS 節點群組
- 豆莢 — Amazon EKS 上的庫伯尼特豆莢
- ReplicationGroups— ElastiCache Redis 的複製群組
- 角色 — IAM 角色
- SpotInstances— Amazon EC2 競價型實例
- 子網路 — VPC 子網路
- 任務 — Amazon ECS 任務

- TransitGateways— 交通閘道
- 卷 — Amazon EBS 卷

如需範例，請參閱 the section called “動作範例”。

AWS FIS 動作參考

此參考資料說明中的常用動作 AWS FIS，包括動作參數和所需 IAM 許可的相關資訊。您也可以使用 AWS FIS 控制台或 AWS Command Line Interface （AWS CLI）中的列表操作命令列出支持 AWS FIS 的操作。

如需詳細資訊，請參閱 的動作 AWS FIS 及 AWS 故障注入服務如何與 IAM 搭配使用。

動作

- 故障注入動作
- 等待動作
- Amazon CloudWatch 行動
- Amazon DynamoDB 作
- Amazon EBS 動作
- Amazon EC2 動作
- Amazon ECS 動作
- Amazon EKS 動作
- Amazon ElastiCache 行動
- 網路動作
- Amazon RDS 動作
- Amazon S3 動作
- Systems Manager 動作

故障注入動作

AWS FIS 支持以下故障注入操作。

動作

- aws:fis:inject-api-internal-error

- aws:fis:inject-api-throttle-error
- aws:fis:inject-api-unavailable-error

aws:fis:inject-api-internal-error

將內部錯誤注入目標 IAM 角色發出的請求中。

資源類型

- aws:iam:role

參數

- duration— 持續時間, 從一分鐘到 12 小時. 在 AWS FIS API 中，該值是 ISO 8601 格式的字串。例如，PT1M 代表一分鐘。在 AWS FIS 主控台中，您可以輸入秒數、分鐘數或小時數。
- service— 目標 AWS API 命名空間。支援的值為 `ec2`。
- percentage— 將故障插入的呼叫百分比 (1-100)。
- operations— 將錯誤插入的作業，使用逗號分隔。如需ec2命名空間的 API 動作清單，請參閱 Amazon EC2 API 參考中的動作。

許可

- `fis:InjectApiInternalError`

aws:fis:inject-api-throttle-error

將節流錯誤注入目標 IAM 角色發出的請求中。

資源類型

- aws:iam:role

參數

- duration— 持續時間, 從一分鐘到 12 小時. 在 AWS FIS API 中，該值是 ISO 8601 格式的字串。例如，PT1M 代表一分鐘。在 AWS FIS 主控台中，您可以輸入秒數、分鐘數或小時數。
- service— 目標 AWS API 命名空間。支援的值為 `ec2`。

- percentage— 將故障插入的呼叫百分比 (1-100)。
- operations— 將錯誤插入的作業，使用逗號分隔。如需ec2命名空間的 API 動作清單，請參閱 Amazon EC2 API 參考中的動作。

許可

- `fis:InjectApiThrottleError`

aws:fis:inject-api-unavailable-error

將無法使用的錯誤注入目標 IAM 角色發出的請求中。

資源類型

- aws:iam:role

參數

- duration— 持續時間, 從一分鐘到 12 小時. 在 AWS FIS API 中，該值是 ISO 8601 格式的字串。例如，PT1M 代表一分鐘。在 AWS FIS 主控台中，您可以輸入秒數、分鐘數或小時數。
- service— 目標 AWS API 命名空間。支援的值為 ec2。
- percentage— 將故障插入的呼叫百分比 (1-100)。
- operations— 將錯誤插入的作業，使用逗號分隔。如需ec2命名空間的 API 動作清單，請參閱 Amazon EC2 API 參考中的動作。

許可

- `fis:InjectApiUnavailableError`

等待動作

AWS FIS 支持以下等待操作。

aws:fis:wait

執行 AWS FIS 等待動作。

參數

- duration— 持續時間, 從一分鐘到 12 小時. 在 AWS FIS API 中，該值是 ISO 8601 格式的字串。例如，PT1M 代表一分鐘。在 AWS FIS 主控台中，您可以輸入秒數、分鐘數或小時數。

許可

- 無

Amazon CloudWatch 行動

AWS FIS 支持以下 Amazon CloudWatch 行動。

aws:cloudwatch:assert-alarm-state

驗證指定的警示是否處於其中一個指定的警示狀態。

資源類型

- 無

參數

- alarmArns— 警報的 ARN，以逗號分隔。您最多可以指定五個鬧鐘。
- alarmStates— 警報狀態，以逗號分隔。可能的警示狀態為OKALARM、和INSUFFICIENT_DATA。

許可

- `cloudwatch:DescribeAlarms`

Amazon DynamoDB 作

AWS FIS 支援以下 Amazon DynamoDB 作。

aws:dynamodb:global-table-pause-replication

將 Amazon DynamoDB 全域表格複寫暫停至任何複本表格。動作開始後，表格可能會繼續複寫最多 5 分鐘。

下列陳述式會動態附加至目標 DynamoDB 全域表的原則：

```
{
   "Statement":[
      {
         "Sid": "DoNotModifyFisDynamoDbPauseReplicationEXPxxxxxxxxxxxxxx"
         "Effect":"Deny",
         "Principal":{
            "AWS":"arn:aws:iam::123456789012:role/aws-service-role/
replication.dynamodb.amazonaws.com/AWSServiceRoleForDynamoDBReplication"
         },
         "Action":[
            "dynamodb:GetItem",
            "dynamodb:PutItem",
            "dynamodb:UpdateItem",
            "dynamodb:DeleteItem",
            "dynamodb:DescribeTable",
            "dynamodb:UpdateTable",
            "dynamodb:Scan",
            "dynamodb:DescribeTimeToLive",
            "dynamodb:UpdateTimeToLive"
         ],
         "Resource":"arn:aws:dynamodb:us-east-1:123456789012:table/ExampleGlobalTable",
         "Condition": {
            "DateLessThan": {
            "aws:CurrentTime": "2024-04-10T09:51:41.511Z"
         }
       }
      }
   ]
}
```

下列陳述式會動態附加至目標 DynamoDB 全域表的串流原則：

```
{
   "Statement":[
      {
         "Sid": "DoNotModifyFisDynamoDbPauseReplicationEXPxxxxxxxxxxxxxx"
         "Effect":"Deny",
         "Principal":{
            "AWS":"arn:aws:iam::123456789012:role/aws-service-role/
replication.dynamodb.amazonaws.com/AWSServiceRoleForDynamoDBReplication"
         },
```

```
         "Action":[
            "dynamodb:GetRecords",
            "dynamodb:DescribeStream",
            "dynamodb:GetShardIterator"
         ],
         "Resource":"arn:aws:dynamodb:us-east-1:123456789012:table/ExampleGlobalTable/
stream/2023-08-31T09:50:24.025",
         "Condition": {
            "DateLessThan": {
            "aws:CurrentTime": "2024-04-10T09:51:41.511Z"
         }
      }
   ]
}
```

如果目標資料表或串流沒有任何附加的資源策略，則會在實驗期間建立資源策略，並在實驗結束時自動刪除。否則，錯誤陳述式會插入現有的原則中，而不會對現有的原則陳述式進行任何其他修改。然後會在實驗結束時從原則中移除錯誤陳述式。

資源類型

- aws:dynamodb:global-table

參數

- duration— 在 AWS FIS API 中，值是 ISO 8601 格式的字串。例如，PT1M 代表一分鐘。在 AWS FIS 主控台中，您可以輸入秒數、分鐘數或小時數。

許可

- dynamodb:PutResourcePolicy
- dynamodb:DeleteResourcePolicy
- dynamodb:GetResourcePolicy
- dynamodb:DescribeTable
- tag:GetResources

Amazon EBS 動作

AWS FIS 支援下列 Amazon EBS 動作。

aws:ebs:pause-volume-io

暫停目標 EBS 磁碟區上的 I/O 作業。目標磁碟區必須位於相同的可用區域，且必須連接至 Nitro System 上建置的執行個體。磁碟區無法附加至 Outpost 上的執行個體。

若要使用 Amazon EC2 主控台啟動實驗，請參閱 Amazon EC2 使用者指南中的 Amazon EBS 上的故障測試。

資源類型

- aws:ec2:ebs-volume

參數

- duration— 持續時間, 從一秒到 12 小時. 在 AWS FIS API 中，該值是 ISO 8601 格式的字串。例如，PT1M 代表一分鐘，PT5S 代表五秒，PT6H 代表六個小時。在 AWS FIS 主控台中，您可以輸入秒數、分鐘數或小時數。如果持續時間很短，例如 PT5S，I/O 會在指定的持續時間內暫停，但由於初始化實驗所需的時間，可能需要更長的時間才能完成實驗。

許可

- `ec2:DescribeVolumes`
- `ec2:PauseVolumeIO`
- `tag:GetResources`

Amazon EC2 動作

AWS FIS 支援下列 Amazon EC2 動作。

動作

- aws:ec2:api-insufficient-instance-capacity-error
- aws:ec2:asg-insufficient-instance-capacity-error
- aws:ec2:reboot-instances
- aws:ec2:send-spot-instance-interruptions
- aws:ec2:stop-instances
- aws:ec2:terminate-instances

AWS FIS 也支援透過 AWS Systems Manager SSM 代理程式進行錯誤插入動作。Systems Manager 使用 SSM 文件，定義要在 EC2 執行個體上執行的動作。您可以使用自己的文件插入自訂錯誤，也可以使用預先設定的 SSM 文件。如需詳細資訊，請參閱 the section called “使用 SSM 文件”。

aws:ec2:api-insufficient-instance-capacity-error

針對目標 IAM 角色提出的要求插入`InsufficientInstanceCapacity`錯誤回應。支援的作業為 RunInstances CreateCapacityReservation、、 StartInstances、 CreateFleet 呼叫。不支援在多個可用區域中包含容量要求的要求。此動作不支援使用資源標籤、篩選器或參數定義目標。

資源類型

- aws:iam:role

參數

- duration— 在 AWS FIS API 中，值是 ISO 8601 格式的字串。例如，PT1M 代表一分鐘。在 AWS FIS 主控台中，您可以輸入秒數、分鐘數或小時數。
- availabilityzoneIdentifiers— 逗號分隔的可用區域清單。支援區域 ID (例如`"use1-az1, use1-az2"`) 和區域名稱 (例如`"us-east-1a"`)。
- percentage— 將故障插入的呼叫百分比 (1-100)。

許可

- `ec2:InjectApiError`條件索引鍵`ec2:FisActionId`值設定為，`aws:ec2:api-insufficient-instance-capacity-error`並將`ec2:FisTargetArns`條件金鑰設定為目標 IAM 角色。

如需政策範例，請參閱 範例：使用條件鍵 `ec2:InjectApiError`。

aws:ec2:asg-insufficient-instance-capacity-error

針對目標「Auto Scaling」群組發出的要求，注入`InsufficientInstanceCapacity`錯誤回應。此動作僅支援使用啟動範本的「Auto Scaling」群組。若要進一步了解執行個體容量不足錯誤，請參閱 Amazon EC2 使用者指南。

資源類型

- aws:ec2:autoscaling-group

參數

- duration— 在 AWS FIS API 中，值是 ISO 8601 格式的字串。例如，PT1M 代表一分鐘。在 AWS FIS 主控台中，您可以輸入秒數、分鐘數或小時數。
- availabilityzoneIdentifiers— 逗號分隔的可用區域清單。支援區域 ID (例如"use1-az1, use1-az2") 和區域名稱 (例如"us-east-1a")。
- percentage - 選用。插入錯誤之目標 Auto Scaling 群組啟動要求的百分比 (1-100)。預設為 100。

許可

- ec2:InjectApiError條件鍵 ec2：FisActionId 值設置為aws:ec2:asg-insufficient-instance-capacity-error，ec2:FisTargetArns條件鍵設置為目標 Auto Scaling 組。
- autoscaling:DescribeAutoScalingGroups

如需政策範例，請參閱 範例：使用條件鍵 ec2:InjectApiError。

aws:ec2:reboot-instances

在目標 Amazon EC2 執行個體RebootInstances上執行亞馬遜 EC2 API 動作。

資源類型

- aws:ec2:instance

參數

- 無

許可

- ec2:RebootInstances
- ec2:DescribeInstances

AWS 受管理政策

- AWSFaultInjectionSimulatorEC2Access

aws:ec2:send-spot-instance-interruptions

中斷目標 Spot 執行個體。在中斷前兩分鐘，傳送 Spot 執行個體中斷通知以鎖定 Spot 執行個體。中斷時間由指定的持續時間BeforeInterruption參數決定。中斷時間兩分鐘後，Spot 執行個體會根據中斷行為終止或停止。在您重新啟動前， AWS FIS 停止的 Spot 執行個體會保持在停止狀態。

啟動動作後，目標執行個體立即收到 EC2 執行個體重新平衡建議。如果您指定持續時間 BeforeInterruption，則重新平衡建議與中斷通知之間可能會有延遲。

如需詳細資訊，請參閱 the section called “測試競價型執行個體中斷”。或者，若要使用 Amazon EC2 主控台啟動實驗，請參閱 Amazon EC2 使用者指南中的啟動競價型執行個體中斷。

資源類型

- aws:ec2:spot-instance

參數

- durationBeforeInterruption— 中斷執行個體之前的等待時間，從 2 到 15 分鐘。在 AWS FIS API 中，該值是 ISO 8601 格式的字串。例如，PT2M 代表兩分鐘。在主 AWS FIS 控台中，您可以輸入分鐘數。

許可

- `ec2:SendSpotInstanceInterruptions`
- `ec2:DescribeInstances`

AWS 受管理政策

- AWSFaultInjectionSimulatorEC2Access

aws:ec2:stop-instances

在目標 Amazon EC2 執行個體StopInstances上執行亞馬遜 EC2 API 動作。

資源類型

- aws:ec2:instance

參數

- startInstancesAfterDuration - 選用。啟動執行個體前的等待時間，從 1 分鐘到 12 小時。在 AWS FIS API 中，該值是 ISO 8601 格式的字串。例如，PT1M 代表一分鐘。在 AWS FIS 主控台中，您可以輸入秒數、分鐘數或小時數。如果執行個體具有加密的 EBS 磁碟區，您必須授與用於加密磁碟區的 KMS 金鑰 AWS FIS 權限，或將實驗角色新增至 KMS 金鑰政策。
- completeIfInstancesTerminated - 選用。如果為 true，且如果也`startInstancesAfterDuration`為 true，則當目標 EC2 執行個體被 FIS 以外的個別要求終止且無法重新啟動時，此動作將不會失敗。例如，Auto Scaling 群組可能會在其控制下終止已停止的 EC2 執行個體，然後再完成此動作。預設值為 false。

許可

- `ec2:StopInstances`
- `ec2:StartInstances`
- `ec2:DescribeInstances` - 選用。需要完整的「IfInstances已終止」，以在動作結束時驗證執行個體狀態。
- `kms:CreateGrant` - 選用。若要重新啟動具有加密磁碟區的執行個體，需要啟動 InstancesAfter

AWS 受管理政策

- AWSFaultInjectionSimulatorEC2Access

aws:ec2:terminate-instances

在目標 Amazon EC2 執行個體TerminateInstances上執行亞馬遜 EC2 API 動作。

資源類型

- aws:ec2:instance

參數

- 無

許可

- `ec2:TerminateInstances`
- `ec2:DescribeInstances`

AWS 受管理政策

- AWSFaultInjectionSimulatorEC2Access

Amazon ECS 動作

AWS FIS 支援下列 Amazon ECS 動作。

動作

- aws:ecs:drain-container-instances
- aws:ecs:stop-task
- aws:ecs:task-cpu-stress
- aws:ecs:task-io-stress
- aws:ecs:task-kill-process
- aws:ecs:task-network-blackhole-port
- aws:ecs:task-network-latency
- aws:ecs:task-network-packet-loss

aws:ecs:drain-container-instances

執行 Amazon ECS API 動作UpdateContainerInstancesState以耗盡目標叢集上基礎 Amazon EC2 執行個體的指定百分比。

資源類型

- aws:ecs:cluster

參數

- drainagePercentage— 百分比 (1-100)。

- duration— 持續時間, 從一分鐘到 12 小時. 在 AWS FIS API 中，該值是 ISO 8601 格式的字串。例如，PT1M 代表一分鐘。在 AWS FIS 主控台中，您可以輸入秒數、分鐘數或小時數。

許可

- `ecs:DescribeClusters`
- `ecs:UpdateContainerInstancesState`
- `ecs:ListContainerInstances`
- `tag:GetResources`

AWS 受管理政策

- AWSFaultInjectionSimulatorECSAccess

aws:ecs:stop-task

執行 Amazon ECS API 動作StopTask以停止目標任務。

資源類型

- aws:ecs:task

參數

- 無

許可

- `ecs:DescribeTasks`
- `ecs:ListTasks`
- `ecs:StopTask`
- `tag:GetResources`

AWS 受管理政策

- AWSFaultInjectionSimulatorECSAccess

aws:ecs:task-cpu-stress

在目標任務上運行 CPU stress。使用AWSFIS執行 CPU 應力 SSM 文件。任務必須由管理 AWS Systems Manager。如需詳細資訊，請參閱 使用 ECS 任務動作。

資源類型

- aws:ecs:task

參數

- duration— stress 測試的持續時間，採用 ISO 8601 格式。
- percent - 選用。目標負載百分比，從 0 (無負載) 到 100 (滿載)。預設為 100。
- workers - 選用。要使用的壓力源數量。預設值為 0，它使用所有應力源。
- installDependencies - 選用。如果此值為`True`，則 Systems Manager 會在 SSM 代理程式的附屬容器上安裝必要的相依性 (如果尚未安裝)。預設值為 `True`。依賴關係是stress-ng。

許可

- `ssm:SendCommand`
- `ssm:ListCommands`
- `ssm:CancelCommand`

aws:ecs:task-io-stress

對目標工作執行 I/O stress。使用 AWSFIS-執行 IOO 應力 SSM 文件。任務必須由管理 AWS Systems Manager。如需詳細資訊，請參閱 使用 ECS 任務動作。

資源類型

- aws:ecs:task

參數

- duration— stress 測試的持續時間，採用 ISO 8601 格式。
- percent - 選用。stress 測試期間檔案系統上要使用的可用空間百分比。預設值為 80%。

- workers - 選用。工作程序數量。Worker 會混合執行循序、隨機和記憶體對應讀取/寫入作業、強制同步處理和快取卸除。多個子進程在同一個文件上執行不同的 I/O 操作。預設為 1。
- installDependencies - 選用。如果此值為`True`，則 Systems Manager 會在 SSM 代理程式的附屬容器上安裝必要的相依性 (如果尚未安裝)。預設值為 `True`。依賴關係是stress-ng。

許可

- `ssm:SendCommand`
- `ssm:ListCommands`
- `ssm:CancelCommand`

aws:ecs:task-kill-process

使用指killall令停止工作中的指定程序。使用執行 AWSFIS-殺死處理序 SSM 文件。任務定義必須`pidMode`設定為`task`。任務必須由管理 AWS Systems Manager。如需詳細資訊，請參閱 使用 ECS 任務動作。

資源類型

- aws:ecs:task

參數

- processName— 要停止的程序名稱。
- signal - 選用。要與指令一起傳送的訊號。可能的值是`SIGTERM`（接收器可以選擇忽略）和`SIGKILL`（不能忽略）。預設值為 `SIGTERM`。
- installDependencies – 選用。如果此值為`True`，則 Systems Manager 會在 SSM 代理程式的附屬容器上安裝必要的相依性 (如果尚未安裝)。預設值為 `True`。依賴關係是killall。

許可

- `ssm:SendCommand`
- `ssm:ListCommands`
- `ssm:CancelCommand`

aws:ecs:task-network-blackhole-port

捨棄指定通訊協定和連接埠的輸入或輸出流量。使用 AWSFIS-執行網路-黑洞連接埠 SS M 文件。任務定義必須pidMode設定為task。任務必須由管理 AWS Systems Manager。您無法在工作定義bridge中設定networkMode為。如需詳細資訊，請參閱 使用 ECS 任務動作。

資源類型

- aws:ecs:task

參數

- duration— 測試的持續時間，採用 ISO 8601 格式。
- port— 連接埠號碼。
- trafficType— 流量的類型。可能的值為 ingress 和 egress。
- protocol - 選用。通訊協定。可能的值為 tcp 和 udp。預設值為 tcp。
- installDependencies – 選用。如果此值為True，則 Systems Manager 會在 SSM 代理程式的附屬容器上安裝必要的相依性 (如果尚未安裝)。預設值為 True。相依性為atddig、和iptables。

許可

- ssm:SendCommand
- ssm:ListCommands
- ssm:CancelCommand

aws:ecs:task-network-latency

使用特定來源或來自特定來源的流量的tc工具，為網路介面增加延遲和抖動。使用AWSFIS執行網路延遲來源 SSM 文件。任務定義必須pidMode設定為task。任務必須由管理 AWS Systems Manager。您無法在工作定義bridge中設定networkMode為。如需詳細資訊，請參閱 使用 ECS 任務動作。

資源類型

- aws:ecs:task

參數

- duration— 測試的持續時間，採用 ISO 8601 格式。
- interface - 選用。網路介面。預設值為 `eth0`。
- delayMilliseconds – 選用。延遲，以毫秒為單位。預設值為 200。
- jitterMilliseconds - 選用。抖動 (以毫秒為單位)。預設為 10。
- sources - 選用。來源，以逗號分隔。可能的值為：IPv4 位址、IPv4 CIDR 區塊、網域名稱和. DYNAMODB S3 如果您指定DYNAMODB或S3，這僅適用於目前區域中的區域端點。預設值為 0.0.0.0/0，其與所有 IPv4 流量相符。
- installDependencies - 選用。如果此值為`True`，則 Systems Manager 會在 SSM 代理程式的附屬容器上安裝必要的相依性 (如果尚未安裝)。預設值為 `True`。相依性為atddig、jq、和tc。

許可

- `ssm:SendCommand`
- `ssm:ListCommands`
- `ssm:CancelCommand`

aws:ecs:task-network-packet-loss

使用該tc工具將數據包丟失添加到網絡接口。使用執行AWSFIS網路封包遺失來源 SS M 文件。任務定義必須`pidMode`設定為`task`。任務必須由管理 AWS Systems Manager。您無法在工作定義`bridge`中設定`networkMode`為。如需詳細資訊，請參閱 使用 ECS 任務動作。

資源類型

- aws:ecs:task

參數

- duration— 測試的持續時間，採用 ISO 8601 格式。
- interface - 選用。網路介面。預設值為 `eth0`。
- lossPercent – 選用。封包遺失的百分比。預設值為 7%。

- sources - 選用。來源，以逗號分隔。可能的值為：IPv4 位址、IPv4 CIDR 區塊、網域名稱和. DYNAMODB S3 如果您指定DYNAMODB或S3，這僅適用於目前區域中的區域端點。預設值為 0.0.0.0/0，其與所有 IPv4 流量相符。
- installDependencies - 選用。如果此值為True，則 Systems Manager 會在 SSM 代理程式的附屬容器上安裝必要的相依性 (如果尚未安裝)。預設值為 True。相依性為atddig、jq、和tc。

許可

- ssm:SendCommand
- ssm:ListCommands
- ssm:CancelCommand

Amazon EKS 動作

AWS FIS 支援以下 Amazon EKS 動作。

動作

- aws:eks:inject-kubernetes-custom-resource
- aws:eks:pod-cpu-stress
- aws:eks:pod-delete
- aws:eks:pod-io-stress
- aws:eks:pod-memory-stress
- aws:eks:pod-network-blackhole-port
- aws:eks:pod-network-latency
- aws:eks:pod-network-packet-loss
- aws:eks:terminate-nodegroup-instances

aws:eks:inject-kubernetes-custom-resource

在單一目標叢集上執行 ChaosMesh 或石蕊實驗。您必須在目標集群上安裝 ChaosMesh 或石蕊。

建立實驗範本並定義類型的目標時aws:eks:cluster，必須將此動作鎖定為單一 Amazon 資源名稱 (ARN)。此動作不支援使用資源標籤、篩選器或參數定義目標。

安裝時 ChaosMesh，您必須指定適當的容器執行階段。從 Amazon EKS 版本 1.23 開始，默認運行時從碼頭更改為. containerd 從版本 1.24 開始，碼頭工人被刪除。

資源類型

- aws:eks:cluster

參數

- kubernetesApiVersion— 庫伯尼特自訂資源的 API 版本。可能的值為 `chaos-mesh.org/v1alpha1` | `litmuschaos.io/v1alpha1`。
- kubernetesKind— Kubernetes 自訂資源種類。該值取決於 API 版本。
  - `chaos-mesh.org/v1alpha1`— 可能的值為 `AWSChaos` `DNSChaos` `GCPChaos` | `HTTPChaos` | `IOChaos` | `JVMChaos` | `KernelChaos` | `NetworkChaos` | `PhysicalMachineChaos` | `PodChaos` `PodHttpChaos` | `PodIOChaos` | `PodNetworkChaos` | `Schedule` | `StressChaos` | `TimeChaos` |
  - `litmuschaos.io/v1alpha1`— 可能的值為`ChaosEngine`。
- kubernetesNamespace— 庫伯尼特斯命名空間。
- kubernetesSpec— 以 JSON 格式顯示的 Kubernetes 自訂資源`spec`區段。
- maxDuration— 自動化執行完成所允許的最長時間，從 1 分鐘到 12 小時。在 AWS FIS API 中，該值是 ISO 8601 格式的字串。例如，PT1M 代表一分鐘。在 AWS FIS 主控台中，您可以輸入秒數、分鐘數或小時數。

許可

此動作不需要 AWS Identity and Access Management (IAM) 許可。使用此動作所需的權限是由 Kubernetes 使用 RBAC 授權所控制。如需詳細資訊，請參閱官方 Kubernetes 文件中的使用 RBAC 授權。如需有關混沌網格的詳細資訊，請參閱官方的混沌網格文件。有關石蕊的更多信息，請參閱官方石蕊文檔。

aws:eks:pod-cpu-stress

在目標網繭上執行 CPU stress。如需詳細資訊，請參閱 使用 EKS 網繭動作。

資源類型

- aws:eks:pod

參數

- duration— stress 測試的持續時間，採用 ISO 8601 格式。
- percent - 選用。目標負載百分比，從 0 (無負載) 到 100 (滿載)。預設為 100。
- workers - 選用。要使用的壓力源數量。預設值為 0，它使用所有應力源。
- kubernetesServiceAccount— Kubernetes 服務帳戶。如需必要許可的詳細資訊，請參閱the section called “設定 Kubernetes 服務帳戶”。
- fisPodContainerImage - 選用。用來建立故障注入器 Pod 的容器映像檔。預設為使用提供的影像 AWS FIS。如需詳細資訊，請參閱 the section called “豆莢容器映像”。
- maxErrorsPercent – 選用。錯誤注入失敗之前可能失敗的目標百分比。預設值為 0。
- fisPodLabels - 選用。連接至 FIS 建立之錯誤協調流程網繭的 Kubernetes 標籤。
- fisPodAnnotations - 選用。附加至 FIS 所建立之錯誤協調流程網繭的 Kubernetes 註解。
- fisPodSecurityPolicy - 選用。Kubernetes 安全性標準原則，用於 FIS 和暫時容器建立的錯誤協調網繭。可能的值為`privileged`、`baseline`和`restricted`。此動作與所有策略層級相容。

許可

- `eks:DescribeCluster`
- `ec2:DescribeSubnets`
- `tag:GetResources`

AWS 受管理政策

- AWSFaultInjectionSimulatorEKSAccess

aws:eks:pod-delete

刪除目標網繭。如需詳細資訊，請參閱 使用 EKS 網繭動作。

資源類型

- aws:eks:pod

參數

- gracePeriodSeconds - 選用。等待網繭正常終止的持續時間 (以秒為單位)。如果值為 0，我們會立即執行動作。如果值為 nil，我們會使用網繭的預設寬限期。
- kubernetesServiceAccount— Kubernetes 服務帳戶。如需必要許可的詳細資訊，請參閱the section called “設定 Kubernetes 服務帳戶”。
- fisPodContainerImage - 選用。用來建立故障注入器 Pod 的容器映像檔。預設為使用提供的影像 AWS FIS。如需詳細資訊，請參閱 the section called “豆莢容器映像”。
- maxErrorsPercent – 選用。錯誤注入失敗之前可能失敗的目標百分比。預設值為 0。
- fisPodLabels - 選用。連接至 FIS 建立之錯誤協調流程網繭的 Kubernetes 標籤。
- fisPodAnnotations - 選用。附加至 FIS 所建立之錯誤協調流程網繭的 Kubernetes 註解。
- fisPodSecurityPolicy - 選用。Kubernetes 安全性標準原則，用於 FIS 和暫時容器建立的錯誤協調網繭。可能的值為`privileged`、`baseline`和`restricted`。此動作與所有策略層級相容。

許可

- `eks:DescribeCluster`
- `ec2:DescribeSubnets`
- `tag:GetResources`

AWS 受管理政策

- AWSFaultInjectionSimulatorEKSAccess

aws:eks:pod-io-stress

在目標網繭上執行 I/O stress。如需詳細資訊，請參閱 使用 EKS 網繭動作。

資源類型

- aws:eks:pod

參數

- duration— stress 測試的持續時間，採用 ISO 8601 格式。

- workers - 選用。工作程序數量。Worker 會混合執行循序、隨機和記憶體對應讀取/寫入作業、強制同步處理和快取卸除。多個子進程在同一個文件上執行不同的 I/O 操作。預設為 1。
- percent - 選用。stress 測試期間檔案系統上要使用的可用空間百分比。預設值為 80%。
- kubernetesServiceAccount— Kubernetes 服務帳戶。如需必要許可的詳細資訊，請參閱the section called “設定 Kubernetes 服務帳戶”。
- fisPodContainerImage - 選用。用來建立故障注入器 Pod 的容器映像檔。預設為使用提供的影像 AWS FIS。如需詳細資訊，請參閱 the section called “豆莢容器映像”。
- maxErrorsPercent – 選用。錯誤注入失敗之前可能失敗的目標百分比。預設值為 0。
- fisPodLabels - 選用。連接至 FIS 建立之錯誤協調流程網繭的 Kubernetes 標籤。
- fisPodAnnotations - 選用。附加至 FIS 所建立之錯誤協調流程網繭的 Kubernetes 註解。
- fisPodSecurityPolicy - 選用。Kubernetes 安全性標準原則，用於 FIS 和暫時容器建立的錯誤協調網繭。可能的值為`privileged`、`baseline`和`restricted`。此動作與所有策略層級相容。

許可

- `eks:DescribeCluster`
- `ec2:DescribeSubnets`
- `tag:GetResources`

AWS 受管理政策

- AWSFaultInjectionSimulatorEKSAccess

aws:eks:pod-memory-stress

對目標網繭執行記憶體 stress。如需詳細資訊，請參閱 使用 EKS 網繭動作。

資源類型

- aws:eks:pod

參數

- duration— stress 測試的持續時間，採用 ISO 8601 格式。
- workers - 選用。要使用的壓力源數量。預設為 1。

- percent - 選用。stress 測試期間要使用的虛擬記憶體百分比。預設值為 80%。
- kubernetesServiceAccount— Kubernetes 服務帳戶。如需必要許可的詳細資訊，請參閱the section called “設定 Kubernetes 服務帳戶”。
- fisPodContainerImage - 選用。用來建立故障注入器 Pod 的容器映像檔。預設為使用提供的影像 AWS FIS。如需詳細資訊，請參閱 the section called “豆莢容器映像”。
- maxErrorsPercent – 選用。錯誤注入失敗之前可能失敗的目標百分比。預設值為 0。
- fisPodLabels - 選用。連接至 FIS 建立之錯誤協調流程網繭的 Kubernetes 標籤。
- fisPodAnnotations - 選用。附加至 FIS 所建立之錯誤協調流程網繭的 Kubernetes 註解。
- fisPodSecurityPolicy - 選用。Kubernetes 安全性標準原則，用於 FIS 和暫時容器建立的錯誤協調網繭。可能的值為`privileged`、`baseline`和`restricted`。此動作與所有策略層級相容。

許可

- `eks:DescribeCluster`
- `ec2:DescribeSubnets`
- `tag:GetResources`

AWS 受管理政策

- AWSFaultInjectionSimulatorEKSAccess

aws:eks:pod-network-blackhole-port

捨棄指定通訊協定和連接埠的輸入或輸出流量。僅與 Kubernetes 安全性標準原則相容。`privileged`如需詳細資訊，請參閱 使用 EKS 網繭動作。

資源類型

- aws:eks:pod

參數

- duration— 測試的持續時間，採用 ISO 8601 格式。
- protocol - 選用。通訊協定。可能的值為 `tcp` 和 udp。預設值為 `tcp`。
- trafficType— 流量的類型。可能的值為 `ingress` 和 `egress`。

- port— 連接埠號碼。
- kubernetesServiceAccount— Kubernetes 服務帳戶。如需必要許可的詳細資訊，請參閱the section called “設定 Kubernetes 服務帳戶”。
- fisPodContainerImage - 選用。用來建立故障注入器 Pod 的容器映像檔。預設為使用提供的影像 AWS FIS。如需詳細資訊，請參閱 the section called “豆莢容器映像”。
- maxErrorsPercent – 選用。錯誤注入失敗之前可能失敗的目標百分比。預設值為 0。
- fisPodLabels - 選用。連接至 FIS 建立之錯誤協調流程網繭的 Kubernetes 標籤。
- fisPodAnnotations - 選用。附加至 FIS 所建立之錯誤協調流程網繭的 Kubernetes 註解。

許可

- `eks:DescribeCluster`
- `ec2:DescribeSubnets`
- `tag:GetResources`

AWS 受管理政策

- AWSFaultInjectionSimulatorEKSAccess

aws:eks:pod-network-latency

使用特定來源或來自特定來源的流量的tc工具，為網路介面增加延遲和抖動。僅與 Kubernetes 安全性標準原則相容。`privileged`如需詳細資訊，請參閱 使用 EKS 網繭動作。

資源類型

- aws:eks:pod

參數

- duration— 測試的持續時間，採用 ISO 8601 格式。
- interface - 選用。網路介面。預設值為 `eth0`。
- delayMilliseconds – 選用。延遲，以毫秒為單位。預設值為 200。
- jitterMilliseconds - 選用。抖動 (以毫秒為單位)。預設為 10。

