



Hooks 使用者指南

AWS CloudFormation



AWS CloudFormation: Hooks 使用者指南

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

什麼是 AWS CloudFormation 勾點？	1
建立和管理勾點	2
概念	3
勾點	3
失敗模式	4
勾點目標	4
目標動作	4
勾點處理常式	5
Guard Hook	5
AWS CLI 使用 Guard Hooks 的 命令	6
勾點的寫入保護規則	6
準備建立 Guard Hook	19
啟用 Guard Hook	21
檢視 Guard Hooks 的日誌	25
刪除 Guard Hook	26
Lambda 勾點	27
AWS CLI 使用 Lambda Hooks 的 命令	27
為勾點建立 Lambda 函數	28
準備建立 Lambda Hook	47
啟用 Lambda 勾點	48
檢視 Lambda Hooks 的日誌	51
刪除 Lambda 勾點	52
自訂勾點	53
必要條件	54
啟動勾點專案	56
建模勾點	59
註冊勾點	126
測試勾點	130
更新勾點	139
取消註冊勾點	139
發佈勾點	140
結構描述語法	147
停用啟用勾點	156
停用和啟用勾點（主控台）	156

停用和啟用勾點 (AWS CLI)	157
組態結構描述	158
勾點組態結構描述屬性	158
勾點組態範例	159
堆疊層級篩選條件	160
FilteringCriteria	161
StackNames	161
StackRoles	162
Include 和 Exclude	162
堆疊層級篩選條件的範例	163
目標篩選條件	167
目標篩選條件的範例	168
使用萬用字元	170
使用 CloudFormation 範本建立勾點	173
文件歷史紀錄	175
.....	clxxvii

什麼是 AWS CloudFormation 勾點？

AWS CloudFormation 勾點是一項功能，可用來確保 CloudFormation 資源、堆疊、變更集符合組織的安全性、營運和成本最佳化最佳實務。CloudFormation Hooks 也可以確保與您的 AWS Cloud Control API 資源具有相同程度的合規。使用 CloudFormation Hooks，您可以提供程式碼，在佈建之前主動檢查 AWS 資源的組態。如果找到不合規的資源，AWS CloudFormation 會失敗操作並防止佈建資源，或發出警告並允許佈建操作繼續。

您可以使用勾點來強制執行各種需求和指導方針。例如，與安全相關的勾點可以驗證安全群組是否適用於 [Amazon Virtual Private Cloud \(Amazon VPC\)](#) 的傳入和傳出流量規則。成本相關的勾點可以限制開發環境只使用較小的 [Amazon Elastic Compute Cloud \(Amazon EC2\)](#) 執行個體類型。專為資料可用性而設計的勾點可以強制執行 [Amazon Relational Database Service \(Amazon RDS\)](#) 的自動備份。

CloudFormation Hooks 是 [AWS CloudFormation 登錄檔](#) 中支援的延伸類型。登錄檔可讓您輕鬆公開和私下分發和啟用勾點。您可以使用預先建置的勾點，或使用 [CloudFormation CLI](#) 建置自己的勾點。

本指南提供 AWS CloudFormation 勾點結構的概觀，以及開發、註冊、測試、管理和發佈您自己的勾點的指南。

建立和管理 AWS CloudFormation 勾點

AWS CloudFormation 勾點提供機制，在允許堆疊建立、修改或刪除之前評估 CloudFormation 資源。此功能可協助您確保 CloudFormation 資源符合組織的安全性、營運和成本最佳化最佳實務。

若要建立勾點，您有三個選項。

- Guard Hook – 使用 AWS CloudFormation Guard 規則評估資源。
- Lambda Hook – 將資源評估的請求轉送至 AWS Lambda 函數。
- Custom Hook – 使用您手動開發的自訂 Hook 處理常式。

Guard Hook

若要建立 Guard Hook，請依照這些主要步驟進行：

1. 使用 Guard 網域特定語言 (DSL)，將資源評估邏輯撰寫為 Guard 政策規則。
2. 將 Guard 政策規則存放在 Amazon S3 儲存貯體中。
3. 導覽至 CloudFormation 主控台並開始建立 Guard Hook。
4. 提供您的 Guard 規則的 Amazon S3 路徑。
5. 選擇 Hook 將評估的特定目標。
6. 選擇將調用勾點的部署動作（建立、更新、刪除）。
7. 選擇 Hook 在評估失敗時如何回應。
8. 組態完成後，請啟用勾點以開始強制執行。

Lambda Hook

若要建立 Lambda 勾點，請遵循這些主要步驟：

1. 將資源評估邏輯寫入 Lambda 函數。
2. 導覽至 CloudFormation 主控台，並開始建立 Lambda Hook。
3. 為您的 Lambda 函數提供 Amazon Resource Name (ARN)。
4. 選擇 Hook 將評估的特定目標。
5. 選擇將調用勾點的部署動作（建立、更新、刪除）。
6. 選擇 Hook 在評估失敗時如何回應。
7. 組態完成後，請啟用勾點以開始強制執行。

Custom Hook

Custom Hooks 是您使用 CloudFormation Command Line Interface (CFN-CLI) 在 CloudFormation 登錄檔中註冊的延伸模組。

若要建立自訂勾點，請依照這些主要步驟進行：

1. 啟動專案 – 產生開發自訂勾點所需的檔案。
2. 勾點 – 撰寫定義勾點的結構描述，以及指定可叫用勾點之操作的處理常式。
3. 註冊並啟用勾點 – 建立勾點後，您需要在要使用勾點的帳戶和區域中註冊它，然後啟用它。

下列主題提供建立和管理勾點的詳細資訊。

主題

- [AWS CloudFormation 勾點概念](#)
- [Guard Hook](#)
- [Lambda 勾點](#)
- [使用 CloudFormation CLI 開發自訂勾點](#)

AWS CloudFormation 勾點概念

下列術語和概念是了解和使用 AWS CloudFormation Hooks 的核心：

- [勾點](#)
- [勾點目標](#)
- [目標動作](#)
- [勾點處理常式](#)

勾點

勾點包含在 CloudFormation 建立、更新或刪除堆疊或特定資源之前立即調用的程式碼。也可以在建立變更集操作期間叫用。勾點可以檢查 CloudFormation 即將佈建的範本、資源或變更集。此外，在 [Cloud Control API](#) 建立、更新或刪除特定資源之前，可以立即叫用勾點。

如果勾點識別不符合勾點邏輯中定義之組織準則的任何組態，則您可以選擇 WARN 使用者或 FAIL，以防止 CloudFormation 佈建資源。

勾點具有下列特性：

- 主動驗證 – 在建立、更新或刪除不合規資源之前，透過識別這些資源來降低風險、營運開銷和成本。
- 自動強制執行 – 在 中提供強制執行 AWS 帳戶，以防止 CloudFormation 佈建不合規的資源。

失敗模式

您的勾點邏輯可以傳回成功或失敗。成功回應將允許操作繼續。不合規資源的失敗可能會導致下列情況：

- FAIL – 停止佈建操作。
- WARN – 允許佈建繼續出現警告訊息。

在WARN模式下建立勾點是監控勾點行為的有效方式，而不會影響堆疊操作。首先，在 WARN 模式中啟用勾點，以了解哪些操作會受到影響。評估潛在影響之後，您可以將勾點切換到 FAIL 模式，以開始防止不合規的操作。

勾點目標

勾點目標指定勾點將評估的操作。這些操作可以是：

- CloudFormation 支援的資源 (Resources)
- 堆疊範本 (STACK)
- 變更集 (CHANGE_SET)
- Cloud Control API (CLOUD_CONTROL) 支援的資源

您可以定義一或多個目標，指定 Hook 將評估的最廣泛操作。例如，您可以撰寫 Hook 目標 RESOURCES 以鎖定所有 AWS 資源 STACK，並鎖定所有堆疊範本。您也可以套用篩選條件，將勾點的範圍縮小到要評估的確切操作。如需詳細資訊，請參閱 [AWS CloudFormation 勾點堆疊層級篩選條件](#) 和 [AWS CloudFormation 勾點目標篩選條件](#)。

目標動作

目標動作是觸發勾點的操作類型。動作可以是 CREATE、UPDATE 或 DELETE。

Note

使用 RESOURCE、STACK 和 CLOUD_CONTROL Hook 目標時，所有目標動作都適用。使用 CHANGE_SET Hook 目標時，只會套用 CREATE 動作。

勾點處理常式

對於自訂勾點，這是處理評估的程式碼。它與目標叫用點和目標動作相關聯，該動作會標記勾點的確切執行點。您編寫的處理常式會託管這些特定點的邏輯。例如，具有 PRE 目標動作 CREATE 的目標調用點會成為 preCreate Hook 處理常式。當相符的目標呼叫點和服務執行相關聯的目標動作時，Hook 處理常式內的程式碼會執行。

有效值：(preCreate | preUpdate | preDelete)

Important

導致狀態的堆疊操作 UpdateCleanup 不會叫用勾點。例如，在下列兩種情況下，不會叫用 Hook 的 preDelete 處理常式：

- 從範本中移除一個資源後，堆疊會更新。
- 會刪除具有更新類型 [取代](#) 的資源。

Guard Hook

若要在帳戶中使用 AWS CloudFormation Guard 勾點，您必須為要使用該勾點的帳戶和區域啟用勾點。啟用勾點可讓它在啟用該勾點的帳戶和區域中的堆疊操作中使用。

當您啟用 Guard Hook 時，CloudFormation 會在您帳戶的登錄檔中，將已啟用的 Hook 建立為私有 Hook。這可讓您設定勾點包含的任何組態屬性。組態屬性會定義如何為指定 AWS 帳戶和區域設定勾點。

主題

- [AWS CLI 使用 Guard Hooks 的命令](#)
- [寫入 Guard 規則以評估 Guard Hooks 的資源](#)
- [準備建立 Guard Hook](#)
- [在帳戶中啟用 Guard Hook](#)

- [檢視您帳戶中 Guard Hooks 的日誌](#)
- [刪除您帳戶中的 Guard Hook](#)

AWS CLI 使用 Guard Hooks 的 命令

使用 Guard Hooks 的 AWS CLI 命令包括：

- [activate-type](#) 啟動 Guard Hook 的啟用程序。
- [set-type-configuration](#) 在帳戶中指定勾點的組態資料。
- [list-types](#) 列出您帳戶中的勾點。
- [describe-type](#) 傳回特定 Hook 或特定 Hook 版本的詳細資訊，包括目前的組態資料。
- [deactivate-type](#) 從您的帳戶中移除先前啟用的勾點。

寫入 Guard 規則以評估 Guard Hooks 的資源

AWS CloudFormation Guard 是開放原始碼和一般用途網域特定語言 (DSL)，可用來撰寫 policy-as-code。本主題說明如何使用 Guard 來撰寫範例規則，這些規則可在 Guard Hook 中執行，以自動評估 CloudFormation 和 AWS Cloud Control API 操作。視您的 Guard Hook 執行時間而定，它也會專注於您的 Guard 規則可用的不同輸入類型。Guard Hook 可設定為在下列操作類型期間執行：

- 資源操作
- 堆疊操作
- 變更集操作

如需撰寫 Guard 規則的詳細資訊，請參閱[撰寫 AWS CloudFormation Guard 規則](#)

主題

- [資源操作 Guard 規則](#)
- [堆疊操作 Guard 規則](#)
- [變更集操作 Guard 規則](#)

資源操作 Guard 規則

每當您建立、更新或刪除資源時，即視為資源操作。例如，如果您執行更新建立新資源的 CloudFormation 堆疊，表示您已完成資源操作。當您使用 Cloud Control API 建立、更新或刪除資源

時，這也被視為資源操作。您可以在 Guard Hook 的 TargetOperations 組態中，將 Guard Hook 設定為目標 RESOURCE 和 CLOUD_CONTROL 操作。當您的 Guard Hook 評估資源操作時，Guard 引擎會評估資源輸入。

主題

- [Guard 資源輸入語法](#)
- [Guard 資源操作輸入範例](#)
- [資源變更的防護規則](#)

Guard 資源輸入語法

Guard 資源輸入是可供 Guard 規則評估的資料。

以下是資源輸入的範例形狀：

```
HookContext:
  AWSAccountID: String
  StackId: String
  HookTypeName: String
  HookTypeVersion: String
  InvocationPoint: [CREATE_PRE_PROVISION, UPDATE_PRE_PROVISION, DELETE_PRE_PROVISION]
  TargetName: String
  TargetType: RESOURCE
  TargetLogicalId: String
  ChangeSetId: String
Resources:
  {ResourceLogicalID}:
    ResourceType: {ResourceType}
    ResourceProperties:
      {ResourceProperties}
Previous:
  ResourceLogicalID:
    ResourceType: {ResourceType}
    ResourceProperties:
      {PreviousResourceProperties}
```

HookContext

AWSAccountID

AWS 帳戶 包含要評估之資源的 ID。

StackId

屬於資源操作一部分的 CloudFormation 堆疊的堆疊 ID。如果發起人是 Cloud Control API，則為空白。

HookTypeName

正在執行的勾點名稱。

HookTypeVersion

正在執行的 Hook 版本。

InvocationPoint

佈建邏輯中 Hook 執行的確切點。

有效值：(CREATE_PRE_PROVISION | UPDATE_PRE_PROVISION | DELETE_PRE_PROVISION)

TargetName

正在評估的資源名稱。

TargetType

要評估之資源的資源類型 (範例：AWS::S3::Bucket)。

TargetLogicalId

正在評估TargetLogicalId的資源的。如果 Hook 的原始伺服器是 CloudFormation，這將是資源的邏輯 ID (也稱為邏輯名稱)。如果 Hook 的原始伺服器是 Cloud Control API，這將會是建構值。

ChangeSetId

執行以造成 Hook 調用的變更集 ID。如果資源變更是由 Cloud Control API 或 create-stack、update-stack或 delete-stack操作啟動，則此值為空。

Resources

ResourceLogicalID

當 CloudFormation 啟動操作時，ResourceLogicalID是 CloudFormation 範本中資源的邏輯 ID。

操作由 Cloud Control API 啟動時，ResourceLogicalID是資源類型、名稱、操作 ID 和請求 ID 的組合。

ResourceType

資源的類型名稱（範例：AWS::S3::Bucket）。

ResourceProperties

正在修改之資源的提議屬性。當 Guard Hook 針對 CloudFormation 資源變更執行時，任何函數、參數和轉換都會完全解決。如果正在刪除資源，則此值將為空。