- sources - 選用。來源，以逗號分隔。可能的值為：IPv4 位址、IPv4 CIDR 區塊、網域名稱和. DYNAMODB S3 如果您指定DYNAMODB或S3，這僅適用於目前區域中的區域端點。預設值為 0.0.0.0/0，其與所有 IPv4 流量相符。
- kubernetesServiceAccount— Kubernetes 服務帳戶。如需必要許可的詳細資訊，請參閱the section called “設定 Kubernetes 服務帳戶”。
- fisPodContainerImage - 選用。用來建立故障注入器 Pod 的容器映像檔。預設為使用提供的影像 AWS FIS。如需詳細資訊，請參閱 the section called “豆莢容器映像”。
- maxErrorsPercent – 選用。錯誤注入失敗之前可能失敗的目標百分比。預設值為 0。
- fisPodLabels - 選用。連接至 FIS 建立之錯誤協調流程網繭的 Kubernetes 標籤。
- fisPodAnnotations - 選用。附加至 FIS 所建立之錯誤協調流程網繭的 Kubernetes 註解。

許可

- `eks:DescribeCluster`
- `ec2:DescribeSubnets`
- `tag:GetResources`

AWS 受管理政策

- AWSFaultInjectionSimulatorEKSAccess

aws:eks:pod-network-packet-loss

使用該tc工具將數據包丟失添加到網絡接口。僅與 Kubernetes 安全性標準原則相容。`privileged`如需詳細資訊，請參閱 使用 EKS 網繭動作。

資源類型

- aws:eks:pod

參數

- duration— 測試的持續時間，採用 ISO 8601 格式。
- interface - 選用。網路介面。預設值為 `eth0`。
- lossPercent – 選用。封包遺失的百分比。預設值為 7%。

- sources - 選用。來源，以逗號分隔。可能的值為：IPv4 位址、IPv4 CIDR 區塊、網域名稱和. DYNAMODB S3 如果您指定DYNAMODB或S3，這僅適用於目前區域中的區域端點。預設值為 0.0.0.0/0，其與所有 IPv4 流量相符。
- kubernetesServiceAccount— Kubernetes 服務帳戶。如需必要許可的詳細資訊，請參閱the section called “設定 Kubernetes 服務帳戶”。
- fisPodContainerImage - 選用。用來建立故障注入器 Pod 的容器映像檔。預設為使用提供的影像 AWS FIS。如需詳細資訊，請參閱 the section called “豆莢容器映像”。
- maxErrorsPercent – 選用。錯誤注入失敗之前可能失敗的目標百分比。預設值為 0。
- fisPodLabels - 選用。連接至 FIS 建立之錯誤協調流程網繭的 Kubernetes 標籤。
- fisPodAnnotations - 選用。附加至 FIS 所建立之錯誤協調流程網繭的 Kubernetes 註解。

許可

- `eks:DescribeCluster`
- `ec2:DescribeSubnets`
- `tag:GetResources`

AWS 受管理政策

- AWSFaultInjectionSimulatorEKSAccess

aws:eks:terminate-nodegroup-instances

在目標節點群組TerminateInstances上執行 Amazon EC2 API 動作。

資源類型

- aws:eks:nodegroup

參數

- instanceTerminationPercentage— 要終止的執行個體百分比 (1-100)。

許可

- `ec2:DescribeInstances`

- ec2:TerminateInstances
- eks:DescribeNodegroup
- tag:GetResources

AWS 受管理政策

- AWSFaultInjectionSimulatorEKSAccess

Amazon ElastiCache 行動

AWS FIS 支援下列 ElastiCache 動作。

aws:elasticache:interrupt-cluster-az-power

中斷目標 Redis 複寫群組指定可用區域中節點的電源。當主要節點為目標時，複寫延遲最少的對應僅供讀取複本會提升為主要節點。在此動作持續時間內，會封鎖指定可用區域中的僅供讀取複本取代，這表示目標複製群組以較低的容量運作。

資源類型

- aws:elasticache:redis-replicationgroup

參數

- duration— 持續時間, 從一分鐘到 12 小時. 在 AWS FIS API 中，該值是 ISO 8601 格式的字串。例如，PT1M 代表一分鐘。在 AWS FIS 主控台中，您可以輸入秒數、分鐘數或小時數。

許可

- elasticache:InterruptClusterAzPower
- elasticache:DescribeReplicationGroups
- tag:GetResources

網路動作

AWS FIS 支援下列網路動作。

動作

- aws:network:disrupt-connectivity
- aws:network:route-table-disrupt-cross-region-connectivity
- aws:network:transit-gateway-disrupt-cross-region-connectivity

aws:network:disrupt-connectivity

拒絕目標子網路的指定流量。使用網路 ACL。

資源類型

- aws:ec2:subnet

參數

- scope— 要拒絕的流量類型。當範圍不是時`all`，網路 ACL 中的項目數目上限為 20。可能值如下：
  - `all`— 拒絕所有進入和離開子網路的流量。請注意，此選項允許子網路內部流量，包括進出子網路介面的流量。
  - `availability-zone`— 拒絕進出其他可用區域中子網路的 VPC 內部流量。VPC 中可以鎖定目標的子網路數目上限為 30 個。
  - `dynamodb`— 拒絕進出目前區域中 DynamoDB 區域端點的流量。
  - `prefix-list`— 拒絕往返於指定前置詞清單的流量。
  - `s3`— 拒絕目前區域中 Amazon S3 區域端點進出的流量。
  - `vpc`— 拒絕流量進入和離開 VPC。
- duration— 持續時間, 從一分鐘到 12 小時. 在 AWS FIS API 中，該值是 ISO 8601 格式的字串。例如，PT1M 代表一分鐘。在 AWS FIS 主控台中，您可以輸入秒數、分鐘數或小時數。
- prefixListIdentifier— 如果範圍是`prefix-list`，則這是客戶管理前綴列表的標識符。您可以指定名稱、識別碼或 ARN。前綴列表最多可以有 10 個條目。

許可

- `ec2:CreateNetworkAcl`— 使用由 FIS=True 管理的標籤建立網路 ACL。
- `ec2:CreateNetworkAclEntry`— 網路 ACL 必須具有以下列方式管理的標籤 = 真。
- `ec2:CreateTags`

- ec2:DeleteNetworkAcl— 網路 ACL 必須具有以下列方式管理的標籤 = 真。
- ec2:DescribeManagedPrefixLists
- ec2:DescribeNetworkAcls
- ec2:DescribeSubnets
- ec2:DescribeVpcs
- ec2:GetManagedPrefixListEntries
- ec2:ReplaceNetworkAclAssociation

AWS 受管理政策

- AWSFaultInjectionSimulatorNetworkAccess

aws:network:route-table-disrupt-cross-region-connectivity

封鎖源自目標子網路且目的地為指定區域的流量。為要隔離的區域建立包含所有路線的路由表格。若要允許 FIS 建立這些路由表，請將 Amazon VPC 配額提高routes per route table到 250，再加上現有路由表中的路由數目。

資源類型

- aws:ec2:subnet

參數

- region— 要隔離的區域的代碼（例如，eu-west-1）。
- duration— 動作持續的時間長度。在 AWS FIS API 中，該值是 ISO 8601 格式的字串。例如，PT1M 代表一分鐘。在 AWS FIS 主控台中，您可以輸入秒數、分鐘數或小時數。

許可

- ec2:AssociateRouteTable
- ec2:CreateManagedPrefixList †
- ec2:CreateNetworkInterface †
- ec2:CreateRoute †
- ec2:CreateRouteTable †

- ec2:CreateTags †
- ec2:DeleteManagedPrefixList †
- ec2:DeleteNetworkInterface †
- ec2:DeleteRouteTable †
- ec2:DescribeManagedPrefixLists
- ec2:DescribeNetworkInterfaces
- ec2:DescribeRouteTables
- ec2:DescribeSubnets
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DisassociateRouteTable
- ec2:GetManagedPrefixListEntries
- ec2:ModifyManagedPrefixList †
- ec2:ModifyVpcEndpoint
- ec2:ReplaceRouteTableAssociation

† 使用標籤的範圍。managedByFIS=true

AWS 受管理政策

- AWSFaultInjectionSimulatorNetworkAccess

aws:network:transit-gateway-disrupt-cross-region-connectivity

封鎖來自目標傳輸閘道對等附件 (目的地至指定區域) 的流量。

資源類型

- aws:ec2:transit-gateway

參數

- region— 要隔離的區域的代碼（例如，eu-west-1）。
- duration— 動作持續的時間長度。在 AWS FIS API 中，該值是 ISO 8601 格式的字串。例如，PT1M 代表一分鐘。在 AWS FIS 主控台中，您可以輸入秒數、分鐘數或小時數。

許可

- ec2:AssociateTransitGatewayRouteTable
- ec2:DescribeTransitGatewayAttachments
- ec2:DescribeTransitGatewayPeeringAttachments
- ec2:DescribeTransitGateways
- ec2:DisassociateTransitGatewayRouteTable

AWS 受管理政策

- AWSFaultInjectionSimulatorNetworkAccess

Amazon RDS 動作

AWS FIS 支援以下 Amazon RDS 動作。

動作

- aws:rds:failover-db-cluster
- aws:rds:reboot-db-instances

aws:rds:failover-db-cluster

在目標 Aurora 資料庫叢集上執行 Amazon RDS API 動作 FailoverDBCluster。

資源類型

- aws:rds:cluster

參數

- 無

許可

- rds:FailoverDBCluster
- rds:DescribeDBClusters

- `tag:GetResources`

AWS 受管理政策

- AWSFaultInjectionSimulatorRDSAccess

aws:rds:reboot-db-instances

在目標資料庫執行個體上執行 Amazon RDS API 動作重新啟動資料庫執行個體。

資源類型

- aws:rds:db

參數

- forceFailover - 選用。如果值為 true，且執行個體為異地同步備份，則強制從一個可用區域到另一個可用區域的容錯移轉。預設值為 false。

許可

- `rds:RebootDBInstance`
- `rds:DescribeDBInstances`
- `tag:GetResources`

AWS 受管理政策

- AWSFaultInjectionSimulatorRDSAccess

Amazon S3 動作

AWS FIS 支援以下 Amazon S3 動作。

動作

- aws:s3:bucket-pause-replication

aws:s3:bucket-pause-replication

暫停從目標來源儲存貯體到目的地值區的複寫。目的地儲存貯體可以位於不同的 AWS 區域，也可以位於與來源儲存貯體相同的區域內。動作開始後，現有物件最多可能會持續複製一小時。此動作僅支援依標記鎖定目標。若要進一步了解 Amazon S3 複寫，請參閱 Amazon S3 使用者指南。

資源類型

- aws:s3:bucket

參數

- duration— 持續時間, 從一分鐘到 12 小時. 在 AWS FIS API 中，該值是 ISO 8601 格式的字串。例如，PT1M 代表一分鐘。在 AWS FIS 主控台中，您可以輸入秒數、分鐘數或小時數。
- region— 目的地儲存貯體所在的 AWS 區域。
- destinationBuckets - 選用。目的地 S3 儲存貯體的逗號分隔清單。
- prefixes - 選用。複寫規則篩選器中 S3 物件金鑰前置詞的逗號分隔清單。目標儲存貯體的複寫規則會暫停以前置詞為基礎的篩選器。

許可

- `S3:PutReplicationConfiguration`條件鍵`S3:IsReplicationPauseRequest`設定為 `True`
- `S3:GetReplicationConfiguration`條件鍵`S3:IsReplicationPauseRequest`設定為 `True`
- `S3:PauseReplication`
- `S3:ListAllMyBuckets`
- `tag:GetResources`

如需政策範例，請參閱 範例：使用條件鍵 `aws:s3:bucket-pause-replication`。

Systems Manager 動作

AWS FIS 支援下列「Systems Manager」動作。

動作

- aws:ssm:send-command
- aws:ssm:start-automation-execution

aws:ssm:send-command

在目標 EC2 執行個體SendCommand上執行 Systems Manager API 動作。系 Systems Manager 文件 (SSM 文件) 會定義 Systems Manager 在執行個體上執行的動作。如需詳細資訊，請參閱 使用動aws:ssm:send-command作。

資源類型

- aws:ec2:instance

參數

- documentArn— 文件的 Amazon 資源名稱 (ARN)。在主控台中，如果您從動作類型中選擇與其中一個預先設定的 AWS FIS SSM 文件相對應的值，就會為您完成此參數。
- documentVersion - 選用。文件的版本。如果為空，則會執行預設版本。
- documentParameters-有條件的。該文檔接受的必要和可選參數。該格式是一個 JSON 對象，其鍵是字符串和值，無論是字符串或字符串數組。
- duration— 持續時間, 從一分鐘到 12 小時. 在 AWS FIS API 中，該值是 ISO 8601 格式的字串。例如，PT1M 代表一分鐘。在 AWS FIS 主控台中，您可以輸入秒數、分鐘數或小時數。

許可

- `ssm:SendCommand`
- `ssm:ListCommands`
- `ssm:CancelCommand`

AWS 受管理政策

- AWSFaultInjectionSimulatorEC2Access

aws:ssm:start-automation-execution

執行系 Systems Manager API 動作StartAutomation執行。

資源類型

- 無

參數

- documentArn— 自動化文件的 Amazon 資源名稱 (ARN)。
- documentVersion - 選用。文件的版本。如果為空，則會執行預設版本。
- documentParameters-有條件的。該文檔接受的必要和可選參數。該格式是一個 JSON 對象，其鍵是字符串和值，無論是字符串或字符串數組。
- maxDuration— 自動化執行完成所允許的最長時間，從 1 分鐘到 12 小時。在 AWS FIS API 中，該值是 ISO 8601 格式的字串。例如，PT1M 代表一分鐘。在 AWS FIS 主控台中，您可以輸入秒數、分鐘數或小時數。

許可

- `ssm:GetAutomationExecution`
- `ssm:StartAutomationExecution`
- `ssm:StopAutomationExecution`
- `iam:PassRole` - 選用。如果自動化文件擔任角色，則為必要。

AWS 受管理政策

- AWSFaultInjectionSimulatorSSMAccess

搭配 FIS 使用 Systems Manager SSM 文件 AWS

AWS FIS 透過 AWS Systems Manager SSM 代理程式和 FI AWS S 動作支援自訂錯誤類型。aws:ssm:send-command可用來建立常見錯誤插入動作的預先設定 Systems Manager SSM 文件 (SSM 文件) 可做為以-前置詞開頭的公用 AWS 文件使用。 AWSFIS

SSM 代理程式是可在 Amazon EC2 執行個體、現場部署伺服器或虛擬機器 (VM) 上安裝和設定的 Amazon 軟體。這使得系統管理員可以管理這些資源。代理程式會處理來自 Systems Manager 的要求，然後依照要求中的指定來執行要求。您可以包含自己的 SSM 文檔來注入自定義錯誤，或引用亞馬遜公共擁有的文檔之一。

要求

對於需要 SSM 代理程式在目標上執行動作的動作，您必須確定下列事項：

- 代理程式已安裝在目標上。SSM 代理程式預設會安裝在某些 Amazon 機器映像 (AMI) 上。否則，您可以在執行個體上安裝 SSM 代理程式。如需詳細資訊，請參閱AWS Systems Manager 使用者指南中的手動安裝 EC2 執行個體的 SSM 代理程式。
- Systems Manager 有權對您的執行個體執行動作。您可以使用 IAM 執行個體設定檔授予存取權。如需詳細資訊，請參閱AWS Systems Manager 使用者指南中的為 Systems Manager 建立 IAM 執行個體設定檔和將 IAM 執行個體設定檔連接至 EC2 執行個體。

使用動aws:ssm:send-command作

SSM 文件定義 Systems Manager 在受管執行個體上執行的動作。Systems Manager 包含許多預先設定的文件，您也可以建立自己的文件。如需有關建立您自己的 SSM 文件的詳細資訊，請參閱《AWS Systems Manager 使用指南》中的〈建立 Systems Manager 文件〉。如需 SSM 文件一般的詳細資訊，請參閱AWS Systems Manager 使用者指南中的AWS Systems Manager 文件。

AWS FIS 提供預先設定的 SSM 文件。您可以在 AWS Systems Manager 主控台的「文件」下方檢視預先設定的 SSM 文件：https://console.aws.amazon.com/systems-manager/documents。您也可以在 AWS FIS 主控台中選擇預先設定的文件。如需詳細資訊，請參閱 預先設定 AWS 的金融資訊系統 SSM 文件。

若要在 AWS FIS 實驗中使用 SSM 文件，您可以使用動作。aws:ssm:send-command此動作會擷取並執行目標執行個體上指定的 SSM 文件。

當您在實驗範本中使用aws:ssm:send-command動作時，您必須指定動作的其他參數，包括：

- documentArn - 必要。SSM 文件的 Amazon 資源名稱 (ARN)。
- documentParameters-有條件的。SSM 文件接受的必要和選用參數。該格式是一個 JSON 對象，其鍵是字符串和值，無論是字符串或字符串數組。
- documentVersion - 選用。要執行之 SSM 文件的版本。

您可以使用 Systems Manager 主控台或命令列來檢視 SSM 文件的資訊 (包括文件的參數)。

使用控制台檢視 SSM 文件的相關資訊

1. 請在以下位置開啟 AWS Systems Manager 主控台。 https://console.aws.amazon.com/systems-manager/
2. 在導覽窗格中，選擇 Documents (文件)。
3. 選取文件，然後選擇「詳細資訊」標籤。

若要使用命令列檢視 SSM 文件的相關資訊

使用 SSM 描述文件命令。

預先設定 AWS 的金融資訊系統 SSM 文件

您可以將預先設定的 AWS FIS SSM 文件與實驗範本中的`aws:ssm:send-command`動作搭配使用。

要求

- FIS 提供的預先設定 SSM 文件 AWS 僅支援下列作業系統：
  - Amazon Linux, Amazon Linux 2, Amazon Linux
  - Ubuntu
  - 六分之七, 八, 9
  - CentOS 7, 8, 9
- AWS FIS 提供的預先設定 SSM 文件僅在 EC2 執行個體上受到支援。在其他類型的受管理節點 (例如內部部署伺服器) 上不支援它們。

若要在 ECS 任務的實驗中使用這些 SSM 文件，請使用對應的。the section called “Amazon ECS 動作”例如，aws:ecs:task-cpu-stress動作會使用AWSFIS-Run-CPU-Stress文件。

Documents

- AWSFIS-Run-CPU-Stress
- AWSFIS-Run-Disk-Fill
- AWSFIS-Run-IO-Stress
- AWSFIS-Run-Kill-Process
- AWSFIS-Run-Memory-Stress
- AWSFIS-Run-Network-Blackhole-Port
- AWSFIS-Run-Network-Latency
- AWSFIS-Run-Network-Latency-Sources
- AWSFIS-Run-Network-Packet-Loss
- AWSFIS-Run-Network-Packet-Loss-Sources

AWSFIS-Run-CPU-Stress

使用此stress-ng工具在執行個體上執行 CPU stress。使用AWSFIS執行 CPU 應力 SSM 文件。

動作類型 (僅限主控台)

aws:ssm:send-command/AWSFIS-Run-CPU-Stress

ARN

arn:aws:ssm:region::document/AWSFIS-Run-CPU-Stress

文件參數

- DurationSeconds - 必要。CPU stress 測試的持續時間，以秒為單位。
- CPU - 選用。要使用的 CPU 壓力源數目。預設值為 0，會使用所有 CPU 壓力源。
- LoadPercent - 選用。目標 CPU 負載百分比，從 0 (無負載) 到 100 (滿載)。預設為 100。
- InstallDependencies - 選用。如果值為`True`，則 Systems Manager 會在目標執行個體上安裝必要的相依性 (如果尚未安裝)。預設值為 `True`。依賴關係是stress-ng。

以下是您可以在控制台中輸入的字符串的示例。

```
{"DurationSeconds":"60", "InstallDependencies":"True"}
```

AWSFIS-Run-Disk-Fill

在執行個體的根磁碟區上配置磁碟空間，以模擬磁碟已滿錯誤。使用 AWSFIS-執行磁碟填滿 SSM 文件。

如果注入此錯誤的實驗已手動或停止狀態停止， AWS FIS 會嘗試透過取消執行中的 SSM 文件來復原。不過，如果磁碟已滿，無論是因為錯誤或錯誤加上應用程式活動，Systems Manager 可能無法完成取消作業。因此，如果您可能需要停止實驗，請確保磁盤不會變為 100% 滿。

動作類型 (僅限主控台)

aws:ssm:send-command/AWSFIS-Run-Disk-Fill

ARN

arn:aws:ssm:region::document/AWSFIS-Run-Disk-Fill

文件參數

- DurationSeconds - 必要。磁碟填滿測試的持續時間，以秒為單位。
- Percent - 選用。磁碟填滿測試期間要配置的磁碟百分比。預設值為 95%。
- InstallDependencies - 選用。如果值為`True`，則 Systems Manager 會在目標執行個體上安裝必要的相依性 (如果尚未安裝)。預設值為 `True`。依賴關係是atd和fallocate。

以下是您可以在控制台中輸入的字符串的示例。

```
{"DurationSeconds":"60", "InstallDependencies":"True"}
```

AWSFIS-Run-IO-Stress

使用stress-ng工具在執行個體上執行 IO stress。使用 AWSFIS-執行 IOO 應力 SSM 文件。

動作類型 (僅限主控台)

aws:ssm:send-command/AWSFIS-Run-IO-Stress

ARN

arn:aws:ssm:region::document/AWSFIS-Run-IO-Stress

文件參數

- DurationSeconds - 必要。IO stress 測試的持續時間，以秒為單位。
- Workers - 選用。混合執行循序、隨機和記憶體對應讀取/寫入作業、強制同步處理和快取卸除的 Worker 數目。多個子進程在同一個文件上執行不同的 I/O 操作。預設為 1。
- Percent - 選用。在 IO stress 測試期間，檔案系統上要使用的可用空間百分比。預設值為 80%。
- InstallDependencies - 選用。如果值為`True`，則 Systems Manager 會在目標執行個體上安裝必要的相依性 (如果尚未安裝)。預設值為 `True`。依賴關係是stress-ng。

以下是您可以在控制台中輸入的字符串的示例。

```
{"Workers":"1", "Percent":"80", "DurationSeconds":"60", "InstallDependencies":"True"}
```

AWSFIS-Run-Kill-Process

使用指killall令停止執行個體中的指定處理程序。使用執行 AWSFIS-殺死處理序 SSM 文件。

動作類型 (僅限主控台)

aws:ssm:send-command/AWSFIS-Run-Kill-Process

ARN

arn:aws:ssm:region::document/AWSFIS-Run-Kill-Process

文件參數

- ProcessName - 必要。要停止的處理程序名稱。
- Signal - 選用。要與指令一起傳送的訊號。可能的值是SIGTERM（接收器可以選擇忽略）和SIGKILL（不能忽略）。預設值為 SIGTERM。
- InstallDependencies – 選用。如果值為True，則 Systems Manager 會在目標執行個體上安裝必要的相依性 (如果尚未安裝)。預設值為 True。依賴關係是killall。

以下是您可以在控制台中輸入的字符串的示例。

```
{"ProcessName":"myapplication", "Signal":"SIGTERM"}
```

AWSFIS-Run-Memory-Stress

使用stress-ng工具在執行個體上執行記憶體 stress。使用 AWSFIS-執行-記憶體-壓力 SSM 文件。

動作類型 (僅限主控台)

aws:ssm:send-command/AWSFIS-Run-Memory-Stress

ARN

arn:aws:ssm:region::document/AWSFIS-Run-Memory-Stress

文件參數

- DurationSeconds - 必要。記憶體 stress 測試的持續時間，以秒為單位。
- Workers - 選用。虛擬記憶體壓力源的數目。預設為 1。
- Percent - 必要。記憶體 stress 測試期間要使用的虛擬記憶體百分比。
- InstallDependencies - 選用。如果值為True，則 Systems Manager 會在目標執行個體上安裝必要的相依性 (如果尚未安裝)。預設值為 True。依賴關係是stress-ng。

以下是您可以在控制台中輸入的字符串的示例。

```
{"Percent":"80", "DurationSeconds":"60", "InstallDependencies":"True"}
```

AWSFIS-Run-Network-Blackhole-Port

使用iptables工具捨棄通訊協定和連接埠的入站或輸出流量。使用 AWSFIS-執行網路-黑洞連接埠 SS M 文件。

動作類型 (僅限主控台)

aws:ssm:send-command/AWSFIS-Run-Network-Blackhole-Port

ARN

arn:aws:ssm:region::document/AWSFIS-Run-Network-Blackhole-Port

文件參數

- Protocol - 必要。通訊協定。可能的值為 `tcp` 和 `udp`。
- Port - 必要。連接埠號碼。
- TrafficType - 選用。流量類型。可能的值為 `ingress` 和 `egress`。預設值為 `ingress`。
- DurationSeconds - 必要。網路黑洞測試的持續時間，以秒為單位。
- InstallDependencies - 選用。如果值為`True`，則 Systems Manager 會在目標執行個體上安裝必要的相依性 (如果尚未安裝)。預設值為 `True`。相依性為atddig、和iptables。

以下是您可以在控制台中輸入的字符串的示例。

```
{"Protocol":"tcp", "Port":"8080", "TrafficType":"egress", "DurationSeconds":"60",
 "InstallDependencies":"True"}
```

AWSFIS-Run-Network-Latency

使用該tc工具為網絡界面添加延遲。使用AWSFIS執行網路延遲 SSM 文件。

動作類型 (僅限主控台)

aws:ssm:send-command/AWSFIS-Run-Network-Latency

ARN

arn:aws:ssm:region::document/AWSFIS-Run-Network-Latency

文件參數

- Interface - 選用。網路介面。預設值為 eth0。
- DelayMilliseconds – 選用。延遲，以毫秒為單位。預設值為 200。
- DurationSeconds - 必要。網路延遲測試的持續時間，以秒為單位。
- InstallDependencies - 選用。如果值為True，則 Systems Manager 會在目標執行個體上安裝必要的相依性 (如果尚未安裝)。預設值為 True。相依性為atddig、和tc。

以下是您可以在控制台中輸入的字符串的示例。

```
{"DelayMilliseconds":"200", "Interface":"eth0", "DurationSeconds":"60",
 "InstallDependencies":"True"}
```

AWSFIS-Run-Network-Latency-Sources

使用特定來源或來自特定來源的流量的tc工具，為網路介面增加延遲和抖動。使用AWSFIS執行網路延遲來源 SSM 文件。

動作類型 (僅限主控台)

aws:ssm:send-command/AWSFIS-Run-Network-Latency-Sources

ARN

arn:aws:ssm:region::document/AWSFIS-Run-Network-Latency-Sources

文件參數

- Interface - 選用。網路介面。預設值為 eth0。
- DelayMilliseconds – 選用。延遲，以毫秒為單位。預設值為 200。
- JitterMilliseconds - 選用。抖動 (以毫秒為單位)。預設為 10。
- Sources - 必要。來源，以逗號分隔。可能的值為：IPv4 位址、IPv4 CIDR 區塊、網域名稱和. DYNAMODB S3 如果您指定DYNAMODB或S3，這僅適用於目前區域中的區域端點。
- TrafficType - 選用。流量類型。可能的值為 ingress 和 egress。預設值為 ingress。
- DurationSeconds - 必要。網路延遲測試的持續時間，以秒為單位。

- InstallDependencies - 選用。如果值為True，則 Systems Manager 會在目標執行個體上安裝必要的相依性 (如果尚未安裝)。預設值為 True。相依性為atddig、jq、和tc。

以下是您可以在控制台中輸入的字符串的示例。

```
{"DelayMilliseconds":"200", "JitterMilliseconds":"15",
 "Sources":"S3,www.example.com,72.21.198.67", "Interface":"eth0",
 "TrafficType":"egress", "DurationSeconds":"60", "InstallDependencies":"True"}
```

AWSFIS-Run-Network-Packet-Loss

使用該tc工具將數據包丟失添加到網絡接口。使用執行AWSFIS網路封包遺失 SSM 文件。

動作類型 (僅限主控台)

aws:ssm:send-command/AWSFIS-Run-Network-Packet-Loss

ARN

arn:aws:ssm:region::document/AWSFIS-Run-Network-Packet-Loss

文件參數

- Interface - 選用。網路介面。預設值為 eth0。
- LossPercent – 選用。封包遺失的百分比。預設值為 7%。
- DurationSeconds - 必要。網路封包遺失測試的持續時間，以秒為單位。
- InstallDependencies - 選用。如果值為True，Systems Manager 會在目標執行個體上安裝必要的相依性。預設值為 True。相依性為atddig、和tc。

以下是您可以在控制台中輸入的字符串的示例。

```
{"LossPercent":"15", "Interface":"eth0", "DurationSeconds":"60",
 "InstallDependencies":"True"}
```

AWSFIS-Run-Network-Packet-Loss-Sources

使用特定來源的流量的tc工具，將封包遺失新增至網路介面。使用執行AWSFIS網路封包遺失來源 SSM 文件。

動作類型 (僅限主控台)

aws:ssm:send-command/AWSFIS-Run-Network-Packet-Loss-Sources

ARN

arn:aws:ssm:region::document/AWSFIS-Run-Network-Packet-Loss-Sources

文件參數

- Interface - 選用。網路介面。預設值為 `eth0`。
- LossPercent – 選用。封包遺失的百分比。預設值為 7%。
- Sources - 必要。來源，以逗號分隔。可能的值為：IPv4 位址、IPv4 CIDR 區塊、網域名稱和. DYNAMODB S3 如果您指定DYNAMODB或S3，這僅適用於目前區域中的區域端點。
- TrafficType - 選用。流量類型。可能的值為 `ingress` 和 `egress`。預設值為 `ingress`。
- DurationSeconds - 必要。網路封包遺失測試的持續時間，以秒為單位。
- InstallDependencies - 選用。如果值為`True`，Systems Manager 會在目標執行個體上安裝必要的相依性。預設值為 `True`。相依性為atddig、jq、和tc。

以下是您可以在控制台中輸入的字符串的示例。

```
{"LossPercent":"15", "Sources":"S3,www.example.com,72.21.198.67", "Interface":"eth0",
 "TrafficType":"egress", "DurationSeconds":"60", "InstallDependencies":"True"}
```

範例

如需實驗範本範例，請參閱〈〉the section called “執行預先設定的 AWS FIS SSM 文件”。

如需教學課程範例，請參閱在執行個體上執行 CPU stress。

故障診斷

請使用下列程序來疑難排解問題。

疑難排解 SSM 文件的問題

1. 請在以下位置開啟 AWS Systems Manager 主控台。 https://console.aws.amazon.com/systems-manager/
2. 在功能窗格中，選擇節點管理 > 執行命令。
3. 在 [命令歷程記錄] 索引標籤上，使用篩選器來尋找文件的執行。
4. 選擇命令的 ID 以開啟其詳細資訊頁面。

5. 選擇執行個體的 ID。檢閱每個步驟的輸出和錯誤。

使用 AWS FIS 提示檔:EC: 工作動作

您可以使用 aws: EC: 任務動作將錯誤插入 Amazon ECS 任務中。

這些動作使用 SSM 代理程式做為附屬容器來執行會執行錯誤注入的 SSM 文件，並透過附屬容器將 Amazon ECS 任務註冊為 SSM 受管執行個體。若要使用這些動作，您需要更新 Amazon ECS 任務定義，以將 SSM 代理程式新增為附屬容器，以便將執行任務註冊為 SSM 受管執行個體。當您執行 AWS FIS 實驗鎖定目標時`aws:ecs:task`， AWS FIS 會將您在 AWS FIS 實驗範本上指定的目標 Amazon ECS 任務對應到一組使用資源標籤的 SSM 受管執行個體 (新增至受管執行個體)。`ECS_TASK_ARN`標籤值是應在其中執行 SSM 文件的關聯 Amazon ECS 任務的 ARN，因此在執行實驗時不應移除。

動作

- the section called “aws:ecs:task-cpu-stress”
- the section called “aws:ecs:task-io-stress”
- the section called “aws:ecs:task-kill-process”
- the section called “aws:ecs:task-network-blackhole-port”
- the section called “aws:ecs:task-network-latency”
- the section called “aws:ecs:task-network-packet-loss”

限制

- 下列動作不適用於 AWS Fargate：
  - aws:ecs:task-kill-process
  - aws:ecs:task-network-blackhole-port
  - aws:ecs:task-network-latency
  - aws:ecs:task-network-packet-loss
- 如果您啟用 ECS Exec，您必須先停用它，才能使用這些動作。

要求

- 將下列權限新增至 AWS FIS 實驗角色：

  - ssm:SendCommand
  - ssm:ListCommands
  - ssm:CancelCommand
- 將下列許可新增至 Amazon ECS 任務 IAM 角色：
  - ssm:CreateActivation
  - ssm:AddTagsToResource
  - iam:PassRole

  請注意，您可以指定代管執行個體角色的 ARN 做為的資源。iam:PassRole
- 建立 Amazon ECS 任務執行 IAM 角色，並新增 AmazonEC TaskExecution RolePolicy S 受管政策。
- 將下列權限新增至已註冊為代管執行個體之工作的代管執行個體角色：
  - ssm:DeleteActivation
  - ssm:DeregisterManagedInstance
- 將 AmazonSSM ManagedInstance Core 受管政策新增至附加到註冊為代管執行個體之工作的代管執行個體角色。
- 將環境變數設定MANAGED_INSTANCE_ROLE_NAME為代管執行個體角色的名稱。
- 將 SSM 代理程式容器新增至 ECS 工作定義。命令指令碼會將 ECS 工作註冊為受管理執行個體。

```
{
    "name": "amazon-ssm-agent",
    "image": "public.ecr.aws/amazon-ssm-agent/amazon-ssm-agent:latest",
    "cpu": 0,
    "links": [],
    "portMappings": [],
    "essential": false,
    "entryPoint": [],
    "command": [
        "/bin/bash",
        "-c",
        "set -e; yum upgrade -y; yum install jq procps awscli -y; term_handler()
 { echo \"Deleting SSM activation $ACTIVATION_ID\"; if ! aws ssm delete-
activation --activation-id $ACTIVATION_ID --region $ECS_TASK_REGION; then
 echo \"SSM activation $ACTIVATION_ID failed to be deleted\" 1>&2; fi;
 MANAGED_INSTANCE_ID=$(jq -e -r .ManagedInstanceID /var/lib/amazon/ssm/registration);
 echo \"Deregistering SSM Managed Instance $MANAGED_INSTANCE_ID\"; if ! aws
 ssm deregister-managed-instance --instance-id $MANAGED_INSTANCE_ID --region
```

```
 $ECS_TASK_REGION; then echo \"SSM Managed Instance $MANAGED_INSTANCE_ID
 failed to be deregistered\" 1>&2; fi; kill -SIGTERM $SSM_AGENT_PID; }; trap
 term_handler SIGTERM SIGINT; if [[ -z $MANAGED_INSTANCE_ROLE_NAME ]]; then
 echo \"Environment variable MANAGED_INSTANCE_ROLE_NAME not set, exiting\"
 1>&2; exit 1; fi; if ! ps ax | grep amazon-ssm-agent | grep -v grep > /dev/
null; then if [[ -n $ECS_CONTAINER_METADATA_URI_V4 ]] ; then echo \"Found ECS
 Container Metadata, running activation with metadata\"; TASK_METADATA=$(curl
 \"${ECS_CONTAINER_METADATA_URI_V4}/task\"); ECS_TASK_AVAILABILITY_ZONE=$(echo
 $TASK_METADATA | jq -e -r '.AvailabilityZone'); ECS_TASK_ARN=$(echo $TASK_METADATA
 | jq -e -r '.TaskARN'); ECS_TASK_REGION=$(echo $ECS_TASK_AVAILABILITY_ZONE | sed
 's/.$//'); ECS_TASK_AVAILABILITY_ZONE_REGEX='^(af|ap|ca|cn|eu|me|sa|us|us-gov)-
(central|north|(north(east|west))|south|south(east|west)|east|west)-[0-9]{1}[a-z]
{1}$'; if ! [[ $ECS_TASK_AVAILABILITY_ZONE =~ $ECS_TASK_AVAILABILITY_ZONE_REGEX ]];
 then echo \"Error extracting Availability Zone from ECS Container Metadata,
 exiting\" 1>&2; exit 1; fi; ECS_TASK_ARN_REGEX='^arn:(aws|aws-cn|aws-us-gov):ecs:
[a-z0-9-]+:[0-9]{12}:task/[a-zA-Z0-9_-]+/[a-zA-Z0-9]+$'; if ! [[ $ECS_TASK_ARN
 =~ $ECS_TASK_ARN_REGEX ]]; then echo \"Error extracting Task ARN from ECS
 Container Metadata, exiting\" 1>&2; exit 1; fi; CREATE_ACTIVATION_OUTPUT=
$(aws ssm create-activation --iam-role $MANAGED_INSTANCE_ROLE_NAME --
tags Key=ECS_TASK_AVAILABILITY_ZONE,Value=$ECS_TASK_AVAILABILITY_ZONE
 Key=ECS_TASK_ARN,Value=$ECS_TASK_ARN Key=FAULT_INJECTION_SIDECAR,Value=true --
region $ECS_TASK_REGION); ACTIVATION_CODE=$(echo $CREATE_ACTIVATION_OUTPUT | jq
 -e -r .ActivationCode); ACTIVATION_ID=$(echo $CREATE_ACTIVATION_OUTPUT | jq -e
 -r .ActivationId); if ! amazon-ssm-agent -register -code $ACTIVATION_CODE -id
 $ACTIVATION_ID -region $ECS_TASK_REGION; then echo \"Failed to register with AWS
 Systems Manager (SSM), exiting\" 1>&2; exit 1; fi; amazon-ssm-agent & SSM_AGENT_PID=
$!; wait $SSM_AGENT_PID; else echo \"ECS Container Metadata not found, exiting\"
 1>&2; exit 1; fi; else echo \"SSM agent is already running, exiting\" 1>&2; exit 1;
 fi"
    ],
    "environment": [
        {
            "name": "MANAGED_INSTANCE_ROLE_NAME",
            "value": "SSMManagedInstanceRole"
        }
    ],
    "environmentFiles": [],
    "mountPoints": [],
    "volumesFrom": [],
    "secrets": [],
    "dnsServers": [],
    "dnsSearchDomains": [],
    "extraHosts": [],
    "dockerSecurityOptions": [],
```

```
    "dockerLabels": {},
    "ulimits": [],
    "logConfiguration": {},
    "systemControls": []
}
```

如需更具可讀性的指令碼版本，請參閱the section called “指令碼的參考版本”。

- 使用、和aws:ecs:task-network-packet-loss動作時 aws:ecs:task-network-blackhole-portaws:ecs:task-network-latency，您必須使用下列其中一個選項來更新 ECS 工作定義中的 SSM 代理程式容器。
  - 選項 1 — 新增特定的 Linux 功能。

```
"linuxParameters": {
    "capabilities": {
        "add": [
            "NET_ADMIN"
        ]
    }
},
```

  - 選項 2 — 新增所有 Linux 功能。

```
"privileged": true,
```

- 使用aws:ecs:task-kill-process、aws:ecs:task-network-blackhole-port、aws:ecs:task-network-latency和aws:ecs:task-network-packet-loss動作時，ECS 任務定義必須pidMode設定為task。

指令碼的參考版本

以下是「需求」部分中更易讀的腳本版本，供您參考。

```
#!/usr/bin/env bash

# This is the activation script used to register ECS tasks as Managed Instances in SSM
# The script retrieves information form the ECS task metadata endpoint to add three
 tags to the Managed Instance
#  - ECS_TASK_AVAILABILITY_ZONE: To allow customers to target Managed Instances / Tasks
 in a specific Availability Zone
```

```
#  - ECS_TASK_ARN: To allow customers to target Managed Instances / Tasks by using the
 Task ARN
#  - FAULT_INJECTION_SIDECAR: To make it clear that the tasks were registered as
 managed instance for fault injection purposes. Value is always 'true'.
# The script will leave the SSM Agent running in the background
# When the container running this script receives a SIGTERM or SIGINT signal, it will
 do the following cleanup:
#  - Delete SSM activation
#  - Deregister SSM managed instance

set -e # stop execution instantly as a query exits while having a non-zero

yum upgrade -y
yum install jq procps awscli -y

term_handler() {
  echo "Deleting SSM activation $ACTIVATION_ID"
  if ! aws ssm delete-activation --activation-id $ACTIVATION_ID --region
 $ECS_TASK_REGION; then
    echo "SSM activation $ACTIVATION_ID failed to be deleted" 1>&2
  fi

  MANAGED_INSTANCE_ID=$(jq -e -r .ManagedInstanceID /var/lib/amazon/ssm/registration)
  echo "Deregistering SSM Managed Instance $MANAGED_INSTANCE_ID"
  if ! aws ssm deregister-managed-instance --instance-id $MANAGED_INSTANCE_ID --region
 $ECS_TASK_REGION; then
    echo "SSM Managed Instance $MANAGED_INSTANCE_ID failed to be deregistered" 1>&2
  fi

  kill -SIGTERM $SSM_AGENT_PID
}
trap term_handler SIGTERM SIGINT

# check if the required IAM role is provided
if [[ -z $MANAGED_INSTANCE_ROLE_NAME ]] ; then
  echo "Environment variable MANAGED_INSTANCE_ROLE_NAME not set, exiting" 1>&2
  exit 1
fi

# check if the agent is already running (it will be if ECS Exec is enabled)
if ! ps ax | grep amazon-ssm-agent | grep -v grep > /dev/null; then

  # check if ECS Container Metadata is available
  if [[ -n $ECS_CONTAINER_METADATA_URI_V4 ]] ; then
```

```
    # Retrieve info from ECS task metadata endpoint
    echo "Found ECS Container Metadata, running activation with metadata"
    TASK_METADATA=$(curl "${ECS_CONTAINER_METADATA_URI_V4}/task")
    ECS_TASK_AVAILABILITY_ZONE=$(echo $TASK_METADATA | jq -e -r '.AvailabilityZone')
    ECS_TASK_ARN=$(echo $TASK_METADATA | jq -e -r '.TaskARN')
    ECS_TASK_REGION=$(echo $ECS_TASK_AVAILABILITY_ZONE | sed 's/.$//')

    # validate ECS_TASK_AVAILABILITY_ZONE
    ECS_TASK_AVAILABILITY_ZONE_REGEX='^(af|ap|ca|cn|eu|me|sa|us|us-gov)-(central|north|
(north(east|west))|south|south(east|west)|east|west)-[0-9]{1}[a-z]{1}$'
    if ! [[ $ECS_TASK_AVAILABILITY_ZONE =~ $ECS_TASK_AVAILABILITY_ZONE_REGEX ]] ; then
      echo "Error extracting Availability Zone from ECS Container Metadata, exiting"
 1>&2
      exit 1
    fi

    # validate ECS_TASK_ARN
    ECS_TASK_ARN_REGEX='^arn:(aws|aws-cn|aws-us-gov):ecs:[a-z0-9-]+:[0-9]{12}:task/[a-
zA-Z0-9_-]+/[a-zA-Z0-9]+$'
    if ! [[ $ECS_TASK_ARN =~ $ECS_TASK_ARN_REGEX ]] ; then
      echo "Error extracting Task ARN from ECS Container Metadata, exiting" 1>&2
      exit 1
    fi

    # Create activation tagging with Availability Zone and Task ARN
    CREATE_ACTIVATION_OUTPUT=$(aws ssm create-activation \
      --iam-role $MANAGED_INSTANCE_ROLE_NAME \
      --tags Key=ECS_TASK_AVAILABILITY_ZONE,Value=$ECS_TASK_AVAILABILITY_ZONE
 Key=ECS_TASK_ARN,Value=$ECS_TASK_ARN Key=FAULT_INJECTION_SIDECAR,Value=true \
      --region $ECS_TASK_REGION)

    ACTIVATION_CODE=$(echo $CREATE_ACTIVATION_OUTPUT | jq -e -r .ActivationCode)
    ACTIVATION_ID=$(echo $CREATE_ACTIVATION_OUTPUT | jq -e -r .ActivationId)

    # Register with AWS Systems Manager (SSM)
    if ! amazon-ssm-agent -register -code $ACTIVATION_CODE -id $ACTIVATION_ID -region
 $ECS_TASK_REGION; then
      echo "Failed to register with AWS Systems Manager (SSM), exiting" 1>&2
      exit 1
    fi

    # the agent needs to run in the background, otherwise the trapped signal
    # won't execute the attached function until this process finishes
```

```
    amazon-ssm-agent &
    SSM_AGENT_PID=$!

    # need to keep the script alive, otherwise the container will terminate
    wait $SSM_AGENT_PID

  else
    echo "ECS Container Metadata not found, exiting" 1>&2
    exit 1
  fi

else
  echo "SSM agent is already running, exiting" 1>&2
  exit 1
fi
```

範例實驗範本

以下是the section called “aws:ecs:task-cpu-stress”動作的範例實驗範本。

```
{
    "description": "Run CPU stress on the target ECS tasks",
    "targets": {
        "myTasks": {
            "resourceType": "aws:ecs:task",
            "resourceArns": [
                "arn:aws:ecs:us-east-1:111122223333:task/my-
cluster/09821742c0e24250b187dfed8EXAMPLE"
            ],
            "selectionMode": "ALL"
        }
    },
    "actions": {
        "EcsTask-cpu-stress": {
            "actionId": "aws:ecs:task-cpu-stress",
            "parameters": {
                "duration": "PT1M"
            },
            "targets": {
                "Tasks": "myTasks"
            }
        }
    },
```

```
    "stopConditions": [
        {
            "source": "none",
        }
    ],
    "roleArn": "arn:aws:iam::111122223333:role/fis-experiment-role",
    "tags": {}
}
```

使用 AWS FIS 提示:EK: 網繭動作

您可以使用 aw: ek: pod 動作，將錯誤插入到 EKS 叢集中執行的 Kubernetes 網繭中。

動作

- the section called “aws:eks:pod-cpu-stress”
- the section called “aws:eks:pod-delete”
- the section called “aws:eks:pod-io-stress”
- the section called “aws:eks:pod-memory-stress”
- the section called “aws:eks:pod-network-blackhole-port”
- the section called “aws:eks:pod-network-latency”
- the section called “aws:eks:pod-network-packet-loss”

限制

- 下列動作不適用於 AWS Fargate：
  - aws:eks:pod-network-blackhole-port
  - aws:eks:pod-network-latency
  - aws:eks:pod-network-packet-loss
- 下列動作不支援`bridge`網路模式：
  - aws:eks:pod-network-blackhole-port
  - aws:eks:pod-network-latency
  - aws:eks:pod-network-packet-loss
- 您無法使用資源 ARN 或資源標籤識別實驗模板中 aw: ek: pod 類型的目標。您必須使用必要的資源參數來識別目標。

- 動作aws:eks:pod-network-latency和不aws:eks:pod-network-packet-loss應 parallel 執行，並且鎖定相同網繭的目標。視您指定的maxErrors參數值而定，動作可能會以「已完成」或「失敗」狀態結束：
  - 如果maxErrorsPercent為 0 (預設值)，動作將以失敗狀態結束。
  - 否則，失敗將加起來的maxErrorsPercent預算。如果失敗的注射次數沒有達到提供的maxErrors，動作將最終處於完成狀態。
  - 您可以從目標網繭中插入的暫時容器的記錄中識別這些失敗。它會失敗Exit Code: 16。
- 動作不aws:eks:pod-network-blackhole-port應與以相同網繭為目標且使用相同網繭的其他動作 parallel 執行trafficType。支援使用不同流量類型的平行動作。
- FIS 只能在目標網繭的設定為readOnlyRootFilesystem: false時監控錯誤插入securityContext的狀態。如果沒有此組態，所有 EKS 網繭動作都將失敗。

要求

- AWS CLI 在您的計算機上安裝。只有當 AWS CLI 您使用建立 IAM 角色時，才需要這個動作。如需詳細資訊，請參閱安裝或更新 AWS CLI.
- 在您電腦上安裝 kubectl。這只需要與 EKS 叢集互動，以配置或監視目標應用程式。如需詳細資訊，請參閱 https://kubernetes.io/docs/tasks/tools/。
- 最低支援的 EKS 版本為 1.23。

為 Kubernetes 服務帳戶建立服務角色

建立要當做服務角色使用的 IAM 角色。如需詳細資訊，請參閱 the section called “實驗角色”。

設定 Kubernetes 服務帳戶

設定 Kubernetes 服務帳戶，以便對指定 Kubernetes 命名空間中的目標執行實驗。*###########myserviceaccount##########*請注意，這default是其中一個標準的 Kubernetes 命名空間。

若要設定您的 Kubernetes 服務帳戶

1. 創建一個名為的文件，rbac.yaml並添加以下內容。

```
kind: ServiceAccount
apiVersion: v1
metadata:
```

```
  namespace: default
  name: myserviceaccount

---
kind: Role
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  namespace: default
  name: role-experiments
rules:
- apiGroups: [""]
  resources: ["configmaps"]
  verbs: [ "get", "create", "patch", "delete"]
- apiGroups: [""]
  resources: ["pods"]
  verbs: ["create", "list", "get", "delete", "deletecollection"]
- apiGroups: [""]
  resources: ["pods/ephemeralcontainers"]
  verbs: ["update"]
- apiGroups: [""]
  resources: ["pods/exec"]
  verbs: ["create"]
- apiGroups: ["apps"]
  resources: ["deployments"]
  verbs: ["get"]

---
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: bind-role-experiments
  namespace: default
subjects:
- kind: ServiceAccount
  name: myserviceaccount
  namespace: default
- apiGroup: rbac.authorization.k8s.io
  kind: User
  name: fis-experiment
roleRef:
  kind: Role
  name: role-experiments
  apiGroup: rbac.authorization.k8s.io
```

2. 執行下列命令。

```
kubectl apply -f rbac.yaml
```

將您的實驗角色對應至 Kubernetes 使用者

使用下列命令建立識別對應。如需詳細資訊，請參閱 eksctl 文件中的 Manage IAM users and roles 一節。

```
eksctl create iamidentitymapping \
    --arn arn:aws:iam::123456789012:role/fis-experiment-role \
    --username fis-experiment \
    --cluster my-cluster
```

豆荚容器映像

AWS FIS 提供的網繭容器映像會託管在 Amazon ECR 中。當您參考來自 Amazon ECR 的影像時，您必須使用完整的映像 URI。

AWS 區域	映像 URI
美國東部 (俄亥俄)	051821878176.dkr.ecr.us-east-2.amazonaws.com/aws-fis-pod:0.1
美國東部 (維吉尼亞北部)	731367659002.dkr.ecr.us-east-1.amazonaws.com/aws-fis-pod:0.1
美國西部 (加利佛尼亞北部)	080694859247.dkr.ecr.us-west-1.amazonaws.com/aws-fis-pod:0.1
美國西部 (奧勒岡)	864386544765.dkr.ecr.us-west-2.amazonaws.com/aws-fis-pod:0.1
非洲 (開普敦)	056821267933.dkr.ecr.af-south-1.amazonaws.com/aws-fis-pod:0.1
亞太區域 (香港)	246405402639.dkr.ecr.ap-east-1.amazonaws.com/aws-fis-pod:0.1

AWS 區域	映像 URI
亞太區域 (孟買)	524781661239.dkr.ecr.ap-south-1.amazonaws.com/aws-fis-pod:0.1
亞太區域 (首爾)	526524659354.dkr.ecr.ap-northeast-2.amazonaws.com/aws-fis-pod:0.1
亞太區域 (新加坡)	316401638346.dkr.ecr.ap-southeast-1.amazonaws.com/aws-fis-pod:0.1
亞太區域 (雪梨)	488104106298.dkr.ecr.ap-southeast-2.amazonaws.com/aws-fis-pod:0.1
亞太區域 (東京)	635234321696.dkr.ecr.ap-northeast-1.amazonaws.com/aws-fis-pod:0.1
加拿大 (中部)	490658072207.dkr.ecr.ca-central-1.amazonaws.com/aws-fis-pod:0.1
歐洲 (法蘭克福)	713827034473.dkr.ecr.eu-central-1.amazonaws.com/aws-fis-pod:0.1
歐洲 (愛爾蘭)	205866052826.dkr.ecr.eu-west-1.amazonaws.com/aws-fis-pod:0.1
歐洲 (倫敦)	327424803546.dkr.ecr.eu-west-2.amazonaws.com/aws-fis-pod:0.1
歐洲 (米蘭)	478809367036.dkr.ecr.eu-south-1.amazonaws.com/aws-fis-pod:0.1
Europe (Paris)	154605889247.dkr.ecr.eu-west-3.amazonaws.com/aws-fis-pod:0.1
歐洲 (斯德哥爾摩)	263175118295.dkr.ecr.eu-north-1.amazonaws.com/aws-fis-pod:0.1
Middle East (Bahrain)	065825543785.dkr.ecr.me-south-1.amazonaws.com/aws-fis-pod:0.1

AWS 區域	映像 URI
南美洲 (聖保羅)	767113787785.dkr.ecr.sa-east-1.amazonaws.com/aws-fis-pod:0.1
AWS GovCloud (美國東部)	246533647532.dkr.ecr.us-gov-east-1.amazonaws.com/aws-fis-pod:0.1
AWS GovCloud (美國西部)	246529956514.dkr.ecr.us-gov-west-1.amazonaws.com/aws-fis-pod:0.1

範例實驗範本

以下是the section called “aws:eks:pod-network-latency”動作的範例實驗範本。

```
{
    "description": "Add latency and jitter to the network interface for the target EKS
 pods",
    "targets": {
        "myPods": {
            "resourceType": "aws:eks:pod",
            "parameters": {
                "clusterIdentifier": "mycluster",
                "namespace": "default",
                "selectorType": "labelSelector",
                "selectorValue": "mylabel=mytarget"
            },
            "selectionMode": "COUNT(3)"
        }
    },
    "actions": {
        "EksPod-latency": {
            "actionId": "aws:eks:pod-network-latency",
            "description": "Add latency",
            "parameters": {
                "kubernetesServiceAccount": "myserviceaccount",
                "duration": "PT5M",
                "delayMilliseconds": "200",
                "jitterMilliseconds": "10",
                "sources": "0.0.0.0/0"
            },
```

```
            "targets": {
                "Pods": "myPods"
            }
        }
    },
    "stopConditions": [
        {
            "source": "none",
        }
    ],
    "roleArn": "arn:aws:iam::111122223333:role/fis-experiment-role",
    "tags": {
        "Name": "EksPodNetworkLatency"
    }
}
```

使用列出 AWS FIS 動作 AWS CLI

您可以使用 AWS Command Line Interface (AWS CLI) 檢視 AWS FIS 支援之動作的相關資訊。

先決條件

AWS CLI 在您的計算機上安裝。若要開始使用，請參閱《 使用者指南AWS Command Line Interface》。若要取得有關的指令的更多資訊 AWS FIS，請參閱《指AWS CLI 令參考》中的 fis。

範例：列出所有動作的名稱

您可以使用列表操作命令列出所有操作的名稱，如下所示。

```
aws fis list-actions --query "actions[*].[id]" --output text | sort
```

下列為範例輸出。

```
aws:cloudwatch:assert-alarm-state
aws:dynamodb:global-table-pause-replication
aws:ebs:pause-volume-io
aws:ec2:api-insufficient-instance-capacity-error
aws:ec2:asg-insufficient-instance-capacity-error
aws:ec2:reboot-instances
aws:ec2:send-spot-instance-interruptions
aws:ec2:stop-instances
aws:ec2:terminate-instances
```

```
aws:ecs:drain-container-instances
aws:ecs:stop-task
aws:eks:inject-kubernetes-custom-resource
aws:eks:terminate-nodegroup-instances
aws:elasticache:interrupt-cluster-az-power
aws:fis:inject-api-internal-error
aws:fis:inject-api-throttle-error
aws:fis:inject-api-unavailable-error
aws:fis:wait
aws:network:disrupt-connectivity
aws:network:route-table-disrupt-cross-region-connectivity
aws:network:transit-gateway-disrupt-cross-region-connectivity
aws:rds:failover-db-cluster
aws:rds:reboot-db-instances
aws:s3:bucket-pause-replication
aws:ssm:send-command
aws:ssm:start-automation-execution
```

範例：檢視動作的相關資訊

取得動作名稱後，您可以使用 get- action 指令檢視有關動作的詳細資訊，如下所示。

```
aws fis get-action --id aws:ec2:reboot-instances
```

下列為範例輸出。

```
{
    "action": {
        "id": "aws:ec2:reboot-instances",
        "description": "Reboot the specified EC2 instances.",
        "targets": {
            "Instances": {
                "resourceType": "aws:ec2:instance"
            }
        },
        "tags": {}
    }
}
```

AWS FIS 的實驗模板

實驗範本包含在實驗期間在指定目標上執行的一個或多個動作。它還包含阻止實驗超出界限的停止條件。建立實驗範本後，您可以使用它來執行實驗。

範本元件

您將使用以下組件來構建實驗模板：

動作集

您要執AWS 行的 FIS 動作。動作可以按照您指定的設定順序執行，也可以同時執行動作。如需詳細資訊，請參閱 動作集。

目標

執行特定動作的 AWS 資源。如需詳細資訊，請參閱 目標。

停止條件

定義應用程式效能無法接受的臨界值的 CloudWatch 警示。如果在實驗執行時觸發停止條件，AWS FIS 會停止實驗。如需詳細資訊，請參閱 停止條件。

實驗角色

授與 AWS FIS 所需權限的 IAM 角色，以便它可以代表您執行實驗。如需詳細資訊，請參閱 實驗角色。

實驗選項

實驗模板的選項。如需詳細資訊，請參閱 實驗選項。

您的帳戶具有 AWS FIS 相關的配額。例如，每個實驗模板的操作數量都有配額。如需詳細資訊，請參閱 限制和配額。

模板語法

以下是實驗模板的語法。

```
{
            "description": "string",
```

```
            "targets": {},
            "actions": {},
            "stopConditions": [],
            "roleArn": "arn:aws:iam::123456789012:role/AllowFISActions",
            "experimentOptions":{},
            "tags": {}
        }
```

如需範例，請參閱 範例範本。

開始使用

若要使用建立實驗範本 AWS Management Console，請參閱建立實驗範本。

若要使用建立實驗範本 AWS CLI，請參閱AWS FIS 實驗範例範本。

AWS FIS 的動作集

若要建立實驗範本，您必須定義一個或多個動作來組成動作集。如需 AWS FIS 提供的預先定義動作清單，請參閱動作。

您只能在實驗期間執行一次動作。若要在同一 AWS 個實驗中多次執行相同的 FIS 動作，請使用不同的名稱多次將其新增至範本。

目錄

動作語法

以下是動作集的語法。

```
{
    "actions": {
        "action_name": {
            "actionId": "aws:service:action-type",
            "description": "string",
```

```
            "parameters": {
                "name": "value"
             },
            "startAfter": ["action_name", ...],
            "targets": {
                "resource_type": "target_name"
            }
        }
    }
}
```

當您定義動作時，請提供下列資訊：

####

動作的名稱。

actionId

動作識別碼。

description

選擇性的描述。

parameters

任何動作參數。

startAfter

在此動作開始之前必須完成的任何動作。否則，動作會在實驗開始時執行。

targets

任何行動目標。

如需範例，請參閱 the section called “動作範例”。

動作時間

如果動作包含可用來指定動作持續時間的參數，依預設，只有在指定的持續時間過後，才會將動作視為完成。如果您已將emptyTargetResolutionMode實驗選項設定為skip，則當未解決目標時，動作將立即完成，且狀態為「略過」。例如，如果您指定的持續時間為 5 分鐘， AWS FIS 會將動作視為 5 分鐘後完成。然後，它會啟動下一個動作，直到所有動作完成為止。

持續時間可以是維護動作條件的時間長度，也可以是監督測量結果的時間長度。例如，會在指定的時間內插入延遲。對於近乎瞬間的動作類型 (例如終止執行個體)，會在指定的時間內監控停止條件。

如果動作在動作參數中包含貼文動作，則貼文動作會在動作完成後執行。完成後續操作所需的時間可能會導致指定的動作持續時間和下一個動作的開始（或實驗結束時，如果所有其他操作都完成）之間的延遲。

動作範例

以下是範例動作。

範例

- 停止 EC2 執行個體
- 中斷 Spot 執行個
- 中斷網路流量
- 終止 EKS 工作人員

範例：停止 EC2 執行個體

*########################## EC2 #####*兩分鐘後，它會重新啟動目標執行個體。

```
"actions": {
    "stopInstances": {
        "actionId": "aws:ec2:stop-instances",
        "parameters": {
            "startInstancesAfterDuration": "PT2M"
        },
        "targets": {
            "Instances": "targetInstances"
        }
    }
}
```

範例：中斷 Spot 執行個體

下列動作會停止使用名為的目標識別出來的 Spot 執行個體*targetSpotInstances*。它會等待兩分鐘，然後再中斷 Spot 執行個體。

```
"actions": {
    "interruptSpotInstances": {
        "actionId": "aws:ec2:send-spot-instance-interruptions",
        "parameters": {
            "durationBeforeInterruption": "PT2M"
        },
        "targets": {
            "SpotInstances": "targetSpotInstances"
        }
    }
}
```

範例：中斷網路流量

下列動作會拒絕目標子網路與其他可用區域中子網路之間的流量。

```
"actions": {
    "disruptAZConnectivity": {
        "actionId": "aws:network:disrupt-connectivity",
        "parameters": {
            "scope": "availability-zone",
            "duration": "PT5M"
        },
        "targets": {
            "Subnets": "targetSubnets"
        }
    }
}
```

範例：終止 EKS 工作程式

下列動作會終止 EKS 叢集中使用命名目標識別的 50% EC2 執行個體。*targetNodeGroups*

```
"actions": {
    "terminateWorkers": {
        "actionId": "aws:eks:terminate-nodegroup-instances",
        "parameters": {
            "instanceTerminationPercentage": "50"
        },
        "targets": {
            "Nodegroups": "targetNodeGroups"
```

```
        }
    }
}
```

AWS 金融機構的目標

目標是在實驗期間由 AWS 故障注入服務 (AWS FIS) 執行動作的一個或多個 AWS 資源。目標可以與實驗位於相同的 AWS 帳戶中，或使用多帳戶實驗位於不同的帳戶中。若要進一步瞭解如何在不同帳戶中鎖定資源，請參閱多帳戶實驗。

您可以在建立實驗範本時定義目標。您可以在實驗模板中對多個操作使用相同的目標。

AWS FIS 會在實驗開始時識別所有目標，然後再開始動作集中的任何動作。 AWS FIS 會使用它為整個實驗選取的目標資源。如果沒有找到目標，則實驗失敗。

內容

- 目標語法
- 資源類型
- 識別目標資源
  - 資源篩選
  - 資源參數
- 選擇模式
- 範例目標
- 範例篩選

目標語法

以下是目標的語法。

```
{
    "targets": {
        "target_name": {
            "resourceType": "resource-type",
            "resourceArns": [
                "resource-arn"
            ],
            "resourceTags": {
```

```
                "tag-key": "tag-value"
            },
            "parameters": {
                "parameter-name": "parameter-value"
            },
            "filters": [
                {
                    "path": "path-string",
                    "values": ["value-string"]
                }
            ],
            "selectionMode": "value"
        }
    }
}
```

當您定義目標時，請提供下列資訊：

####

目標的名稱。

resourceType

資源類型。

resourceArns

特定資源的 Amazon 資源名稱（ARN）。

resourceTags

套用至特定資源的標籤。

parameters

使用特定屬性識別目標的參數。

filters

資源篩選器會使用特定屬性來設定識別目標資源的範圍。

selectionMode

已識別資源的選取模式。

如需範例，請參閱 the section called “範例目標”。

資源類型

每個 AWS FIS 動作都會針對特定的 AWS 資源類型執行。定義目標時，您必須只指定一種資源類型。當您指定動作的目標時，目標必須是動作支援的資源類型。

AWS FIS 支援下列資源類型：

- aws: 動態:全域表 — Amazon DynamoDB 全域表
- aw: ec2: 自動擴展組 — 一個 Amazon EC2 自 Auto Scaling 組
- 想法:ec2: EBS-體積 — 一個 Amazon EBS 體積
- 提問：ec2：實例-一個 Amazon EC2 實例
- aw:ec2: 現場實例 — 一個 Amazon EC2 現貨實例
- aw: ec2: 子網 — Amazon VPC 子網
- aw: ec2: 傳輸網關 — 一個傳輸網關
- 提出：EC：集群-Amazon ECS 集群
- 提出：EC：任務-Amazon ECS 任務
- aws: EK: 集群 — 一個 Amazon EKS 集群
- aws: EK: 節點組 — Amazon EKS 節點組
- aws: EK: POD — 一個庫伯尼特斯吊艙
- AW: 彈性:重新複製組 — Redis 的複製組 ElastiCache
- aw:iam: 角色 — IAM 角色
- aws: RDS: 叢集 — Amazon Aurora 資料庫叢集
- awds: 資料庫 — 一個 Amazon RDS 資料庫執行個體
- aws：S3：桶-一個 Amazon S3 存儲桶

識別目標資源

在 AWS FIS 主控台中定義目標時，您可以選擇要鎖定目標的特定資 AWS 源 (特定資源類型)。或者，您可以讓 AWS FIS 根據您提供的條件來識別資源群組。

若要識別目標資源，您可以指定下列項目：

- 資源 ID — 特定資源的 AWS 資源 ID。所有資源 ID 都必須代表相同類型的資源。
- 資源標籤 — 套用至特定 AWS 資源的標籤。

- 資源篩選器 — 代表具有特定屬性之資源的路徑和值。如需詳細資訊，請參閱 資源篩選。
- 資源參數 — 代表符合特定條件之資源的參數。如需詳細資訊，請參閱 資源參數。

考量事項

- 您無法同時為相同目標指定資源 ID 和資源標籤。
- 您無法同時為相同目標指定資源 ID 和資源篩選器。
- 如果您指定具有空白標籤值的資源標籤，則該標籤不等同於萬用字元。它匹配具有指定標籤鍵和空標籤值的標籤的資源。

資源篩選

資源篩選器是根據特定屬性識別目標資源的查詢。 AWS FIS 會根據您指定的資源類型，將查詢套用至包含 AWS 資源規範描述的 API 動作的輸出。具有與查詢相符之屬性的資源會包含在目標定義中。

每個篩選器都以屬性路徑和可能的值表示。路徑是一系列元素，以句點分隔，描述在資源的「描述」動作輸出中達到屬性的路徑。每個元素必須在帕斯卡的情況下表示，即使描述動作的資源的輸出是駱駝情況下。例如，您應該使用`AvailabilityZone`，而不是`availablityZone`作為屬性元素。

```
"filters": [
    {
        "path": "component.component.component",
        "values": [
            "string"
        ]
    }
],
```

下表包含 API 動作和 AWS CLI 命令，您可以用來取得每個資源類型的規範描述。 AWS FIS 會代表您執行這些動作，以套用您指定的篩選器。對應的文件說明預設包含在結果中的資源。例如，最近終止例證的`DescribeInstances`狀態文件可能會出現在結果中。

資源類型	API 動作	AWS CLI 命令
aws:ec2:autoscaling-group	DescribeAutoScalingGroups	描述自動縮放群組
aws:ec2:ebs-volume	DescribeVolumes	描述卷

資源類型	API 動作	AWS CLI 命令
aws:ec2:instance	DescribeInstances	描述實例
aws:ec2:subnet	DescribeSubnets	describe-subnets
aws:ec2:transit-gateway	DescribeTransit閘道器	描述傳輸閘道
aws:ecs:cluster	DescribeClusters	describe-clusters
aws:ecs:task	DescribeTasks	描述任務
aws:eks:cluster	DescribeClusters	describe-clusters
aws:eks:nodegroup	DescribeNodegroup	描述節點群組
aws:elasticache:redis-replicationgroup	DescribeReplication群組	描述複製群組
aws:iam:role	ListRoles	列表角色
aws:rds:cluster	DescribeDBClusters	describe-db-clusters
aws:rds:db	DescribeDBInstances	describe-db-instances
aws:s3:bucket	ListBuckets	列表桶