Previous

ResourceLogicalID

當 CloudFormation 啟動操作時，ResourceLogicalID是 CloudFormation 範本中資源的邏輯 ID。

操作由 Cloud Control API 啟動時，ResourceLogicalID是資源類型、名稱、操作 ID 和請求 ID 的組合。

ResourceType

資源的類型名稱（範例：AWS::S3::Bucket）。

ResourceProperties

與要修改之資源相關聯的目前屬性。如果正在刪除資源，則此值將為空。

Guard 資源操作輸入範例

下列範例輸入顯示 Guard Hook，其將接收變更AWS::S3::Bucket的資源定義。這是可供 Guard 評估的資料。

```
HookContext:
  AwsAccountId: "00000000"
  StackId: ""
  HookTypeName: org::s3policy::hook
  HookTypeVersion: "00001"
  InvocationPoint: UPDATE_PRE_PROVISION
  TargetName: AWS::S3::Bucket
  TargetType: RESOURCE
  TargetLogicalId: MyS3Bucket
```

```

ChangeSetId: ""
Resources:
  MyS3Bucket:
    Type: AWS::S3::Bucket
    Properties:
      BucketName: amzn-s3-demo-bucket
      ObjectLockEnabled: true
Previous:
  MyS3Bucket:
    Type: AWS::S3::Bucket
    Properties:
      BucketName: amzn-s3-demo-bucket
      ObjectLockEnabled: false

```

若要查看資源類型可用的所有屬性，請參閱 [AWS::S3::Bucket](#)。

資源變更的防護規則

當 Guard Hook 評估資源變更時，一開始會下載使用 Hook 設定的所有規則。接著會根據資源輸入評估這些規則。如果任何規則未通過評估，則勾點將會失敗。如果沒有失敗，勾點將會通過。

下列範例是 Guard 規則，評估 ObjectLockEnabled 屬性是否 true 適用於任何 AWS::S3::Bucket 資源類型。

```

let s3_buckets_default_lock_enabled = Resources.*[ Type == 'AWS::S3::Bucket']

rule S3_BUCKET_DEFAULT_LOCK_ENABLED when %s3_buckets_default_lock_enabled !empty {
  %s3_buckets_default_lock_enabled.Properties.ObjectLockEnabled exists
  %s3_buckets_default_lock_enabled.Properties.ObjectLockEnabled == true
  <<
    Violation: S3 Bucket ObjectLockEnabled must be set to true.
    Fix: Set the S3 property ObjectLockEnabled parameter to true.
  >>
}

```

當此規則針對下列輸入執行時，將會失敗，因為 ObjectLockEnabled 屬性未設定為 true。

```

Resources:
  MyS3Bucket:
    Type: AWS::S3::Bucket
    Properties:
      BucketName: amzn-s3-demo-bucket

```

```
ObjectLockEnabled: false
```

當此規則針對下列輸入執行時，將會傳遞，因為 ObjectLockEnabled 設定為 true。

```
Resources:
  MyS3Bucket:
    Type: AWS::S3::Bucket
    Properties:
      BucketName: amzn-s3-demo-bucket
      ObjectLockEnabled: true
```

當勾點失敗時，失敗的規則會傳播回 CloudFormation 或 Cloud Control API。如果已為 Guard Hook 設定記錄儲存貯體，則會在該處提供其他規則意見回饋。此額外意見回饋包含 Violation 和 Fix 資訊。

堆疊操作 Guard 規則

建立、更新或刪除 CloudFormation 堆疊時，您可以藉由評估新範本，並可能封鎖堆疊操作以繼續，來設定 Guard Hook 開始。您可以在 Hook 的 TargetOperations 組態中將 Guard Hook 設定為目標 STACK 操作。

主題

- [Guard 堆疊輸入語法](#)
- [Guard 堆疊操作輸入範例](#)
- [堆疊變更的防護規則](#)

Guard 堆疊輸入語法

Guard 堆疊操作的輸入提供整個 CloudFormation 範本，供您的 Guard 規則評估。

以下是堆疊輸入的範例形狀：

```
HookContext:
  AWSAccountID: String
  StackId: String
  HookTypeName: String
  HookTypeVersion: String
  InvocationPoint: [CREATE_PRE_PROVISION, UPDATE_PRE_PROVISION, DELETE_PRE_PROVISION]
  TargetName: String
  TargetType: STACK
  ChangeSetId: String
```

```
{Proposed CloudFormation Template}
```

[Previous:](#)

```
{CloudFormation Template}
```

HookContext

AWSAccountID

AWS 帳戶 包含 資源的 ID。

StackId

屬於堆疊操作一部分的 CloudFormation 堆疊的堆疊 ID。

HookTypeName

正在執行的勾點名稱。

HookTypeVersion

正在執行的 Hook 版本。

InvocationPoint

佈建邏輯中 Hook 執行的確切點。

有效值：(CREATE_PRE_PROVISION | UPDATE_PRE_PROVISION | DELETE_PRE_PROVISION)

TargetName

正在評估的堆疊名稱。

TargetType

此值將作為堆疊層級勾點執行STACK時。

ChangeSetId

執行以造成 Hook 調用的變更集 ID。如果堆疊操作是由 create-stack、或 delete-stack 操作啟動 update-stack，則此值為空。

Proposed CloudFormation Template

傳遞給 CloudFormation create-stack 或 update-stack 操作的完整 CloudFormation 範本值。這包括 Resources、Outputs 和 等物件 Properties。它可以是 JSON 或 YAML 字串，取決於提供給 CloudFormation 的內容。

在delete-stack操作中，此值將為空。

Previous

上次成功部署的 CloudFormation 範本。如果正在建立或刪除堆疊，則此值為空。

在delete-stack操作中，此值將為空。

Note

提供的範本是傳遞至 create或 update堆疊操作的範本。刪除堆疊時，不會提供任何範本值。

Guard 堆疊操作輸入範例

下列範例輸入顯示將接收完整範本和先前部署範本的 Guard Hook。此範例中的範本使用 JSON 格式。

```
HookContext:
  AwsAccountId: 123456789012
  StackId: arn:aws:cloudformation:us-east-1:123456789012:stack/myteststack
  HookTypeName: org::templatechecker::hook
  HookTypeVersion: "00001"
  InvocationPoint: UPDATE_PRE_PROVISION
  TargetName: my-example-stack
  TargetType: CHANGE_SET
  TargetLogicalId: arn:aws:cloudformation:us-east-1:123456789012:changeSet/
SampleChangeSet/12a3b456-0e10-4ce0-9052-5d484a8c4e5b
  ChangeSetId: arn:aws:cloudformation:us-east-1:123456789012:changeSet/
SampleChangeSet/12a3b456-0e10-4ce0-9052-5d484a8c4e5b
Resources: {
  "S3Bucket": {
    "Type": "AWS::S3::Bucket",
    "Properties": {
      "BucketEncryption": {
        "ServerSideEncryptionConfiguration": [
          {"ServerSideEncryptionByDefault":
            {"SSEAlgorithm": "aws:kms",
             "KMSMasterKeyID": "KMS-KEY-ARN" },
           "BucketKeyEnabled": true }
        ]
      }
    }
  }
}
```

```

    }
  }
  Previous: {
    "AWSTemplateFormatVersion": "2010-09-09",
    "Resources": {
      "S3Bucket": {
        "Type": "AWS::S3::Bucket",
        "Properties": {}
      }
    }
  }
}

```

堆疊變更的防護規則

當 Guard Hook 評估堆疊變更時，一開始會下載使用 Hook 設定的所有規則。接著會根據資源輸入評估這些規則。如果任何規則未通過評估，則勾點將會失敗。如果沒有失敗，勾點將會通過。

下列範例是 Guard 規則，評估是否有任何 `AWS::S3::Bucket` 資源類型包含名為 `BucketEncryption` 的屬性，並將 `SSEAlgorithm` 設定為 `aws:kms` 或 `AES256`。

```

let s3_buckets_s3_default_encryption = Resources.*[ Type == 'AWS::S3::Bucket']

rule S3_DEFAULT_ENCRYPTION_KMS when %s3_buckets_s3_default_encryption !empty {
  %s3_buckets_s3_default_encryption.Properties.BucketEncryption exists

  %s3_buckets_s3_default_encryption.Properties.BucketEncryption.ServerSideEncryptionConfiguration
  in ["aws:kms","AES256"]
  <<
    Violation: S3 Bucket default encryption must be set.
    Fix: Set the S3 Bucket property
    BucketEncryption.ServerSideEncryptionConfiguration.ServerSideEncryptionByDefault.SSEAlgorithm
  to either "aws:kms" or "AES256"
  >>
}

```

當規則針對下列範本執行時，它會 fail。

```

AWSTemplateFormatVersion: 2010-09-09
Description: S3 bucket without default encryption
Resources:
  EncryptedS3Bucket:
    Type: 'AWS::S3::Bucket'

```

Properties:

```
BucketName: !Sub 'encryptedbucket-${AWS::Region}-${AWS::AccountId}'
```

當規則針對下列範本執行時，它會 pass。

```
AWSTemplateFormatVersion: 2010-09-09
Description: S3 bucket with default encryption using SSE-KMS with an S3 Bucket Key
Resources:
  EncryptedS3Bucket:
    Type: 'AWS::S3::Bucket'
    Properties:
      BucketName: !Sub 'encryptedbucket-${AWS::Region}-${AWS::AccountId}'
      BucketEncryption:
        ServerSideEncryptionConfiguration:
          - ServerSideEncryptionByDefault:
              SSEAlgorithm: 'aws:kms'
              KMSMasterKeyID: KMS-KEY-ARN
              BucketKeyEnabled: true
```

變更集操作 Guard 規則

建立 CloudFormation 變更集時，您可以設定 Guard Hook 來評估範本，以及變更集中所提議的變更，以封鎖變更集執行。

主題

- [護衛變更集輸入語法](#)
- [Guard 變更集操作輸入範例](#)
- [變更集操作的防護規則](#)

護衛變更集輸入語法

Guard 變更集輸入是可供 Guard 規則評估的資料。

以下是變更集輸入的範例形狀：

HookContext:

```
AWSAccountID: String
StackId: String
HookTypeName: String
```

```

HookTypeVersion: String
InvocationPoint: [CREATE_PRE_PROVISION, UPDATE_PRE_PROVISION, DELETE_PRE_PROVISION]
TargetName: CHANGE_SET
TargetType: CHANGE_SET
TargetLogicalId: ChangeSet ID
ChangeSetId: String
{Proposed CloudFormation Template}
Previous:
  {CloudFormation Template}
Changes: [{ResourceChange}]

```

ResourceChange 模型語法為：

```

logicalResourceId: String
resourceType: String
##: CREATE, UPDATE, DELETE
lineNumber: Number
beforeContext: JSON String
afterContext: JSON String

```

HookContext

AWSAccountID

AWS 帳戶 包含 資源的 ID。

StackId

屬於堆疊操作一部分的 CloudFormation 堆疊的堆疊 ID。

HookTypeName

正在執行的勾點名稱。

HookTypeVersion

正在執行的 Hook 版本。

InvocationPoint

佈建邏輯中 Hook 執行的確切點。

有效值：(CREATE_PRE_PROVISION | UPDATE_PRE_PROVISION | DELETE_PRE_PROVISION)

TargetName

正在評估的堆疊名稱。

TargetType

此值將作為變更集層級勾點執行CHANGE_SET時。

TargetLogicalId

此值將是變更集的 ARN。

ChangeSetId

執行以造成 Hook 調用的變更集 ID。如果堆疊操作是由 create-stack、或 delete-stack 操作啟動 update-stack，則此值為空。

Proposed CloudFormation Template

提供給 create-change-set 操作的完整 CloudFormation 範本。它可以是 JSON 或 YAML 字串，取決於提供給 CloudFormation 的內容。

Previous

上次成功部署的 CloudFormation 範本。如果正在建立或刪除堆疊，則此值為空。

Changes

Changes 模型。這會列出資源變更。

變更

logicalResourceId

已變更資源的邏輯資源名稱。

resourceType

要變更的資源類型。

動作

在資源上執行的操作類型。

有效值：(CREATE | UPDATE | DELETE)

lineNumber

範本中與變更相關聯的行號。

beforeContext

變更前資源屬性的 JSON 字串：

```
{"properties": {"property1": "value"}}
```

afterContext

變更後資源屬性的 JSON 字串：

```
{"properties": {"property1": "new value"}}
```

Guard 變更集操作輸入範例

下列範例輸入顯示將接收完整範本的 Guard Hook、先前部署的範本，以及資源變更清單。此範例中的範本使用 JSON 格式。

```
HookContext:
  AwsAccountId: "000000000"
  StackId: my-example-stack
  HookTypeName: org::templatechecker::hook
  HookTypeVersion: "00001"
  InvocationPoint: UPDATE_PRE_PROVISION
  TargetName: my-example-stack
  TargetType: STACK
  TargetLogicalId: arn...:changeSet/change-set
  ChangeSetId: ""
Resources: {
  "S3Bucket": {
    "Type": "AWS::S3::Bucket",
    "Properties": {
      "BucketName": "amzn-s3-demo-bucket",
      "VersioningConfiguration": {
        "Status": "Enabled"
      }
    }
  }
}
Previous: {
  "AWSTemplateFormatVersion": "2010-09-09",
  "Resources": {
    "S3Bucket": {
      "Type": "AWS::S3::Bucket",
```

```

        "Properties": {
            "BucketName": "amzn-s3-demo-bucket",
            "VersioningConfiguration": {
                "Status": "Suspended"
            }
        }
    }
}
Changes: [
    {
        "logicalResourceId": "S3Bucket",
        "resourceType": "AWS::S3::Bucket",
        "action": "UPDATE",
        "lineNumber": 5,
        "beforeContext": "{\"Properties\":{\"VersioningConfiguration\":{\"Status\": \"Suspended\"}}}",
        "afterContext": "{\"Properties\":{\"VersioningConfiguration\":{\"Status\": \"Enabled\"}}}"
    }
]

```

變更集操作的防護規則

下列範例是 Guard 規則，可評估 Amazon S3 儲存貯體的變更，並確保 VersionConfiguration 不會停用。

```

let s3_buckets_changing = Changes[resourceType == 'AWS::S3::Bucket']

rule S3_VERSIONING_STAY_ENABLED when %s3_buckets_changing !empty {
    let afterContext = json_parse(%s3_buckets_changing.afterContext)
    when %afterContext.Properties.VersioningConfiguration.Status !empty {
        %afterContext.Properties.VersioningConfiguration.Status == 'Enabled'
    }
}

```

準備建立 Guard Hook

建立 Guard Hook 之前，您必須完成下列先決條件：

- 您必須已建立 Guard 規則。如需詳細資訊，請參閱 [勾點的寫入保護規則](#)。

- 建立勾點的使用者或角色必須具有足夠的許可，才能啟用勾點。
- 若要使用 AWS CLI 或 SDK 建立 Guard Hook，您必須手動建立具有 IAM 許可和信任政策的執行角色，以允許 CloudFormation 叫用 Guard Hook。

建立 Guard Hook 的執行角色

Hook 會使用執行角色來取得在中叫用 Hook 所需的許可 AWS 帳戶。

如果您從 建立 Guard Hook，則可以自動建立此角色 AWS Management Console；否則，您必須自行建立此角色。

下一節說明如何設定建立 Guard Hook 的許可。

所需的許可

請遵循 IAM 使用者指南中的[使用自訂信任政策建立角色](#)的指示，以使用自訂信任政策建立角色。

然後，完成下列步驟以設定您的許可：

1. 將下列最低權限政策連接至您要用來建立 Guard Hook 的 IAM 角色。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": [
        "arn:aws:s3::my-guard-output-bucket/*",
        "arn:aws:s3::my-guard-rules-bucket"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject"
      ],
      "Resource": [
```