下列邏輯適用於所有資源篩選器：

- 過濾器內的值-OR
- 跨過濾器的值 — AND

如需範例，請參閱 the section called “範例篩選”。

資源參數

資源參數會根據特定條件識別目標資源。

下列資源類型支援參數。

aws:ec2:ebs-volume

- availabilityZoneIdentifier— 包含目標磁碟區之可用區域的程式碼 (例如 us-east-1a)。

aws:ec2:subnet

- availabilityZoneIdentifier— 包含目標子網路之可用區域的程式碼 (例如 us-east-1a) 或 AZ 識別碼 (例如，use1-az1)。
- vpc— 包含目標子網路的 VPC。每個帳戶不支援一個以上的 VPC。

aws:ecs:task

- cluster— 包含目標作業的叢集。
- service— 包含目標工作的服務。

aws:eks:pod

- availabilityZoneIdentifier - 選用。包含目標網繭的可用區域。例如 us-east-1d。我們透過比較網繭的 HoSTIP 和叢集子網路的 CIDR 來判斷網繭的可用區域。
- clusterIdentifier - 必要。目標 EKS 叢集的名稱或 ARN。
- namespace - 必要。目標網繭的 Kubernetes 命名空間。
- selectorType - 必要。選擇器類型。可能的值為 labelSelector、deploymentName 和 podName。
- selectorValue - 必要。選擇器值。此值取決於的值selectorType。
- targetContainerName - 選用。網繭規格中定義的目標容器名稱。預設值是每個目標網繭規格中定義的第一個容器。

aws:rds:cluster

- writerAvailabilityZoneIdentifiers - 選用。資料庫叢集之寫入器的可用區域。可能的值為：以逗號分隔的可用區域識別碼清單、all。

aws:rds:db

- availabilityZoneIdentifiers - 選用。受影響之資料庫執行個體的可用區域。可能的值為：以逗號分隔的可用區域識別碼清單、all。

aws:elasticache:redis-replicationgroup

- availabilityZoneIdentifier - 必要。包含目標節點之可用區域的程式碼 (例如 US-east-1a) 或 AZ 識別碼 (例如，use1-az1)。

選擇模式

您可以透過指定選取模式來限定已識別資源的範圍。 AWS FIS 支援下列選取模式：

- ALL— 在所有目標上執行動作。
- COUNT(n)— 對指定數目的目標執行動作，從識別的目標隨機選擇。例如，COUNT (1) 會選取其中一個已識別的目標。
- PERCENT(n)— 對指定百分比的目標執行動作，從識別的目標隨機選擇。例如，百分比 (25) 會選取已識別目標的 25%。

如果您的資源數為奇數，並指定 50%， AWS FIS 會向下捨入。例如，如果您新增五個 Amazon EC2 執行個體做為目標，並將範圍新增為 50%， AWS FIS 會捨入為兩個執行個體。您無法指定少於一個資源的百分比。例如，如果您將四個 Amazon EC2 執行個體和範圍新增到 5%， AWS FIS 就無法選取執行個體。

如果您使用相同的目標資源類型定義多個目標， AWS FIS 可以多次選取相同的資源。

無論您使用哪種選取模式，如果您指定的範圍未識別資源，則實驗都會失敗。

範例目標

以下是範例目標。

範例

- 具有指定標籤的指定 VPC 中的執行個體
- 具有指定參數的任務

範例：指定 VPC 中具有指定標籤的執行個體

此範例的可能目標是指定 VPC 中具有標籤env=prod的 Amazon EC2 執行個體。選取模式會指定 AWS FIS 隨機選擇其中一個目標。

```
{
    "targets": {
        "randomInstance": {
            "resourceType": "aws:ec2:instance",
            "resourceTags": {
                "env": "prod"
            },
            "filters": [
                {
```

```
                    "path": "VpcId",
                    "values": [
                        "vpc-aabbcc11223344556"
                    ]
                }
            ],
            "selectionMode": "COUNT(1)"
        }
    }
}
```

範例：具有指定參數的工作

此範例可能的目標是具有指定叢集和服務的 Amazon ECS 任務。選取模式會指定 AWS FIS 隨機選擇其中一個目標。

```
{
    "targets": {
        "randomTask": {
            "resourceType": "aws:ecs:task",
            "parameters": {
                "cluster": "myCluster",
                "service": "myService"
            },
            "selectionMode": "COUNT(1)"
        }
    }
}
```

範例篩選

以下是範例篩選器。

範例

- EC2 執行個體
- 資料庫叢集

範例：EC2 執行個體

當您為支援 aw: ec2: 執行個體資源類型的動作指定篩選器時， AWS FIS 會使用 Amazon EC2 describe-instances 命令並套用篩選器來識別目標。

該describe-instances命令返回 JSON 輸出，其中每個實例都是下的結構Instances。以下是部分輸出，其中包含標有##的欄位。我們將提供使用這些欄位從 JSON 輸出結構中指定屬性路徑的範例。

```
{
    "Reservations": [
        {
            "Groups": [],
            "Instances": [
                {
                    "ImageId": "ami-00111111111111111",
                    "InstanceId": "i-00aaaaaaaaaaaaaa",
                    "InstanceType": "t2.micro",
                    "KeyName": "virginia-kp",
                    "LaunchTime": "2020-09-30T11:38:17.000Z",
                    "Monitoring": {
                        "State": "disabled"
                    },
                    "Placement": {
                        "AvailabilityZone": "us-east-1a",
                        "GroupName": "",
                        "Tenancy": "default"
                    },
                    "PrivateDnsName": "ip-10-0-1-240.ec2.internal",
                    "PrivateIpAddress": "10.0.1.240",
                    "ProductCodes": [],
                    "PublicDnsName": "ec2-203-0-113-17.compute-1.amazonaws.com",
                    "PublicIpAddress": "203.0.113.17",
                    "State": {
                        "Code": 16,
                        "Name": "running"
                    },
                    "StateTransitionReason": "",
                    "SubnetId": "subnet-aabbcc11223344556",
                    "VpcId": "vpc-00bbbbbbbbbbbbbbb",
                    ...
                },
                ...
                {
                    ...
                }
```

```
            ],
            "OwnerId": "123456789012",
            "ReservationId": "r-aaaaaabbbbb111111"
        },
        ...
    ]
}
```

若要使用資源篩選選取特定可用區域中的執行處理，請指定可用區域的屬性路徑AvailabilityZone和可用區域的程式碼作為值。例如：

```
"filters": [
    {
        "path": "Placement.AvailabilityZone",
        "values": [ "us-east-1a" ]
    }
],
```

若要使用資源篩選器選取特定子網路中的執行個體，請指定子網路的屬性路徑SubnetId和子網路的 ID 做為值。例如：

```
"filters": [
    {
        "path": "SubnetId",
        "values": [ "subnet-aabbcc11223344556" ]
    }
],
```

若要選取處於特定執行個體狀態的執行個體，請指定屬性路徑Name和下列其中一個狀態名稱作為值：pendingrunningshutting-down| terminated | stopping | | stopped。例如：

```
"filters": [
    {
        "path": "State.Name",
        "values": [ "running" ]
    }
],
```

範例：Amazon RDS 叢集 (資料庫叢集)

當您為支援 aw: RDS: 叢集資源類型的動作指定篩選器時， AWS FIS 會執行 Amazon RDS describe-db-clusters 命令並套用篩選器來識別目標。

此命describe-db-clusters令會針對每個資料庫叢集傳回類似下列內容的 JSON 輸出。以下是部分輸出，其中包含標有##的欄位。我們將提供使用這些欄位從 JSON 輸出結構中指定屬性路徑的範例。

```
[
    {
        "AllocatedStorage": 1,
        "AvailabilityZones": [
            "us-east-2a",
            "us-east-2b",
            "us-east-2c"
        ],
        "BackupRetentionPeriod": 7,
        "DatabaseName": "",
        "DBClusterIdentifier": "database-1",
        "DBClusterParameterGroup": "default.aurora-postgresql11",
        "DBSubnetGroup": "default-vpc-01234567abc123456",
        "Status": "available",
        "EarliestRestorableTime": "2020-11-13T15:08:32.211Z",
        "Endpoint": "database-1.cluster-example.us-east-2.rds.amazonaws.com",
        "ReaderEndpoint": "database-1.cluster-ro-example.us-east-2.rds.amazonaws.com",
        "MultiAZ": false,
        "Engine": "aurora-postgresql",
        "EngineVersion": "11.7",
        ...
    }
]
```

若要套用僅傳回使用特定資料庫引擎之資料庫叢集的資源篩選器，請將屬性路徑指定aurora-postgresql為Engine和值，如下列範例所示。

```
"filters": [
    {
        "path": "Engine",
        "values": [ "aurora-postgresql" ]
    }
],
```

若要套用僅傳回特定可用區域中資料庫叢集的資源篩選器，請指定屬性路徑和值，如下列範例所示。

```
"filters": [
    {
        "path": "AvailabilityZones",
        "values": [ "us-east-2a" ]
    }
],
```

AWS FIS 的停止條件

AWS 故障注入服務 (AWS FIS) 提供控制和護欄，讓您在工作負載上安全地執行實驗。 AWS 停止條件是一種在實驗達到您定義為 Amazon CloudWatch 警示的閾值時停止實驗的機制。如果在實驗期間觸發停止條件， AWS FIS 會停止實驗。您無法繼續已停止的實驗。

若要建立停止條件，請先定義應用程式或服務的穩定狀態。穩定狀態是指應用程式以最佳方式執行時，根據業務或技術指標來定義。例如，延遲、CPU 負載或重試次數。您可以使用穩定狀態來建立 CloudWatch 警示，如果您的應用程式或服務達到無法接受其效能的狀態，可用來停止實驗。如需詳細資訊，請參閱 Amazon 使用 CloudWatch 者指南中的使用 Amazon CloudWatch 警示。

您的帳戶擁有可在實驗範本中指定的停止條件數量的配額。如需詳細資訊，請參閱 AWS 故障注入服務的配額和限制。

停止條件語法

建立實驗範本時，您可以透過指定您建立的 CloudWatch 警報來指定一個或多個停止條件。

```
{
    "stopConditions": [
        {
            "source": "aws:cloudwatch:alarm",
            "value": "arn:aws:cloudwatch:region:123456789012:alarm:alarm-name"
        }
    ]
}
```

下列範例指出實驗範本未指定停止條件。

```
{
    "stopConditions": [
        {
```

```
            "source": "none"
        }
    ]
}
```

進一步了解

如需示範如何建立 CloudWatch 警示並將停止條件新增至實驗範本的自學課程，請參閱〈〉在執行個體上執行 CPU stress。

如需 AWS FIS 支援之資源類型可用之 CloudWatch 測量結果的詳細資訊，請參閱下列內容：

- 使用監控執行個體 CloudWatch
- Amazon ECS 指標 CloudWatch
- 使用監控 Amazon RDS 指標 CloudWatch
- 監視執行命令測量結果 CloudWatch

適用於 AWS FIS 實驗的 IAM 角色

AWS Identity and Access Management (IAM) 是一種 AWS 服務，讓管理員能夠安全地控制對 AWS 資源的存取權限。若要使用 AWS FIS，您必須建立 IAM 角色，以授予 AWS FIS 所需權限，以便 AWS FIS 可以代表您執行實驗。您可以在建立實驗範本時指定此實驗角色。對於單一帳戶實驗，實驗角色的 IAM 政策必須授予權限，才能修改您在實驗範本中指定為目標的資源。對於多帳戶實驗，實驗角色必須授予協調器角色權限，才能為每個目標帳戶擔任 IAM 角色。如需詳細資訊，請參閱 多帳戶實驗的權限。

我們建議您遵循授與最少權限的標準安全性做法。您可以在策略中指定特定的資源 ARN 或標籤來執行此操作。

為了協助您快速開始使用 AWS FIS，我們提供AWS受管理的政策，您可以在建立實驗角色時指定這些原則。或者，您也可以在建立自己的內嵌政策文件時使用這些原則作為模型。

目錄

必要條件

在您開始之前，請先安裝AWS CLI並建立必要的信任原則。

安裝 AWS CLI

開始之前，請先安裝並設定 AWS CLI。設定 AWS CLI 時，系統會提示您輸入 AWS 登入資料。本程序中的範例假設您也設定了預設「區域」。否則，請將 `--region` 選項新增至每個命令。如需詳細資訊，請參閱安裝或更新 AWS CLI 和設定 AWS CLI。

建立信任關係原則

實驗角色必須具有可讓 AWS FIS 服務擔任該角色的信任關係。建立名為的文字檔案，`fis-role-trust-policy.json`並新增下列信任關係原則。

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

建議您使用 `aws:SourceAccount` 和 `aws:SourceArn` 條件索引鍵，保護自己免受混淆代理人問題的困擾。源帳戶是實驗的所有者，源 ARN 是實驗的 ARN。例如，您應該將下列條件區塊新增至您的信任原則。

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account_id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:fis:region:account_id:experiment/*"
    }
}
```

新增假設目標帳戶角色的權限 (僅限多帳戶實驗)

對於多帳戶實驗，您需要允許 Orchestrator 帳戶擔任目標帳戶角色的權限。您可以修改下列範例並新增為內嵌政策文件，以承擔目標帳戶角色：

```
{
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource":[
        "arn:aws:iam::target_account_id:role/role_name"
    ]
}
```

選項 1：建立實驗角色並附加受AWS管政策

使用 AWS FIS 的其中一個AWS受管理的原則快速開始使用。

建立實驗角色並附加受AWS管政策

1. 確認您的實驗中有 AWS FIS 動作的受管政策。否則，您將需要創建自己的內嵌政策文檔。如需詳細資訊，請參閱 the section called “AWS 受管理政策”。
2. 使用下列 create-role 命令建立角色，並新增您在必要條件中建立的信任原則。

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

3. 使用下列attach-role-policy命令來附加AWS受管理的策略。

```
aws iam attach-role-policy --role-name my-fis-role --policy-arn fis-policy-arn
```

其中*fis-policy-arn*是下列其中一項：

- arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEC2Access
- arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorECSAccess
- arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEKSAccess
- arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorNetworkAccess
- arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorRDSAccess
- arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorSSMAccess

選項 2：建立實驗角色並新增內嵌政策文件

對於沒有受管理策略的動作，或僅包含特定實驗所需的權限，請使用此選項。

若要建立實驗並新增內嵌政策文件

1. 使用下列 create-role 命令建立角色，並新增您在必要條件中建立的信任原則。

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

2. 建立名為的文字檔案，fis-role-permissions-policy.json並新增權限原則。有關可用作起點的範例，請參閱以下內容。

   - 錯誤注入動作 — 從下列原則開始。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowFISExperimentRoleFaultInjectionActions",
            "Effect": "Allow",
            "Action": [
                "fis:InjectApiInternalError",
                "fis:InjectApiThrottleError",
                "fis:InjectApiUnavailableError"
            ],
            "Resource": "arn:*:fis:*:*:experiment/*"
        }
    ]
}
```

   - Amazon EBS 動作 — 從下列政策開始。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVolumes"
            ],
            "Resource": "*"
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:PauseVolumeIO"
            ],
            "Resource": "arn:aws:ec2:*:*:volume/*"
        }
    ]
}
```

- Amazon EC2 動作 — 從AWSFaultInjectionSimulatorEC2Access政策開始。
- Amazon ECS 動作 — 從AWSFaultInjectionSimulatorECSAccess政策開始。
- Amazon EKS 行動 — 從AWSFaultInjectionSimulatorEKSAccess政策開始。
- 網路動作 — 從AWSFaultInjectionSimulatorNetworkAccess原則開始。
- Amazon RDS 動作 — 從AWSFaultInjectionSimulatorRDSAccess政策開始。
- Systems Manager 動作 — 從AWSFaultInjectionSimulatorSSMAccess原則開始。

3. 使用下列put-role-policy命令來新增您在上一個步驟中建立的權限原則。

```
aws iam put-role-policy --role-name my-fis-role --policy-name my-fis-policy --
policy-document file://fis-role-permissions-policy.json
```

實驗選項

實驗選項是實驗的可選設置。您可以在實驗模板上定義某些實驗選項。開始實驗時會設定其他實驗選項。

以下是您在實驗模板上定義的實驗選項的語法。

```
{
        "experimentOptions": {
        "accountTargeting": "single-account | multi-account",
            "emptyTargetResolutionMode": "fail | skip"
    }
}
```

如果您在建立實驗樣板時未指定任何實驗選項，則會使用每個選項的預設值。

以下是您在開始實驗時設定的實驗選項的語法。

```
{
        "experimentOptions": {
            "actionsMode": "run-all | skip-all"
     }
}
```

如果您在開始實驗時未指定任何實驗選項，則使`run-all`用預設值。

目錄

帳戶定位

如果您有多個 AWS 帳戶，其中包含要在實驗中定位的資源，則可以使用帳戶定位實驗選項來定義多帳戶實驗。您可以從影響多個目標帳戶中資源的協調器帳戶執行多帳戶實驗。控制器帳戶擁有 AWS FIS 實驗模板和實驗。目標帳戶是個別 AWS 帳戶，其中包含可能受 AWS FIS 實驗影響的資源。如需詳細資訊，請參閱 多帳戶實驗 AWS FIS。

您可以使用帳戶鎖定目標來指出目標資源的位置。您可以為帳戶鎖定目標提供兩個值：

- 單一帳戶 — 預設。實驗只會針對執行實 AWS FIS 驗的 AWS 帳戶中的資源。
- 多帳戶 — 實驗可針對多個 AWS 帳戶中的資源。

目標帳戶組態

若要執行多帳戶實驗，您必須定義一或多個目標帳戶設定。目標帳號設定會為每個帳號指定 accountId、roleArn 和說明，其中包含實驗中目標的資源。實驗範本的目標帳戶設定的帳戶 ID 必須是唯一的。

當您創建多帳戶實驗模板時，實驗模板將返回一個只讀字段`targetAccountConfigurationsCount`，該字段是實驗模板的所有目標帳戶配置的計數。

以下是目標帳戶組態的語法。

```
{
```

```
    accountId: "123456789012",
    roleArn: "arn:aws:iam::123456789012:role/AllowFISActions",
    description: "fis-ec2-test"
}
```

當您建立目標帳戶組態時，請提供下列資訊：

accountId

目標帳戶的 12 位數 AWS 帳戶識別碼。

roleArn

一種 IAM 角色，授與 AWS FIS 許可以在目標帳戶中執行動作。

description

選擇性的描述。

若要深入瞭解如何使用目標帳戶設定，請參閱the section called “使用多帳戶實驗”。

清空目標解析度模式

此模式提供了允許實驗完成的選項，即使目標資源未解析也是如此。

- 失敗 — 預設值。如果沒有解析目標的資源，則會立即終止實驗，狀態為`failed`。
- skip — 如果沒有針對目標解析任何資源，則實驗將繼續進行，且會略過任何沒有解決目標的動作。無法略過具有使用唯一識別碼 (例如 ARN) 定義之目標的動作。如果找不到使用唯一標識符定義的目標，則實驗將立即終止，狀態為 `failed`

動作模式

動作模式是一個可選參數，您可以在開始實驗時指定它。您可以將動作模式設定為，以`skip-all`便在將錯誤注入目標資源之前產生目標預覽。目標預覽可讓您驗證下列項目：

- 您已經配置了實驗模板以定位所期望的資源。開始此實驗時所針對的實際資源可能與預覽版不同，因為資源可能會隨機移除、更新或取樣。
- 您的日誌配置已正確設置。
- 對於多帳戶實驗，您已為每個目標帳戶配置正確設置 IAM 角色。

> **Note**
>
> 此skip-all模式不允許您驗證您是否具有執行 AWS FIS 實驗和對資源採取動作的必要權限。

動作模式參數接受下列值：

- run-all-（默認）實驗將對目標資源採取行動。
- skip-all-實驗將跳過對目標資源的所有操作。

若要進一步瞭解如何在開始實驗時設定動作模式參數，請參閱從實驗範本產生目標預覽。

使用 AWS FIS 實驗範本

您可以使用 AWS FIS 主控台或命令列建立和管理實驗範本。建立實驗範本後，您可以使用它來執行實驗。

任務

- 建立實驗範本
- 檢視實驗範本
- 從實驗範本產生目標預覽
- 從範本開始實驗
- 更新實驗範本
- 標籤實驗模板
- 刪除實驗範本

建立實驗範本

開始之前，請先完成以下任務：

- 計劃你的實驗。
- 建立 IAM 角色，以授與 AWS FIS 服務權限，以代表您執行動作。如需詳細資訊，請參閱 適用於 AWS FIS 實驗的 IAM 角色。
- 請確定您可以存取 AWS FIS。如需詳細資訊，請參閱 AWS FIS 原則範例。

使用控制台建立實驗範本

1. 開啟 AWS 金融資訊系統控制台，網址為 https://console.aws.amazon.com/fis/。
2. 在導覽窗格中，選擇 [實驗範本]。
3. 選擇創建實驗模板。
4. (選擇性) 對於指定帳戶，請選擇 [多個帳戶] 以設定多帳戶實驗範本。
5. 針對「帳戶指定」，選擇「確認」
6. 在「描述」和「名稱」中，輸入範本的描述和名稱。
7. 對於 「動作」，指定範本的動作集。針對每個動作，選擇「新增動作」並完成下列動作：

   - 在「名稱」中，輸入動作的名稱。

     允許的字元包括英數字元、連字號 (-) 和底線 (_)。名稱必須以字母開頭。不可使用空格。在此範本中，每個動作名稱都必須是唯一的。
   - (選擇性) 在說明中，輸入動作的說明。長度上限為 512 個字元。
   - (選擇性) 對於「開始後」，請選取在此範本中定義的另一個動作，此動作必須在目前動作開始之前完成。否則，動作會在實驗開始時執行。
   - 針對「動作類型」，選擇 AWS FIS 動作。
   - 在「目標」中，選擇您在「目標」段落中定義的目標。如果您尚未定義此動作的目標， AWS FIS 會為您建立新目標。
   - 對於動作參數，指定動作的參數。只有在 AWS FIS 動作具有參數時，才會顯示此區段。
   - 選擇儲存。
8. 針對「目標」，定義要在其上執行動作的目標資源。您必須指定至少一個資源 ID 或一個資源標籤做為目標。選擇 「編輯」以編輯在上一個步驟中為您建立的 AWS FIS 目標，或選擇「新增目標」。針對每個目標，執行下列動作：

   - 在名稱中，輸入目標的名稱。

     允許的字元包括英數字元、連字號 (-) 和底線 (_)。名稱必須以字母開頭。不可使用空格。在此範本中，每個目標名稱都必須是唯一的。
   - 對於 [資源類型]，請選擇動作支援的資源類型。
   - 對於 Target 方法，請執行下列其中一項作業：
     - 選擇資源 ID，然後選擇或新增資源 ID。
     - 選擇 [資源標籤]、[篩選器] 和 [參數]，然後新增您需要的標籤和篩選器。如需詳細資訊，請參閱 the section called “識別目標資源”。

- 對於「選取」模式，請選擇「計數」，針對指定數目的已識別目標執行動作，或選擇「百分比」，針對已識別目標的指定百分比執行動作。依預設，動作會在所有已識別的目標上執行。
- 選擇儲存。

9. 若要使用您建立的目標更新動作，請在「動作」下找到動作，選擇「編輯」，然後更新 Target。您可以針對多個動作使用相同的目標。
10. （僅適用於多帳戶實驗）對於 Target 帳戶組態，為每個目標帳戶新增角色 ARN 和可選描述。若要使用 CSV 檔案上傳目標帳戶角色 ARN，請選擇 [上傳所有目標帳戶的角色 ARN]，然後選擇 [選擇 .CSV 檔案]
11. 對於「服務存取」，請選擇「使用現有的 IAM 角色」，然後按照本教學課程的先決條件中所述選擇您建立的 IAM 角色。如果未顯示您的角色，請確認其具有必要的信任關係。如需詳細資訊，請參閱 the section called “實驗角色”。
12. (選擇性) 對於停止條件，請針對停止條件選取 Amazon CloudWatch 警示。如需詳細資訊，請參閱 AWS FIS 的停止條件。
13. (選擇性) 針對記錄，設定目的地選項。若要將日誌傳送到 S3 儲存貯體，請選擇「傳送到 Amazon S3 儲存貯體」，然後輸入儲存貯體名稱和前置詞。如果要將記錄檔傳送至 CloudWatch 記錄檔，請選擇「傳送至 CloudWatch 記錄檔」並輸入記錄群組。
14. (選擇性) 對於標籤，請選擇「新增標籤」，然後指定標籤鍵和標籤值。您新增的標籤會套用至您的實驗範本，而不是使用範本執行的實驗。
15. 選擇創建實驗模板。出現確認提示時，輸入**create**並選擇「創建實驗模板」。

若要使用 CLI 建立實驗範本

使用 create-experiment-template 命令。

您可以從 JSON 檔案載入實驗範本。

使用 `--cli-input-json` 參數。

```
aws fis create-experiment-template --cli-input-json fileb://<path-to-json-file>
```

如需詳細資訊，請參閱《AWS Command Line Interface 使用指南》中的 < 產生 CLI 架構範本 > 。如需範本範本，請參閱AWS FIS 實驗範例範本。

檢視實驗範本

您可以檢視您建立的實驗範本。

使用控制台檢視實驗範本

1. 開啟 AWS 金融資訊系統控制台，網址為 https://console.aws.amazon.com/fis/。
2. 在導覽窗格中，選擇 [實驗範本]。
3. 若要檢視有關特定範本的資訊，請選取「實驗範本 ID」。
4. 在「詳細資料」區段中，您可以檢視範本的描述和停止條件。
5. 若要檢視實驗範本的動作，請選擇 [動作]。
6. 若要檢視實驗範本的目標，請選擇「目標」。
7. 若要檢視實驗範本的標籤，請選擇 [標籤]。

若要使用 CLI 檢視實驗範本

使用指list-experiment-templates令取得實驗範本清單，並使用get-experiment-template指令取得有關特定實驗樣板的資訊。

從實驗範本產生目標預覽

在開始實驗之前，您可以生成目標預覽，以驗證您的實驗模板是否已配置為定位預期的資源。開始實驗時所針對的資源可能與預覽版中的資源不同，因為資源可能會隨機移除、更新或取樣。當您產生目標預覽時，您會開始跳過所有動作的實驗。

> **Note**
>
> 產生目標預覽不允許您確認您擁有對資源採取動作的必要權限。

使用控制台啟動目標預覽

1. 開啟 AWS 金融資訊系統控制台，網址為 https://console.aws.amazon.com/fis/。
2. 在導覽窗格中，選擇 [實驗範本]。
3. 若要檢視實驗範本的目標，請選擇「目標」。
4. 若要驗證實驗範本的目標資源，請選擇「產生預覽」。當您執行實驗時，此目標預覽會自動更新最近實驗中的目標。

使用 CLI 啟動目標預覽

- 執行下列開始實驗指令。以您自己的值取代斜體值。

```
aws fis start-experiment \
    --experiment-options actionsMode=skip-all \
    --experiment-template-id EXTxxxxxxxxx
```

從範本開始實驗

建立實驗範本後，您可以使用該範本開始實驗。

當您開始實驗時，我們會建立指定範本的快照，並使用該快照執行實驗。因此，如果在實驗運行時更新或刪除實驗模板，那麼這些更改不會影響正在運行的實驗。

當您開始實驗時， AWS FIS 會代表您建立服務連結角色。如需詳細資訊，請參閱 使用服務連結角色進行 AWS 錯誤注入服務。

開始實驗後，您可以隨時停止實驗。如需詳細資訊，請參閱 停止實驗。

使用控制台開始實驗

1. 開啟 AWS 金融資訊系統控制台，網址為 https://console.aws.amazon.com/fis/。
2. 在導覽窗格中，選擇 [實驗範本]。
3. (選擇性) 若要產生預覽以驗證您的目標：
   - 選擇「目標」。
   - 選擇「產生預覽」。
4. 選擇實驗模板，然後選擇開始實驗。
5. （可選）要在實驗中添加標籤，請選擇「添加新標籤」，然後輸入標籤鍵和標籤值。
6. 選擇 Start experiment (開始實驗)。出現確認提示時，輸入**start**並選擇「開始實驗」。

使用 CLI 開始實驗

使用「開始實驗」指令。

更新實驗範本

您可以更新現有的實驗範本。當您更新實驗範本時，這些變更不會影響任何使用該範本的執行中實驗。

使用控制台更新實驗範本

1. 開啟 AWS 金融資訊系統控制台，網址為 https://console.aws.amazon.com/fis/。
2. 在導覽窗格中，選擇 [實驗範本]。
3. 選取實驗範本，然後選擇 [動作]、[更新實驗範本]。
4. 視需要修改範本詳細資料，然後選擇 [更新實驗範本]。

若要使用 CLI 更新實驗範本

使用 update-experiment-template 命令。

標籤實驗模板

您可以將自己的標籤應用於實驗模板，以幫助您組織它們。您也可以實作以標籤為基礎的 IAM 政策，以控制對實驗範本的存取。

使用控制台標記實驗範本

1. 開啟 AWS 金融資訊系統控制台，網址為 https://console.aws.amazon.com/fis/。
2. 在導覽窗格中，選擇 [實驗範本]。
3. 選取實驗範本，然後選擇 [動作]、[管理標籤]。
4. 若要新增標籤，請選擇 [新增標籤]，然後指定機碼和值。

   若要移除標記，請為標籤選擇「移除」。
5. 選擇儲存。

若要使用 CLI 標記實驗範本

使用標籤資源命令。

刪除實驗範本

如果您不再需要實驗範本，可以將其刪除。刪除實驗範本時，任何使用該範本的執行中實驗都不會受到影響。實驗繼續運行，直到完成或停止。但是，已刪除的實驗範本無法從主控台的 [實驗] 頁面中檢視。

使用控制台刪除實驗範本

1. 開啟 AWS 金融資訊系統控制台，網址為 https://console.aws.amazon.com/fis/。

2. 在導覽窗格中，選擇 [實驗範本]。
3. 選取實驗範本，然後選擇 [動作] > [刪除實驗範本]。
4. 當系統提示您進行確認時，請輸入**delete**並選擇刪除實驗範本。

若要使用 CLI 刪除實驗範本

使用 delete-experiment-template 命令。

AWS FIS 實驗範例範本

如果您使用 AWS FIS API 或命令列工具建立實驗範本，您可以在 JavaScript 物件標記法 (JSON) 中建構範本。若要取得有關實驗範本元件的更多資訊，請參閱〈〉範本元件。

若要使用其中一個範例範本建立實驗，請將其儲存至 JSON 檔案 (例如`my-template.json`)，將預留位置值以*##*取代為您自己的值，然後執行下列建立實驗範本命令。

```
aws fis create-experiment-template --cli-input-json file://my-template.json
```

範例範本

- 根據篩選器停止 EC2 執行個體
- 停止指定數量的 EC2 執行個體
- 執行預先設定的 AWS FIS SSM 文件
- 執行預先定義的自動化手冊
- 使用目標 IAM 角色調節 EC2 執行個體上的 API 動作
- Kubernetes 叢集中網繭的壓力測試 CPU

根據篩選器停止 EC2 執行個體

下列範例會使用指定 VPC 中的指定標籤停止指定區域中所有執行中的 Amazon EC2 執行個體。它在兩分鐘後重新啟動它們。

```
{
    "tags": {
        "Name": "StopEC2InstancesWithFilters"
    },
    "description": "Stop and restart all instances in us-east-1b with the tag env=prod
 in the specified VPC",
    "targets": {
        "myInstances": {
            "resourceType": "aws:ec2:instance",
            "resourceTags": {
                "env": "prod"
            },
            "filters": [
                {
```

```
                    "path": "Placement.AvailabilityZone",
                    "values": ["us-east-1b"]
                },
                {
                    "path": "State.Name",
                    "values": ["running"]
                },
                {
                    "path": "VpcId",
                    "values": [ "vpc-aabbcc11223344556"]
                }
            ],
            "selectionMode": "ALL"
        }
    },
    "actions": {
        "StopInstances": {
            "actionId": "aws:ec2:stop-instances",
            "description": "stop the instances",
            "parameters": {
                "startInstancesAfterDuration": "PT2M"
            },
            "targets": {
                "Instances": "myInstances"
            }
        }
    },
    "stopConditions": [
        {
            "source": "aws:cloudwatch:alarm",
            "value": "arn:aws:cloudwatch:us-east-1:111122223333:alarm:alarm-name"
        }
    ],
    "roleArn": "arn:aws:iam::111122223333:role/role-name"
}
```

停止指定數量的 EC2 執行個體

下列範例會停止具有指定標籤的三個執行個體。 AWS FIS 會選取要隨機停止的特定執行個體。會在兩分鐘後重新啟動這些執行個體。

```
{
```

```
    "tags": {
        "Name": "StopEC2InstancesByCount"
    },
    "description": "Stop and restart three instances with the specified tag",
    "targets": {
        "myInstances": {
            "resourceType": "aws:ec2:instance",
            "resourceTags": {
                "env": "prod"
            },
            "selectionMode": "COUNT(3)"
        }
    },
    "actions": {
        "StopInstances": {
            "actionId": "aws:ec2:stop-instances",
            "description": "stop the instances",
            "parameters": {
                "startInstancesAfterDuration": "PT2M"
            },
            "targets": {
                "Instances": "myInstances"
            }
        }
    },
    "stopConditions": [
        {
            "source": "aws:cloudwatch:alarm",
            "value": "arn:aws:cloudwatch:us-east-1:111122223333:alarm:alarm-name"
        }
    ],
    "roleArn": "arn:aws:iam::111122223333:role/role-name"
}
```

執行預先設定的 AWS FIS SSM 文件

下列範例會使用預先設定的 AWS FIS SSM 文件-執行 CPU 壓力，在指定的 EC2 執行個體上執行 60 秒的 CPU 故障注入。AWSFIS AWS FIS 會監控實驗兩分鐘。

```
{
    "tags": {
        "Name": "CPUStress"
```

```
    },
    "description": "Run a CPU fault injection on the specified instance",
    "targets": {
        "myInstance": {
            "resourceType": "aws:ec2:instance",
            "resourceArns": ["arn:aws:ec2:us-east-1:111122223333:instance/instance-
id"],
            "selectionMode": "ALL"
        }
    },
    "actions": {
        "CPUStress": {
            "actionId": "aws:ssm:send-command",
            "description": "run cpu stress using ssm",
            "parameters": {
                "duration": "PT2M",
                "documentArn": "arn:aws:ssm:us-east-1::document/AWSFIS-Run-CPU-Stress",
                "documentParameters": "{\"DurationSeconds\": \"60\",
 \"InstallDependencies\": \"True\", \"CPU\": \"0\"}"
            },
            "targets": {
                "Instances": "myInstance"
            }
        }
    },
    "stopConditions": [
        {
            "source": "aws:cloudwatch:alarm",
            "value": "arn:aws:cloudwatch:us-east-1:111122223333:alarm:alarm-name"
        }
    ],
    "roleArn": "arn:aws:iam::111122223333:role/role-name"
}
```

執行預先定義的自動化手冊

下列範例會使用 AWS 發佈通知 Systems Manager 所提供的工作流程簿，將通知發佈至 Amazon SNS。角色必須具有將通知發佈至指定 SNS 主題的權限。

```
{
    "description": "Publish event through SNS",
    "stopConditions": [
```

```
        {
            "source": "none"
        }
    ],
    "targets": {
    },
    "actions": {
        "sendToSns": {
            "actionId": "aws:ssm:start-automation-execution",
            "description": "Publish message to SNS",
            "parameters": {
                "documentArn": "arn:aws:ssm:us-east-1::document/AWS-
PublishSNSNotification",
                "documentParameters": "{\"Message\": \"Hello, world\", \"TopicArn\":
 \"arn:aws:sns:us-east-1:111122223333:topic-name\"}",
                "maxDuration": "PT1M"
            },
            "targets": {
            }
        }
    },
    "roleArn": "arn:aws:iam::111122223333:role/role-name"
}
```

使用目標 IAM 角色調節 EC2 執行個體上的 API 動作

下列範例會限制動作定義中針對目標定義中指定的 IAM 角色進行的 API 呼叫所指定的 100% API 呼叫。

> **Note**
>
> 如果您想要鎖定屬於 Auto Scaling 群組成員的 EC2 執行個體，請使用 aw:ec2: asg-不足-執行個體容量錯誤動作，並改為由 Auto Scaling 群組鎖定目標。如需詳細資訊，請參閱
>
> 針對目標「Auto Scaling」群組發出的要求，注入InsufficientInstanceCapacity錯誤回應。此動作僅支援使用啟動範本的「Auto Scaling」群組。若要進一步了解執行個體容量不足錯誤，請參閱 Amazon EC2 使用者指南。

資源類型

- aws:ec2:autoscaling-group

參數

- duration— 在 AWS FIS API 中，值是 ISO 8601 格式的字串。例如，PT1M 代表一分鐘。在 AWS FIS 主控台中，您可以輸入秒數、分鐘數或小時數。

- availabilityzoneIdentifiers— 逗號分隔的可用區域清單。支援區域 ID (例如"use1-az1, use1-az2") 和區域名稱 (例如"us-east-1a")。
- percentage - 選用。插入錯誤之目標 Auto Scaling 群組啟動要求的百分比 (1-100)。預設為 100。

許可

- ec2:InjectApiError條件鍵 ec2：FisActionId 值設置為aws:ec2:asg-insufficient-instance-capacity-error，ec2:FisTargetArns條件鍵設置為目標 Auto Scaling 組。

- autoscaling:DescribeAutoScalingGroups

如需政策範例，請參閱 範例：使用條件鍵 ec2:InjectApiError。

。

```
{
    "tags": {
        "Name": "ThrottleEC2APIActions"
    },
    "description": "Throttle the specified EC2 API actions on the specified IAM role",
    "targets": {
        "myRole": {
            "resourceType": "aws:iam:role",
            "resourceArns": ["arn:aws:iam::111122223333:role/role-name"],
            "selectionMode": "ALL"
        }
    },
    "actions": {
```

```
        "ThrottleAPI": {
            "actionId": "aws:fis:inject-api-throttle-error",
            "description": "Throttle APIs for 5 minutes",
            "parameters": {
                "service": "ec2",
                "operations": "DescribeInstances,DescribeVolumes",
                "percentage": "100",
                "duration": "PT2M"
            },
            "targets": {
                "Roles": "myRole"
            }
        }
    },
    "stopConditions": [
        {
            "source": "aws:cloudwatch:alarm",
            "value": "arn:aws:cloudwatch:us-east-1:111122223333:alarm:alarm-name"
        }
    ],
    "roleArn": "arn:aws:iam::111122223333:role/role-name"
}
```

Kubernetes 叢集中網繭的壓力測試 CPU

下列範例使用混沌網格對 Amazon EKS Kubernetes 叢集中網繭的 CPU 進行 stress 測試一分鐘。

```
{
    "description": "ChaosMesh StressChaos example",
    "targets": {
        "Cluster-Target-1": {
            "resourceType": "aws:eks:cluster",
            "resourceArns": [
                "arn:aws:eks:arn:aws::111122223333:cluster/cluster-id"
            ],
            "selectionMode": "ALL"
        }
    },
    "actions": {
        "TestCPUStress": {
            "actionId": "aws:eks:inject-kubernetes-custom-resource",
            "parameters": {
                "maxDuration": "PT2M",
```

```
                "kubernetesApiVersion": "chaos-mesh.org/v1alpha1",
                "kubernetesKind": "StressChaos",
                "kubernetesNamespace": "default",
                "kubernetesSpec": "{\"selector\":{\"namespaces\":[\"default\"],
\"labelSelectors\":{\"run\":\"nginx\"}},\"mode\":\"all\",\"stressors\": {\"cpu\":
{\"workers\":1,\"load\":50}},\"duration\":\"1m\"}"
            },
            "targets": {
                "Cluster": "Cluster-Target-1"
            }
        }
    },
    "stopConditions": [{
        "source": "none"
    }],
    "roleArn": "arn:aws:iam::111122223333:role/role-name",
    "tags": {}
}
```

下列範例使用石蕊對 Amazon EKS Kubernetes 叢集中網繭的 CPU 進行 stress 測試一分鐘。

```
{
    "description": "Litmus CPU Hog",
    "targets": {
        "MyCluster": {
            "resourceType": "aws:eks:cluster",
            "resourceArns": [
                "arn:aws:eks:arn:aws::111122223333:cluster/cluster-id"
            ],
            "selectionMode": "ALL"
        }
    },
    "actions": {
        "MyAction": {
            "actionId": "aws:eks:inject-kubernetes-custom-resource",
            "parameters": {
                "maxDuration": "PT2M",
                "kubernetesApiVersion": "litmuschaos.io/v1alpha1",
                "kubernetesKind": "ChaosEngine",
                "kubernetesNamespace": "litmus",
                "kubernetesSpec": "{\"engineState\":\"active\",\"appinfo\":
{\"appns\":\"default\",\"applabel\":\"run=nginx\",\"appkind\":\"deployment\"},
\"chaosServiceAccount\":\"litmus-admin\",\"experiments\":[{\"name\":\"pod-cpu-hog
```

```
\",\"spec\":{\"components\":{\"env\":[{\"name\":\"TOTAL_CHAOS_DURATION\",\"value\":
\"60\"},{\"name\":\"CPU_CORES\",\"value\":\"1\"},{\"name\":\"PODS_AFFECTED_PERC\",
\"value\":\"100\"},{\"name\":\"CONTAINER_RUNTIME\",\"value\":\"docker\"},{\"name\":
\"SOCKET_PATH\",\"value\":\"/var/run/docker.sock\"}]},\"probe\":[]}}],\"annotationCheck
\":\"false\"}"
            },
            "targets": {
                "Cluster": "MyCluster"
            }
        }
    },
    "stopConditions": [{
        "source": "none"
    }],
    "roleArn": "arn:aws:iam::111122223333:role/role-name",
    "tags": {}
}
```

多帳戶實驗 AWS FIS

透過多帳戶實驗，您可以在跨區域內多個 AWS 帳戶的應用程式上設定和執行實際故障情境。您可以從影響多個目標帳戶中資源的協調器帳戶執行多帳戶實驗。

當您執行多帳戶實驗時，包含受影響資源的目標帳戶會透過其 AWS Health 儀表板收到通知，讓目標帳戶中的使用者感知。透過多帳戶實驗，您可以：

- 使用提供的中央控制項和護欄，在跨越多個帳戶的應用程式上執行實際故障案例。 AWS FIS
- 使用具有精細許可和標籤的 IAM 角色來定義每個目標的範圍，控制多帳戶實驗的效果。
- 集中查看每個帳戶從日誌 AWS Management Console 和通過 AWS FIS 日誌 AWS FIS 採取的操作。
- 監控和稽核 AWS 在每個帳戶中進行的 API 呼叫 AWS FIS CloudTrail。

本節可協助您開始進行多帳戶實驗。

主題

多帳戶實驗的概念

以下是多帳戶實驗的關鍵概念：

協調器帳戶

Orchestrator 帳戶充當中央帳戶，可在 AWS FIS 主控台中設定和管理實驗，以及集中記錄。控制器帳戶擁有 AWS FIS 實驗模板和實驗。

目標帳戶

目標帳戶是個別 AWS 帳戶，其資源可能受到 AWS FIS 多帳戶實驗的影響。

目標帳戶組態

您可以通過將目標帳戶配置添加到實驗模板中來定義屬於實驗一部分的目標帳戶。目標帳戶配置是多帳戶實驗所需的實驗模板元素。您可以透過設定帳戶 ID、IAM 角色和選用說明，為每個目標 AWS 帳戶定義一個帳戶。

多帳戶實驗的先決條件

要在多帳戶實驗中使用停止條件，您必須先配置跨帳戶警報。IAM 角色是在您建立多帳戶實驗範本時定義的。您可以在建立範本之前建立必要的 IAM 角色。

內容

多帳戶實驗的權限

多帳戶實驗使用 IAM 角色鏈接授予許可，以 AWS FIS 對目標帳戶中的資源採取動作。對於多帳戶實驗，您可以在每個目標帳戶和協調器帳戶中設定 IAM 角色。這些 IAM 角色需要目標帳戶和協調器帳戶之間，以及協調器帳戶與之間的信任關係。 AWS FIS

目標帳戶的 IAM 角色包含對資源採取行動所需的許可，並透過新增目標帳戶設定為實驗範本建立。您將為協調器帳戶建立 IAM 角色，並具有擔任目標帳戶角色並與之建立信任關係的 AWS FIS權限。此 IAM 角色用作實`roleArn`驗範本的。

若要深入了解角色鏈結，請參閱角色術語和概念。 在 IAM 的使用者指南中

在下列範例中，您將設定管理員帳戶 A 的權限，以便`aws:ebs:pause-volume-io`在目標帳戶 B 中執行實驗。

1. 在帳戶 B 中，建立具有執行動作所需許可的 IAM 角色。如需每個動作所需的權限，請參閱the section called “動作參考”。下列範例顯示目標帳戶授與執行 EBS 暫停磁碟區 IO 動作the section called “aws:ebs:pause-volume-io”的權限。

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

```
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVolumes"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:PauseVolumeIO"
            ],
            "Resource": "arn:aws:ec2:region:accountIdB:volume/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        }
    ]
}
```

2. 接下來，在帳戶 B 中新增信任政策，以建立與帳戶 A 的信任關係。選擇帳戶 A 的 IAM 角色名稱，您將在步驟 3 中建立該名稱。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
           "Effect": "Allow",
            "Principal": {
                "AWS": "AccountIdA"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringLike":{
                    "sts:ExternalId": "arn:aws:fis:region:accountIdA:experiment/*"
                },
                "ArnEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::accountIdA:role/role_name"
                }
            }
```

```
        }
    ]
}
```

3. 在帳戶 A 中，建立 IAM 角色。此角色名稱必須符合您在步驟 2 中信任原則中指定的角色。若要鎖定多個帳戶，您可以授與協調管理員權限來擔任每個角色。下列範例顯示帳戶 A 假設帳戶 B 的權限。如果您有其他目標帳戶，則會將其他角色 ARN 新增至此策略。每個目標帳戶只能有一個角色 ARN。

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

4. 帳戶 A 的這個 IAM 角色`roleArn`用作實驗範本的。下列範例顯示 IAM 角色中所需的信任政策，該政策授與 AWS FIS 權限，以假設帳戶 A (協調器帳戶)。

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

您也可以使用堆疊集一次佈建多個 IAM 角色。若要使用 CloudFormation StackSets，您必須在 AWS 帳戶中設定必要的 StackSet 權限。要進一步了解，請參閱使用 AWS CloudFormation StackSets。

多帳戶實驗的停止條件（可選）

停止條件是一種在實驗達到您定義為警報的閾值時停止實驗的機制。要為多帳戶實驗設置停止條件，您可以使用跨帳戶警報。您必須在每個目標帳戶中啟用共用，才能使用唯讀權限讓 Orchestrator 帳戶可以使用警示。共用後，您可以使用 Metric Math 合併來自不同目標帳戶的指標。然後，您可以將此警報添加為實驗的停止條件。

若要進一步了解跨帳戶儀表板，請參閱中的啟用跨帳戶功能。 CloudWatch

使用多帳戶實驗

您可以使用 AWS FIS 控制台或命令行創建和管理多帳戶實驗模板。您可以通過將帳戶定位實驗選項指定為`"multi-account"`並添加目標帳戶配置來創建多帳戶實驗。建立多帳戶實驗範本後，您可以使用它來執行實驗。

內容

多帳戶實驗的最佳做法

以下是使用多帳戶實驗的最佳作法：

- 當您設定多帳戶實驗的目標時，我們建議您在所有目標帳戶中使用一致的資源標籤鎖定目標。 AWS FIS 實驗將解析每個目標帳戶中具有一致標籤的資源。動作必須解析任何目標帳號中至少一個目標資源，否則將會失敗，但`emptyTargetResolutionMode`設定為的實驗除外`skip`。每個帳號會套用動作配額。如果您想要依資源 ARN 鎖定資源，則會套用每個動作相同的單一帳號限制。
- 當您使用參數或篩選器鎖定一或多個可用區域中的資源時，您應該指定 AZ ID，而不是 AZ 名稱。AZ ID 是跨帳戶可用區域的唯一且一致的識別碼。若要了解如何尋找帳戶中可用區域的 AZ ID，請參閱 AWS 資源的可用區域 ID。

建立多帳戶實驗範本

若要瞭解如何透過 AWS Management Console

請參閱建立實驗範本。

若要使用 CLI 建立實驗範本

1. 打開 AWS Command Line Interface
2. 要在帳戶定位實驗選項設置為"multi-account"（例如my-template.json）的情況下從已保存的 JSON 文件創建實驗，請將佔位符值替換為##，然後運行以下創建實驗模板命令。

```
aws fis create-experiment-template --cli-input-json file://my-template.json
```

這將在響應中返回實驗模板。id從響應中復制，這是實驗模板的 ID。

3. 執行建立目標帳戶組態指令，將目標帳戶設定新增至實驗範本。使用id從步驟 2 做為參數的值，以##取代預留位置--experiment-template-id值，然後執行下列指令。--description 為選用參數。針對每個目標帳戶重複此步驟。

```
aws fis create-target-account-configuration --experiment-template-id EXTxxxxxxxxx
 --account-id 111122223333 --role-arn arn:aws:iam::111122223333:role/role-name --
description "my description"
```

4. 執行取得目標帳戶組態命令，以擷取特定目標帳戶組態的詳細資料。

```
aws fis get-target-account-configuration --experiment-template-id EXTxxxxxxxxx --
account-id 111122223333
```

5. 新增所有目標帳戶組態後，您可以執行清單目標帳戶組態命令，以查看是否已建立目標帳戶組態。

```
aws fis list-target-account-configurations --experiment-template-id EXTxxxxxxxxx
```

您也可以執行 get-試驗範本命令來確認您已加入目標帳戶組態。該模板將返回一個只讀字段，targetAccountConfigurationsCount該字段是實驗模板上所有目標帳戶配置的計數。

6. 準備就緒後，您可以使用「開始實驗」指令執行實驗範本。

```
aws fis start-experiment --experiment-template-id EXTxxxxxxxxx
```

更新目標帳戶組態

如果您想要變更帳號的角色 ARN 或說明，可以更新現有的目標帳戶組態。當您更新目標帳戶組態時，這些變更不會影響任何使用該範本的執行中實驗。

若要使用更新目標帳戶組態 AWS Management Console

1. 開啟主 AWS FIS 控台，網址為 https://console.aws.amazon.com/fis/。
2. 在導航窗格中，選擇實驗模板
3. 選取實驗範本，然後選擇 [動作]、[更新實驗範本]。
4. 修改目標帳戶設定，然後選擇 [更新實驗範本]。

使用 CLI 更新目標帳戶組態

##########################--role-arn和--description參數是可選的，如果不包含，則不會更新。

```
aws fis update-target-account-configuration --experiment-template-id EXTxxxxxxxxx
 --account-id 111122223333 --role-arn arn:aws:iam::111122223333:role/role-name --
description "my description"
```

刪除目標帳戶組態

如果您不再需要目標帳戶設定，可以將其刪除。當您刪除目標帳戶組態時，任何使用該範本的執行中實驗都不會受到影響。實驗繼續運行，直到完成或停止。

若要使用刪除目標帳戶組態 AWS Management Console

1. 開啟主 AWS FIS 控台，網址為 https://console.aws.amazon.com/fis/。
2. 在導覽窗格中，選擇 [實驗範本]。
3. 選取實驗範本，然後選擇 [動作]、[更新]。
4. 在 [目標帳戶組態] 下，針對您要刪除的目標帳戶角色 ARN 選取 [移除]。

使用 CLI 刪除目標帳戶組態

##

```
aws fis update-target-account-configuration --experiment-template-id EXTxxxxxxxxx --
account-id 111122223333
```

AWS FIS 情境庫

案例定義了客戶可套用來測試應用程式復原能力的事件或條件，例如執行應用程式的運算資源中斷。案例由 AWS 建立和擁有，並為您提供一組預先定義的目標和錯誤動作 (例如，停止自動調度資源群組中 30% 的執行個體)，以減少無差異的繁重工作，以避免常見的應用程式損壞。

主題

- 使用 AWS FIS 案例
- 案例程式庫中的 AWS FIS 案例
- AZ Availability: Power Interruption
- Cross-Region: Connectivity

使用 AWS FIS 案例

案例是透過僅限主控台的案例程式庫提供，並使用實驗範本執行。 AWS FIS 為了使用案例執行實驗，您將從程式庫中選取案例，指定與工作負載詳細資料相符的參數，並將其儲存為帳戶中的實驗範本。

主題

- 檢視案例
- 使用案例
- 匯出案例

檢視案例

若要使用主控台檢視案例：

1. 在開啟 AWS FIS 主控台https://console.aws.amazon.com/fis/。
2. 在功能窗格中，選擇方案庫。
3. 若要檢視特定案例的相關資訊，請選取案例卡以開啟分割面板。
   - 在頁面底部分割面板的 [說明] 索引標籤中，您可以檢視案例的簡短說明。您也可以找到先決條件的簡短摘要，其中包含必要的目標資源摘要，以及準備與案例搭配使用的資源所需採取的任何動作。最後，您還可以查看有關場景中的目標和操作的其他信息，以及使用默認設置成功運行實驗時的預期持續時間。

- 在頁面底部分割面板中的「內容」(Content) 標籤中，您可以預覽將從案例建立的實驗範本的部分填入版本。
- 在頁面底部分割面板的 [詳細資料] 索引標籤中，您可以找到如何實作案例的詳細說明。這可能包含有關場景的各個方面如何近似的詳細信息。在適用的情況下，您還可以閱讀用作停止條件的指標，並提供從實驗中學習的觀察性。最後，您將找到如何擴展生成的實驗模板的建議。

使用案例

若要使用主控台的案例：

1. 在開啟 AWS FIS 主控台https://console.aws.amazon.com/fis/。
2. 在功能窗格中，選擇方案庫。
3. 若要檢視特定案例的相關資訊，請選取案例卡以顯示分割面板
4. 若要使用案例，請選取案例卡，然後選擇使用案例建立範本。
5. 在創建實驗模板視圖填充任何缺少的項目。
   a. 某些案例可讓您大量編輯跨多個動作或目標共用的參數。一旦您對案例進行任何變更 (包括由批量參數編輯所做的變更)，就會停用此功能。若要使用此功能，請選取「編輯主體參數」按鈕。在模式中編輯參數，然後選取 [儲存] 按鈕。
   b. 某些實驗模板可能缺少動作或目標參數，這些參數會在每個動作和目標卡上突出顯示。選取每張卡片的 [編輯] 按鈕、新增遺失的資訊，然後選取記憶卡上的 [儲存] 按鈕。
   c. 所有範本都需要服務存取執行角色。您可以為此實驗模板選擇現有角色或創建新角色。
   d. 我們建議您選取現有的 AWS CloudWatch 警示，以定義一或多個選擇性停止條件。進一步了解 AWS FIS 的停止條件。如果您尚未設定警報，可以按照使用 Amazon CloudWatch Alarps 中的說明進行操作，稍後更新實驗範本。
   e. 我們建議您將選用的實驗日 CloudWatch 誌啟用到 Amazon 日誌或 Amazon S3 儲存貯體。進一步了解 AWSFIS 的實驗記錄。如果您尚未配置適當的資源，則可以稍後更新實驗模板。
6. 在「建立實驗範本」中選取「建立實驗範本」。
7. 從 AWS FIS 主控台的 [實驗範本] 檢視中，選取 [開始實驗]。進一步了解 金融信息 AWS 系統的實驗。

匯出案例

案例是僅限控制台的體驗。雖然與實驗模板類似，但情景不是完整的實驗模板，也無法直接導入到中 AWS FIS。如果您希望將案例用作自己的自動化操作的一部分，則可以使用以下兩種路徑之一：

1. 請按照中的步驟使用案例建立有效的 AWS FIS 實驗範本並匯出該範本。
2. 按照步驟 3 中檢視案例和步驟 3 中的步驟，從「內容」選項卡複製並保存方案內容，然後手動添加缺少的參數以創建有效的實驗模板。

案例程式庫中的 AWS FIS 案例

案例程式庫中包含的案例設計為在可能的情況下使用標籤，而每個案例描述的必要條件及其運作方式區段中的必要標籤。您可以使用這些預先定義的標籤來標記資源，也可以使用批量參數編輯體驗來設定自己的標籤 (請參閱使用案例)。

本參考資料說明 AWS FIS 案例程式庫中的常見案例。您也可以使用 AWS FIS 主控台列出支援的案例。

如需詳細資訊，請參閱使用案例。

AWS FIS 支援下列 Amazon EC2 案例。這些案例使用標籤鎖定執行個體。您可以使用自己的標籤或使用案例中包含的預設標籤。其中一些案例會使用 SSM 文件。

- EC2 stress：執行個體故障-透過停止一或多個 EC2 執行個體探索執行個體故障的影響。

  目前區域中貼附特定標籤的目標例證。在這種情況下，我們將停止這些實例，並在動作持續時間結束時重新啟動它們，默認情況下為 5 分鐘。
- EC2 stress：磁碟-探索磁碟使用率增加對 EC2 應用程式的影響。

  在這個案例中，我們將針對目前區域中已附加特定標籤的 EC2 執行個體。在這個案例中，您可以自訂在動作持續時間內針對目標 EC2 執行個體插入的磁碟使用量增加，預設情況下，每個磁碟 stress 動作為 5 分鐘。
- EC2 stress：CPU-探索 CPU 增加對 EC2 型應用程式的影響。

  在這個案例中，我們將針對目前區域中已附加特定標籤的 EC2 執行個體。在這個案例中，您可以自訂在動作持續時間內，針對目標 EC2 執行個體注入的 CPU stress 增加量，依預設為每個 CPU stress 動作 5 分鐘。
- EC2 stress：記憶體-探索增加記憶體使用率對 EC2 應用程式的影響。

  在這個案例中，我們將針對目前區域中已附加特定標籤的 EC2 執行個體。在這個案例中，您可以自訂在動作持續時間內，針對目標 EC2 執行個體注入的記憶體 stress 不斷增加的記憶體 stress，預設為每個記憶體壓力動作 5 分鐘。
- EC2 stress：網路延遲-探索網路延遲增加對 EC2 型應用程式的影響。

在這個案例中，我們將針對目前區域中已附加特定標籤的 EC2 執行個體。在這個案例中，您可以自訂在動作持續時間內在目標 EC2 執行個體上插入的網路延遲量增加，預設情況下每個延遲動作為 5 分鐘。

AWS FIS 支援下列 Amazon EKS 案例。這些案例會使用 Kubernetes 應用程式標籤來鎖定 EKS 網繭的目標。您可以使用自己的標籤或使用案例中包含的預設標籤。如需有關具有 FIS 的 EKS 的更多資訊，請參閱。使用 EKS 網繭動作

- EKS stress：Pod 刪除-透過刪除一或多個網繭來探索 EKS 網繭故障的影響。

  在這個案例中，我們會將目標鎖定目前區域中與應用程式標籤相關聯的網繭。在這種情況下，我們將終止所有匹配的 Pod。重新建立網繭將由 Kubernetes 組態控制。

- EKS stress：CPU-探索增加 CPU 對 EKS 應用程式的影響。

  在這個案例中，我們會將目標鎖定目前區域中與應用程式標籤相關聯的網繭。在此案例中，您可以自訂在動作持續時間內，針對目標 EKS 網繭所注入的 CPU stress 增加量，依預設為每個 CPU stress 動作 5 分鐘。

- EKS stress：磁碟-探索磁碟使用率增加對 EKS 應用程式的影響。

  在這個案例中，我們會將目標鎖定目前區域中與應用程式標籤相關聯的網繭。在此案例中，您可以自訂在動作持續時間內在目標 EKS 網繭上插入的磁碟 stress 增加量，依預設為每個 CPU stress 動作 5 分鐘。

- EKS stress：記憶體-探索增加記憶體使用率對 EKS 應用程式的影響。

  在這個案例中，我們會將目標鎖定目前區域中與應用程式標籤相關聯的網繭。在此案例中，您可以自訂在動作持續時間內在目標 EKS 網繭上注入的記憶體 stress 增加量，依預設為每個記憶體 stress 動作 5 分鐘。

- EKS stress：網路延遲-探索增加網路延遲對 EKS 型應用程式的影響。

  在這個案例中，我們會將目標鎖定目前區域中與應用程式標籤相關聯的網繭。在此案例中，您可以自訂在動作持續時間內在目標 EKS 網繭上插入的網路延遲量增加，依預設為每個延遲動作 5 分鐘。

AWS FIS 支援異地同步備份和多區域應用程式的下列案例。這些案例以多種資源類型為目標。

- AZ Availability: Power Interruption-在可用區域 (AZ) 中注入完全中斷電源的預期症狀。進一步了解 AZ Availability: Power Interruption。

- Cross-Region: Connectivity-封鎖從實驗區域到目標區域的應用程式網路流量，並暫停跨區域資料複製。進一步了解使用Cross-Region: Connectivity.

AZ Availability: Power Interruption

您可以使用此AZ Availability: Power Interruption案例來引發可用區域 (AZ) 完全中斷電源的預期症狀。

此案例可用於證明異地同步備份應用程式在單一完整 AZ 電源中斷期間如預期般運作。其中包括區域運算遺失 (Amazon EC2、EKS 和 ECS)、AZ 中沒有重新擴展運算、子網路連線中斷、RDS 容錯移轉、ElastiCache 容錯移轉和無回應的 EBS 磁碟區。依預設，將略過找不到目標的動作。

動作

下列動作共同產生單一 AZ 完全電源中斷的許多預期症狀。AZ 可用性：電源中斷只會影響預期在單一 AZ 電源中斷期間會產生影響的服務。根據預設，案例會注入 30 分鐘的電源中斷症狀，然後再注入 30 分鐘的時間，可能會注入復原期間可能發生的症狀。

停止執行個體

在 AZ 電源中斷期間，受影響可用區域中的 EC2 執行個體將關閉。恢復電源後，實例將重新啟動。 AZ Availability: Power Interruption包括 aw: ec2: stop-執行個體，可在中斷持續時間內停止受影響 AZ 中的所有執行個體。持續時間過後，執行個體便會重新啟動。停止由 Amazon EKS 管理的 EC2 執行個體會導致相依的 EKS 網繭遭到刪除。停止由 Amazon ECS 管理的 EC2 執行個體會導致停止相依的 ECS 任務。

此動作鎖定在受影響 AZ 中執行的 EC2 執行個體。依預設，它會針對具有以值命名的標籤`AzImpairmentPower`的執行個體`StopInstances`。您可以將此標籤添加到實例中，也可以在實驗模板中用自己的標籤替換默認標籤。依預設，如果找不到有效的實例，則會略過此動作。

停止 ASG 實例

在 AZ 電源中斷期間，受影響的可用區域中由 Auto Scaling 群組管理的 EC2 執行個體將會關閉。恢復電源後，實例將重新啟動。 AZ Availability: Power Interruption包括 aw: ec2：停止執行個體，可在中斷持續時間內停止受影響的 AZ 中的所有執行個體，包括由 Auto S caling 管理的執行個體。持續時間過後，執行個體便會重新啟動。

此動作鎖定在受影響 AZ 中執行的 EC2 執行個體。依預設，它會針對具有以值命名的標籤`AzImpairmentPower`的執行個體`IceAsg`。您可以將此標籤添加到實例中，也可以在實驗模板中用自己的標籤替換默認標籤。依預設，如果找不到有效的實例，則會略過此動作。

暫停實例啟動

在 AZ 電源中斷期間，在 AZ 中佈建容量的 EC2 API 呼叫將會失敗。特別是，下列 API 會受到影響：ec2:StartInstancesec2:CreateFleet、和ec2:RunInstances。 AZ Availability: Power Interruption includes包括 aw: ec2: API 不足-執行個體容量錯誤，以防止在受影響的可用區域中佈建新的執行個體。

此動作鎖定用於佈建執行個體的 IAM 角色。這些必須使用 ARN 定位。依預設，如果找不到有效的 IAM 角色，則會略過此動作。

暫停 ASG 調整比例

在 AZ 電源中斷期間，Auto Scaling 控制平面為復原 AZ 中遺失的容量所發出的 EC2 API 呼叫將會失敗。特別是，下列 API 會受到影響：ec2:StartInstancesec2:CreateFleet、和ec2:RunInstances。 AZ Availability: Power Interruption包括 aw: ec2: asg-執行個體容量錯誤，以防止在受影響的 AZ 中佈建新的執行個體。這也可以防止 Amazon EKS 和 Amazon ECS 在受影響的可用區域擴展。

此動作會鎖定「Auto Scaling」群組。依預設，它會以「Auto Scaling」群組的目標為目標，其名稱為AzImpairmentPower值為IceAsg。您可以將此標記添加到 Auto Scaling 組中，或者在實驗模板中用自己的標籤替換默認標籤。依預設，如果找不到有效的「Auto Scaling」群組，則會略過此動作。

暫停網路連線

在 AZ 電源中斷期間，AZ 中的網路將無法使用。發生這種情況時，某些 AWS 服務可能需要幾分鐘才能更新 DNS，以反映受影響 AZ 中的私有端點無法使用。在此期間，DNS 查閱可能會傳回無法存取的 IP 位址。 AZ Availability: Power Interruption包括 aws: network: 中斷連線，以封鎖受影響 AZ 中所有子網路的所有網路連線 2 分鐘。這會強制大多數應用程式的逾時和 DNS 重新整理。在 2 分鐘後結束動作，可在 AZ 繼續無法使用的情況下繼續復原區域服務 DNS。

此動作會鎖定子網路。依預設，它會以值命名為AzImpairmentPower的標籤鎖定叢集DisruptSubnet。您可以將此標籤新增至子網路，或在實驗範本中以您自己的標籤取代預設標籤。依預設，如果找不到有效的子網路，則會略過此動作。

容錯移轉 RDS

在 AZ 電源中斷期間，受影響的可用區域中的 RDS 節點將會關閉。受影響可用區域中的單一 AZ RDS 節點將完全無法使用。對於異地同步備份叢集，寫入器節點將容錯移轉至未受影響的 AZ，且受影響可用區中的讀取器節點將無法使用。對於異地同步備份叢集，如果寫入器位於受影響的可用區域中，則 AZ Availability: Power Interruption包括 aw: RDS: 容錯移轉 db 叢集以進行容錯移轉。

此動作以 RDS 叢集為目標。依預設，它會以值命名為`AzImpairmentPower`的標籤鎖定叢集`DisruptRds`。您可以將此標記添加到集群中，也可以在實驗模板中用自己的標籤替換默認標籤。依預設，如果找不到有效的叢集，則會略過此動作。

暫停 ElastiCache 雷迪斯

AZ 電源中斷期間，AZ 中的 ElastiCache 節點無法使用。 AZ Availability: Power Interruption包括：彈性：中斷叢集- AZ-電源，以終止受影響的 AZ 中的節點。 ElastiCache 在中斷期間，不會在受影響的可用區域中佈建新的執行個體，因此叢集將維持在較低的容量。

此動作以 ElastiCache 叢集為目標。依預設，它會以值命名為`AzImpairmentPower`的標籤鎖定叢集`ElasticacheImpact`。您可以將此標記添加到集群中，也可以在實驗模板中用自己的標籤替換默認標籤。依預設，如果找不到有效的叢集，則會略過此動作。請注意，只有在受影響的 AZ 中具有寫入器節點的叢集才會被視為有效目標。

暫停 EBS I/O

AZ 電源中斷後，一旦恢復電源，只有極小的執行個體可能會遇到無回應的 EBS 磁碟區。 AZ Availability: Power Interruption包括提示：eb-io：暫停，使 1 個 EBS 卷處於無響應狀態。

根據預設，只有設定為在執行個體終止後持續存在的磁碟區才會成為目標。此動作的目標磁碟區具`AzImpairmentPower`有以值命名的標籤`APIPauseVolume`。您可以將此標籤添加到卷中，也可以在實驗模板中用自己的標籤替換默認標籤。依預設，如果找不到有效的磁碟區，則會略過此動作。

限制

- 此案例不包含停止條件。應將應用程序的正確停止條件添加到實驗模板中。
- 不支援在 AWS Fargate 上執行的 Amazon EKS 網繭。
- 不支援在 AWS Fargate 上執行的 Amazon ECS 任務。
- 不支援具有兩個可讀取待命資料庫執行個體的 Amazon RDS 異地同步備份。在此情況下，執行個體將終止、RDS 將容錯移轉，且容量將立即佈建回受影響的可用區域中。受影響 AZ 中的可讀取待命狀態將保持可用狀態。

要求

- 將必要的權限新增至 AWS FIS 實驗角色。
- 資源標籤必須應用於要被實驗定位的資源。這些可以使用您自己的標記慣例或在案例中定義的預設標籤。

許可

以下政策授予 AWS FIS 執行AZ Availability: Power Interruption案例實驗的必要許可。此原則必須附加至實驗角色。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowFISExperimentLoggingActionsCloudwatch",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:PutResourcePolicy",
                "logs:DescribeResourcePolicies",
                "logs:DescribeLogGroups"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:network-acl/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkAcl",
                    "aws:RequestTag/managedByFIS": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateNetworkAcl",
            "Resource": "arn:aws:ec2:*:*:network-acl/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/managedByFIS": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "ec2:CreateNetworkAclEntry",
                "ec2:DeleteNetworkAcl"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-acl/*",
                "arn:aws:ec2:*:*:vpc/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/managedByFIS": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateNetworkAcl",
            "Resource": "arn:aws:ec2:*:*:vpc/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeManagedPrefixLists",
                "ec2:DescribeSubnets",
                "ec2:DescribeNetworkAcls"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:ReplaceNetworkAclAssociation",
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:network-acl/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "rds:FailoverDBCluster"
            ],
            "Resource": [
                "arn:aws:rds:*:*:cluster:*"
            ]
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "rds:RebootDBInstance"
            ],
            "Resource": [
                "arn:aws:rds:*:*:db:*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "elasticache:DescribeReplicationGroups",
                "elasticache:InterruptClusterAzPower"
            ],
            "Resource": [
                "arn:aws:elasticache:*:*:replicationgroup:*"
            ]
        },
        {
            "Sid": "TargetResolutionByTags",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Resource": "arn:aws:ec2:*:*:instance/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances"
            ],
            "Resource": "*"
        },
        {
```