```
        "arn:aws:s3:::my-guard-output-bucket/*"
    ]
}
]
```

2. 將信任政策新增至角色，授予您的 Hook 擔任角色的許可。以下顯示您可以使用的範例信任政策。

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

在帳戶中啟用 Guard Hook

下列主題說明如何在帳戶中啟用 Guard Hook，這使其可在其啟用的帳戶和區域中使用。

主題

- [啟用 Guard Hook \(主控台\)](#)
- [啟用 Guard Hook \(AWS CLI\)](#)
- [相關資源](#)


啟用 Guard Hook (主控台)

啟用 Guard Hook 以用於您的帳戶

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/cloudformation> 開啟 AWS CloudFormation 主控台。
2. 在畫面頂端的導覽列上，選擇您要建立連接所在的 AWS 區域。

3. 如果您尚未建立任何 Guard 規則，請建立您的 Guard 規則，將其存放在 Amazon S3 中，然後返回此程序。請參閱 [中的範例規則](#) [寫入 Guard 規則以評估 Guard Hooks 的資源](#) 以開始使用。

如果您已建立 Guard 規則並將其存放在 S3 中，請繼續下一個步驟。

 Note

存放在 S3 中的物件必須具有下列其中一個副檔名：`.guard`、`.zip` 或 `.tar.gz`。


4. 對於 Guard Hook 來源，請將您的 Guard 規則存放在 S3 中，執行下列動作：
 - 對於 S3 URI，指定規則檔案的 S3 路徑，或使用瀏覽 S3 按鈕開啟對話方塊以瀏覽並選取 S3 物件。
 - (選用) 對於物件版本，如果您的 S3 儲存貯體已啟用版本控制，您可以選取 S3 物件的特定版本。

Guard Hook 每次叫用 Hook 時都會從 S3 下載您的規則。為了防止意外變更或刪除，我們建議您在設定 Guard Hook 時使用版本。

5. (選用) 針對 Guard 輸出報告的 S3 儲存貯體，指定要存放 Guard 輸出報告的 S3 儲存貯體。此報告包含 Guard 規則驗證的結果。

若要設定輸出報告目的地，請選擇下列其中一個選項：

- 選取使用與 Guard 規則存放相同的儲存貯體核取方塊，以使用 Guard 規則所在的相同儲存貯體。
 - 選擇不同的 S3 儲存貯體名稱來存放 Guard 輸出報告。
6. (選用) 展開 Guard 規則輸入參數，然後在 S3 中儲存您的 Guard 規則輸入參數下提供以下資訊：
 - 針對 S3 URI，指定參數檔案的 S3 路徑，或使用瀏覽 S3 按鈕開啟對話方塊來瀏覽並選取 S3 物件。
 - (選用) 對於物件版本，如果您的 S3 儲存貯體已啟用版本控制，您可以選取 S3 物件的特定版本。
 7. 選擇 Next (下一步)。
 8. 針對勾點名稱，選擇下列其中一個選項：
 - 提供簡短的描述性名稱，該名稱將在之後新增 `Private::Guard::`。例如，如果您輸入 *MyTestHook*，則完整的勾點名稱會變成 `Private::Guard::MyTestHook`。

- 使用此格式提供完整的勾點名稱（也稱為別名）：`Provider::ServiceName::HookName`
9. 對於勾點目標，選擇要評估的項目：
 - 堆疊 — 在使用者建立、更新或刪除堆疊時評估堆疊範本。
 - 資源 — 評估使用者更新堆疊時的個別資源變更。
 - 變更集 — 評估使用者建立變更集時的計劃更新。
 - 雲端控制 API — 評估 [Cloud Control API](#) 啟動的建立、更新或刪除操作。
 10. 針對動作，選擇哪些動作（建立、更新、刪除）將調用您的勾點。
 11. 針對勾點模式，選擇當規則未通過其評估時勾點的回應方式：
 - 警告 — 向使用者發出警告，但允許動作繼續。這對於非關鍵驗證或資訊檢查非常有用。
 - 失敗 — 防止動作繼續。這有助於強制執行嚴格的合規或安全政策。
 12. 針對執行角色，選擇 CloudFormation Hooks 從 S3 擷取您的 Guard 規則所擔任的 IAM 角色，並選擇性地撰寫詳細的 Guard 輸出報告。您可以允許 CloudFormation 自動為您建立執行角色，也可以指定您已建立的角色。
 13. 選擇 Next (下一步)。
 14. (選用) 對於勾點篩選條件，請執行下列動作：
 - a. 針對資源篩選條件，指定哪些資源類型可以叫用勾點。這可確保僅針對相關資源叫用勾點。
 - b. 針對篩選條件，選擇套用堆疊名稱和堆疊角色篩選條件的邏輯：
 - 所有堆疊名稱和堆疊角色 – 只有在所有指定的篩選條件相符時才會叫用勾點。
 - 任何堆疊名稱和堆疊角色 – 如果至少一個指定的篩選條件相符，則會叫用勾點。
- 
- Note**
- 對於雲端控制 API 操作，會忽略所有堆疊名稱和堆疊角色篩選條件。
- c. 對於堆疊名稱，請包含或排除 Hook 調用中的特定堆疊。
 - 針對包含，指定要包含的堆疊名稱。當您有一小組想要鎖定的特定堆疊時，請使用此選項。只有此清單中指定的堆疊才會叫用勾點。
 - 針對排除，指定要排除的堆疊名稱。當您想要在大多數堆疊上叫用勾點，但排除幾個特定的勾點時，請使用此選項。除了此處列出的堆疊之外，所有堆疊都會叫用勾點。
 - d. 對於 Stack 角色，請根據其相關聯的 IAM 角色，從 Hook 調用中包含或排除特定堆疊。

- 針對包含，指定一或多個 IAM 角色 ARNs 至與這些角色相關聯的目標堆疊。只有這些角色啟動的堆疊操作才會叫用勾點。
- 針對排除，為您要排除的堆疊指定一或多個 IAM 角色 ARNs。除了由指定角色啟動的以外，所有堆疊都會叫用勾點。

15. 選擇 Next (下一步)。

16. 在檢閱和啟用頁面上，檢閱您的選擇。若要進行變更，請在相關區段上選擇編輯。

17. 當您準備好繼續時，請選擇啟用勾點。

啟用 Guard Hook (AWS CLI)

在繼續之前，請確認您已建立 Guard 規則，以及您將搭配此勾點使用的執行角色。如需詳細資訊，請參閱 [寫入 Guard 規則以評估 Guard Hooks 的資源](#) 和 [建立 Guard Hook 的執行角色](#)。

啟用 Guard Hook 以用於您的帳戶 (AWS CLI)

1. 若要開始啟用勾點，請使用下列 `activate-type` 命令，將預留位置取代為您的特定值。此命令會授權勾點使用來自的指定執行角色 AWS 帳戶。

```
aws cloudformation activate-type --type HOOK \  
  --type-name AWS::Hooks::GuardHook \  
  --publisher-id aws-hooks \  
  --type-name-alias Private::Guard::MyTestHook \  
  --execution-role arn:aws:iam::123456789012:role/my-execution-role \  
  --region us-west-2
```

2. 若要完成啟用勾點，您必須使用 JSON 組態檔案進行設定。

使用 `cat` 命令來建立具有下列結構的 JSON 檔案。如需詳細資訊，請參閱 [勾點組態結構描述語法參考](#)。

```
$ cat > config.json  
{  
  "CloudFormationConfiguration": {  
    "HookConfiguration": {  
      "HookInvocationStatus": "ENABLED",  
      "TargetOperations": [  
        "STACK",  
        "RESOURCE",  
        "CHANGE_SET"  
      ]  
    }  
  }  
}
```

```
    ],
    "FailureMode": "WARN",
    "Properties": {
      "ruleLocation": "s3://amzn-s3-demo-bucket/MyGuardRules.guard",
      "logBucket": "amzn-s3-demo-logging-bucket"
    }
  }
}
```

- `HookInvocationStatus` : 將設定為 `ENABLED` 以啟用勾點。
 - `TargetOperations` : 指定要執行勾點的操作。
 - `FailureMode` : 設為 `FAIL` 或 `WARN`。
 - `ruleLocation` : 將取代為儲存規則的 S3 URI。存放在 S3 中的物件必須具有下列其中一個副檔名：`.guard`、`.zip`和 `.tar.gz`。
 - `logBucket` : (選用) 指定 Guard JSON 報告的 S3 儲存貯體名稱。
3. 使用下列[set-type-configuration](#)命令以及您建立的 JSON 檔案來套用組態。將預留位置取代為您的特定值。

```
aws cloudformation set-type-configuration \
  --configuration file://config.json \
  --type-arn "arn:aws:cloudformation:us-west-2:123456789012:type/hook/MyTestHook" \
  --region us-west-2
```

相關資源

我們提供範本範例，供您用來了解如何在 CloudFormation 堆疊範本中宣告 Guard Hook。如需詳細資訊，請參閱「AWS CloudFormation 使用者指南」中的 [AWS::CloudFormation::GuardHook](#)。

檢視您帳戶中 Guard Hooks 的日誌

當您啟用 Guard Hook 時，您可以將 Amazon S3 儲存貯體指定為 Hook 輸出報告的目的地。啟用後，Hook 會自動將 Guard 規則驗證的結果存放在指定的儲存貯體中。然後，您可以在 Amazon S3 主控台中檢視這些結果。

在 Amazon S3 主控台中檢視 Guard Hook 日誌

檢視 Guard Hook 輸出日誌檔案

1. 登入 <https://console.aws.amazon.com/s3/>。
2. 在畫面頂端的導覽列上，選擇您的 AWS 區域。
3. 選擇儲存貯體。
4. 選擇您為 Guard 輸出報告選取的儲存貯體。
5. 選擇所需的驗證輸出報告日誌檔案。
6. 選擇您要下載檔案或開啟檔案以檢視。

刪除您帳戶中的 Guard Hook

當您不再需要已啟用的 Guard Hook 時，請使用下列程序在帳戶中將其刪除。

若要暫時停用勾點，而不是將其刪除，請參閱[停用和啟用 AWS CloudFormation 勾點](#)。

主題

- [在帳戶中刪除 Guard Hook \(主控台 \)](#)
- [刪除您帳戶中的 Guard Hook \(AWS CLI\)](#)

在帳戶中刪除 Guard Hook (主控台)

在帳戶中刪除 Guard Hook

1. 登入 AWS Management Console ，並在 <https://console.aws.amazon.com/cloudformation> 開啟 AWS CloudFormation 主控台。
2. 在畫面頂端的導覽列上，選擇 AWS 區域 勾點所在的。
3. 從導覽窗格中，選擇勾點。
4. 在勾點頁面上，尋找要刪除的 Guard Hook。
5. 選取勾點旁的核取方塊，然後選擇刪除。
6. 提示確認時，輸入勾點名稱以確認刪除指定的勾點，然後選擇刪除。

刪除您帳戶中的 Guard Hook (AWS CLI)

Note

您必須先停用勾點，才能刪除勾點。如需詳細資訊，請參閱[在帳戶中停用和啟用勾點 \(AWS CLI\)](#)。

使用下列 `deactivate-type` 命令來停用 勾點，該勾點會從您的帳戶中移除它。將預留位置取代為您的特定值。

```
aws cloudformation deactivate-type \  
  --type-arn "arn:aws:cloudformation:us-west-2:123456789012:type/hook/MyTestHook" \  
  --region us-west-2
```

Lambda 勾點

若要在帳戶中使用 AWS Lambda 勾點，您必須先為要使用該勾點的帳戶和區域啟用勾點。啟用勾點可讓它在啟用該勾點的帳戶和區域中的堆疊操作中使用。

當您啟用 Lambda Hook 時，CloudFormation 會在您帳戶的登錄檔中為已啟用的 Hook 建立項目，做為私有 Hook。這可讓您設定勾點包含的任何組態屬性。組態屬性會定義如何為指定 AWS 帳戶 和 區域設定勾點。

主題

- [AWS CLI 使用 Lambda Hooks 的 命令](#)
- [建立 Lambda 函數來評估 Lambda Hooks 的資源](#)
- [準備建立 Lambda Hook](#)
- [在您的帳戶中啟用 Lambda Hook](#)
- [檢視您帳戶中 Lambda Hooks 的日誌](#)
- [刪除您帳戶中的 Lambda Hooks](#)

AWS CLI 使用 Lambda Hooks 的 命令

使用 Lambda Hooks 的 AWS CLI 命令包括：

- [activate-type](#) 啟動 Lambda Hook 的啟用程序。

- [set-type-configuration](#) 在帳戶中指定勾點的組態資料。
- [list-types](#) 列出您帳戶中的勾點。
- [describe-type](#) 傳回特定 Hook 或特定 Hook 版本的詳細資訊，包括目前的組態資料。
- [deactivate-type](#) 從您的帳戶中移除先前啟用的勾點。

建立 Lambda 函數來評估 Lambda Hooks 的資源

AWS CloudFormation Lambda Hooks 可讓您針對自己的自訂程式碼評估 CloudFormation 和 AWS Cloud Control API 操作。您的勾點可能會封鎖操作以繼續，或向發起人發出警告，並允許操作繼續。當您建立 Lambda Hook 時，您可以將其設定為攔截和評估下列 CloudFormation 操作：

- 資源操作
- 堆疊操作
- 變更集操作

主題

- [開發 Lambda Hook](#)
- [使用 Lambda Hooks 評估資源操作](#)
- [使用 Lambda Hooks 評估堆疊操作](#)
- [使用 Lambda Hooks 評估變更集操作](#)

開發 Lambda Hook

當 Hooks 調用 Lambda 時，Lambda 最多會等待 30 秒來評估輸入。Lambda 將傳回 JSON 回應，指出勾點是否成功或失敗。

主題

- [請求輸入](#)
- [回應輸入](#)
- [範例](#)

請求輸入

傳遞至 Lambda 函數的輸入取決於勾點目標操作（範例：堆疊、資源或變更集）。

回應輸入

為了在請求成功或失敗時與 Hooks 通訊，您的 Lambda 函數需要傳回 JSON 回應。

以下是回應 Hooks 預期的範例形狀：