```
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant"
            ],
            "Resource": [
                "arn:aws:kms:*:*:key/*"
            ],
            "Condition": {
                "StringLike": {
                    "kms:ViaService": "ec2.*.amazonaws.com"
                },
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVolumes"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:PauseVolumeIO"
            ],
            "Resource": "arn:aws:ec2:*:*:volume/*"
        },
        {
            "Sid": "AllowInjectAPI",
            "Effect": "Allow",
            "Action": [
                "ec2:InjectApiError"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "ec2:FisActionId": [
                        "aws:ec2:api-insufficient-instance-capacity-error",
                        "aws:ec2:asg-insufficient-instance-capacity-error"
```

```
                    ]
                }
            }
        },
        {
            "Sid": "DescribeAsg",
            "Effect": "Allow",
            "Action": [
                "autoscaling:DescribeAutoScalingGroups"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

案例內容

下列內容定義案例。您可以儲存此 JSON，並使用 AWS Command Line Interface (AWS CLI) (AWS CLI) 的「建立實驗範本」命令建立實驗範本。如需最新版本的案例，請造訪 FIS 主控台中的案例程式庫。

```
{
    "targets": {
        "IAM-role": {
            "resourceType": "aws:iam:role",
            "resourceArns": [],
            "selectionMode": "ALL"
        },
        "EBS-Volumes": {
            "resourceType": "aws:ec2:ebs-volume",
            "resourceTags": {
                "AzImpairmentPower": "ApiPauseVolume"
            },
            "selectionMode": "COUNT(1)",
            "parameters": {
                "availabilityZoneIdentifier": "us-east-1a"
            },
            "filters": [
                {
                    "path": "Attachments.DeleteOnTermination",
```

```
                    "values": [
                        "false"
                    ]
                }
            ]
        },
        "EC2-Instances": {
            "resourceType": "aws:ec2:instance",
            "resourceTags": {
                "AzImpairmentPower": "StopInstances"
            },
            "filters": [
                {
                    "path": "State.Name",
                    "values": [
                        "running"
                    ]
                },
                {
                    "path": "Placement.AvailabilityZone",
                    "values": [
                        "us-east-1a"
                    ]
                }
            ],
            "selectionMode": "ALL"
        },
        "ASG": {
            "resourceType": "aws:ec2:autoscaling-group",
            "resourceTags": {
                "AzImpairmentPower": "IceAsg"
            },
            "selectionMode": "ALL"
        },
        "ASG-EC2-Instances": {
            "resourceType": "aws:ec2:instance",
            "resourceTags": {
                "AzImpairmentPower": "IceAsg"
            },
            "filters": [
                {
                    "path": "State.Name",
                    "values": [
                        "running"
```

```
                    ]
                },
                {
                    "path": "Placement.AvailabilityZone",
                    "values": [
                        "us-east-1a"
                    ]
                }
            ],
            "selectionMode": "ALL"
        },
        "Subnet": {
            "resourceType": "aws:ec2:subnet",
            "resourceTags": {
                "AzImpairmentPower": "DisruptSubnet"
            },
            "filters": [
                {
                    "path": "AvailabilityZone",
                    "values": [
                        "us-east-1a"
                    ]
                }
            ],
            "selectionMode": "ALL",
            "parameters": {}
        },
        "RDS-Cluster": {
            "resourceType": "aws:rds:cluster",
            "resourceTags": {
                "AzImpairmentPower": "DisruptRds"
            },
            "selectionMode": "ALL",
            "parameters": {
                "writerAvailabilityZoneIdentifiers": "us-east-1a"
            }
        },
        "ElastiCache-Cluster": {
            "resourceType": "aws:elasticache:redis-replicationgroup",
            "resourceTags": {
                "AzImpairmentPower": "DisruptElasticache"
            },
            "selectionMode": "ALL",
            "parameters": {
```

```
                "availabilityZoneIdentifier": "us-east-1a"
            }
        }
    },
    "actions": {
        "Pause-Instance-Launches": {
            "actionId": "aws:ec2:api-insufficient-instance-capacity-error",
            "parameters": {
                "availabilityZoneIdentifiers": "us-east-1a",
                "duration": "PT30M",
                "percentage": "100"
            },
            "targets": {
                "Roles": "IAM-role"
            }
        },
        "Pause-EBS-IO": {
            "actionId": "aws:ebs:pause-volume-io",
            "parameters": {
                "duration": "PT30M"
            },
            "targets": {
                "Volumes": "EBS-Volumes"
            },
            "startAfter": [
                "Stop-Instances",
                "Stop-ASG-Instances"
            ]
        },
        "Stop-Instances": {
            "actionId": "aws:ec2:stop-instances",
            "parameters": {
                "completeIfInstancesTerminated": "true",
                "startInstancesAfterDuration": "PT30M"
            },
            "targets": {
                "Instances": "EC2-Instances"
            }
        },
        "Pause-ASG-Scaling": {
            "actionId": "aws:ec2:asg-insufficient-instance-capacity-error",
            "parameters": {
                "availabilityZoneIdentifiers": "us-east-1a",
                "duration": "PT30M",
```

```
                "percentage": "100"
            },
            "targets": {
                "AutoScalingGroups": "ASG"
            }
        },
        "Stop-ASG-Instances": {
            "actionId": "aws:ec2:stop-instances",
            "parameters": {
                "completeIfInstancesTerminated": "true",
                "startInstancesAfterDuration": "PT30M"
            },
            "targets": {
                "Instances": "ASG-EC2-Instances"
            }
        },
        "Pause-network-connectivity": {
            "actionId": "aws:network:disrupt-connectivity",
            "parameters": {
                "duration": "PT2M",
                "scope": "all"
            },
            "targets": {
                "Subnets": "Subnet"
            }
        },
        "Failover-RDS": {
            "actionId": "aws:rds:failover-db-cluster",
            "parameters": {},
            "targets": {
                "Clusters": "RDS-Cluster"
            }
        },
        "Pause-ElastiCache": {
            "actionId": "aws:elasticache:interrupt-cluster-az-power",
            "parameters": {
                "duration": "PT30M"
            },
            "targets": {
                "ReplicationGroups": "ElastiCache-Cluster"
            }
        }
    },
    "stopConditions": [
```

```
        {
            "source": "aws:cloudwatch:alarm",
            "value": ""
        }
    ],
    "roleArn": "",
    "tags": {
        "Name": "AZ Impairment: Power Interruption"
    },
    "logConfiguration": {
        "logSchemaVersion": 2
    },
    "experimentOptions": {
        "accountTargeting": "single-account",
        "emptyTargetResolutionMode": "skip"
    },
    "description": "Affect multiple resource types in a single AZ, targeting by tags
 and explicit ARNs, to approximate power interruption in one AZ."
}
```

Cross-Region: Connectivity

您可以使用此Cross-Region: Connectivity案例封鎖從實驗區域到目的地區域的應用程式網路流量，並暫停 Amazon S3 和 Amazon DynamoDB 的跨區域複寫。跨區域：連線能力會影響您執行實驗所在地區的輸出應用程式流量 (實驗區域)。來自您希望從實驗區域（目的地區域）隔離的區域的無狀態入站流量可能不會被阻止。來自 AWS 受管服務的流量可能不會遭到封鎖。

此案例可用於證明當目的地區域中的資源無法從實驗區域存取時，多區域應用程式會如預期運作。它包括通過定位運輸網關和路由表阻止從實驗區域到目的地區域的網絡流量。它也會暫停 S3 和 DynamoDB 的跨區域複寫。依預設，將略過找不到目標的動作。

動作

下列動作共同封鎖包含 AWS 服務的跨區域連線。動作會 parallel 執行。根據預設，此案例會封鎖流量 3 小時，您最多可以增加 12 小時持續時間。

中斷 Transit Gateway 連線

Cross Region: Connectivity包括 aws: net: 網路:傳輸閘道中斷的跨區域連線能力，可封鎖從實驗區域中 VPC 到目的地區域中的 VPC 的跨區域網路流量 (由傳輸閘道連接)。這不會影響實驗區域內對 VPC 端點的存取，但會封鎖來自目標區域中目的地 VPC 端點的實驗區域的流量。

此動作針對連接實驗區域和目的地區域的運輸閘道。依預設，它會以值命名`DisruptTransitGateway`的標籤鎖定傳輸閘道`Allowed`。您可以將此標籤新增至公共交通閘道，或在實驗範本中以您自己的標籤取代預設標籤。依預設，如果找不到有效的傳輸閘道，則會略過此動作。

中斷子網路連線

Cross Region: Connectivity包括 aws: network: 路由表中斷-跨區域連線，可封鎖從實驗區域中 VPC 到目的地區域中公有 AWS IP 區塊的跨區域網路流量。這些公有 IP 區塊包括目的地區域中的 AWS 服務端點，例如 S3 區域端點，以及用於受管服務的 AWS IP 區塊，例如用於負載平衡器和 Amazon API Gateway 的 IP 地址。此動作也會封鎖跨區域 VPC 對等連線的網路連線，從實驗區域到目的地區域。它不會影響實驗區域中對 VPC 端點的訪問，但會阻止來自目標區域中目的地 VPC 端點的實驗區域的流量。

此動作針對實驗區域中的子網路。依預設，它會使用以值命名`DisruptSubnet`的標籤來鎖定子網路。`Allowed`您可以將此標籤新增至子網路，或在實驗範本中以您自己的標籤取代預設標籤。依預設，如果找不到有效的子網路，則會略過此動作。

暫停 S3 複寫

Cross Region: Connectivity包括 aw:s3: 儲存貯體暫停複寫，以暫停從實驗區域到目標儲存貯體的目標區域的 S3 複寫。從目的地區域複製到實驗區域將不受影響。在案例結束之後，儲存貯體複寫將會從暫停的時間點繼續進行。請注意，複寫保持所有物件同步所需的時間，會根據實驗的持續時間以及物件上傳至值區的速率而有所不同。

此動作鎖定實驗區域中啟用跨區域複寫 (CRR) 的 S3 儲存貯體到目的地區域中的 S3 儲存貯體。依預設，它會以值命名為`DisruptS3`的標籤鎖定值區`Allowed`。您可以將此標籤添加到存儲桶中，也可以在實驗模板中用自己的標籤替換默認標籤。依預設，如果找不到有效的值區，則會略過此動作。

暫 DynamoDB 複寫

Cross-Region: Connectivity包括 aw: dynamodb: 全域表暫停複寫，以暫停實驗區域與所有其他區域 (包括目的地區域) 之間的複寫。這樣可以防止複製進出實驗區域，但不會影響其他區域之間的複製。在

案例結束之後，資料表複寫將會從暫停的時間點繼續進行。請注意，複寫保持所有資料同步所需的時間會根據實驗持續時間和資料表的變更率而有所不同。

此動作會針對實驗區域中的 DynamoDB 全域表。依預設，它會以值命名的標籤DisruptDynamoDb來鎖定表格Allowed。您可以將此標籤添加到表格中，也可以在實驗模板中用自己的標籤替換默認標籤。依預設，如果找不到有效的全域表格，則會略過此動作。

限制

- 此案例不包含停止條件。應將應用程序的正確停止條件添加到實驗模板中。

要求

- 將必要的權限新增至 AWS FIS 實驗角色。
- 資源標籤必須應用於要被實驗定位的資源。這些可以使用您自己的標記慣例或在案例中定義的預設標籤。

許可

以下政策授予 AWS FIS 執行Cross-Region: Connectivity案例實驗的必要許可。此原則必須附加至實驗角色。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RouteTableDisruptConnectivity1",
            "Effect": "Allow",
            "Action": "ec2:CreateRouteTable",
            "Resource": "arn:aws:ec2:*:*:route-table/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/managedByFIS": "true"
                }
            }
        },
        {
            "Sid": "RouteTableDisruptConnectivity2",
            "Effect": "Allow",
            "Action": "ec2:CreateRouteTable",
```

```
            "Resource": "arn:aws:ec2:*:*:vpc/*"
        },
        {
            "Sid": "RouteTableDisruptConnectivity21",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:route-table/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateRouteTable",
                    "aws:RequestTag/managedByFIS": "true"
                }
            }
        },
        {
            "Sid": "RouteTableDisruptConnectivity3",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface",
                    "aws:RequestTag/managedByFIS": "true"
                }
            }
        },
        {
            "Sid": "RouteTableDisruptConnectivity4",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:prefix-list/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateManagedPrefixList",
                    "aws:RequestTag/managedByFIS": "true"
                }
            }
        },
        {
            "Sid": "RouteTableDisruptConnectivity5",
            "Effect": "Allow",
            "Action": "ec2:DeleteRouteTable",
            "Resource": [
                "arn:aws:ec2:*:*:route-table/*",
```

```
                "arn:aws:ec2:*:*:vpc/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/managedByFIS": "true"
                }
            }
        },
        {
            "Sid": "RouteTableDisruptConnectivity6",
            "Effect": "Allow",
            "Action": "ec2:CreateRoute",
            "Resource": "arn:aws:ec2:*:*:route-table/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/managedByFIS": "true"
                }
            }
        },
        {
            "Sid": "RouteTableDisruptConnectivity7",
            "Effect": "Allow",
            "Action": "ec2:CreateNetworkInterface",
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/managedByFIS": "true"
                }
            }
        },
        {
            "Sid": "RouteTableDisruptConnectivity8",
            "Effect": "Allow",
            "Action": "ec2:CreateNetworkInterface",
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:security-group/*"
            ]
        },
        {
            "Sid": "RouteTableDisruptConnectivity9",
            "Effect": "Allow",
            "Action": "ec2:DeleteNetworkInterface",
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
```

```
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/managedByFIS": "true"
                }
            }
        },
        {
            "Sid": "RouteTableDisruptConnectivity10",
            "Effect": "Allow",
            "Action": "ec2:CreateManagedPrefixList",
            "Resource": "arn:aws:ec2:*:*:prefix-list/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/managedByFIS": "true"
                }
            }
        },
        {
            "Sid": "RouteTableDisruptConnectivity11",
            "Effect": "Allow",
            "Action": "ec2:DeleteManagedPrefixList",
            "Resource": "arn:aws:ec2:*:*:prefix-list/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/managedByFIS": "true"
                }
            }
        },
        {
            "Sid": "RouteTableDisruptConnectivity12",
            "Effect": "Allow",
            "Action": "ec2:ModifyManagedPrefixList",
            "Resource": "arn:aws:ec2:*:*:prefix-list/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/managedByFIS": "true"
                }
            }
        },
        {
            "Sid": "RouteTableDisruptConnectivity13",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces",
```

```
                "ec2:DescribeVpcs",
                "ec2:DescribeVpcPeeringConnections",
                "ec2:DescribeManagedPrefixLists",
                "ec2:DescribeSubnets",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcEndpoints"
            ],
            "Resource": "*"
        },
        {
            "Sid": "RouteTableDisruptConnectivity14",
            "Effect": "Allow",
            "Action": "ec2:ReplaceRouteTableAssociation",
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:route-table/*"
            ]
        },
        {
            "Sid": "RouteTableDisruptConnectivity15",
            "Effect": "Allow",
            "Action": "ec2:GetManagedPrefixListEntries",
            "Resource": "arn:aws:ec2:*:*:prefix-list/*"
        },
        {
            "Sid": "RouteTableDisruptConnectivity16",
            "Effect": "Allow",
            "Action": "ec2:AssociateRouteTable",
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:route-table/*"
            ]
        },
        {
            "Sid": "RouteTableDisruptConnectivity17",
            "Effect": "Allow",
            "Action": "ec2:DisassociateRouteTable",
            "Resource": [
                "arn:aws:ec2:*:*:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/managedByFIS": "true"
                }
```

```
            }
        },
        {
            "Sid": "RouteTableDisruptConnectivity18",
            "Effect": "Allow",
            "Action": "ec2:DisassociateRouteTable",
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*"
            ]
        },
        {
            "Sid": "RouteTableDisruptConnectivity19",
            "Effect": "Allow",
            "Action": "ec2:ModifyVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:*:*:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/managedByFIS": "true"
                }
            }
        },
        {
            "Sid": "RouteTableDisruptConnectivity20",
            "Effect": "Allow",
            "Action": "ec2:ModifyVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:*:*:vpc-endpoint/*"
            ]
        },
        {
            "Sid": "TransitGatewayDisruptConnectivity1",
            "Effect": "Allow",
            "Action": [
                "ec2:DisassociateTransitGatewayRouteTable",
                "ec2:AssociateTransitGatewayRouteTable"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:transit-gateway-route-table/*",
                "arn:aws:ec2:*:*:transit-gateway-attachment/*"
            ]
        },
        {
```

```
            "Sid": "TransitGatewayDisruptConnectivity2",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeTransitGatewayPeeringAttachments",
                "ec2:DescribeTransitGatewayAttachments",
                "ec2:DescribeTransitGateways"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3CrossRegion1",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3CrossRegion2",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3CrossRegion3",
            "Effect": "Allow",
            "Action": [
                "s3:PauseReplication"
            ],
            "Resource": "arn:aws:s3:::*",
            "Condition": {
                "StringLike": {
                    "s3:DestinationRegion": "*"
                }
            }
        },
        {
            "Sid": "S3CrossRegion4",
            "Effect": "Allow",
            "Action": [
                "s3:GetReplicationConfiguration",
                "s3:PutReplicationConfiguration"
```

```
            ],
            "Resource": "arn:aws:s3:::*",
            "Condition": {
                "BoolIfExists": {
                    "s3:isReplicationPauseRequest": "true"
                }
            }
        },
        {
            "Sid": "DdbCrossRegion1",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DdbCrossRegion2",
            "Effect": "Allow",
            "Action": [
                "dynamodb:DescribeTable",
                "dynamodb:DescribeGlobalTable"
            ],
            "Resource": [
                "arn:aws:dynamodb:*:*:table/*",
                "arn:aws:dynamodb:*:*:global-table/*"
            ]
        },
        {
            "Sid": "DdbCrossRegion3",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:GetKeyPolicy",
                "kms:PutKeyPolicy"
            ],
            "Resource": "arn:aws:kms:*:*:key/*"
        }
    ]
}
```

案例內容

下列內容定義案例。您可以儲存此 JSON，並使用 AWS Command Line Interface (AWS CLI) (AWS CLI) 的「建立實驗範本」命令建立實驗範本。如需最新版本的案例，請造訪 FIS 主控台中的案例程式庫。

```
{
        "targets": {
                "Transit-Gateway": {
                        "resourceType": "aws:ec2:transit-gateway",
                        "resourceTags": {
                                "TgwTag": "TgwValue"
                        },
                        "selectionMode": "ALL"
                },
                "Subnet": {
                        "resourceType": "aws:ec2:subnet",
                        "resourceTags": {
                                "SubnetKey": "SubnetValue"
                        },
                        "selectionMode": "ALL",
                        "parameters": {}
                },
                "S3-Bucket": {
                        "resourceType": "aws:s3:bucket",
                        "resourceTags": {
                                "S3Impact": "Allowed"
                        },
                        "selectionMode": "ALL"
                },
                "DynamoDB-Global-Table": {
                        "resourceType": "aws:dynamodb:encrypted-global-table",
                        "resourceTags": {
                                "DisruptDynamoDb": "Allowed"
                        },
                        "selectionMode": "ALL"
                }
        },
        "actions": {
                "Disrupt-Transit-Gateway-Connectivity": {
                        "actionId": "aws:network:transit-gateway-disrupt-cross-region-
connectivity",
                        "parameters": {
```

```
                                "duration": "PT3H",
                                "region": "eu-west-1"
                        },
                        "targets": {
                                "TransitGateways": "Transit-Gateway"
                        }
                },
                "Disrupt-Subnet-Connectivity": {
                        "actionId": "aws:network:route-table-disrupt-cross-region-
connectivity",
                        "parameters": {
                                "duration": "PT3H",
                                "region": "eu-west-1"
                        },
                        "targets": {
                                "Subnets": "Subnet"
                        }
                },
                "Pause-S3-Replication": {
                        "actionId": "aws:s3:bucket-pause-replication",
                        "parameters": {
                                "duration": "PT3H",
                                "region": "eu-west-1"
                        },
                        "targets": {
                                "Buckets": "S3-Bucket"
                        }
                },
                "Pause-DynamoDB-Replication": {
                        "actionId": "aws:dynamodb:encrypted-global-table-pause-
replication",
                        "parameters": {
                                "duration": "PT3H"
                        },
                        "targets": {
                                "Tables": "DynamoDB-Global-Table"
                        }
                }
        },
        "stopConditions": [
                {
                        "source": "none"
                }
        ],
```

```
        "roleArn": "",
        "logConfiguration": {
                "logSchemaVersion": 2
        },
        "tags": {
                "Name": "Cross-Region: Connectivity"
        },
        "experimentOptions": {
                "accountTargeting": "single-account",
                "emptyTargetResolutionMode": "skip"
        },
        "description": "Block application network traffic from experiment Region to
 target Region and pause cross-Region replication"
}
```

金融信息 AWS 系統的實驗

AWS FIS 可讓您對 AWS 工作負載執行故障注入實驗。若要開始使用，請建立實驗範本。建立實驗範本後，您可以使用它來開始實驗。

當發生以下情況之一時，實驗就會完成：

- 範本中的所有動作都已順利完成。
- 觸發停止條件。
- 因為發生錯誤而無法完成動作。例如，如果找不到目標。
- 實驗是手動停止的。

您無法繼續已停止或失敗的實驗。您也無法重新執行已完成的實驗。但是，您可以從同一個實驗模板開始新的實驗。您可以選擇性地更新實驗樣板，然後再次在新實驗中指定它。

任務

- 開始實驗
- 檢視您的實驗
- 標記實驗
- 停止實驗
- 列出已解析目標

開始實驗

您可以從實驗範本開始實驗。如需詳細資訊，請參閱 從範本開始實驗。

您可以使用將實驗安排為一次性任務或重複性任務 Amazon EventBridge。如需詳細資訊，請參閱 教學課程：排程重複實驗。

您可以使用以下任何功能監視您的實驗：

- 在 AWS FIS 主控台中檢視您的實驗。如需詳細資訊，請參閱 檢視您的實驗。
- 檢視實驗中目標資源的 Amazon CloudWatch 指標，或檢視 AWS FIS 使用量指標。如需詳細資訊，請參閱 監視器使用 CloudWatch。

- 啟用實驗日誌記錄以捕獲有關實驗運行時的詳細信息。如需更多資訊，請參閱實驗記錄。

檢視您的實驗

您可以檢視執行中實驗的進度，也可以檢視已完成、停止或失敗的實驗。

已停止、完成和失敗的實驗會在 120 天後自動從您的帳戶中移除。

若要使用主控台檢視實驗

1. 開啟 AWS 金融資訊系統控制台，網址為 https://console.aws.amazon.com/fis/。
2. 在導覽窗格中，選擇 [實驗]。
3. 選擇實驗的實驗 ID 以打開其詳細信息頁面。
4. 執行下列其中一項或多項：
   - 檢查詳細信息，狀態實驗的狀態。
   - 選擇 [動作] 索引標籤以取得實驗動作的相關資訊。
   - 選擇 [目標] 索引標籤以取得實驗目標的相關資訊。
   - 選擇「時間軸」(Timeline) 標籤，根據動作的開始和結束時間來視覺化呈現。

若要使用 CLI 檢視實驗

使用列表實驗命令獲取實驗列表，並使用 get-lab 命令獲取有關特定實驗的信息。

实验状态

實驗可以處於以下狀態之一：

- 待決 — 實驗正在等待中。
- 啟動 — 實驗正準備開始。
- 執行中 — 實驗正在執行中。
- 已完成 — 實驗中的所有操作都已成功完成。
- stop — 已觸發停止條件或手動停止實驗。
- 已停止 — 停止實驗中的所有正在運行或待處理的操作。
- fail — 由於錯誤，例如權限不足或語法不正確，導致實驗失敗。

動作狀態

動作可以處於下列其中一種狀態：

- 待處理-動作處於待處理狀態，可能是因為實驗尚未開始，要么動作將在實驗中稍後開始。
- 啟動 — 動作正準備開始。
- 執行中 — 動作正在執行中。
- 已完成 — 動作已順利完成。
- 已取消 — 實驗在動作開始前停止。
- 略過 — 已略過動作。
- 停止 — 動作正在停止。
- 已停止 — 停止實驗中的所有正在運行或待處理的操作。
- fail — 動作因為用戶端錯誤 (例如權限不足或語法不正確) 而失敗。

標記實驗

您可以將標籤應用於實驗以幫助您組織它們。您也可以實作以標籤為基礎的 IAM 政策，以控制對實驗的存取。

使用控制台標記實驗

1. 開啟 AWS 金融資訊系統控制台，網址為 https://console.aws.amazon.com/fis/。
2. 在導覽窗格中，選擇 [實驗]。
3. 選取實驗，然後選擇 [動作]、[管理標籤]。
4. 若要新增標籤，請選擇「新增標籤」，然後指定機碼和值。

   若要移除標記，請為標籤選擇「移除」。
5. 選擇儲存。

若要使用 CLI 標記實驗

使用標籤資源命令。

停止實驗

您可以隨時停止執行中的實驗。當您停止實驗時，任何尚未完成某個動作的貼文動作都會在實驗停止之前完成。您無法繼續已停止的實驗。

使用控制台停止實驗

1. 開啟 AWS 金融資訊系統控制台，網址為 https://console.aws.amazon.com/fis/。
2. 在導覽窗格中，選擇 [實驗]。
3. 選擇實驗，然後選擇停止實驗。
4. 在確認對話方塊中，選擇 [停止實驗]。

若要使用 CLI 停止實驗

使用停止實驗指令。

列出已解析目標

您可以在目標解析結束後檢視實驗已解決目標的資訊。

使用主控台檢視已解析的目標

1. 開啟 AWS 金融資訊系統控制台，網址為 https://console.aws.amazon.com/fis/。
2. 在導覽窗格中，選擇 [實驗]。
3. 選取實驗，然後選擇 [報告]。
4. 在資源下檢視已解析的目標資訊。

使用 CLI 檢視已解析的目標

使用清單實驗解析- 目標指令。

實驗排程器

使用 AWS 故障注入服務 (FIS)，您可以在 AWS 工作負載上執行故障注入實驗。這些實驗在包含要在指定目標上執行的一或多個動作的範本上執行。現在，您可以從 FIS Console 將實驗排定為一次性工作或重複執行的工作。除了排程規則之外，FIS 現在還提供了新的排程功能。FIS 現在與 EventBridge 排程器整合，並代表您建立規則。 EventBridge Scheduler 是無伺服器排程器，可讓您從單一中央受管理的服務建立、執行及管理工作。

> **Important**
>
> AWS GovCloud (美國東部) 和 AWS (美國西部) 不提供實驗排程器。 AWS Fault Injection Service GovCloud

主題

開始使用

執行角色是 AWS 容錯注入服務假設的 IAM 角色，以便與 EventBridge 排程器互動，以及讓事件橋接排程器啟動 FIS 實驗。您可以將權限原則附加至此角色，以授與 EventBridge排程器呼叫 FIS 實驗的存取權。下列步驟說明如何建立新的執行角色，以及允許 EventBridge 啟動實驗的原則。

使用 AWS CLI 建立排程器角色

這是事件橋接器所需的 IAM 角色，才能代表客戶安排實驗。

1. 複製下列假設角色 JSON 原則，並將其儲存為本機 `fis-execution-role.json`。此信任原則允許 EventBridge 排程器代表您擔任該角色。

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

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

2. 從 AWS Command Line Interface (AWS CLI) (AWS CLI) 輸入以下命令以建立新角色。取代`FisSchedulerExecutionRole`為您要賦予此角色的名稱。

```
aws iam create-role --role-name FisSchedulerExecutionRole --assume-role-policy-
document file://fis-execution-role.json
```

如果成功，您將看到以下輸出：

```
{
    "Role": {
        "Path": "/",
        "RoleName": "FisSchedulerExecutionRole",
        "RoleId": "AROAZL22PDN5A6WKRBQNU",
        "Arn": "arn:aws:iam::123456789012:role/FisSchedulerExecutionRole",
        "CreateDate": "2023-08-24T17:23:05+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Principal": {
                        "Service": "scheduler.amazonaws.com"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }
    }
}
```

3. 若要建立允許 EventBridge 排程器叫用實驗的新原則，請複製下列 JSON 並在本機儲存為 `fis-start-experiment-permissions.json`。下列政策允許 EventBridge Scheduler 在您帳戶中的所有實驗範本上呼叫`fis:StartExperiment`動作。如果您想將角色限制為單個實驗模板，請將*在的末尾替換為實驗模板的 ID。`"arn:aws:fis:*:*:experiment-template/*"`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "fis:StartExperiment",
            "Resource": [
                "arn:aws:fis:*:*:experiment-template/*",
                "arn:aws:fis:*:*:experiment/*"
            ]
        }
    ]
}
```

4. 執行下列命令以建立新的權限原則。取代 `FisSchedulerPolicy`為您要提供此原則的名稱。

```
aws iam create-policy --policy-name FisSchedulerPolicy --policy-document file://fis-start-experiment-permissions.json
```

如果成功，你會看到下面的輸出。請注意政策 ARN。您在下一個步驟中使用此 ARN 將原則附加到我們的執行角色。

```
{
    "Policy": {
        "PolicyName": "FisSchedulerPolicy",
        "PolicyId": "ANPAZL22PDN5ESVUWXLBD",
        "Arn": "arn:aws:iam::123456789012:policy/FisSchedulerPolicy",
        "Path": "/",
        "DefaultVersionId": "v1",
        "AttachmentCount": 0,
        "PermissionsBoundaryUsageCount": 0,
        "IsAttachable": true,
        "CreateDate": "2023-08-24T17:34:45+00:00",
        "UpdateDate": "2023-08-24T17:34:45+00:00"
    }
}
```

5. 執行下列命令，將原則附加至您的執行角色。取代your-policy-arn為您在上一個步驟中建立之原則的 ARN。FisSchedulerExecutionRole以執行角色的名稱取代。

```
aws iam attach-role-policy --policy-arn your-policy-arn --role-name
 FisSchedulerExecutionRole
```

作attach-role-policy業不會在命令列上傳回應。

6. 您可以限制排程器僅執行具有特定標籤值的 AWS FIS 實驗。例如，以下政策授予所有 AWS FIS 實驗範本的 fis:StartExperiment許可，但限制排程器僅執行已標記的實驗。Purpose=Schedule

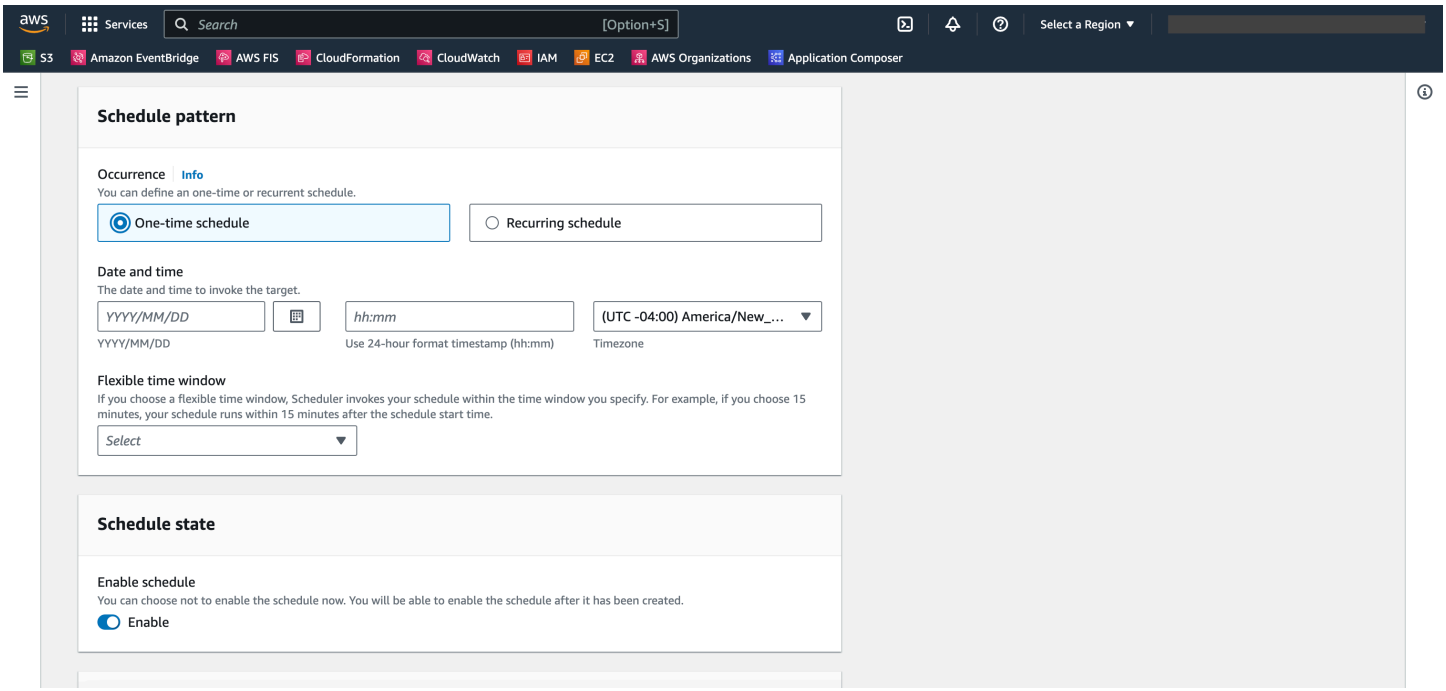
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "fis:StartExperiment",
            "Resource": "arn:aws:fis:*:*:experiment/*"
        },
        {
            "Effect": "Allow",
            "Action": "fis:StartExperiment",
            "Resource": "arn:aws:fis:*:*:experiment-template/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Purpose": "Schedule"
                }
            }
        }
    ]
}
```

安排 FIS 實驗

在安排實驗之前，您需要一個或多实验模板個排程才能叫用。您可以使用現有的 AWS 資源，或建立新的資源。

創建實驗模板後，單擊「操作」，然後選擇「計劃實驗」。您將被重定向到計劃實驗頁面。系統會為您填寫排程名稱。

遵循排程模式區段，然後選擇一次性排程或週期性。填寫必要的輸入欄位並瀏覽至權限。



預設情況下會啟用排程狀態。注意：如果您停用排程狀態，即使您建立排程，也不會排程實驗。

AWS FIS 實驗調度程序是建立在EventBridge 調度程序的頂部。您可以參考文件以瞭解支援的各種排程類型。

使用主控台更新排程

1. 開啟 AWS FIS 主控台。
2. 在左側導覽窗格中，選擇 [實驗範本]。
3. 選擇您要為其建立明細表的實驗樣板。
4. 點擊操作，然後從下拉列表中選擇計劃實驗。
   a. 在「排程名稱」下，會 auto 填入名稱。
   b. 在排程模式下，選取週期性排程。
   c. 在「排程類型」下，您可以選取以比率為基礎的排程，請參閱排程型態。
   d. 在 R ate 表達式下，選擇比實驗執行時間慢的速率，例如 5 分鐘。
   e. 在「時間範圍」下，選取您的時區。

f. 在開始日期和時間下，指定開始日期和時間。

g. 在結束日期和時間下，指定結束日期和時間

h. 在「排程狀態」下，切換「啟用排程選項」。

i. 在 [權限] 下，選取 [使用現有角色]，然後搜尋 `FisSchedulerExecutionRole`。

j. 選擇下一步。

5. 選取 [檢閱並建立排程]、檢閱排程器詳細資料，然後選擇 [建立排程]。

更新實驗時間表

您可以更新實驗時間表，使其發生在適合您的特定日期和時間。

使用控制台更新實驗執行

1. 開啟 Amazon FIS 主控台。
2. 在導覽窗格中，選擇 [實驗範本]。
3. 選擇資源類型：已為其建立排程的實驗範本。
4. 按一下範本的實驗 ID。然後導覽至排程標籤。
5. 檢查是否存在與實驗相關聯的現有時間表。選取相關的排程，然後按一下「更新排程」按鈕。

使用控制台禁用或刪除實驗執行

若要停止實驗按排程執行或執行，您可以刪除或停用規則。以下步驟將引導您如何刪除或禁用實驗執行。

若要刪除或停用規則

1. 開啟 Amazon FIS 主控台。
2. 在導覽窗格中，選擇 [實驗範本]。
3. 選擇資源類型：已為其建立排程的實驗範本。
4. 按一下範本的實驗 ID。然後導覽至排程標籤。
5. 檢查是否存在與實驗相關聯的現有時間表。選取相關的排程，然後按一下「更新排程」按鈕。
6. 執行以下任意一項：

a. 若要刪除排程，請選取「刪除排程」規則旁邊的按鈕。輸入`delete`並按一下「刪除排程」按鈕。

b. 若要停用排程，請選取規則旁邊的按鈕 [停用排程]。鍵入`disable`並按一下「停用排程」按鈕。

監控AWS金融系統

您可以使用下列工具來監控AWS故障注入服務 (AWSFIS) 實驗的進度和影響。

AWSFIS 控制台和 AWS CLI

使用 AWS FIS 主控台或監視執行中實驗的進度。AWS CLI您可以檢視實驗中每個動作的狀態，以及每個動作的結果。如需詳細資訊，請參閱 the section called “檢視您的實驗”。

CloudWatch 使用量度和警示

使用 CloudWatch 使用量度來提供您帳戶資源使用情況的可見度。 AWSFIS 使用量度對應於AWS服務配額。您可以設定警示，在您的用量接近服務配額時發出警示。如需詳細資訊，請參閱 監視器使用 CloudWatch。

您也可以透過建立定義實驗何時超出邊界的 CloudWatch 警報，為 AWS FIS 實驗建立停止條件。觸發警報時，實驗停止。如需詳細資訊，請參閱 停止條件。如需有關建立 CloudWatch 警示的詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的根據靜態閾值建立 CloudWatch 警示和根據異常偵測建立警示。 CloudWatch

AWSFIS 實驗記錄

啟用實驗日誌記錄以在實驗運行時捕獲有關實驗的詳細信息。如需更多資訊，請參閱 實驗記錄。

實驗狀態變更事件

Amazon EventBridge 可讓您自動回應系統事件或資源變更。 AWSFIS 會在實驗狀態變更時發出通知。您可以為感興趣的事件建立規則，以指定事件符合規則時要採取的自動化動作。例如，傳送通知給 Amazon SNS 主題或叫用 Lambda 函數。如需詳細資訊，請參閱 監視器使用 EventBridge。

CloudTrail 日誌

用AWS CloudTrail於擷取有關 AWS FIS API 呼叫的詳細資訊，並將它們作為日誌檔存放在 Amazon S3 中。 CloudTrail 還會記錄對您正在執行實驗之資源的服務 API 進行的呼叫。您可以使用這些 CloudTrail 記錄來判斷撥打哪些呼叫、來源 IP 位址呼叫來源、撥打電話的人員、撥打電話的時間等等。

AWSHealth 儀表板

AWS Health 讓您持續掌握資源效能以及AWS服務和帳戶的可用性。當您開始實驗時，AWSFIS 會向您的 AWS Health 儀表板發出通知。每個帳戶中的實驗期間都會顯示該通知，該帳戶包含實驗中目標的資源，包括多帳戶實驗。僅包含不包含目標之動作的多帳戶實驗，例如`aws:ssm:start-`

`automation-execution`和`aws:fis:wait`，將不會發出通知。有關用於實驗的角色的信息將列在「受影響的資源」下。若要進一步了解 AWS Health 儀表板，請參閱 AWS Health 使用者指南中的 AWS Health 儀表板。

> **Note**
>
> AWS Health 以最大的方式交付活動。

使用亞馬遜監控AWS FIS 使用量指標 CloudWatch

您可以使 CloudWatch 用 Amazon 監控AWS FIS 實驗對目標的影響。您也可以監控AWS FIS 使用情況。

如需檢視實驗狀態的詳細資訊，請參閱檢視您的實驗。

監控AWS FIS 實驗

規劃AWS FIS 實驗時，請確定可用於識別實驗目標資源類型的基準線或「穩定狀態」的 CloudWatch 指標。開始實驗後，您可以監視透過實驗範本選取的目標的這些 CloudWatch指標。

如需AWS FIS 支援之目標資源類型之可用 CloudWatch 測量結果的詳細資訊，請參閱下列內容：

- 使用監控執行個體 CloudWatch
- 亞馬遜 ECS CloudWatch 指標
- 使用 Amazon RDS 指標 CloudWatch
- 監視執行命令測量結果 CloudWatch

AWSFIS 用量指標

您可使用用用用 CloudWatch 用用用用用用用用用用用用用用用用用用用用用用用用用用 使用這些指標，以 CloudWatch 圖表和儀表板視覺化目前的服務使用狀況。

AWSFIS 用量指標對應到AWS Service Quotas。您可以設定警示，在您的用量接近服務配額時發出警示。如需有關 CloudWatch 警示的詳細資訊，請參閱 Amazon CloudWatch 使用者指南。

AWSFIS 會在 AWS/ 使用命名空間中發佈下列量度。

指標	描述
ResourceCount	您的帳戶中正在執行的特定資源總數。資源由與指標相關聯的維度定義。

以下維度用於強化AWS FIS 發佈的用量指標。

維度	描述
Service	包含該資源的 AWS 服務的名稱。對AWS於 FIS 用量指標，此維度的值為FIS。
Type	正在報告的實體類型。目前，AWSFIS 用量指標的唯一有效值為Resource。
Resource	正在執行的資源類型。可能的值ExperimentTemplates 適用於實驗範本和使ActiveExperiments 用中實驗。
Class	此維度保留給 future 使用。

使用 AWS Amazon 監控 FIS 實驗 EventBridge

當實驗狀態發生變化時， AWS FIS 會發出通知。這些通知可透過 Amazon EventBridge （以前稱為活動）作為 CloudWatch 事件提供。 AWS FIS 會以最大的努力為基礎發出這些事件。活動會以近乎即時 EventBridge 的方式傳送到。

使用 EventBridge，您可以建立規則來觸發程式設計動作以回應事件。例如，您可以設定可呼叫 SNS 主題的規則來傳送電子郵件通知，或叫用 Lambda 函數採取某些動作。

如需詳細資訊 EventBridge，請參閱 Amazon EventBridge 使用者指南 EventBridge中的開始使用 Amazon。

以下是實驗狀態更改事件的語法：

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
```

```
    "detail-type": "FIS Experiment State Change",
    "source": "aws.fis",
    "account": "123456789012",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "region",
    "resources": [
        "arn:aws:fis:region:account_id:experiment/experiment-id"
    ],
    "detail": {
        "experiment-id": "EXPaBCD1efg2HIJkL3",
        "experiment-template-id": "EXTa1b2c3de5f6g7h",
        "new-state": {
            "status": "new_value",
            "reason": "reason_string"
        },
        "old-state": {
           "status": "old_value",
           "reason": "reason_string"
        }
    }
}
```

`experiment-id`

狀態變更之實驗的 ID。

`experiment-template-id`

實驗使用的實驗模板的 ID。

`new_value`

實驗的新狀態。可能值如下：

- `completed`
- `failed`
- `initiating`
- `running`
- `stopped`
- `stopping`

`old_value`

實驗的先前狀態。可能值如下：

- initiating
- pending
- running
- stopping

AWSFIS 的實驗記錄

您可以使用實驗日誌記錄來捕獲有關實驗運行時的詳細信息。

系統會根據與每個記錄目標類型相關聯的費用向您收取實驗記錄的費用。如需詳細資訊，請參閱 Amazon CloudWatch 定價 (在付費方案、日誌、付費日誌下) 和 Amazon S3 定價。

許可

您必須授與 AWS FIS 權限，才能將記錄檔傳送至您設定的每個記錄目的地。如需詳細資訊，請參閱 Amazon CloudWatch 日誌使用者指南中的以下內容：

- 傳送至記錄 CloudWatch 檔的記錄
- 傳送到 Amazon S3 的日誌

記錄檔結構

以下是在實驗日誌中使用的模式。目前的結構描述版本為 2。的欄位取`details`決於的值`log_type`。的欄位取`resolved_targets`決於的值`target_type`。如需詳細資訊，請參閱 the section called “記錄記錄範例”。

```
{
    "id": "EXP123abc456def789",
    "log_type": "experiment-start | target-resolution-start | target-resolution-detail
 | target-resolution-end | action-start | action-error | action-end | experiment-end",
    "event_timestamp": "yyyy-mm-ddThh:mm:ssZ",
    "version": "2",
    "details": {
        "account_id":"123456789012",
        "action_end_time": "yyyy-mm-ddThh:mm:ssZ",
        "action_id": "String",
        "action_name": "String",
```

```
        "action_start_time": "yyyy-mm-ddThh:mm:ssZ",
        "action_state": {
            "status": "pending | initiating | running | completed | cancelled |
 stopping | stopped | failed",
            "reason": "String"
        },
        "action_targets": "String to string map",
        "error_information": "String",
        "experiment_end_time": "yyyy-mm-ddThh:mm:ssZ",
        "experiment_state": {
            "status": "pending | initiating | running | completed | stopping | stopped
 | failed",
            "reason": "String"
        },
        "experiment_start_time": "yyyy-mm-ddThh:mm:ssZ",
        "experiment_template_id": "String",
        "page": Number,
        "parameters": "String to string map",
        "resolved_targets": [
            {
               "field": "value"
            }
        ],
        "resolved_targets_count": Number,
        "status": "failed | completed",
        "target_name": "String",
        "target_resolution_end_time": "yyyy-mm-ddThh:mm:ssZ",
        "target_resolution_start_time": "yyyy-mm-ddThh:mm:ssZ",
        "target_type": "String",
        "total_pages": Number,
        "total_resolved_targets_count": Number

    }
}
```

版本備註

- 版本 2 介紹：
  - 該target_type字段，并將該resolved_targets字段從 ARN 列表變更為對象列表。resolved_targets物件的有效欄位取決於的值target_type，這是目標的資源類型。
  - 新增account_id欄位的action-error和target-resolution-detail事件類型。
- 版本 1 是初始版本。

記錄目的地

AWSFIS 支援將記錄傳送至下列目的地：

- Amazon S3 儲存貯體
- Amazon CloudWatch 日誌日誌組

S3 日誌交付

記錄會傳送至下列位置。

```
bucket-and-optional-prefix/AWSLogs/account-id/fis/region/experiment-
id/YYYY/MM/DD/account-id_awsfislogs_region_experiment-id_YYYYMMDDHHMMZ_hash.log
```

記錄檔可能需要數分鐘才會傳送至儲存貯體。

CloudWatch 記錄檔傳送

```
######## /aws/fis/ ############
```

記錄檔會在不到一分鐘的時間內傳送至記錄群組。

記錄記錄範例

以下是在隨機選取的 EC2 執行個體上執行aws:ec2:reboot-instances動作的實驗範例日誌記錄。

記錄

- 實驗開始
- target-resolution-start
- target-resolution-detail
- target-resolution-end
- 動作開始
- 動作結束
- 動作錯誤
- 實驗結束

實驗開始

以下是事件的範例記experiment-start錄。

```
{
    "id": "EXPhjAXCGY78HV2a4A",
    "log_type": "experiment-start",
    "event_timestamp": "2023-05-31T18:50:45Z",
    "version": "2",
    "details": {
        "experiment_template_id": "EXTCDh1M8HHkhxoaQ",
        "experiment_start_time": "2023-05-31T18:50:43Z"
    }
}
```

target-resolution-start

以下是事件的範例記target-resolution-start錄。

```
{
    "id": "EXPhjAXCGY78HV2a4A",
    "log_type": "target-resolution-start",
    "event_timestamp": "2023-05-31T18:50:45Z",
    "version": "2",
    "details": {
        "target_resolution_start_time": "2023-05-31T18:50:45Z",
        "target_name": "EC2InstancesToReboot"
    }
}
```

target-resolution-detail

以下是事件的範例記target-resolution-detail錄。如果目標解析失敗，記錄也會包含error_information欄位。

```
{
    "id": "EXPhjAXCGY78HV2a4A",
    "log_type": "target-resolution-detail",
    "event_timestamp": "2023-05-31T18:50:45Z",
    "version": "2",
    "details": {
        "target_resolution_end_time": "2023-05-31T18:50:45Z",
        "target_name": "EC2InstancesToReboot",
```

```
        "target_type": "aws:ec2:instance",
        "account_id": "123456789012",
        "resolved_targets_count": 2,
        "status": "completed"

    }
}
```

target-resolution-end

如果目標解析失敗，記錄也會包含error_information欄位。如果大total_pages於 1，則已解決的目標數目超過一筆記錄的大小限制。還有其他target-resolution-end記錄包含剩餘的已解析目標。

以下是 EC2 動作target-resolution-end事件的範例記錄。

```
{
    "id": "EXPhjAXCGY78HV2a4A",
    "log_type": "target-resolution-end",
    "event_timestamp": "2023-05-31T18:50:45Z",
    "version": "2",
    "details": {
        "target_resolution_end_time": "2023-05-31T18:50:46Z",
        "target_name": "EC2InstanceToReboot",
        "target_type": "aws:ec2:instance",
        "resolved_targets": [
            {
                "arn": "arn:aws:ec2:us-east-1:123456789012:instance/
i-0f7ee2abffc330de5"
            }
        ],
        "page": 1,
        "total_pages": 1
    }
}
```

以下是 EKS 動作之target-resolution-end事件的範例記錄。

```
{
    "id": "EXP24YfiucfyVPJpEJn",
    "log_type": "target-resolution-end",
    "event_timestamp": "2023-05-31T18:50:45Z",
```

```
    "version": "2",
    "details": {
        "target_resolution_end_time": "2023-05-31T18:50:46Z",
        "target_name": "myPods",
        "target_type": "aws:eks:pod",
        "resolved_targets": [
            {
                "pod_name": "example-696fb6498b-sxhw5",
                "namespace": "default",
                "cluster_arn": "arn:aws:eks:us-east-1:123456789012:cluster/fis-demo-
cluster",
                "target_container_name": "example"
            }
        ],
        "page": 1,
        "total_pages": 1
    }
}
```

動作開始

以下是事件的範例記action-start錄。如果實驗範本指定動作的參數，則記錄也會包含parameters欄位。

```
{
    "id": "EXPhjAXCGY78HV2a4A",
    "log_type": "action-start",
    "event_timestamp": "2023-05-31T18:50:56Z",
    "version": "2",
    "details": {
        "action_name": "Reboot",
        "action_id": "aws:ec2:reboot-instances",
        "action_start_time": "2023-05-31T18:50:56Z",
        "action_targets": {"Instances":"EC2InstancesToReboot"}
    }
}
```

動作錯誤

以下是事件的範例記action-error錄。只有在動作失敗時才會傳回此事件。會針對動作失敗的每個帳戶傳回此動作。

```
{
    "id": "EXPhjAXCGY78HV2a4A",
    "log_type": "action-error",
    "event_timestamp": "2023-05-31T18:50:56Z",
    "version": "2",
    "details": {
        "action_name": "pause-io",
        "action_id": "aws:ebs:pause-volume-io",
        "account_id": "123456789012",
        "action_state": {
            "status": "failed",
            "reason":"Unable to start Pause Volume IO. Target volumes must be attached
 to an instance type based on the Nitro system. VolumeId(s): [vol-1234567890abcdef0]:"
        }
    }
}
```

動作結束

以下是事件的範例記action-end錄。

```
{
    "id": "EXPhjAXCGY78HV2a4A",
    "log_type": "action-end",
    "event_timestamp": "2023-05-31T18:50:56Z",
    "version": "2",
    "details": {
        "action_name": "Reboot",
        "action_id": "aws:ec2:reboot-instances",
        "action_end_time": "2023-05-31T18:50:56Z",
        "action_state": {
            "status": "completed",
            "reason": "Action was completed."
        }
    }
}
```

實驗結束

以下是事件的範例記experiment-end錄。

```
{
```

```
    "id": "EXPhjAXCGY78HV2a4A",
    "log_type": "experiment-end",
    "event_timestamp": "2023-05-31T18:50:57Z",
    "version": "2",
    "details": {
        "experiment_end_time": "2023-05-31T18:50:57Z",
        "experiment_state": {
            "status": "completed",
            "reason": "Experiment completed"
        }
    }
}
```

啟用實驗記錄

默認情況下禁用實驗日誌記錄。要接收實驗的實驗日誌，您必須在啟用日誌記錄的情況下從實驗模板創建實驗。當您第一次執行設定為使用先前未使用過的目的地進行記錄的實驗時，我們會延遲實驗以設定至此目的地的記錄傳遞，這需要大約 15 秒的時間。

使用控制台啟用實驗記錄

1. 開啟AWS金融資訊系統控制台，網址為 https://console.aws.amazon.com/fis/。
2. 在導覽窗格中，選擇 [實驗範本]。
3. 選取實驗範本，然後選擇 [動作]、[更新實驗範本]。
4. 對於記錄檔，設定目的地選項。若要將日誌傳送到 S3 儲存貯體，請選擇「傳送到 Amazon S3 儲存貯體」，然後輸入儲存貯體名稱和前置詞。如果要將記錄檔傳送至 CloudWatch 記錄檔，請選擇「傳送至 CloudWatch 記錄檔」並輸入記錄群組。
5. 選擇更新實驗模板。

若要啟用實驗記錄，請使用 AWS CLI

使用指update-experiment-template令並指定記錄組態。

停用實驗記錄

如果您不想再接收實驗的日誌，則可以禁用實驗日誌記錄。

若要使用主控台停用實驗記錄

1. 開啟AWS金融資訊系統控制台，網址為 https://console.aws.amazon.com/fis/。

2. 在導覽窗格中，選擇 [實驗範本]。
3. 選取實驗範本，然後選擇 [動作]、[更新實驗範本]。
4. 對於日誌，請清除傳送到 Amazon S3 儲存貯體並傳送到 CloudWatch 日誌。
5. 選擇更新實驗模板。

若要停用實驗記錄，請使用 AWS CLI

使用命update-experiment-template令並指定空白記錄組態。

使用 AWS CloudTrail 記錄 API 呼叫

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

若要進一步了解 CloudTrail，請參閱使AWS CloudTrail用者指南。

使用 CloudTrail

CloudTrail 在您創建帳戶AWS 帳戶時啟用。當活動在 AWS FIS 中發生時，該活動會與事件歷史記錄中的其他AWS服務 CloudTrail 事件一起記錄在事件中。您可以檢視、搜尋和下載 AWS 帳戶 的最新事件。如需詳細資訊，請參閱檢視具有事 CloudTrail 件記錄的事件。

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

- 為您的AWS帳戶建立追蹤
- CloudTrail 支援的服務與整合
- 設定的 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 記錄檔並從多個帳戶接收 CloudTrail 記錄檔

所AWS有 FIS 動作均由記錄， CloudTrail 並記錄在AWS錯誤注入服務 API 參考中。對於在目標資源上執行的實驗動作，請檢視擁有該資源之服務的 API 參考文件。例如，如需在 Amazon EC2 執行個體上執行的動作，請參閱 Amazon EC2 API 參考資料。

每一筆事件或日誌項目都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 該請求是否使用根或使用者憑證提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 該請求是否由另一項 AWS 服務提出。

如需詳細資訊，請參閱 CloudTrail 使用者身分元素。

瞭解 AWS FIS 記錄檔項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。事件代表來自任何來源的單一請求，包括有關請求的操作，動作的日期和時間，請求參數等信息。 CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

以下是呼叫 AWS FIS `StopExperiment` 動作的範例 CloudTrail 記錄項目。

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AKIAIOSFODNN7EXAMPLE:jdoe",
    "arn": "arn:aws:sts::111122223333:assumed-role/example/jdoe",
    "accountId": "111122223333",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AKIAIOSFODNN7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/example",
        "accountId": "111122223333",
        "userName": "example"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2020-12-03T09:40:42Z",
        "mfaAuthenticated": "false"
```

```
      }
    }
  },
  "eventTime": "2020-12-03T09:44:20Z",
  "eventSource": "fis.amazonaws.com",
  "eventName": "StopExperiment",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.51.100.25",
  "userAgent": "Boto3/1.22.9 Python/3.8.13 Linux/5.4.186-113.361.amzn2int.x86_64
Botocore/1.25.9",
  "requestParameters": {
    "clientToken": "1234abc5-6def-789g-012h-ijklm34no56p",
    "experimentTemplateId": "ABCDE1fgHIJkLmNop",
    "tags": {}
  },
  "responseElements": {
    "experiment": {
      "actions": {
        "exampleAction1": {
          "actionId": "aws:ec2:stop-instances",
          "duration": "PT10M",
          "state": {
            "reason": "Initial state",
            "status": "pending"
          },
          "targets": {
            "Instances": "exampleTag1"
          }
        },
        "exampleAction2": {
          "actionId": "aws:ec2:stop-instances",
          "duration": "PT10M",
          "state": {
            "reason": "Initial state",
            "status": "pending"
          },
          "targets": {
            "Instances": "exampleTag2"
          }
        }
      },
      "creationTime": 1605788649.95,
      "endTime": 1606988660.846,
      "experimentTemplateId": "ABCDE1fgHIJkLmNop",
```

```
      "id": "ABCDE1fgHIJkLmNop",
      "roleArn": "arn:aws:iam::111122223333:role/AllowFISActions",
      "startTime": 1605788650.109,
      "state": {
        "reason": "Experiment stopped",
        "status": "stopping"
      },
      "stopConditions": [
        {
          "source": "aws:cloudwatch:alarm",
          "value": "arn:aws:cloudwatch:us-east-1:111122223333:alarm:example"
        }
      ],
      "tags": {},
      "targets": {
        "ExampleTag1": {
          "resourceTags": {
            "Example": "tag1"
          },
          "resourceType": "aws:ec2:instance",
          "selectionMode": "RANDOM(1)"
        },
        "ExampleTag2": {
          "resourceTags": {
            "Example": "tag2"
          },
          "resourceType": "aws:ec2:instance",
          "selectionMode": "RANDOM(1)"
        }
      }
    }
  },
  "requestID": "1abcd23e-f4gh-567j-klm8-9np01q234r56",
  "eventID": "1234a56b-c78d-9e0f-g1h2-34jk56m7n890",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "eventCategory": "Management"

}
```

以下是 API 動作的範例 CloudTrail 記錄項目，AWSFIS 作為實驗 (包括 aws:ssm:send-command AWS FIS 動作的一部分) 叫用。該userIdentity元素反映了使用假定角色獲得的臨時認證發出的請求。假定角色的名稱會顯示在中userName。實驗的識別碼, EXP21NT17WZA6dnugz, 出現在principalId並作為假定角色的 ARN 的一部分.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROATZZZ4JPIXUEXAMPLE:EXP21nT17WMzA6dnUgz",
        "arn": "arn:aws:sts::111122223333:assumed-role/AllowActions/
EXP21nT17WMzA6dnUgz",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROATZZZ4JPIXUEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/AllowActions",
                "accountId": "111122223333",
                "userName": "AllowActions"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-05-30T13:23:19Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "fis.amazonaws.com"
    },
    "eventTime": "2022-05-30T13:23:19Z",
    "eventSource": "ssm.amazonaws.com",
    "eventName": "ListCommands",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "fis.amazonaws.com",
    "userAgent": "fis.amazonaws.com",
    "requestParameters": {
        "commandId": "51dab97f-489b-41a8-a8a9-c9854955dc65"
    },
    "responseElements": null,
    "requestID": "23709ced-c19e-471a-9d95-cf1a06b50ee6",
    "eventID": "145fe5a6-e9d5-45cc-be25-b7923b950c83",
    "readOnly": true,
```

```
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

AWS 故障注入服務中的安全

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

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

- 雲端的安全性 — AWS 負責保護在 AWS 雲端中執行 AWS 服務的基礎架構。 AWS 還為您提供可以安全使用的服務。若要瞭解適用於 AWS 錯誤注入服務的相容性計畫，請參閱AWS 符合性計劃的合規計劃AWS服務範圍。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您瞭解如何在使用 AWS FIS 時套用共同的責任模型。下列主題說明如何設定 AWS FIS 以符合安全性與合規性目標。您也會學到如何使用其他可 AWS 協助您監控和保護 AWS FIS 資源的服務。

目錄

AWS 故障注入服務中的資料保護

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

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

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

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

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

靜態加密

AWS FIS 一律會加密您的靜態資料。 AWS FIS 中的資料會使用透明伺服器端加密進行靜態加密。這可協助降低保護敏感資料所涉及的操作負擔和複雜性。您可以透過靜態加密，建立符合加密合規和法規要求，而且對安全性要求甚高的應用程式。

傳輸中加密

AWS FIS 會加密服務與其他整合式 AWS 服務之間傳輸中的資料。 AWS FIS 與整合式服務之間傳遞的所有資料都會使用傳輸層安全性 (TLS) 加密。如需其他整合式 AWS 服務的詳細資訊，請參閱支援 AWS 服務。

AWS 故障注入服務的身分識別與存取管理

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

目錄

- 使用服務連結角色進行 AWS 錯誤注入服務
- AWSAWS 錯誤注入服務的受管理原則

物件

使用方式 AWS Identity and Access Management (IAM) 會根據您在 AWS FIS 中執行的工作而有所不同。

服務使用者 — 如果您使 AWS 用 FIS 服務執行工作，則管理員會為您提供所需的認證和權限。當您使用更多 AWS FIS 功能來完成工作時，您可能需要額外的權限。了解存取許可的管理方式可協助您向管理員請求正確的許可。

服務管理員 — 如果您負責公司的 AWS FIS 資源，您可能擁有 AWS FIS 的完整存取權。決定您的服務使用者應存取哪些 AWS FIS 功能和資源是您的工作。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。

IAM 管理員 — 如果您 AWS 是 IAM 管理員，可能需要瞭解如何撰寫政策來管理 FIS 存取權的詳細資訊。

使用身分驗證

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

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

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

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

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

AWS 帳戶 根使用者

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

聯合身分

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

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

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連線並同步到自己身分識別來源中的一組使用者和群組，以便在所有應用程式 AWS 帳戶 和應用程式中使用。如需 IAM Identity Center 的詳細資訊，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 使用者是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定許可。建議您盡可能依賴暫時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 IAM 使用者指南中的為需要長期憑證的使用案例定期輪換存取金鑰。

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

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

IAM 角色

IAM 角色是您 AWS 帳戶 內部具有特定許可的身分。它類似 IAM 使用者，但不與特定的人員相關聯。您可以切換角色，在中暫時擔任 IAM 角色。 AWS Management Console 您可以透過呼叫 AWS CLI

或 AWS API 作業或使用自訂 URL 來擔任角色。如需使用角色的方法詳細資訊，請參閱 IAM 使用者指南中的使用 IAM 角色。

使用暫時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 — 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。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。若要了解跨帳戶存取角色和以資源為基礎的政策之間的差異，請參閱 IAM 使用者指南中的 IAM 中的跨帳戶資源存取。
- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉寄存取工作階段 (FAS) — 當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。
  - 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務服務。
  - 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon EC2 上執行的應用程式 — 您可以使用 IAM 角色來管理在 EC2 執行個體上執行的應用程式以及發出 AWS CLI 或 AWS API 請求的臨時登入資料。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並提供給其所有應用程式，請建立連接至執行個體的執行個體設定檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得暫時憑證。如需詳細資訊，請參閱 IAM 使用者指南中的利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式。

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

使用政策管理存取權

您可以透 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS ，當與身分識別或資源相關聯時，會定義其權限。 AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以 JSON 文件的形式儲存在中。如需 JSON 政策文件結構和內容的詳細資訊，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哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

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

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

身分型政策

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

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

資源型政策

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

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

存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些主體 (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 和 Amazon VPC 是支援 ACL 的服務範例。 AWS WAF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原則類型。這些政策類型可設定較常見政策類型授予您的最大許可。

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

AWS 故障注入服務如何與 IAM 搭配使用

在您使用 IAM 管理 AWS FIS 的存取權限之前，請先了解哪些 IAM 功能可用於 AWS FIS。

可搭配 AWS 故障注入服務使用的 IAM 功能

IAM 功能	AWS FIS 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)	是
臨時憑證	是
主體許可	是
服務角色	是
服務連結角色	是

若要深入瞭解 AWS FIS 和其他 AWS 服務如何搭配大多數 IAM 功能運作，請參閱 IAM 使用者指南中的搭配 IAM 使用的AWS 服務。

FIS 的以身分識別為基礎的原則 AWS

支援身分型政策	是

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

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

FIS 的身分識別原則範例 AWS

若要檢視 AWS FIS 身分型原則的範例，請參閱。AWS 故障注入服務政策範例

FIS 內以資源為基礎的原則 AWS

支援以資源基礎的政策	否

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

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，作為資源型政策的主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主體和資源位於不同時 AWS 帳戶，受信任帳戶中的 IAM 管理員也必須授與主體實體 (使用者或角色) 權限，才能存取資源。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱 IAM 使用者指南中的 IAM 中的跨帳戶資源存取。

AWS FIS 的政策動作

支援政策動作	是

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

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

政策會使用動作來授予執行相關聯動作的許可。

若要查看 AWS FIS 動作清單，請參閱服務授權參考中的 AWS 錯誤注入服務所定義的動作。

AWS FIS 中的原則動作會在動作之前使用下列前置詞：

```
fis
```

如需在單一陳述式中指定多個動作，請用逗號分隔。

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

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

```
"Action": "fis:List*"
```

AWS 金融機構的政策資源

支援政策資源	是

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

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

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

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

某些 AWS FIS API 動作支援多種資源。若要在單一陳述式中指定多項資源，請使用逗號分隔 ARN。

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

```
]
```

若要查看 AWS FIS 資源類型及其 ARN 的清單，請參閱服務授權參考中的AWS 錯誤注入服務定義的資源類型。若要瞭解可以使用哪些動作指定每個資源的 ARN，請參閱AWS 錯誤注入服務定義的動作。

AWS FIS 的原則條件索引鍵

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哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

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

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

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

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

若要查看 AWS FIS 條件金鑰清單，請參閱服務授權參考中的 AWS 錯誤注入服務的條件金鑰。若要瞭解可以使用條件索引鍵的動作和資源，請參閱AWS 錯誤注入服務定義的動作。

若要檢視 AWS FIS 身分型原則的範例，請參閱。AWS 故障注入服務政策範例

金融資訊系統中的 AWS ACL

支援 ACL	否

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

ABAC 與 FIS AWS

支援 ABAC (政策中的標籤)	是

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

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

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

若要檢視以身分識別為基礎的原則範例，以根據該資源的標籤限制對資源的存取，請參閱。範例：使用標籤來控制資源使用

搭配 AWS FIS 使用臨時登入資料

支援臨時憑證	是

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

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

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

FIS 的 AWS 跨服務主體權限

支援轉寄存取工作階段 (FAS)	是

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

AWS FIS 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給 AWS 服務服務。

FIS 的 AWS 服務連結角色

支援服務連結角色	是

服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需有關建立或管理 AWS FIS 服務連結角色的詳細資訊，請參閱。使用服務連結角色進行 AWS 錯誤注入服務

AWS 故障注入服務政策範例

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

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

如需 AWS FIS 定義的動作和資源類型的詳細資訊，包括每個資源類型的 ARN 格式，請參閱服務授權參考中的AWS 錯誤注入服務的動作、資源和條件索引鍵。

目錄

政策最佳實務

以身分識別 AWS 為基礎的原則會決定某人是否可以在您的帳戶中建立、存取或刪除 FIS 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始授與使用者和工作負載的權限，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們可用在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低權限許可 – 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。您也可以使用條件來授與對服務動作的存取權 (如透過特定 AWS 服務) 使用 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，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。

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

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

範例：使用 AWS FIS 主控台

若要存取「 AWS 錯誤注入服務」主控台，您必須擁有最少一組權限。這些權限必須允許您 AWS 帳戶列出並檢視. AWS 如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

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

下列範例原則授與使用 FIS 主控台列出及檢視所 AWS 有 FI AWS S 資源的權限，但不允許建立、更新或刪除這些資源。它還授予檢視您可以在實驗範本中指定之所 AWS 有 FIS 動作所使用的可用資源的權限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "FISReadOnlyActions",
            "Effect": "Allow",
            "Action": [
                "fis:List*",
                "fis:Get*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AdditionalReadOnlyActions",
            "Effect": "Allow",
            "Action": [
                "ssm:Describe*",
                "ssm:Get*",
                "ssm:List*",
                "ec2:DescribeInstances",
                "rds:DescribeDBClusters",
                "ecs:DescribeClusters",
                "ecs:ListContainerInstances",
```

```
                "eks:DescribeNodegroup",
                "cloudwatch:DescribeAlarms",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PermissionsToCreateServiceLinkedRole",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "fis.amazonaws.com"
                }
            }
        }
    ]
}
```