```
{
  "hookStatus": "SUCCESS" or "FAILED" or "IN_PROGRESS",
  "errorCode": None or "NonCompliant" or "InternalFailure"
  "message": String,
  "clientRequestToken": String
  "callbackContext": None,
  "callbackDelaySeconds": Integer,
}
```

hookStatus

勾點的狀態。此為必要欄位。

有效值：(SUCCESS | FAILED | IN_PROGRESS)

Note

勾點可以傳回 IN_PROGRESS 3 次。如果未傳回任何結果，勾點將會失敗。對於 Lambda Hook，這表示您的 Lambda 函數最多可叫用 3 次。

errorCode

顯示操作是否已評估並判斷為無效，或者如果勾點中發生錯誤，則阻止評估。如果勾點失敗，則此欄位為必要欄位。

有效值：(NonCompliant | InternalFailure)

message

給發起人的訊息，說明勾點成功或失敗的原因。

Note

評估 CloudFormation 操作時，此欄位會截斷為 4096 個字元。

評估 Cloud Control API 操作時，此欄位會截斷為 1024 個字元。

clientRequestToken

作為 Hook 請求輸入而提供的請求字符。此為必要欄位。

callbackContext

如果您表示 hookStatus 是 IN_PROGRESS，則當您重新叫用 Lambda 函數時，會傳遞作為輸入提供的額外內容。

callbackDelaySeconds

Hooks 應該等待多久才能再次叫用此 Hook。

範例

以下是成功回應的範例：

```
{
  "hookStatus": "SUCCESS",
  "message": "compliant",
  "clientRequestToken": "123avjdjk31"
}
```

以下是失敗回應的範例：

```
{
  "hookStatus": "FAILED",
  "errorCode": "NON_COMPLIANT",
  "message": "S3 Bucket Versioning must be enabled.",
  "clientRequestToken": "123avjdjk31"
}
```

使用 Lambda Hooks 評估資源操作

每當您建立、更新或刪除資源時，即視為資源操作。例如，如果您執行更新建立新資源的 CloudFormation 堆疊，表示您已完成資源操作。當您使用 Cloud Control API 建立、更新或刪除資源時，這也被視為資源操作。您可以在 Hook TargetOperations 組態中將 CloudFormation Lambda Hook 設定為目標 RESOURCE 和 CLOUD_CONTROL 操作。

Note

只有在使用來自 `cloud-control delete-resource` 或的操作觸發程序刪除資源時，才會叫用 `delete Hook` 處理常式 `cloudformation delete-stack`。

主題

- [Lambda Hook 資源輸入語法](#)
- [Lambda Hook 資源變更輸入範例](#)
- [資源操作的 Lambda 函數範例](#)

Lambda Hook 資源輸入語法

當您的 Lambda 被叫用進行資源操作時，您將會收到 JSON 輸入，其中包含資源屬性、提議屬性和 Hook 叫用的相關內容。

以下是 JSON 輸入的範例形狀：

```
{
  "awsAccountId": String,
  "stackId": String,
  "changeSetId": String,
  "hookTypeName": String,
  "hookTypeVersion": String,
  "hookModel": {
    "LambdaFunction": String
  },
  "actionInvocationPoint": "CREATE_PRE_PROVISION" or "UPDATE_PRE_PROVISION" or
"DELETE_PRE_PROVISION"
  "requestData": {
    "targetName": String,
    "targetType": String,
    "targetLogicalId": String,
    "targetModel": {
      "resourceProperties": {...},
      "previousResourceProperties": {...}
    }
  },
  "requestContext": {
    "##": 1,

```

```
    "callbackContext": null
  }
}
```

awsAccountId

AWS 帳戶 包含要評估之資源的 ID。

stackId

此操作所屬的 CloudFormation 堆疊的堆疊 ID。如果發起人是 Cloud Control API，則此欄位為空白。

changeSetId

啟動勾點調用的變更集 ID。如果資源變更是由 Cloud Control API 或 create-stack、update-stack 或 delete-stack 操作啟動，則此值為空。

hookTypeName

正在執行的勾點名稱。

hookTypeVersion

正在執行的勾點版本。

hookModel

LambdaFunction

Hook 調用的目前 Lambda ARN。

actionInvocationPoint

佈建邏輯中 Hook 執行的確切點。

有效值：(CREATE_PRE_PROVISION | UPDATE_PRE_PROVISION | DELETE_PRE_PROVISION)

requestData

targetName

要建立的目標資源名稱。

targetType

要建立的目標類型，例如 AWS::S3::Bucket。

targetLogicalId

要評估之資源的邏輯 ID。如果 Hook 調用的原始伺服器是 CloudFormation，這將是 CloudFormation 範本中定義的邏輯資源 ID。如果此 Hook 調用的原始伺服器是 Cloud Control API，這會是建構值。

targetModel

resourceProperties

正在修改之資源的提議屬性。如果正在刪除資源，則此值將為空。

previousResourceProperties

目前與正在修改的資源相關聯的屬性。如果正在建立資源，則此值將為空。

requestContext

調用

目前執行勾點的嘗試。

callbackContext

如果 Hook was 設定為 IN_PROGRESS，並 callbackContext 傳回，則撤銷後將會在這裡。

Lambda Hook 資源變更輸入範例

在下列範例輸入中，Guard Hook 將收到變更 `AWS::DynamoDB::Table` 的資源定義。ProvisionedThroughput 和 ReadCapacityUnits 參數會從 3 更新為 10。

如需 資源可用屬性的詳細資訊，請參閱 [AWS::DynamoDB::Table](#)。

```
{
  "awsAccountId": "123456789",
  "stackId": "arn:aws:cloudformation:eu-central-1:123456789:stack/test-stack/123456abcd",
  "hookTypeName": "my::lambda::resourcehookfunction",
  "hookTypeVersion": "00000008",
  "hookModel": {
    "LambdaFunction": "arn:aws:lambda:eu-central-1:123456789:function:resourcehookfunction"
  },
  "actionInvocationPoint": "UPDATE_PRE_PROVISION",
  "requestData": {
    "targetName": "AWS::DynamoDB::Table",
    "targetType": "AWS::DynamoDB::Table",
```

```
"targetLogicalId": "DDBTable",
"targetModel": {
  "resourceProperties": {
    "AttributeDefinitions": [
      {
        "AttributeType": "S",
        "AttributeName": "Album"
      },
      {
        "AttributeType": "S",
        "AttributeName": "Artist"
      }
    ],
    "ProvisionedThroughput": {
      "WriteCapacityUnits": 5,
      "ReadCapacityUnits": 10
    },
    "KeySchema": [
      {
        "KeyType": "HASH",
        "AttributeName": "Album"
      },
      {
        "KeyType": "RANGE",
        "AttributeName": "Artist"
      }
    ]
  },
  "previousResourceProperties": {
    "AttributeDefinitions": [
      {
        "AttributeType": "S",
        "AttributeName": "Album"
      },
      {
        "AttributeType": "S",
        "AttributeName": "Artist"
      }
    ],
    "ProvisionedThroughput": {
      "WriteCapacityUnits": 5,
      "ReadCapacityUnits": 5
    },
    "KeySchema": [
```

```

        {
            "KeyType": "HASH",
            "AttributeName": "Album"
        },
        {
            "KeyType": "RANGE",
            "AttributeName": "Artist"
        }
    ]
}
},
"requestContext": {
    "invocation": 1,
    "callbackContext": null
}
}

```

資源操作的 Lambda 函數範例

下列範例 Lambda Hook 目標為 Node.js。這是一個簡單的函數，會讓 DynamoDB 的任何資源更新失敗，嘗試將 ProvisionedThroughput ReadCapacity 設定為大於 10 的。如果勾點成功，訊息「ReadCapacity 已正確設定」將顯示給發起人。如果請求驗證失敗，勾點將會失敗，狀態為「ReadCapacity 不能超過 10。」

```

export const handler = async (event, context) => {
    var targetModel = event?.requestData?.targetModel;
    var targetName = event?.requestData?.targetName;
    var response = {
        "hookStatus": "SUCCESS",
        "message": "ReadCapacity is correctly configured.",
        "clientRequestToken": event.clientRequestToken
    };

    if (targetName == "AWS::DynamoDB::Table") {
        var readCapacity =
targetModel?.resourceProperties?.ProvisionedThroughput?.ReadCapacityUnits;
        if (readCapacity > 10) {
            response.hookStatus = "FAILED";
            response.errorCode = "NonCompliant";
            response.message = "ReadCapacity must be cannot be more than 10.";
        }
    }
}

```

```
    return response;
};
```

使用 Lambda Hooks 評估堆疊操作

每當您使用新範本建立、更新或刪除堆疊時，都可以透過評估新範本並可能封鎖堆疊操作以繼續，來設定 CloudFormation Lambda Hook 開始。您可以在 Hook TargetOperations 組態中將 CloudFormation Lambda Hook 設定為目標 STACK 操作。

主題

- [Lambda Hook 堆疊輸入語法](#)
- [Lambda Hook 堆疊變更輸入範例](#)
- [堆疊操作的 Lambda 函數範例](#)

Lambda Hook 堆疊輸入語法

當您的 Lambda 被叫用進行堆疊操作時，您將會收到 JSON 請求，其中包含 Hook 叫用內容 `actionInvocationPoint`、和 請求內容。由於 CloudFormation 範本的大小，以及 Lambda 函數接受的有限輸入大小，實際範本會存放在 Amazon S3 物件中。的輸入 `requestData` 包含另一個物件的 Amazon S3 已簽章 URL，其中包含目前和先前的範本版本。

以下是 JSON 輸入的範例形狀：

```
{
  "clientRequestToken": String,
  "awsAccountId": String,
  "stackID": String,
  "changeSetId": String,
  "hookTypeName": String,
  "hookTypeVersion": String,
  "hookModel": {
    "LambdaFunction": String
  },
  "actionInvocationPoint": "CREATE_PRE_PROVISION" or "UPDATE_PRE_PROVISION" or
  "DELETE_PRE_PROVISION"
  "requestData": {
    "targetName": "STACK",
    "targetType": "STACK",
    "targetLogicalId": String,
    "payload": String (S3 Presigned URL)
  }
}
```



```
    },  
    "requestContext": {  
      "invocation": Integer,  
      "callbackContext": String  
    }  
  }  
}
```

clientRequestToken

作為 Hook 請求輸入而提供的請求字符。此為必要欄位。

awsAccountId

AWS 帳戶 包含要評估之堆疊的 ID。

stackID

CloudFormation 堆疊的堆疊 ID。

changeSetId

啟動勾點調用的變更集 ID。如果堆疊變更是由 Cloud Control API 或 `update-stack` 或 `delete-stack` 操作啟動 `create-stack`，則此值為空。

hookTypeName

正在執行的勾點名稱。

hookTypeVersion

正在執行的勾點版本。

hookModel

LambdaFunction

Hook 調用的目前 Lambda ARN。

actionInvocationPoint

佈建邏輯中 Hook 執行的確切點。

有效值：(CREATE_PRE_PROVISION | UPDATE_PRE_PROVISION | DELETE_PRE_PROVISION)

requestData

targetName

此值將為 STACK。

targetType

此值將為 STACK。

targetLogicalId

堆疊名稱。

payload

Amazon S3 預先簽章的 URL，其中包含具有目前和先前範本定義的 JSON 物件。

requestContext

如果正在重新叫用勾點，則會設定此物件。

invocation

目前執行勾點的嘗試。

callbackContext

如果勾點設定為 callbackContext IN_PROGRESS 並傳回，則撤銷時將會在這裡。

請求資料中的 payload 屬性是程式碼需要擷取的 URL。收到 URL 後，您會取得具有下列結構描述的物件：

```
{
  "template": String,
  "previousTemplate": String
}
```

template

提供給 create-stack 或 update-stack 的完整 CloudFormation 範本。它可以是 JSON 或 YAML 字串，取決於提供給 CloudFormation 的內容。

在 delete-stack 操作中，此值將為空。

previousTemplate

先前的 CloudFormation 範本。它可以是 JSON 或 YAML 字串，取決於提供給 CloudFormation 的內容。

在 delete-stack 操作中，此值將為空。

Lambda Hook 堆疊變更輸入範例

以下是堆疊變更輸入的範例。Hook 正在評估將 `更新ObjectLockEnabled` 為 `true` 的變更，並新增 Amazon SQS 佇列：

```
{
  "clientRequestToken": "f8da6d11-b23f-48f4-814c-0fb6a667f50e",
  "awsAccountId": "123456789",
  "stackId": "arn:aws:cloudformation:eu-central-1:123456789:stack/david-ddb-test-stack/400b40f0-8e72-11ef-80ab-02f2902f0df1",
  "changeSetId": null,
  "hookTypeName": "my::lambda::stackhook",
  "hookTypeVersion": "00000008",
  "hookModel": {
    "LambdaFunction": "arn:aws:lambda:eu-central-1:123456789:function:stackhookfunction"
  },
  "actionInvocationPoint": "UPDATE_PRE_PROVISION",
  "requestData": {
    "targetName": "STACK",
    "targetType": "STACK",
    "targetLogicalId": "my-cloudformation-stack",
    "payload": "https://s3....."
  },
  "requestContext": {
    "invocation": 1,
    "callbackContext": null
  }
}
```

這是 `payload` 的範例 `requestData`：

```
{
  "template": "{\"Resources\":{\"S3Bucket\":{\"Type\":\"AWS::S3::Bucket\", \"Properties\":{\"ObjectLockEnabled\":true}},\"SQSQueue\":{\"Type\":\"AWS::SQS::Queue\", \"Properties\":{\"QueueName\":\"NewQueue\"}}}}",
  "previousTemplate": "{\"Resources\":{\"S3Bucket\":{\"Type\":\"AWS::S3::Bucket\", \"Properties\":{\"ObjectLockEnabled\":false}}}}"
```

堆疊操作的 Lambda 函數範例

下列範例 Lambda Hook 以 為目標Node.js。這是下載堆疊操作承載、剖析範本 JSON 並傳回 的簡單函數SUCCESS。

```
export const handler = async (event, context) => {
  var targetType = event?.requestData?.targetType;
  var payloadUrl = event?.requestData?.payload;

  var response = {
    "hookStatus": "SUCCESS",
    "message": "Stack update is compliant",
    "clientRequestToken": event.clientRequestToken
  };
  try {
    const templateHookPayloadRequest = await fetch(payloadUrl);
    const templateHookPayload = await templateHookPayloadRequest.json()
    if (templateHookPayload.template) {
      // Do something with the template templateHookPayload.template
      // JSON or YAML
    }
    if (templateHookPayload.previousTemplate) {
      // Do something with the template templateHookPayload.previousTemplate
      // JSON or YAML
    }
  } catch (error) {
    console.log(error);
    response.hookStatus = "FAILED";
    response.message = "Failed to evaluate stack operation.";
    response.errorCode = "InternalFailure";
  }
  return response;
};
```

使用 Lambda Hooks 評估變更集操作

每當您建立變更集時，都可以設定 CloudFormation Lambda Hook 來先評估新的變更集，並可能封鎖其執行。您可以在 Hook TargetOperations組態中將 CloudFormation Lambda Hook 設定為目標CHANGE_SET操作。

主題

- [Lambda Hook 變更集輸入語法](#)

- [Lambda Hook 變更集變更輸入範例](#)
- [變更集操作的範例 Lambda 函數](#)

Lambda Hook 變更集輸入語法

變更集操作的輸入類似於堆疊操作，但 承載requestData也包含變更集引入的資源變更清單。

以下是 JSON 輸入的範例形狀：