範例：列出可用 AWS 的 FIS 動作

下列原則授與列出可用 AWS FIS 動作的權限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fis:ListActions"
            ],
            "Resource": "arn:aws:fis:*:*:action/*"
        }
    ]
}
```

範例：為特定動作建立實驗範本

下列政策授予建立動作實驗範本的權限`aws:ec2:stop-instances`。

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

```
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "fis:CreateExperimentTemplate"
      ],
      "Resource": [
        "arn:aws:fis:*:*:action/aws:ec2:stop-instances",
        "arn:aws:fis:*:*:experiment-template/*"
      ]
    },
    {
      "Sid": "PolicyPassRoleExample",
      "Effect": "Allow",
      "Action": [
          "iam:PassRole"
      ],
      "Resource": [
        "arn:aws:iam::account-id:role/role-name"
      ]
    }
  ]
}
```

範例：開始實驗

下列政策授予使用指定 IAM 角色和實驗範本開始實驗的權限。它也允許 AWS FIS 代表使用者建立服務連結角色。如需詳細資訊，請參閱 使用服務連結角色進行 AWS 錯誤注入服務。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "fis:StartExperiment"
      ],
      "Resource": [
        "arn:aws:fis:*:*:experiment-template/experiment-template-id",
        "arn:aws:fis:*:*:experiment/*"
      ]
```

```
    },
    {
        "Sid": "PolicyExampleforServiceLinkedRole",
        "Effect": "Allow",
        "Action": "iam:CreateServiceLinkedRole",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "iam:AWSServiceName": "fis.amazonaws.com"
            }
        }
    }
  ]
}
```

範例：使用標籤來控制資源使用

下列政策授予從具有標籤的實驗範本執行實驗的權限Purpose=Test。它不授予創建或修改實驗模板或使用沒有指定標籤的模板運行實驗的權限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "fis:StartExperiment",
            "Resource": "arn:aws:fis:*:*:experiment-template/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Purpose": "Test"
                }
            }
        }
    ]
}
```

範例：刪除具有特定標籤的實驗範本

以下策略授予刪除帶有標籤的實驗模板的權限Purpose=Test。

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

```
        {
            "Effect": "Allow",
            "Action": [
                "fis:DeleteExperimentTemplate"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Purpose": "Test"
                }
            }
        }
    ]
}
```

範例：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 使用者檢視連接到他們使用者身分的內嵌及受管政策。此原則包含在主控台上或以程式設計方式使用 AWS CLI 或 AWS API 完成此動作的權限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
```

```
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

範例：使用條件鍵 **ec2:InjectApiError**

下列範例原則使用ec2:FisTargetArns條件索引鍵來限定目標資源的範圍。此原則允許 AWS FIS 動作aws:ec2:api-insufficient-instance-capacity-error和aws:ec2:asg-insufficient-instance-capacity-error。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:InjectApiError",
            "Resource": "*",
            "Condition": {
                "ForAllValues:StringEquals": {
                    "ec2:FisActionId": [
                        "aws:ec2:api-insufficient-instance-capacity-error",
                    ],
                    "ec2:FisTargetArns": [
                        "arn:aws:iam:*:*:role:role-name"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:InjectApiError",
            "Resource": "*",
            "Condition": {
                "ForAllValues:StringEquals": {
                    "ec2:FisActionId": [
                        "aws:ec2:asg-insufficient-instance-capacity-error"
                    ],
```

```
                    "ec2:FisTargetArns": [

 "arn:aws:autoscaling:*:*:autoScalingGroup:uuid:autoScalingGroupName/asg-name"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "autoscaling:DescribeAutoScalingGroups",
            "Resource": "*"
        }
    ]
}
```

範例：使用條件鍵 aws:s3:bucket-pause-replication

下列範例原則會使用S3:IsReplicationPauseRequest條件索引鍵來允許PutReplicationConfiguration且GetReplicationConfiguration僅在 AWS FIS 動作環境中由 AWS FIS 使用時。aws:s3:bucket-pause-replication

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "S3:PauseReplication"
            ],
            "Resource": "arn:aws:s3:::mybucket",
            "Condition": {
                "StringEquals": {
                    "s3:DestinationRegion": "region"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "S3:PutReplicationConfiguration",
                "S3:GetReplicationConfiguration"
            ],
            "Resource": "arn:aws:s3:::mybucket",
```

```
            "Condition": {
                "BoolIfExists": {
                    "s3:IsReplicationPauseRequest": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "S3:ListBucket"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        }
    ]
    }
```

使用服務連結角色進行 AWS 錯誤注入服務

AWS 故障注入服務使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至 AWS FIS 的唯一 IAM 角色類型。服務連結角色由 AWS FIS 預先定義，並包含服務代表您呼叫其他 AWS 服務所需的所有權限。

服務連結角色可讓設定 AWS FIS 更容易，因為您不必手動新增必要的權限來管理實驗的監視和資源選擇。 AWS FIS 會定義其服務連結角色的權限，除非另有定義，否則只有 AWS FIS 可以擔任其角色。定義的許可包括信任政策和許可政策，且該許可政策無法附加至其他 IAM 實體。

除了服務連結角色之外，您還必須指定 IAM 角色，以授予修改您在實驗範本中指定為目標的資源的權限。如需詳細資訊，請參閱 適用於 AWS FIS 實驗的 IAM 角色。

您必須先刪除相關的 資源，才能刪除服務連結角色。這樣可以保護您 AWS 的 FIS 資源，因為您無法不小心移除存取資源的權限。

FIS 的 AWS 服務連結角色權限

AWS FIS 使用名為的服務連結角色AWSServiceRoleForFIS來管理實驗的監視和資源選擇。

服AWSServiceRoleForFIS務連結角色會信任下列服務擔任該角色：

- fis.amazonaws.com

AWSServiceRoleForFIS服務連結角色使用受管政策 AmazonFI ServiceRole S 政策。此原則可讓 AWS FIS 管理實驗的監控和資源選擇。如需詳細資訊，請參閱AWS 受管政策參考中的 AmazonFIS ServiceRole 政策。

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。若要成功建立AWSServiceRoleForFIS服務連結角色，與 AWS FIS 搭配使用的 IAM 身分必須具有必要的許可。若要授予必要許可，請將下列政策連接至 IAM 身分。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "fis.amazonaws.com"
                }
            }
        }
    ]
}
```

如需詳細資訊，請參閱 IAM 使用者指南中的服務連結角色許可。

建立 FIS 的 AWS 服務連結角色

您不需要手動建立一個服務連結角色。當您在 AWS Management Console、或 AWS API 中開始 AWS FIS 實驗時 AWS CLI， AWS FIS 會為您建立服務連結角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您開始 FIS 實驗時 AWS ， AWS FIS 會再次為您建立服務連結角色。

編輯 FIS 的服務連結角色 AWS

AWS FIS 不允許您編輯AWSServiceRoleForFIS服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱 IAM 使用者指南中的編輯服務連結角色。

刪除 FIS 的服務連結角色 AWS

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。然而，在手動刪除服務連結角色之前，您必須先清除資源。

> **Note**
>
> 如果 AWS FIS 服務在您嘗試清理資源時正在使用此角色，則清除可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

若要清除所使用的 AWS FIS 資源 AWSServiceRoleForFIS

請確定目前沒有任何實驗正在執行中。如有必要，請停止實驗。如需詳細資訊，請參閱 停止實驗。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台或 AWS API 刪除AWSServiceRoleForFIS服務連結角色。 AWS CLI如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

AWS FIS 服務連結角色的支援區域

AWS FIS 支援在所有提供服務的區域中使用服務連結角色。如需詳細資訊，請參閱AWS 錯誤注入服務端點和配額。

AWSAWS 錯誤注入服務的受管理原則

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

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

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

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

AWS 管理策略：亞馬遜 FIS ServiceRole 政策

此原則會附加至名為的服務連結角色，AWSServiceRoleForFIS以允許 AWS FIS 管理實驗的監視和資源選擇。如需詳細資訊，請參閱 使用服務連結角色進行 AWS 錯誤注入服務。

AWS 受管理的策略： AWSFaultInjectionSimulatorEC2Access

在實驗角色中使用此政策可授予 AWS FIS 許可，以執行使用適用於 Amazon EC2 的AWS FIS 動作的實驗。如需詳細資訊，請參閱 the section called “實驗角色”。

若要檢視此原則的權限，請參閱AWS 受管理AWSFaultInjectionSimulatorEC2Access的策略參考中的。

AWS 受管理的策略： AWSFaultInjectionSimulatorECSAccess

在實驗角色中使用此政策可授予 AWS FIS 許可，以執行使用適用於 Amazon EC AWS S 的 FIS 動作的實驗。如需詳細資訊，請參閱 the section called “實驗角色”。

若要檢視此原則的權限，請參閱AWS 受管理AWSFaultInjectionSimulatorECSAccess的策略參考中的。

AWS 受管理的策略： AWSFaultInjectionSimulatorEKSAccess

在實驗角色中使用此政策可授予 AWS FIS 許可，以執行使用適用於 Amazon EKS 的AWS FIS 動作的實驗。如需詳細資訊，請參閱 the section called “實驗角色”。

若要檢視此原則的權限，請參閱AWS 受管理AWSFaultInjectionSimulatorEKSAccess的策略參考中的。

AWS 受管理的策略： AWSFaultInjectionSimulatorNetworkAccess

在實驗角色中使用此原則可授予 AWS FIS 權限，以執行使用 AWS FIS 網路動作的實驗。如需詳細資訊，請參閱 the section called “實驗角色”。

若要檢視此原則的權限，請參閱AWS 受管理AWSFaultInjectionSimulatorNetworkAccess的策略參考中的。

AWS 受管理的策略： AWSFaultInjectionSimulatorRDSAccess

在實驗角色中使用此政策可授予 AWS FIS 許可，以執行使用適用於 Amazon RDS 的AWS FIS 動作的實驗的實驗。如需詳細資訊，請參閱 the section called “實驗角色”。

若要檢視此原則的權限，請參閱AWS 受管理AWSFaultInjectionSimulatorRDSAccess的策略參考中的。

AWS 受管理的策略： AWSFaultInjectionSimulatorSSMAccess

在實驗角色中使用此原則可授予 AWS FIS 權限，以執行使用「Systems Manager」AWS FIS 動作的實驗。如需詳細資訊，請參閱 the section called “實驗角色”。

若要檢視此原則的權限，請參閱AWS 受管理AWSFaultInjectionSimulatorSSMAccess的策略參考中的。

AWSAWS 受管理原則的 FIS 更新

檢視由於此服務開始追蹤這些變更以來， AWS FIS 的 AWS 受管理原則更新詳細資料。

變更	描述	日期
AWSFaultInjectionSimulatorECSAccess – 更新現有政策	新增允許 AWS FIS 解析 ECS 目標的權限。	2024年1月25日
AWSFaultInjectionSimulatorNetworkAccess – 更新現有政策	新增允許 AWS FIS 使用aws:network:route-table-disrupt-cross-region-connectivity和aws:network:transit-gateway-disrupt-cross-region-connectivity動作執行實驗的權限。	2024年1月25日
AWSFaultInjectionSimulatorEC2Access – 更新現有政策	新增許可以允許 AWS FIS 解析 EC2 執行個體。	2023 年 11 月 13 日
AWSFaultInjectionSimulatorEKSAccess – 更新現有政策	新增允許 AWS FIS 解析 EKS 目標的權限。	2023 年 11 月 13 日
AWSFaultInjectionSimulatorRDSAccess – 更新現有政策	已新增允許 AWS FIS 解析 RDS 目標的權限。	2023 年 11 月 13 日
AWSFaultInjectionSimulatorEC2Access – 更新現有政策	新增許可，允許 AWS FIS 在 EC2 執行個體上執行 SSM 文件並終止 EC2 執行個體。	2023 年 6 月 2 日

變更	描述	日期
AWSFaultInjectionSimulatorSSMAccess – 更新現有政策	已新增許可，以允許 AWS FIS 在 EC2 執行個體上執行 SSM 文件。	2023 年 6 月 2 日
AWSFaultInjectionSimulatorECSAccess – 更新現有政策	新增允許 AWS FIS 使用新aws:ecs:task動作執行實驗的權限。	2023 年 6 月 1 日
AWSFaultInjectionSimulatorEKSAccess – 更新現有政策	新增允許 AWS FIS 使用新aws:eks:pod動作執行實驗的權限。	2023 年 6 月 1 日
AWSFaultInjectionSimulatorEC2Access – 新政策	已新增政策，允許 AWS FIS 執行針對 Amazon EC2 使用 AWS FIS 動作的實驗。	2022 年 10 月 26 日
AWSFaultInjectionSimulatorECSAccess – 新政策	已新增政策，允許 AWS FIS 執行針對 Amazon EC AWS S 使用 FIS 動作的實驗。	2022 年 10 月 26 日
AWSFaultInjectionSimulatorEKSAccess – 新政策	新增政策允許 AWS FIS 執行針對 Amazon EKS 使用 AWS FIS 動作的實驗。	2022 年 10 月 26 日
AWSFaultInjectionSimulatorNetworkAccess – 新政策	已新增原則，允許 AWS FIS 執行使用 AWS FIS 網路動作的實驗。	2022 年 10 月 26 日
AWSFaultInjectionSimulatorRDSAccess – 新政策	已新增政策，允許 AWS FIS 執行針對 Amazon RDS 使用 AWS FIS 動作的實驗。	2022 年 10 月 26 日
AWSFaultInjectionSimulatorSSMAccess – 新政策	已新增原則，允許 AWS FIS 執行對 Systems Manager 使用 AWS FIS 動作的實驗。	2022 年 10 月 26 日
亞馬遜 FIS ServiceRole 政策 — 更新現有政策	已新增允許 AWS FIS 描述子網路的權限。	2022 年 10 月 26 日
亞馬遜 FIS ServiceRole 政策 — 更新現有政策	已新增允許 AWS FIS 描述 EKS 叢集的權限。	2022 年 7 月 7 日

變更	描述	日期
亞馬遜 FIS ServiceRole 政策 — 更新現有政策	已新增權限，以允許 AWS FIS 列出和描述叢集中的工作。	2022 年 2 月 7 日
亞馬遜 FIS ServiceRole 政策 — 更新現有政策	移除`events:DescribeRule` 動作的`events:ManagedBy` 條件。	2022 年 1 月 6 日
亞馬遜 FIS ServiceRole 政策 — 更新現有政策	新增權限以允許 AWS FIS 擷取停止條件中使用之 CloudWatch 警示的歷史記錄。	2021 年 6 月 30 日
AWS FIS 開始追蹤變更	AWS FIS 開始追蹤其 AWS 受管理原則的變更	2021 年 3 月 1 日

AWS 故障注入服務的基礎設施安全

作為託管服務， AWS 故障注入服務受到 AWS 全球網絡安全性的保護。有關 AWS 安全服務以及如何 AWS 保護基礎架構的詳細資訊，請參閱AWS 雲端安全 若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全性支柱架構良 AWS 好的架構中的基礎結構保護。

您可以使用 AWS 已發佈的 API 呼叫透過網路存取 AWS FIS。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

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

使用介面 VPC 端點存取 AWS FIS ()AWS PrivateLink

您可以建立介面 VPC 端點，在 VPC 和 AWS 錯誤注入服務之間建立私人連線。VPC 端點採用這項技術 AWS PrivateLink，可讓您在沒有網際網路閘道、NAT 裝置、VPN 連線或 AWS 直 Connect 連線的情況下私密存取 AWS FIS API。VPC 中的執行個體不需要公用 IP 位址即可與 AWS FIS API 進行通訊。

每個介面端點都由子網路中的一個或多個彈性網路介面表示。

如需詳細資訊，請參閱AWS PrivateLink 指南 AWS PrivateLink中的 AWS 服務 透過存取。

AWS FIS 虛擬私人雲端端點的注意事項

在為 AWS FIS 設定介面 VPC 端點之前，請參閱指南中的AWS 服務 使用介面 VPC 端點存取。AWS PrivateLink

AWS FIS 支援從您的 VPC 呼叫其所有 API 動作。

建立 FIS 的 AWS 介面 VPC 人雲端端點

您可以使用 Amazon VPC 主控台或 () AWS 為 FIS 服務建立 VPC 端點。 AWS Command Line Interface AWS CLI如需詳細資訊，請參閱《AWS PrivateLink 指南》中的建立 VPC 端點。

使用下列服務名稱建立 AWS FIS 的 VPC 端點：`com.amazonaws.region.fis`

如果您為端點啟用私有 DNS，則可以使用該區域的預設 DNS 名稱向 AWS FIS 發出 API 要求，例如，`fis.us-east-1.amazonaws.com`。

建立 FIS 的 VPC 私人雲端端點原則 AWS

您可以將端點策略附加到控制 AWS FIS 存取的 VPC 端點。此政策會指定下列資訊：

- 可執行動作的主體。
- 可執行的動作。
- 可供執行動作的資源。

如需詳細資訊，請參閱AWS PrivateLink 指南中的使用端點策略控制對 VPC 端點的存取。

範例：特定 AWS FIS 動作的 VPC 端點原則

下列 VPC 端點策略會將所有資源上列出 AWS FIS 動作的存取權授與所有主體。

```
{
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "fis:ListExperimentTemplates",
            "fis:StartExperiment",
```

```
            "fis:StopExperiment",
            "fis:GetExperiment"
         ],
         "Resource":"*",
         "Principal":"*"
      }
   ]
}
```

範例：拒絕從特定存取的 VPC 端點原則 AWS 帳戶

下列 VPC 端點策略會拒絕指定 AWS 帳戶 存取所有動作和資源，但授與所有其他所有動作和資源的 AWS 帳戶 存取權。

```
{
   "Statement":[
      {
         "Effect": "Allow",
         "Action": "*",
         "Resource": "*",
         "Principal": "*"
      },
      {
         "Effect":"Deny",
         "Action": "*",
         "Resource": "*",
         "Principal": {
           "AWS": [ "123456789012" ]
         }
      }
   ]
}
```

標記您的 AWS FIS 資源

標籤是您或 AWS 指派給 AWS 資源的中繼資料標籤。每個標籤皆包含鍵與值。對於您指派的標籤，您可以定義索引鍵與值。例如，您可以將鍵定義為，purpose並將值定義test為資源。

標籤可協助您執行以下操作：

- 識別和組織您的 AWS 資源。許多 AWS 服務支援標記，因此您可以對來自不同服務的資源指派相同的標籤，指出資源是相關的。
- 控制對 AWS 資源的存取。如需詳細資訊，請參閱《IAM 使用者指南》中的使用標籤控制存取權限。

標記限制

下列基本限制適用於 AWS FIS 資源的標籤：

- 可指派給資源的標籤數目上限：50
- 索引鍵長度上限：128 個 Unicode 字元
- 數值長度上限：256 個 Unicode 字元
- 索引鍵和值的有效字元：a-z、A-Z、0-9、空格及下列字元：_.:/= +-和 @
- 鍵和值會區分大小寫
- 您不能用aws:作密鑰的前綴，因為它保留供AWS使用

使用標籤

下列AWS故障注入服務 (AWSFIS) 資源支援標記：

- 動作
- Experiments
- 实验模板

您可以使用控制台來處理實驗和實驗模板的標籤。如需詳細資訊，請參閱下列內容：

- 標記實驗
- 標籤實驗模板

您可以使用下列AWS CLI指令來處理動作、實驗和實驗範本的標籤：

- 標籤資源 — 將標籤新增至資源。
- 取消標記資源 — 從資源中移除標籤。
- list-tags-for-resource— 列出特定資源的標籤。

AWS 故障注入服務的配額和限制

您的每項 AWS 服務都 AWS 帳戶 有預設配額 (先前稱為限制)。除非另有說明，否則每個配額都是區域特定規定。您可以要求提高某些配額，但並非所有配額都能提高。

若要檢視 AWS FIS 的配額，請開啟 Service Quotas 主控台。在瀏覽窗格中，選擇AWS 服務，然後選取AWS 錯誤注入服務。

若要請求提高配額，請參閱《Service Quotas 使用者指南》中的請求提高配額。

您 AWS 帳戶 有下列與 AWS FIS 相關的配額。

名稱	預設	可調整	描述
以小時為單位的動作	每個支持地區：12	否	在目前「區域」中，允許在此帳戶中執行一項動作的時數上限。
每個實驗模板的操作	每個受支援的區域：20	否	在當前區域中，您可以在此帳戶的實驗模板中創建的最大操作數。
活动实验	每個受支援的區域：5	否	您可以在目前「區域」的此帳戶中同時執行的最大使用中實驗數目。
在幾天內完成實驗數據保留	每個支持地區：120	否	AWS FIS 允許的最大天數保留目前「區域」中此帳戶中已完成實驗的相關資料。
以小時為單位的實驗	每個支持地區：12	否	在目前區域中，允許在此帳戶中執行一項實驗的最大時數。

名稱	預設	可調整	描述
实验模板	每個受支援的區域：500	否	您可以在當前區域中在此帳戶中創建的實驗模板的最大數量。
aws 中的受管理前置詞清單數目上限:網路:路由表中斷-跨區域連線	每個受支援的區域：15	否	AWS: net: 路由表-disrupt-cross-region-connectivity 每個動作允許的受管理前綴清單數目上限。
AWS 中路由表的數目上限:網路:路由表中斷-跨區域連線	每個受支援的區域：10	否	AWS：網絡：路由表-disrupt-cross-region-connectivity 允許的最大數量的路由表，每個動作。
AWS 中的路由數目上限:網路:路由表中斷-跨區域連線	每個受支援的區域：200	否	aw:net: 路由表-disrupt-cross-region-connectivity 允許的最大路由數量, 每個動作.
每個實驗的平行動作	每個受支援的區域：10	否	在當前區域中，您可以在此帳戶的實驗中 parallel 運行的最大操作數。
每個實驗模板的停止條件	每個受支援的區域：5	否	您可以在當前區域中此帳戶中添加到實驗模板中的最大停止條件數。
aw:ec2: asg-執行個體不足-容量錯誤的目標 Auto Scaling 群組	每個受支援的區域：5	是	每個實驗使用標籤識別目標時，aw: ec2: asg-insufficient-instance-capacity-error 可以定位的 Auto Scaling 群組數目上限。

名稱	預設	可調整	描述
aws 的目標儲存貯體:S3: 暫停-暫停複寫	每個受支援的區域：20	是	aw:s3: 在您使用標籤識別目標時，每個實驗bucket-pause-replication 可以鎖定的 S3 儲存貯體數目上限。
AWS 的目標叢集:EC: 排水容器執行個體	每個受支援的區域：5	是	當您使用標籤，每個實驗識別目標時，aw:ecs: drain-container-instances 可以定位的叢集數目上限。
aws 的目標叢集:RS: 容錯移轉-DB 叢集	每個受支援的區域：5	是	當您使用標籤，每個實驗識別目標時，aw:rds: failover-db-cluster 可以鎖定叢集的最大數目。
aws 的目標資料庫例證:RS: 重新啟動 db 例證	每個受支援的區域：5	是	當您使用標籤，每個實驗識別目標時，aw:rds: reboot-db-instances 可以定位的 DbInstance 的最大數目。
aw: ec2: 重新啟動執行個體的目標執行個體	每個受支援的區域：5	是	當您每個實驗使用標籤識別目標時，aw:ec2：重新啟動實例可以定位的最大實例數。
aw: ec2: 停止執行個體的目標執行個體	每個受支援的區域：5	是	當您使用標記識別每個實驗的目標時，aw: ec2: stop-instance 可以鎖定的執行個體數目上限。

名稱	預設	可調整	描述
aw: ec2: 終止執行個體的目標執行個體	每個受支援的區域：5	是	當您使用每個實驗使用標籤識別目標時，aw: ec2: 終止執行個體可以鎖定的最大執行個體數目。
AWS 的目標執行個體:SSM: 傳送指令	每個受支援的區域：5	是	當您每個實驗使用標籤識別目標時，aw: ssm: ssm: send-command 可以鎖定的最大實例數。
aws 的目標節點群組:EK: 終止節點群組執行個體	每個受支援的區域：5	是	每個實驗使用標籤識別目標時，aw:eks: terminate-nodegroup-instances 可以定位的節點群組數目上限。
Aw 的目標網繭:EK: POD-CPU stress	每個受支援的區域：50	是	當您每個實驗使用參數識別目標時，aw:eks: pod-cpu-stress 可以鎖定的網繭數目上限。
Aw 的目標網繭:EK: POD-刪除	每個受支援的區域：50	是	當您每個實驗使用參數識別目標時，aw:ek: Pod-刪除可以鎖定的網繭數目上限。
適用於 Aw 的目標網繭：EK：POD-IO stress	每個受支援的區域：50	是	當您每個實驗使用參數識別目標時，aw:eks: pod-io-stress 可以鎖定的網繭數目上限。

名稱	預設	可調整	描述
針對 Aw 的目標 Pod：EK：POD 記憶體 stress	每個受支援的區域：50	是	當您每個實驗使用參數識別目標時，aw:eks: pod-memory-stress 可以鎖定的網繭數目上限。
Aw 的目標網繭:EK: POD-網路-黑洞連接埠	每個受支援的區域：50	是	當您每個實驗使用參數識別目標時，aw:eks: pod-network-blackhole-port 可以鎖定的網繭數目上限。
適用於 Aw 的目標網繭:Ek: POD-網路延遲	每個受支援的區域：50	是	當您每個實驗使用參數識別目標時，aw:eks: pod-network-latency 可以鎖定的網繭數目上限。
Aw 的目標網繭：EK：網路封包遺失	每個受支援的區域：50	是	當您每個實驗使用參數識別目標時，aw:eks: pod-network-packet-loss 可以鎖定的網繭數目上限。
aws ReplicationGroups 的目標:彈性:中斷叢集-AZ-功率	每個受支援的區域：5	是	ReplicationGroups 該 aws 的最大數量：elasticache：interrupt-cluster-az-power 可以在每個實驗使用標籤/參數識別目標時定位。
aws SpotInstances 的目標：ec2：發送點實例中斷	每個受支援的區域：5	是	當您使用標籤識別目標時， SpotInstances 該 aw:ec2: send-spot-instance-interruptions 可以定位的最大數量，每個實驗。

名稱	預設	可調整	描述
AWS 的目標子網路:網路:中斷連線	每個受支援的區域：5	是	當您每個實驗使用標籤識別目標時，aw: network: 中斷連線可以鎖定的子網路數目上限。5 以上的配額僅適用於參數範圍：all。如果其他範圍類型需要更高的配額，請透過 https://console.aws.amazon.com/support/home#/ 聯絡客戶支援。
AWS 的目標子網路:網路:路由表中斷-跨區域連線	每個受支援的區域：6	是	當您每個實驗使用標籤識別目標時，aw:network: network-table-disrupt-cross-region-connectivity 可以鎖定的子網路數目上限。
Aw 的目標工作:EC: 停止工作	每個受支援的區域：5	是	當您使用標籤，每個實驗識別目標時，可以針對的任務提出：EC：stop-任務的最大數量。
Aw 的目標工作:EC: 工作 CPU stress	每個受支援的區域：5	是	當您使用標籤/參數，每個實驗識別目標時，aw:ecs: task-cpu-stress 可以定位的最大任務數量。
Aw 的目標工作:EC: 作業-IO stress	每個受支援的區域：5	是	當您使用標籤/參數，每個實驗識別目標時，aw:ecs: task-io-stress 可以定位的最大任務數量。

名稱	預設	可調整	描述
Aw 的目標工作:EC: 工作殺死程序	每個受支援的區域：5	是	當您使用標籤/參數，每個實驗識別目標時，aw:ecs:task-kill-process 可以定位的最大任務數量。
Aw 的目標工作:EC: 工作網路-黑洞連接埠	每個受支援的區域：5	是	當您使用標籤/參數，每個實驗識別目標時，aw:ecs:task-network-blackhole-port 可以定位的最大任務數量。
Aw 的目標工作:EC: 工作網路延遲	每個受支援的區域：5	是	當您使用標籤/參數，每個實驗識別目標時，aw:ecs:task-network-latency 可以定位的最大任務數量。
aws 的目標工作:EC: 工作-網路封包遺失	每個受支援的區域：5	是	當您使用標籤/參數，每個實驗識別目標時，aw:ecs:task-network-packet-loss 可以定位的最大任務數量。
AWS TransitGateways 的目標:網路:傳輸閘道中斷的跨區域連線	每個受支援的區域：5	是	當您使用每個實驗使用標籤識別目標時，aws:網路:Transit-Gateway-disrupt-cross-region-connectivity 可以鎖定的傳輸閘道數目上限。
每個實驗模板的目標帳戶配置	每個受支援的區域：10	是	在目前區域中，您可以為此帳戶中的實驗範本建立的目標帳戶設定數目上限。

名稱	預設	可調整	描述
AWS 的目標資料表:動作 global-table-pause-replication	每個受支援的區域：5	是	在每個實驗中，aw: dynamodb: global-table-pause-replication 可以定位的全局表的最大數量。

您對 AWS FIS 的使用受到以下額外限制：

名稱	限制
`aws:elasticache:interrupt-cluster-az-power` 行動的目標	每個區域每天每個帳戶限制為 10 個`aws:elasticache:redis-replicationgroup` 叢集受損。您可以透過在 AWS 支援中心主控台建立 Support 案例來要求提高申請。

文件歷史紀錄

下表說明「AWS 故障注入服務使用者指南」中的重要文件更新。

變更	描述	日期
新動作	您現在可以使用此aws:dynamodb:global-table-pause-replication 動作來暫停目標全域表格及其複本表格之間的資料複製。將不再支援該aws:dynamodb:encrypted-global-table-pause-replication 動作。	2024年4月24日
新動作模式實驗選項	您可以將動作模式設定為，以skip-all便在執行實驗之前產生目標預覽。	2024年3月13日
AWS 受管理策略更新	AWS FIS 更新了現有的受管理策略。	2024年1月25日
新案例和動作	您現在可以使用 AWS FIS 案例跨區域：連線能力和 AZ 可用性：電源中斷。	2023 年 11 月 30 日
新動作	您現在可以使用aws:ec2:asg-insufficient-instance-capacity-error動作。	2023 年 11 月 30 日
新動作	您現在可以使用aws:ec2:api-insufficient-instance-capacity-error動作。	2023 年 11 月 30 日
新動作	您現在可以使用aws:network:route-table-disrupt-cross-region-connectivity動作。	2023 年 11 月 30 日

新動作	您現在可以使用aws:network:transit-gateway-disrupt-cross-region-connectivity動作。	2023 年 11 月 30 日
新動作	您現在可以使用aws:dynamodb:encrypted-global-table-pause-replication動作。	2023 年 11 月 30 日
新動作	您現在可以使用aws:s3:bucket-pause-replication動作。	2023 年 11 月 30 日
新動作	您現在可以使用aws:elasticache:interrupt-cluster-az-power動作。	2023 年 11 月 30 日
新的實驗選項	您現在可以使用 AWS FIS 實驗選項來指定帳戶和空白目標解析度。	2023 年 11 月 27 日
AWS 金融機構的名稱變更	將服務名稱更新為 AWS 錯誤注入服務。	2023 年 11 月 15 日
AWS 受管理策略更新	AWS FIS 更新了現有的受管理策略。	2023 年 11 月 13 日
新的案例程式庫	您現在可以使用 AWS FIS 案例程式庫功能。	2023 年 11 月 7 日
新的實驗排程器	您現在可以使用 AWS FIS 實驗排程器功能。	2023 年 11 月 7 日
AWS 受管理策略更新	AWS FIS 更新了現有的受管理策略。	2023 年 6 月 2 日
新動作	您可以使用新的aws:ecs:task和aws:eks:pod動作。	2023 年 6 月 1 日

AWS 受管理策略更新	AWS FIS 更新了現有的受管理策略。	2023 年 6 月 1 日
新的預先設定 SSM 文件	您可以使用下列預先設定的 SSM 文件： AWSFIS-執行磁碟填入。	2023 年 4 月 28 日
新動作	您可以使用此aws:ebs:pause-volume-io動作來暫停目標磁碟區及其所連接的執行個體之間的 I/O。	2023 年 1 月 27 日
新動作	您可以使用此aws:network:disrupt-connectivity動作來拒絕目標子網路的特定流量類型。	2022 年 10 月 26 日
新動作	您可以使用此aws:eks:inject-kubernetes-custom-resource動作在單一目標叢集上執行 ChaosMesh 或石蕊實驗。	2022 年 7 月 7 日
實驗記錄	您可以設定實驗範本，將實驗活動日誌傳送到 CloudWatch 日誌或 S3 儲存貯體。	2022 年 2 月 28 日
新通知	當實驗狀態改變時， AWS FIS 會發出通知。這些通知會以活動形式透過 Amazon 提供 EventBridge。	2022 年 2 月 24 日
新動作	您可以使用動aws:ecs:stop-task作來停止指定的工作。	2022 年 2 月 9 日
新動作	您可以使用此aws:cloudwatch:assert-alarm-state動作來驗證指定的警示是否處於其中一個指定的警示狀態。	2021 年 11 月 5 日

新的預先設定 SSM 文件	您可以使用下列預先設定的 SSM 文件： AWSFIS-執行 IOO 壓力、執行網路-黑洞連接埠、執行網路延遲來源、執行網路封包遺失和執行網路封包遺 AWSFIS失來源。 AWSFIS AWSFIS AWSFIS	2021 年 11 月 4 日
新動作	您可以使用此aws:ec2:send-spot-instance-interruptions動作傳送 Spot 執行個體中斷通知給目標 Spot 執行個體，然後中斷目標 Spot 執行個體。	2021 年 10 月 20 日
新動作	您可以使用aws:ssm:start-automation-execution動作來啟動自動化工作流程簿的執行。	2021 年 9 月 17 日
初始版本	AWS 故障注入服務用戶指南的初始版本。	2021 年 3 月 15 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。