```
{
  "clientRequesttoken": String,
  "awsAccountId": String,
  "stackID": String,
  "changeSetId": String,
  "hookTypeName": String,
  "hookTypeVersion": String,
  "hookModel": {
    "LambdaFunction":String
  },
  "requestData": {
    "targetName": "CHANGE_SET",
    "targetType": "CHANGE_SET",
    "targetLogicalId": String,
    "payload": String (S3 Presigned URL)
  },
  "requestContext": {
    "invocation": Integer,
    "callbackContext": String
  }
}
```

clientRequesttoken

作為 Hook 請求輸入而提供的請求字符。此為必要欄位。

awsAccountId

AWS 帳戶 包含要評估之堆疊的 ID。

stackID

CloudFormation 堆疊的堆疊 ID。

changeSetId

啟動勾點調用的變更集 ID。

hookTypeName

正在執行的勾點名稱。

hookTypeVersion

正在執行的勾點版本。

hookModel

LambdaFunction

Hook 調用的目前 Lambda ARN。

requestData

targetName

此值將為 CHANGE_SET。

targetType

此值將為 CHANGE_SET。

targetLogicalId

變更集 ARN。

payload

Amazon S3 預先簽章的 URL，其中包含具有目前範本的 JSON 物件，以及此變更集引入的變更清單。

requestContext

如果正在重新叫用勾點，則會設定此物件。

invocation

目前執行勾點的嘗試。

callbackContext

如果勾點設定為 callbackContext IN_PROGRESS 並傳回，則撤銷時將會在這裡。

請求資料中的 payload 屬性是程式碼需要擷取的 URL。收到 URL 後，您會取得具有下列結構描述的物件：

```
{
  "template": String,
  "changedResources": [
    {
      "action": String,
      "beforeContext": JSON String,
      "afterContext": JSON String,
      "lineNumber": Integer,
      "logicalResourceId": String,
      "resourceType": String
    }
  ]
}
```

template

提供給 create-stack 或 update-stack 的完整 CloudFormation 範本。它可以是 JSON 或 YAML 字串，取決於提供給 CloudFormation 的內容。

changedResources

已變更資源的清單。

action

套用至資源的變更類型。

有效值：(CREATE | UPDATE | DELETE)

beforeContext

變更前資源屬性的 JSON 字串。建立資源時，此值為 null。此 JSON 字串中的所有布林值和數值都是 STRINGS。

afterContext

如果執行此變更集，資源屬性的 JSON 字串。正在刪除資源時，此值為 null。此 JSON 字串中的所有布林值和數值都是 STRINGS。

lineNumber

範本中造成此變更的行號。如果動作是 null，則 DELETE 此值將為 Null。

logicalResourceId

要變更之資源的邏輯資源 ID。

resourceType

正在變更的資源類型。

Lambda Hook 變更集變更輸入範例

以下是變更集變更輸入的範例。在下列範例中，您可以看到變更集所引進的變更。第一個變更是刪除名為 `的佇列CoolQueue`。第二個變更是新增名為 `的新佇列NewCoolQueue`。上次變更是 `的更新DynamoDBTable`。

```
{
  "clientRequestToken": "f8da6d11-b23f-48f4-814c-0fb6a667f50e",
  "awsAccountId": "123456789",
  "stackId": "arn:aws:cloudformation:eu-central-1:123456789:stack/david-ddb-test-stack/400b40f0-8e72-11ef-80ab-02f2902f0df1",
  "changeSetId": "arn:aws:cloudformation:eu-central-1:123456789:changeSet/davids-change-set/59ebd63c-7c89-4771-a576-74c3047c15c6",
  "hookTypeName": "my::lambda::changesethook",
  "hookTypeVersion": "00000008",
  "hookModel": {
    "LambdaFunction": "arn:aws:lambda:eu-central-1:123456789:function:changesethookfunction"
  },
  "actionInvocationPoint": "CREATE_PRE_PROVISION",
  "requestData": {
    "targetName": "CHANGE_SET",
    "targetType": "CHANGE_SET",
    "targetLogicalId": "arn:aws:cloudformation:eu-central-1:123456789:changeSet/davids-change-set/59ebd63c-7c89-4771-a576-74c3047c15c6",
    "payload": "https://s3....."
  },
  "requestContext": {
    "invocation": 1,
    "callbackContext": null
  }
}
```

這是 payload 的範例 `requestData.payload` :

```
{
  template: 'Resources:\n' +
    '  DynamoDBTable:\n' +
```



```

'   Type: AWS::DynamoDB::Table\n' +
'   Properties:\n' +
'     AttributeDefinitions:\n' +
'       - AttributeName: "PK"\n' +
'         AttributeType: "S"\n' +
'     BillingMode: "PAY_PER_REQUEST"\n' +
'     KeySchema:\n' +
'       - AttributeName: "PK"\n' +
'         KeyType: "HASH"\n' +
'     PointInTimeRecoverySpecification:\n' +
'       PointInTimeRecoveryEnabled: false\n' +
'   NewSQSQueue:\n' +
'     Type: AWS::SQS::Queue\n' +
'     Properties:\n' +
'       QueueName: "NewCoolQueue"',
changedResources: [
  {
    logicalResourceId: 'SQSQueue',
    resourceType: 'AWS::SQS::Queue',
    action: 'DELETE',
    lineNumber: null,
    beforeContext: '{"Properties":{"QueueName":"CoolQueue"}}',
    afterContext: null
  },
  {
    logicalResourceId: 'NewSQSQueue',
    resourceType: 'AWS::SQS::Queue',
    action: 'CREATE',
    lineNumber: 14,
    beforeContext: null,
    afterContext: '{"Properties":{"QueueName":"NewCoolQueue"}}'
  },
  {
    logicalResourceId: 'DynamoDBTable',
    resourceType: 'AWS::DynamoDB::Table',
    action: 'UPDATE',
    lineNumber: 2,
    beforeContext: '{"Properties":
{"BillingMode":"PAY_PER_REQUEST","AttributeDefinitions":
[{"AttributeType":"S","AttributeName":"PK"}],"KeySchema":
[{"KeyType":"HASH","AttributeName":"PK"}]}' ,
    afterContext: '{"Properties":
{"BillingMode":"PAY_PER_REQUEST","PointInTimeRecoverySpecification":
{"PointInTimeRecoveryEnabled":"false"},"AttributeDefinitions":

```

```
[{"AttributeType":"S","AttributeName":"PK"}],"KeySchema":
[{"KeyType":"HASH","AttributeName":"PK"}]}'
  }
]
}
```

變更集操作的範例 Lambda 函數

下列範例 Lambda Hook 以 為目標Node.js。這是一個簡單的函數，可下載變更集操作承載，逐一完成每個變更，然後在屬性傳回 之前列印前後的 SUCCESS。

```
export const handler = async (event, context) => {
  var payloadUrl = event?.requestData?.payload;
  var response = {
    "hookStatus": "SUCCESS",
    "message": "Change set changes are compliant",
    "clientRequestToken": event.clientRequestToken
  };
  try {
    const changeSetHookPayloadRequest = await fetch(payloadUrl);
    const changeSetHookPayload = await changeSetHookPayloadRequest.json();
    const changes = changeSetHookPayload.changedResources || [];
    for(const change of changes) {
      var beforeContext = {};
      var afterContext = {};
      if(change.beforeContext) {
        beforeContext = JSON.parse(change.beforeContext);
      }
      if(change.afterContext) {
        afterContext = JSON.parse(change.afterContext);
      }
      console.log(beforeContext)
      console.log(afterContext)
      // Evaluate Change here
    }
  } catch (error) {
    console.log(error);
    response.hookStatus = "FAILED";
    response.message = "Failed to evaluate change set operation.";
    response.errorCode = "InternalFailure";
  }
  return response;
};
```

準備建立 Lambda Hook

建立 Lambda Hook 之前，您必須完成下列先決條件：

- 您必須已建立 Lambda 函數。如需詳細資訊，請參閱 [為勾點建立 Lambda 函數](#)。
- 建立勾點的使用者或角色必須具有足夠的許可，才能啟用勾點。
- 若要使用 AWS CLI 或 開發套件來建立 Lambda Hook，您必須手動建立具有 IAM 許可和信任政策的執行角色，以允許 CloudFormation 叫用 Lambda Hook。

建立 Lambda Hook 的執行角色

Hook 會使用執行角色來取得在 中叫用 Hook 所需的許可 AWS 帳戶。

如果您從 建立 Lambda Hook，則可以自動建立此角色 AWS Management Console；否則，您必須自行建立此角色。

下一節說明如何設定建立 Lambda Hook 的許可。

所需的許可

請遵循 IAM 使用者指南中的 [使用自訂信任政策建立角色](#) 的指示，以使用自訂信任政策建立角色。

然後，完成下列步驟以設定您的許可：

1. 將下列最低權限政策連接至您要用來建立 Lambda Hook 的 IAM 角色。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "lambda:InvokeFunction",
      "Resource": "arn:aws:lambda:us-west-2:123456789012:function:my-function-  
name"
    }
  ]
}
```

2. 將信任政策新增至角色，授予您的 Hook 擔任角色的許可。以下顯示您可以使用的範例信任政策。

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

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

在您的帳戶中啟用 Lambda Hook

下列主題說明如何在帳戶中啟用 Lambda Hook，這使其可在其啟用的帳戶和區域中使用。

主題

- [啟用 Lambda Hook \(主控台\)](#)
- [啟用 Lambda Hook \(AWS CLI\)](#)
- [相關資源](#)

啟用 Lambda Hook (主控台)

啟用 Lambda Hook 以用於您的帳戶

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/cloudformation> 開啟 AWS CloudFormation 主控台。
2. 在畫面頂端的導覽列上，選擇您要建立連接所在的 AWS 區域。
3. 如果您尚未為勾點建立 Lambda 函數，請執行下列動作：
 - 開啟 Lambda 主控台中的 [Functions \(函數\) 頁面](#)。
 - 建立您將與此勾點搭配使用的 Lambda 函數，然後返回此程序。如需詳細資訊，請參閱 [建立 Lambda 函數來評估 Lambda Hooks 的資源](#)。

如果您已建立 Lambda 函數，請繼續下一個步驟。

4. 針對勾點名稱，選擇下列其中一個選項：

- 提供簡短的描述性名稱，該名稱將在之後新增 `Private::Lambda::`。例如，如果您輸入 `MyTestHook`，則完整的勾點名稱會變成 `Private::Lambda::MyTestHook`。
 - 使用此格式提供完整的勾點名稱（也稱為別名）：`Provider::ServiceName::HookName`
5. 針對 Lambda 函數，提供要與這個勾點搭配使用的 Lambda 函數。您可以使用：
 - 不含尾碼的完整 Amazon Resource Name (ARN)。
 - 具有版本或別名尾碼的合格 ARN。
 6. 對於勾點目標，選擇要評估的內容：
 - 堆疊 — 在使用者建立、更新或刪除堆疊時評估堆疊範本。
 - 資源 — 評估使用者更新堆疊時的個別資源變更。
 - 變更集 — 評估使用者建立變更集時的計劃更新。
 - Cloud Control API — 評估由 [Cloud Control API](#) 啟動的建立、更新或刪除操作。
 7. 針對動作，選擇哪些動作（建立、更新、刪除）將調用您的勾點。
 8. 對於勾點模式，選擇勾點在勾點調用 Lambda 函數傳回 FAILED 回應時回應的方式：
 - 警告 — 向使用者發出警告，但允許動作繼續。這對於非關鍵驗證或資訊檢查非常有用。
 - 失敗 — 防止動作繼續。這有助於強制執行嚴格的合規或安全政策。
 9. 針對執行角色，選擇 Hook 用來叫用 Lambda 函數的 IAM 角色。您可以允許 CloudFormation 自動為您建立執行角色，也可以指定您已建立的角色。
 10. 選擇 Next (下一步)。
 11. (選用) 對於勾點篩選條件，請執行下列動作：
 - a. 針對資源篩選條件，指定哪些資源類型可以叫用勾點。這可確保僅針對相關資源叫用勾點。
 - b. 針對篩選條件，選擇套用堆疊名稱和堆疊角色篩選條件的邏輯：
 - 所有堆疊名稱和堆疊角色 – 只有在所有指定的篩選條件相符時才會叫用勾點。
 - 任何堆疊名稱和堆疊角色 – 如果至少一個指定的篩選條件相符，則會叫用勾點。
 - c. 對於堆疊名稱，請包含或排除 Hook 調用中的特定堆疊。

Note

對於雲端控制 API 操作，會忽略所有堆疊名稱和堆疊角色篩選條件。

- 針對包含，指定要包含的堆疊名稱。當您有一小組想要鎖定的特定堆疊時，請使用此選項。只有此清單中指定的堆疊才會叫用勾點。
 - 針對排除，指定要排除的堆疊名稱。當您想要在大多數堆疊上叫用勾點，但排除幾個特定的勾點時，請使用此選項。除了此處列出的堆疊之外，所有堆疊都會叫用勾點。
- d. 對於 Stack 角色，根據其相關聯的 IAM 角色，從 Hook 調用中包含或排除特定堆疊。
- 針對包含，指定一或多個 IAM 角色 ARNs 至與這些角色相關聯的目標堆疊。只有這些角色啟動的堆疊操作才會叫用勾點。
 - 針對排除，為您要排除的堆疊指定一或多個 IAM 角色 ARNs。除了由指定角色啟動的以外，所有堆疊都會叫用勾點。
12. 選擇 Next (下一步)。
 13. 在檢閱和啟用頁面上，檢閱您的選擇。若要進行變更，請在相關區段中選擇編輯。
 14. 當您準備好繼續時，請選擇啟用勾點。

啟用 Lambda Hook (AWS CLI)

在繼續之前，請確認您已建立 Lambda 函數，以及您將搭配此勾點使用的執行角色。如需詳細資訊，請參閱 [建立 Lambda 函數來評估 Lambda Hooks 的資源](#) 和 [建立 Lambda Hook 的執行角色](#)。

啟用 Lambda Hook 以用於您的帳戶 (AWS CLI)

1. 若要開始啟用勾點，請使用下列 [activate-type](#) 命令，將預留位置取代為您的特定值。此命令會授權勾點使用來自的指定執行角色 AWS 帳戶。

```
aws cloudformation activate-type --type HOOK \
  --type-name AWS::Hooks::LambdaHook \
  --publisher-id aws-hooks \
  --execution-role arn:aws:iam::123456789012:role/my-execution-role \
  --type-name-alias Private::Lambda::MyTestHook \
  --region us-west-2
```

2. 若要完成啟用勾點，您必須使用 JSON 組態檔案進行設定。

使用 cat 命令來建立具有下列結構的 JSON 檔案。如需詳細資訊，請參閱 [勾點組態結構描述語法參考](#)。

```
$ cat > config.json
{
```

```
"CloudFormationConfiguration": {
  "HookConfiguration": {
    "HookInvocationStatus": "ENABLED",
    "TargetOperations": [
      "CLoud_CONTROL"
    ],
    "FailureMode": "WARN",
    "Properties": {
      "LambdaFunction": "arn:aws:lambda:us-
west-2:123456789012:function:MyFunction"
    }
  }
}
```

- `HookInvocationStatus` : 將設定為 `ENABLED` 以啟用勾點。
 - `TargetOperations` : 指定要執行勾點的操作。
 - `FailureMode` : 設為 `FAIL` 或 `WARN`。
 - `LambdaFunction` : 指定 Lambda 函數的 ARN。
3. 使用下列[set-type-configuration](#)命令以及您建立的 JSON 檔案來套用組態。將預留位置取代為您的特定值。

```
aws cloudformation set-type-configuration \
  --configuration file://config.json \
  --type-arn "arn:aws:cloudformation:us-west-2:123456789012:type/hook/MyTestHook" \
  --region us-west-2
```

相關資源

我們提供範本範例，供您用來了解如何在 CloudFormation 堆疊範本中宣告 Lambda Hook。如需詳細資訊，請參閱「AWS CloudFormation 使用者指南」中的 [AWS::CloudFormation::LambdaHook](#)。

檢視您帳戶中 Lambda Hooks 的日誌

使用 Lambda Hook 時，可以在 Lambda 主控台中找到您的驗證輸出報告日誌檔案。

在 Lambda 主控台中檢視 Lambda Hook 日誌

檢視 Lambda Hook 輸出日誌檔案

1. 登入 Lambda 主控台。
2. 在畫面頂端的導覽列上，選擇您的 AWS 區域。
3. 選擇函數。
4. 選擇所需的 Lambda 函數。
5. 選擇測試標籤。
6. 選擇 CloudWatch Logs Live Trail
7. 選擇下拉式選單，然後選擇您要檢視的日誌群組。
8. 選擇 開始使用。日誌會顯示在 CloudWatch Logs Live Trail 視窗中。根據您的偏好設定，選擇在資料欄中檢視或以純文字檢視。
 - 您可以在新增篩選條件模式欄位中新增更多篩選條件，藉此將篩選條件新增至結果。此欄位可讓您篩選結果，只包含符合指定模式的事件。

如需檢視 Lambda 函數日誌的詳細資訊，請參閱[檢視 Lambda 函數的 CloudWatch Logs](#)。

刪除您帳戶中的 Lambda Hooks

當您不再需要已啟用的 Lambda Hook 時，請使用下列程序來刪除帳戶中的 Lambda Hook。

若要暫時停用勾點，而不是將其刪除，請參閱[停用和啟用 AWS CloudFormation 勾點](#)。

主題

- [刪除您帳戶中的 Lambda Hook \(主控台\)](#)
- [刪除您帳戶中的 Lambda Hook \(AWS CLI\)](#)

刪除您帳戶中的 Lambda Hook (主控台)

刪除您帳戶中的 Lambda Hook

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/cloudformation> 開啟 AWS CloudFormation 主控台。
2. 在畫面頂端的導覽列上，選擇 AWS 區域 勾點所在的。

3. 從導覽窗格中，選擇勾點。
4. 在勾點頁面上，尋找要刪除的 Lambda 勾點。
5. 選取勾點旁的核取方塊，然後選擇刪除。
6. 出現確認提示時，輸入勾點名稱以確認刪除指定的勾點，然後選擇刪除。

刪除您帳戶中的 Lambda Hook (AWS CLI)

Note

您必須先停用勾點，才能刪除勾點。如需詳細資訊，請參閱[在帳戶中停用和啟用勾點 \(AWS CLI\)](#)。

使用下列 `deactivate-type` 命令來停用 勾點，該勾點會從您的帳戶中移除它。將預留位置取代為您的特定值。

```
aws cloudformation deactivate-type \  
  --type-arn "arn:aws:cloudformation:us-west-2:123456789012:type/hook/MyTestHook" \  
  --region us-west-2
```

使用 CloudFormation CLI 開發自訂勾點

本節適用於想要開發自訂勾點並在登錄檔中 AWS CloudFormation 註冊的客戶。

開發自訂勾點有三個主要步驟：

1. 啟動

若要開發自訂勾點，您必須設定和使用 CloudFormation CLI。若要啟動 Hook 的專案及其必要檔案，請使用 CloudFormation CLI `init` 命令並指定您要建立 Hook。如需詳細資訊，請參閱[啟動自訂 AWS CloudFormation 勾點專案](#)。

2. 模型

若要建立、撰寫和驗證您的勾點結構描述，請定義勾點、其屬性及其屬性。

CloudFormation CLI 會建立對應至特定 Hook 調用點的空白處理常式函數。將您自己的邏輯新增至這些處理常式，以控制 Hook 調用期間在其目標生命週期的每個階段發生的情況。如需詳細資訊，請參閱[建立自訂 AWS CloudFormation 勾點模型](#)。

3. 註冊

若要註冊勾點，請提交您的勾點以註冊為私有或公有第三方延伸。向 [submit](#) 操作註冊您的勾點。如需詳細資訊，請參閱 [向註冊自訂勾點 AWS CloudFormation](#)。

下列任務與註冊您的勾點相關聯：

- a. 發佈 – 勾點會發佈至登錄檔。
- b. 設定 – 當類型組態調用堆疊時，會設定勾點。

Note

30 秒後掛鉤逾時。

下列主題會引導您使用 Python 或 Java 開發、註冊和發佈自訂勾點。

主題

- [開發自訂 AWS CloudFormation 勾點的先決條件](#)
- [啟動自訂 AWS CloudFormation 勾點專案](#)
- [建立自訂 AWS CloudFormation 勾點模型](#)
- [向註冊自訂勾點 AWS CloudFormation](#)
- [在中測試自訂勾點 AWS 帳戶](#)
- [更新自訂勾點](#)
- [從 CloudFormation 登錄檔取消註冊自訂勾點](#)
- [公開發佈勾點](#)
- [AWS CloudFormation 勾點的結構描述語法參考](#)

開發自訂 AWS CloudFormation 勾點的先決條件

您可以使用 Java 或 Python 開發自訂勾點。以下是開發自訂勾點的先決條件：

Java 先決條件

- [Apache Maven](#)
- [JDK 17](#)

Note

如果您打算使用 [CloudFormation 命令列界面 \(CLI\)](#) 啟動 Java 的 Hooks 專案，您也必須安裝 Python 3.8 或更新版本。CloudFormation CLI 的 Java 外掛程式可以透過 pip(Python 的套件管理員) 安裝，該程式使用 Python 解散。

若要為 Java Hooks 專案實作 Hook 處理常式，您可以下載 [Java Hook 處理常式範例檔案](#)。

Python 先決條件

- [Python 3.8 版或更新版本。](#)

若要為 Python Hooks 專案實作 Hook 處理常式，您可以下載 [Python Hook 處理常式範例檔案](#)。

開發勾點的許可

除了 CloudFormation Create、Update 和 Delete 堆疊許可之外，您將需要存取下列 AWS CloudFormation 操作。存取這些操作是透過您 IAM 角色的 CloudFormation 政策來管理。

- [register-type](#)
- [list-types](#)
- [deregister-type](#)
- [set-type-configuration](#)

設定 Hooks 的開發環境

若要開發勾點，您應該熟悉 [CloudFormation 範本](#)，以及 Python 或 Java。

若要安裝 CloudFormation CLI 和相關聯的外掛程式：

1. 使用 Python 套件管理員 pip，安裝 CloudFormation CLI。

```
pip3 install cloudformation-cli
```

2. 安裝 CloudFormation CLI 的 Python 或 Java 外掛程式。

Python

```
pip3 install cloudformation-cli-python-plugin
```

Java

```
pip3 install cloudformation-cli-java-plugin
```

若要升級 CloudFormation CLI 和外掛程式，您可以使用升級選項。

Python

```
pip3 install --upgrade cloudformation-cli cloudformation-cli-python-plugin
```

Java

```
pip3 install --upgrade cloudformation-cli cloudformation-cli-java-plugin
```

啟動自訂 AWS CloudFormation 勾點專案

建立自訂 Hooks 專案的第一步是啟動專案。您可以使用 CloudFormation CLI `init` 命令來啟動自訂 Hooks 專案。

`init` 命令會啟動精靈，引導您設定專案，包括 Hooks 結構描述檔案。使用此結構描述檔案作為定義勾點形狀和語意的起點。如需詳細資訊，請參閱[結構描述語法](#)。

若要啟動 Hook 專案：

1. 建立專案的目錄。

```
mkdir ~/mycompany-testing-mytesthook
```

2. 導覽至新目錄。

```
cd ~/mycompany-testing-mytesthook
```

3. 使用 CloudFormation CLI `init` 命令啟動專案。

```
cfn init
```

命令會傳回下列輸出：

```
Initializing new project
```

4. `init` 命令會啟動精靈，引導您設定專案。出現提示時，輸入 `h` 以指定 Hooks 專案。

```
Do you want to develop a new resource(r) a module(m) or a hook(h)?
```

```
h
```

5. 輸入勾點類型的名稱。

```
What's the name of your hook type?
(Organization::Service::Hook)
```

```
MyCompany::Testing::MyTestHook
```

6. 如果只安裝一種語言外掛程式，預設會選取該外掛程式。如果已安裝多個語言外掛程式，您可以選擇所需的語言。輸入您選擇的語言的數字選擇。

```
Select a language for code generation:
[1] java
[2] python38
[3] python39
(enter an integer):
```

7. 根據所選的開發語言設定封裝。

Python

(選用) 針對與平台無關的封裝選擇 Docker。雖然 Docker 並非必要，但強烈建議您更輕鬆地進行封裝。

```
Use docker for platform-independent packaging (Y/n)?
```

```
This is highly recommended unless you are experienced with cross-platform Python packaging.
```

Java

設定 Java 套件名稱，然後選擇 codegen 模型。您可以使用預設套件名稱，或建立新的套件名稱。

Enter a package name (empty for default 'com.mycompany.testing.mytesthook'):

Choose codegen model - 1 (default) or 2 (guided-aws):

結果：您已成功啟動專案，並產生開發勾點所需的檔案。以下是構成 Python 3.8 的 Hooks 專案的目錄和檔案範例。

```
mycompany-testing-mytesthook.json
rpdk.log
README.md
requirements.txt
hook-role.yaml
template.yml
docs
  README.md
src
  __init__.py
  handlers.py
  models.py
target_models
  aws_s3_bucket.py
```

Note

src 目錄中的檔案會根據您的語言選擇建立。產生的檔案中有一些有用的註解和範例。當您執行 generate 命令來新增處理常式的執行時間程式碼時 models.py，某些檔案，例如，會在稍後的步驟中自動更新。

建立自訂 AWS CloudFormation 勾點模型

建立自訂 AWS CloudFormation 勾點的模型需要建立定義勾點、其屬性及其屬性的結構描述。當您使用 `cfn init` 命令建立自訂 Hook 專案時，Hook 結構描述範例會建立為 JSON 格式的文字檔案 `hook-name.json`。

目標調用點和目標動作會指定叫用勾點的確切點。勾點處理常式託管這些點的可執行自訂邏輯。例如，CREATE 操作的目標動作會使用 `preCreate` 處理常式。當 Hook 目標和服務執行相符動作時，您在處理常式中寫入的程式碼會叫用。勾點目標是叫用勾點的目的地。您可以指定目標，例如 AWS CloudFormation 公有資源、私有資源或自訂資源。Hooks 支援無限數量的 Hook 目標。

結構描述包含勾點所需的許可。編寫勾點需要您為每個勾點處理常式指定許可。CloudFormation 鼓勵作者撰寫遵循授予最低權限或僅授予執行任務所需許可之標準安全建議的政策。判斷使用者（和角色）需要執行的動作，然後制定政策，讓他們僅執行這些 Hook 操作的任務。CloudFormation 使用這些許可來縮小範圍勾點使用者提供的許可。這些許可會傳遞給勾點。勾點處理常式使用這些許可來存取 AWS 資源。

您可以使用下列結構描述檔案作為定義勾點的起點。使用勾點結構描述指定您要實作的處理常式。如果您選擇不實作特定處理常式，請從 Hook 結構描述的處理常式區段中移除它。如需結構描述的詳細資訊，請參閱 [結構描述語法](#)。

```
{
  "typeName": "MyCompany::Testing::MyTestHook",
  "description": "Verifies S3 bucket and SQS queues properties before create and update",
  "sourceUrl": "https://mycorp.com/my-repo.git",
  "documentationUrl": "https://mycorp.com/documentation",
  "typeConfiguration": {
    "properties": {
      "minBuckets": {
        "description": "Minimum number of compliant buckets",
        "type": "string"
      },
      "minQueues": {
        "description": "Minimum number of compliant queues",
        "type": "string"
      },
      "encryptionAlgorithm": {
        "description": "Encryption algorithm for SSE",
        "default": "AES256",
        "type": "string"
      }
    }
  }
}
```

```
    },
    "required":[

    ],
    "additionalProperties":false
  },
  "handlers":{
    "preCreate":{
      "targetNames":[
        "AWS::S3::Bucket",
        "AWS::SQS::Queue"
      ],
      "permissions":[

      ]
    },
    "preUpdate":{
      "targetNames":[
        "AWS::S3::Bucket",
        "AWS::SQS::Queue"
      ],
      "permissions":[

      ]
    },
    "preDelete":{
      "targetNames":[
        "AWS::S3::Bucket",
        "AWS::SQS::Queue"
      ],
      "permissions":[
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetEncryptionConfiguration",
        "sqs:ListQueues",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl"
      ]
    }
  },
  "additionalProperties":false
}
```


主題

- [使用 Java 建立自訂 AWS CloudFormation 勾點的模型](#)
- [使用 Python 建立自訂 AWS CloudFormation 勾點的模型](#)

使用 Java 建立自訂 AWS CloudFormation 勾點的模型

建立自訂 AWS CloudFormation 勾點的模型需要建立定義勾點、其屬性及其屬性的結構描述。本教學課程將逐步引導您使用 Java 建立自訂勾點模型。

步驟 1：新增專案相依性

以 Java 為基礎的 Hooks 專案依賴 Maven pom.xml 的檔案做為相依性。展開以下區段，並將原始程式碼複製到專案根目錄的 pom.xml 檔案。

勾點專案相依性 (pom.xml)

```
<?xml version="1.0" encoding="UTF-8"?>
<project
  xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/
maven-v4_0_0.xsd">
  <modelVersion>4.0.0</modelVersion>

  <groupId>com.mycompany.testing.mytesthook</groupId>
  <artifactId>mycompany-testing-mytesthook-handler</artifactId>
  <name>mycompany-testing-mytesthook-handler</name>
  <version>1.0-SNAPSHOT</version>
  <packaging>jar</packaging>

  <properties>
    <maven.compiler.source>1.8</maven.compiler.source>
    <maven.compiler.target>1.8</maven.compiler.target>
    <project.build.sourceEncoding>UTF-8</project.build.sourceEncoding>
    <project.reporting.outputEncoding>UTF-8</project.reporting.outputEncoding>
    <aws.java.sdk.version>2.16.1</aws.java.sdk.version>
    <checkstyle.version>8.36.2</checkstyle.version>
    <commons-io.version>2.8.0</commons-io.version>
    <jackson.version>2.11.3</jackson.version>
    <maven-checkstyle-plugin.version>3.1.1</maven-checkstyle-plugin.version>
    <mockito.version>3.6.0</mockito.version>
    <spotbugs.version>4.1.4</spotbugs.version>
```

```
<spotless.version>2.5.0</spotless.version>
<maven-javadoc-plugin.version>3.2.0</maven-javadoc-plugin.version>
<maven-source-plugin.version>3.2.1</maven-source-plugin.version>
<cfn.generate.args/>
</properties>

<dependencyManagement>
  <dependencies>
    <dependency>
      <groupId>software.amazon.awssdk</groupId>
      <artifactId>bom</artifactId>
      <version>2.16.1</version>
      <type>pom</type>
      <scope>import</scope>
    </dependency>
  </dependencies>
</dependencyManagement>

<dependencies>
  <!-- https://mvnrepository.com/artifact/software.amazon.cloudformation/aws-
cloudformation-rpdk-java-plugin -->
  <dependency>
    <groupId>software.amazon.cloudformation</groupId>
    <artifactId>aws-cloudformation-rpdk-java-plugin</artifactId>
    <version>[2.0.0,3.0.0)</version>
  </dependency>

  <!-- AWS Java SDK v2 Dependencies -->
  <dependency>
    <groupId>software.amazon.awssdk</groupId>
    <artifactId>sdk-core</artifactId>
  </dependency>
  <dependency>
    <groupId>software.amazon.awssdk</groupId>
    <artifactId>cloudformation</artifactId>
  </dependency>
  <dependency>
    <groupId>software.amazon.awssdk</groupId>
    <artifactId>s3</artifactId>
  </dependency>
  <dependency>
    <groupId>software.amazon.awssdk</groupId>
    <artifactId>utils</artifactId>
  </dependency>
</dependencies>
```

```
<dependency>
  <groupId>software.amazon.awssdk</groupId>
  <artifactId>apache-client</artifactId>
</dependency>
<dependency>
  <groupId>software.amazon.awssdk</groupId>
  <artifactId>sqs</artifactId>
</dependency>

<!-- Test dependency for Java Providers -->
<dependency>
  <groupId>software.amazon.cloudformation</groupId>
  <artifactId>cloudformation-cli-java-plugin-testing-support</artifactId>
  <version>1.0.0</version>
</dependency>

<!-- https://mvnrepository.com/artifact/com.amazonaws/aws-java-sdk-s3 -->
<dependency>
  <groupId>com.amazonaws</groupId>
  <artifactId>aws-java-sdk-s3</artifactId>
  <version>1.12.85</version>
</dependency>

<!-- https://mvnrepository.com/artifact/commons-io/commons-io -->
<dependency>
  <groupId>commons-io</groupId>
  <artifactId>commons-io</artifactId>
  <version>${commons-io.version}</version>
</dependency>
<!-- https://mvnrepository.com/artifact/org.apache.commons/commons-lang3 -->
<dependency>
  <groupId>org.apache.commons</groupId>
  <artifactId>commons-lang3</artifactId>
  <version>3.9</version>
</dependency>
<!-- https://mvnrepository.com/artifact/org.apache.commons/commons-collections4 -->
-->
<dependency>
  <groupId>org.apache.commons</groupId>
  <artifactId>commons-collections4</artifactId>
  <version>4.4</version>
</dependency>
<!-- https://mvnrepository.com/artifact/com.google.guava/guava -->
<dependency>
```

```
    <groupId>com.google.guava</groupId>
    <artifactId>guava</artifactId>
    <version>29.0-jre</version>
</dependency>
<!-- https://mvnrepository.com/artifact/com.amazonaws/aws-java-sdk-
cloudformation -->
<dependency>
    <groupId>com.amazonaws</groupId>
    <artifactId>aws-java-sdk-cloudformation</artifactId>
    <version>1.11.555</version>
    <scope>test</scope>
</dependency>

<!-- https://mvnrepository.com/artifact/commons-codec/commons-codec -->
<dependency>
    <groupId>commons-codec</groupId>
    <artifactId>commons-codec</artifactId>
    <version>1.14</version>
</dependency>
<!-- https://mvnrepository.com/artifact/software.amazon.cloudformation/aws-
cloudformation-resource-schema -->
<dependency>
    <groupId>software.amazon.cloudformation</groupId>
    <artifactId>aws-cloudformation-resource-schema</artifactId>
    <version>[2.0.5, 3.0.0)</version>
</dependency>
<!-- https://mvnrepository.com/artifact/com.fasterxml.jackson.dataformat/
jackson-databind -->
<dependency>
    <groupId>com.fasterxml.jackson.core</groupId>
    <artifactId>jackson-databind</artifactId>
    <version>${jackson.version}</version>
</dependency>
<!-- https://mvnrepository.com/artifact/com.fasterxml.jackson.dataformat/
jackson-dataformat-cbor -->
<dependency>
    <groupId>com.fasterxml.jackson.dataformat</groupId>
    <artifactId>jackson-dataformat-cbor</artifactId>
    <version>${jackson.version}</version>
</dependency>

<dependency>
    <groupId>com.fasterxml.jackson.datatype</groupId>
    <artifactId>jackson-datatype-jsr310</artifactId>
```

```
        <version>${jackson.version}</version>
    </dependency>

    <!-- https://mvnrepository.com/artifact/com.fasterxml.jackson.module/jackson-
modules-java8 -->
    <dependency>
        <groupId>com.fasterxml.jackson.module</groupId>
        <artifactId>jackson-modules-java8</artifactId>
        <version>${jackson.version}</version>
        <type>pom</type>
        <scope>runtime</scope>
    </dependency>

    <!-- https://mvnrepository.com/artifact/org.json/json -->
    <dependency>
        <groupId>org.json</groupId>
        <artifactId>json</artifactId>
        <version>20180813</version>
    </dependency>
    <!-- https://mvnrepository.com/artifact/com.amazonaws/aws-java-sdk-core -->
    <dependency>
        <groupId>com.amazonaws</groupId>
        <artifactId>aws-java-sdk-core</artifactId>
        <version>1.11.1034</version>
    </dependency>
    <!-- https://mvnrepository.com/artifact/com.amazonaws/aws-lambda-java-core -->
    <dependency>
        <groupId>com.amazonaws</groupId>
        <artifactId>aws-lambda-java-core</artifactId>
        <version>1.2.0</version>
    </dependency>
    <!-- https://mvnrepository.com/artifact/com.amazonaws/aws-lambda-java-log4j2 --
>
    <dependency>
        <groupId>com.amazonaws</groupId>
        <artifactId>aws-lambda-java-log4j2</artifactId>
        <version>1.2.0</version>
    </dependency>

    <!-- https://mvnrepository.com/artifact/com.google.code.gson/gson -->
    <dependency>
        <groupId>com.google.code.gson</groupId>
        <artifactId>gson</artifactId>
        <version>2.8.8</version>
```

```
</dependency>

<!-- https://mvnrepository.com/artifact/org.projectlombok/lombok -->
<dependency>
  <groupId>org.projectlombok</groupId>
  <artifactId>lombok</artifactId>
  <version>1.18.4</version>
  <scope>provided</scope>
</dependency>
<!-- https://mvnrepository.com/artifact/org.apache.logging.log4j/log4j-api -->
<dependency>
  <groupId>org.apache.logging.log4j</groupId>
  <artifactId>log4j-api</artifactId>
  <version>2.17.1</version>
</dependency>
<!-- https://mvnrepository.com/artifact/org.apache.logging.log4j/log4j-core -->
>
<dependency>
  <groupId>org.apache.logging.log4j</groupId>
  <artifactId>log4j-core</artifactId>
  <version>2.17.1</version>
</dependency>
<!-- https://mvnrepository.com/artifact/org.apache.logging.log4j/log4j-slf4j-impl -->
impl -->
<dependency>
  <groupId>org.apache.logging.log4j</groupId>
  <artifactId>log4j-slf4j-impl</artifactId>
  <version>2.17.1</version>
</dependency>

<!-- https://mvnrepository.com/artifact/org.assertj/assertj-core -->
<dependency>
  <groupId>org.assertj</groupId>
  <artifactId>assertj-core</artifactId>
  <version>3.12.2</version>
  <scope>test</scope>
</dependency>
<!-- https://mvnrepository.com/artifact/org.junit.jupiter/junit-jupiter -->
<dependency>
  <groupId>org.junit.jupiter</groupId>
  <artifactId>junit-jupiter</artifactId>
  <version>5.5.0-M1</version>
  <scope>test</scope>
```

```
</dependency>
<!-- https://mvnrepository.com/artifact/org.mockito/mockito-core -->
<dependency>
  <groupId>org.mockito</groupId>
  <artifactId>mockito-core</artifactId>
  <version>3.6.0</version>
  <scope>test</scope>
</dependency>
<!-- https://mvnrepository.com/artifact/org.mockito/mockito-junit-jupiter -->
<dependency>
  <groupId>org.mockito</groupId>
  <artifactId>mockito-junit-jupiter</artifactId>
  <version>3.6.0</version>
  <scope>test</scope>
</dependency>
</dependencies>

<build>
  <plugins>
    <plugin>
      <groupId>org.apache.maven.plugins</groupId>
      <artifactId>maven-compiler-plugin</artifactId>
      <version>3.8.1</version>
      <configuration>
        <compilerArgs>
          <arg>-Xlint:all, -options, -processing</arg>
        </compilerArgs>
      </configuration>
    </plugin>
    <plugin>
      <groupId>org.apache.maven.plugins</groupId>
      <artifactId>maven-shade-plugin</artifactId>
      <version>2.3</version>
      <configuration>
        <createDependencyReducedPom>>false</createDependencyReducedPom>
        <filters>
          <filter>
            <artifact>*:*</artifact>
            <excludes>
              <exclude>**/Log4j2Plugins.dat</exclude>
            </excludes>
          </filter>
        </filters>
      </configuration>
    </plugin>
  </plugins>
</build>
```

```

        <executions>
            <execution>
                <phase>package</phase>
                <goals>
                    <goal>shade</goal>
                </goals>
            </execution>
        </executions>
    </plugin>
    <plugin>
        <groupId>org.codehaus.mojo</groupId>
        <artifactId>exec-maven-plugin</artifactId>
        <version>1.6.0</version>
        <executions>
            <execution>
                <id>generate</id>
                <phase>generate-sources</phase>
                <goals>
                    <goal>exec</goal>
                </goals>
                <configuration>
                    <executable>cfn</executable>
                    <commandlineArgs>generate ${cfn.generate.args}</
commandlineArgs>
                    <workingDirectory>${project.basedir}</workingDirectory>
                </configuration>
            </execution>
        </executions>
    </plugin>
    <plugin>
        <groupId>org.codehaus.mojo</groupId>
        <artifactId>build-helper-maven-plugin</artifactId>
        <version>3.0.0</version>
        <executions>
            <execution>
                <id>add-source</id>
                <phase>generate-sources</phase>
                <goals>
                    <goal>add-source</goal>
                </goals>
                <configuration>
                    <sources>
                        <source>${project.basedir}/target/generated-sources/
rpdk</source>

```



```
        </sources>
      </configuration>
    </execution>
  </executions>
</plugin>
<plugin>
  <groupId>org.apache.maven.plugins</groupId>
  <artifactId>maven-resources-plugin</artifactId>
  <version>2.4</version>
</plugin>
<plugin>
  <artifactId>maven-surefire-plugin</artifactId>
  <version>3.0.0-M3</version>
</plugin>
<plugin>
  <groupId>org.jacoco</groupId>
  <artifactId>jacoco-maven-plugin</artifactId>
  <version>0.8.4</version>
  <configuration>
    <excludes>
      <exclude>**/BaseHookConfiguration*</exclude>
      <exclude>**/BaseHookHandler*</exclude>
      <exclude>**/HookHandlerWrapper*</exclude>
      <exclude>**/ResourceModel*</exclude>
      <exclude>**/TypeConfigurationModel*</exclude>
      <exclude>**/model/**/*</exclude>
    </excludes>
  </configuration>
  <executions>
    <execution>
      <goals>
        <goal>prepare-agent</goal>
      </goals>
    </execution>
    <execution>
      <id>report</id>
      <phase>test</phase>
      <goals>
        <goal>report</goal>
      </goals>
    </execution>
    <execution>
      <id>jacoco-check</id>
      <goals>
```

```

        <goal>check</goal>
    </goals>
    <configuration>
        <rules>
            <rule>
                <element>PACKAGE</element>
                <limits>
                    <limit>
                        <counter>BRANCH</counter>
                        <value>COVEREDRATIO</value>
                        <minimum>0.8</minimum>
                    </limit>
                    <limit>
                        <counter>INSTRUCTION</counter>
                        <value>COVEREDRATIO</value>
                        <minimum>0.8</minimum>
                    </limit>
                </limits>
            </rule>
        </rules>
    </configuration>
</execution>
</executions>
</plugin>
</plugins>
<resources>
    <resource>
        <directory>${project.basedir}</directory>
        <includes>
            <include>mycompany-testing-mytesthook.json</include>
        </includes>
    </resource>
    <resource>
        <directory>${project.basedir}/target/loaded-target-schemas</directory>
        <includes>
            <include>**/*.json</include>
        </includes>
    </resource>
</resources>
</build>
</project>

```

步驟 2：產生勾點專案套件

產生您的 Hook 專案套件。CloudFormation CLI 會建立空的處理常式函數，其對應至目標生命週期中的特定 Hook 動作，如 Hook 規格所定義。

```
cfn generate
```

命令會傳回下列輸出：

```
Generated files for MyCompany::Testing::MyTestHook
```

Note

確保您的 Lambda 執行時間是 up-to-date，以避免使用已棄用版本。如需詳細資訊，請參閱 [更](#)
[新資源類型和勾點的 Lambda 執行時間](#)。

步驟 3：新增勾點處理常式

將您自己的 Hook 處理常式執行時間程式碼新增至您選擇實作的處理常式。例如，您可以新增下列程式碼進行記錄。

```
logger.log("Internal testing Hook triggered for target: " +  
request.getHookContext().getTargetName());
```

CloudFormation CLI 會產生純舊 Java 物件 (Java POJO)。以下是從產生的輸出範例 `AWS::S3::Bucket`。

Example `AwsS3BucketTargetModel.java`

```
package com.mycompany.testing.mytesthook.model.aws.s3.bucket;  
  
import...  
  
@Data  
@NoArgsConstructor  
@EqualsAndHashCode(callSuper = true)  
@ToString(callSuper = true)
```

```

@JsonAutoDetect(fieldVisibility = Visibility.ANY, getterVisibility = Visibility.NONE,
    setterVisibility = Visibility.NONE)
public class AwsS3BucketTargetModel extends ResourceHookTargetModel<AwsS3Bucket> {

    @JsonIgnore
    private static final TypeReference<AwsS3Bucket> TARGET_REFERENCE =
        new TypeReference<AwsS3Bucket>() {};

    @JsonIgnore
    private static final TypeReference<AwsS3BucketTargetModel> MODEL_REFERENCE =
        new TypeReference<AwsS3BucketTargetModel>() {};

    @JsonIgnore
    public static final String TARGET_TYPE_NAME = "AWS::S3::Bucket";

    @JsonIgnore
    public TypeReference<AwsS3Bucket> getHookTargetTypeReference() {
        return TARGET_REFERENCE;
    }

    @JsonIgnore
    public TypeReference<AwsS3BucketTargetModel> getTargetModelTypeReference() {
        return MODEL_REFERENCE;
    }
}

```

Example AwsS3Bucket.java

```

package com.mycompany.testing.mytesthook.model.aws.s3.bucket;

import ...

@Data
@Builder
@AllArgsConstructor
@NoArgsConstructor
@EqualsAndHashCode(callSuper = true)
@ToString(callSuper = true)
@JsonAutoDetect(fieldVisibility = Visibility.ANY, getterVisibility = Visibility.NONE,
    setterVisibility = Visibility.NONE)
public class AwsS3Bucket extends ResourceHookTarget {

```

```
@JsonIgnore
public static final String TYPE_NAME = "AWS::S3::Bucket";

@JsonIgnore
public static final String IDENTIFIER_KEY_ID = "/properties/Id";

@JsonProperty("InventoryConfigurations")
private List<InventoryConfiguration> inventoryConfigurations;

@JsonProperty("WebsiteConfiguration")
private WebsiteConfiguration websiteConfiguration;

@JsonProperty("DualStackDomainName")
private String dualStackDomainName;

@JsonProperty("AccessControl")
private String accessControl;

@JsonProperty("AnalyticsConfigurations")
private List<AnalyticsConfiguration> analyticsConfigurations;

@JsonProperty("AccelerateConfiguration")
private AccelerateConfiguration accelerateConfiguration;

@JsonProperty("PublicAccessBlockConfiguration")
private PublicAccessBlockConfiguration publicAccessBlockConfiguration;

@JsonProperty("BucketName")
private String bucketName;

@JsonProperty("RegionalDomainName")
private String regionalDomainName;

@JsonProperty("OwnershipControls")
private OwnershipControls ownershipControls;

@JsonProperty("ObjectLockConfiguration")
private ObjectLockConfiguration objectLockConfiguration;

@JsonProperty("ObjectLockEnabled")
private Boolean objectLockEnabled;

@JsonProperty("LoggingConfiguration")
private LoggingConfiguration loggingConfiguration;
```

```
@JsonProperty("ReplicationConfiguration")
private ReplicationConfiguration replicationConfiguration;

@JsonProperty("Tags")
private List<Tag> tags;

@JsonProperty("DomainName")
private String domainName;

@JsonProperty("BucketEncryption")
private BucketEncryption bucketEncryption;

@JsonProperty("WebsiteURL")
private String websiteURL;

@JsonProperty("NotificationConfiguration")
private NotificationConfiguration notificationConfiguration;

@JsonProperty("LifecycleConfiguration")
private LifecycleConfiguration lifecycleConfiguration;

@JsonProperty("VersioningConfiguration")
private VersioningConfiguration versioningConfiguration;

@JsonProperty("MetricsConfigurations")
private List<MetricsConfiguration> metricsConfigurations;

@JsonProperty("IntelligentTieringConfigurations")
private List<IntelligentTieringConfiguration> intelligentTieringConfigurations;

@JsonProperty("CorsConfiguration")
private CorsConfiguration corsConfiguration;

@JsonProperty("Id")
private String id;

@JsonProperty("Arn")
private String arn;

@JsonPropertyIgnore
public JSONObject getPrimaryIdentifier() {
    final JSONObject identifier = new JSONObject();
    if (this.getId() != null) {
```

```
        identifier.put(IDENTIFIER_KEY_ID, this.getId());
    }

    // only return the identifier if it can be used, i.e. if all components are
    present
    return identifier.length() == 1 ? identifier : null;
}

@JsonIgnore
public List<JSONObject> getAdditionalIdentifiers() {
    final List<JSONObject> identifiers = new ArrayList<JSONObject>();
    // only return the identifiers if any can be used
    return identifiers.isEmpty() ? null : identifiers;
}
}
```

Example BucketEncryption.java

```
package software.amazon.testing.mytesthook.model.aws.s3.bucket;

import ...

@Data
@Builder
@AllArgsConstructor
@NoArgsConstructor
@JsonAutoDetect(fieldVisibility = Visibility.ANY, getterVisibility = Visibility.NONE,
    setterVisibility = Visibility.NONE)
public class BucketEncryption {
    @JsonProperty("ServerSideEncryptionConfiguration")
    private List<ServerSideEncryptionRule> serverSideEncryptionConfiguration;
}
}
```

Example ServerSideEncryptionRule.java

```
package com.mycompany.testing.mytesthook.model.aws.s3.bucket;

import ...

@Data
```

```
@Builder
@AllArgsConstructor
@NoArgsConstructor
@JsonAutoDetect(fieldVisibility = Visibility.ANY, getterVisibility = Visibility.NONE,
    setterVisibility = Visibility.NONE)
public class ServerSideEncryptionRule {
    @JsonProperty("BucketKeyEnabled")
    private Boolean bucketKeyEnabled;

    @JsonProperty("ServerSideEncryptionByDefault")
    private ServerSideEncryptionByDefault serverSideEncryptionByDefault;
}
```

Example ServerSideEncryptionByDefault.java

```
package com.mycompany.testing.mytesthook.model.aws.s3.bucket;

import ...

@Data
@Builder
@AllArgsConstructor
@NoArgsConstructor
@JsonAutoDetect(fieldVisibility = Visibility.ANY, getterVisibility = Visibility.NONE,
    setterVisibility = Visibility.NONE)
public class ServerSideEncryptionByDefault {
    @JsonProperty("SSEAlgorithm")
    private String sSEAlgorithm;

    @JsonProperty("KMSMasterKeyID")
    private String kMSMasterKeyID;
}
```

產生 POJOs 後，您現在可以撰寫實際實作 Hook 功能的處理常式。在此範例中，請實作處理常式的 `preCreate` 和 `preUpdate` 呼叫點。

步驟 4：實作勾點處理常式

主題

- [編碼 API 用戶端建置器](#)

- [編碼 API 請求建立器](#)
- [實作協助程式程式碼](#)
- [實作基本處理常式](#)
- [實作preCreate處理常式](#)
- [編碼preCreate處理常式](#)
- [更新preCreate測試](#)
- [實作preUpdate處理常式](#)
- [編碼preUpdate處理常式](#)
- [更新preUpdate測試](#)
- [實作preDelete處理常式](#)
- [編碼preDelete處理常式](#)
- [更新preDelete處理常式](#)

編碼 API 用戶端建置器

1. 在您的 IDE 中，開啟ClientBuilder.java位於 src/main/java/com/mycompany/testing/mytesthook 資料夾的檔案。
2. 使用下列程式碼取代ClientBuilder.java檔案的整個內容。

Example ClientBuilder.java

```
package com.awscommunity.kms.encryptionsettings;

import software.amazon.awssdk.services.ec2.Ec2Client;
import software.amazon.cloudformation.HookLambdaWrapper;

/**
 * Describes static HTTP clients (to consume less memory) for API calls that
 * this hook makes to a number of AWS services.
 */
public final class ClientBuilder {

    private ClientBuilder() {
    }

    /**
     * Create an HTTP client for Amazon EC2.
     */
}
```

```
    *
    * @return Ec2Client An {@link Ec2Client} object.
    */
    public static Ec2Client getEc2Client() {
        return
        Ec2Client.builder().httpClient(HookLambdaWrapper.HTTP_CLIENT).build();
    }
}
```

編碼 API 請求建立器

1. 在您的 IDE 中，開啟 `Translator.java` 位於 `src/main/java/com/mycompany/testing/mytesthook` 資料夾的檔案。
2. 使用下列程式碼取代 `Translator.java` 檔案的整個內容。

Example Translator.java

```
package com.mycompany.testing.mytesthook;

import software.amazon.awssdk.services.s3.model.GetBucketEncryptionRequest;
import software.amazon.awssdk.services.s3.model.ListBucketsRequest;
import software.amazon.awssdk.services.sqs.model.ListQueuesRequest;
import software.amazon.cloudformation.proxy.hook.targetmodel.HookTargetModel;

/**
 * This class is a centralized placeholder for
 * - api request construction
 * - object translation to/from aws sdk
 */

public class Translator {

    static ListBucketsRequest translateToListBucketsRequest(final HookTargetModel
targetModel) {
        return ListBucketsRequest.builder().build();
    }

    static ListQueuesRequest translateToListQueuesRequest(final String nextToken) {
        return ListQueuesRequest.builder().nextToken(nextToken).build();
    }
}
```

```
static ListBucketsRequest createListBucketsRequest() {
    return ListBucketsRequest.builder().build();
}

static ListQueuesRequest createListQueuesRequest() {
    return createListQueuesRequest(null);
}

static ListQueuesRequest createListQueuesRequest(final String nextToken) {
    return ListQueuesRequest.builder().nextToken(nextToken).build();
}

static GetBucketEncryptionRequest createGetBucketEncryptionRequest(final String
bucket) {
    return GetBucketEncryptionRequest.builder().bucket(bucket).build();
}
}
```

實作協助程式程式碼

1. 在您的 IDE 中，開啟 `AbstractTestBase.java` 位於 `src/main/java/com/mycompany/testing/mytesthook` 資料夾的檔案。
2. 使用下列程式碼取代 `AbstractTestBase.java` 檔案的整個內容。

Example Translator.java

```
package com.mycompany.testing.mytesthook;

import com.google.common.collect.ImmutableMap;
import org.mockito.Mockito;
import software.amazon.awssdk.auth.credentials.AwsCredentialsProvider;
import software.amazon.awssdk.auth.credentials.AwsSessionCredentials;
import software.amazon.awssdk.auth.credentials.StaticCredentialsProvider;
import software.amazon.awssdk.awscore.AwsRequest;
import software.amazon.awssdk.awscore.AwsRequestOverrideConfiguration;
import software.amazon.awssdk.awscore.AwsResponse;
import software.amazon.awssdk.core.SdkClient;
import software.amazon.awssdk.core.pagination.sync.SdkIterable;
import software.amazon.cloudformation.proxy.AmazonWebServicesClientProxy;
import software.amazon.cloudformation.proxy.Credentials;
import software.amazon.cloudformation.proxy.LoggerProxy;
import software.amazon.cloudformation.proxy.OperationStatus;
```

```
import software.amazon.cloudformation.proxy.ProgressEvent;
import software.amazon.cloudformation.proxy.ProxyClient;
import software.amazon.cloudformation.proxy.hook.targetmodel.HookTargetModel;

import javax.annotation.Nonnull;
import java.time.Duration;
import java.util.concurrent.CompletableFuture;
import java.util.function.Function;
import java.util.function.Supplier;

import static org.assertj.core.api.Assertions.assertThat;

@lombok.Getter
public class AbstractTestBase {
    protected final AwsSessionCredentials awsSessionCredential;
    protected final AwsCredentialsProvider v2CredentialsProvider;
    protected final AwsRequestOverrideConfiguration configuration;
    protected final LoggerProxy loggerProxy;
    protected final Supplier<Long> awsLambdaRuntime = () ->
Duration.ofMinutes(15).toMillis();
    protected final AmazonWebServicesClientProxy proxy;
    protected final Credentials mockCredentials =
        new Credentials("mockAccessId", "mockSecretKey", "mockSessionToken");

    @lombok.Setter
    private SdkClient serviceClient;

    protected AbstractTestBase() {
        loggerProxy = Mockito.mock(LoggerProxy.class);
        awsSessionCredential =
AwsSessionCredentials.create(mockCredentials.getAccessKeyId(),
        mockCredentials.getSecretAccessKey(),
mockCredentials.getSessionToken());
        v2CredentialsProvider =
StaticCredentialsProvider.create(awsSessionCredential);
        configuration = AwsRequestOverrideConfiguration.builder()
            .credentialsProvider(v2CredentialsProvider)
            .build();
        proxy = new AmazonWebServicesClientProxy(
            loggerProxy,
            mockCredentials,
            awsLambdaRuntime
        ) {
            @Override
```

```

        public <ClientT> ProxyClient<ClientT> newProxy(@NonNull
Supplier<ClientT> client) {
            return new ProxyClient<ClientT>() {
                @Override
                public <RequestT extends AwsRequest, ResponseT extends
AwsResponse>
                    ResponseT injectCredentialsAndInvokeV2(RequestT request,
Function<RequestT,
ResponseT> requestFunction) {
                        return proxy.injectCredentialsAndInvokeV2(request,
requestFunction);
                    }

                @Override
                public <RequestT extends AwsRequest, ResponseT extends
AwsResponse> CompletableFuture<ResponseT>
                    injectCredentialsAndInvokeV2Async(RequestT request,
Function<RequestT, CompletableFuture<ResponseT>> requestFunction) {
                        return proxy.injectCredentialsAndInvokeV2Async(request,
requestFunction);
                    }

                @Override
                public <RequestT extends AwsRequest, ResponseT extends
AwsResponse, IterableT extends SdkIterable<ResponseT>>
                    IterableT
                    injectCredentialsAndInvokeIterableV2(RequestT request,
Function<RequestT, IterableT> requestFunction) {
                        return proxy.injectCredentialsAndInvokeIterableV2(request,
requestFunction);
                    }

                @SuppressWarnings("unchecked")
                @Override
                public ClientT client() {
                    return (ClientT) serviceClient;
                }
            };
        }
    };
}

```

```

protected void assertResponse(final ProgressEvent<HookTargetModel,
CallbackContext> response, final OperationStatus expectedStatus, final String
expectedMsg) {
    assertThat(response).isNotNull();
    assertThat(response.getStatus()).isEqualTo(expectedStatus);
    assertThat(response.getCallbackContext()).isNull();
    assertThat(response.getCallbackDelaySeconds()).isEqualTo(0);
    assertThat(response.getMessage()).isNotNull();
    assertThat(response.getMessage()).isEqualTo(expectedMsg);
}

protected HookTargetModel createHookTargetModel(final Object
resourceProperties) {
    return HookTargetModel.of(ImmutableMap.of("ResourceProperties",
resourceProperties));
}

protected HookTargetModel createHookTargetModel(final Object
resourceProperties, final Object previousResourceProperties) {
    return HookTargetModel.of(
        ImmutableMap.of(
            "ResourceProperties", resourceProperties,
            "PreviousResourceProperties", previousResourceProperties
        )
    );
}
}

```

實作基本處理常式

1. 在您的 IDE 中，開啟 `BaseHookHandlerStd.java` 位於 `src/main/java/com/mycompany/testing/mytesthook` 資料夾的檔案。
2. 使用下列程式碼取代 `BaseHookHandlerStd.java` 檔案的整個內容。

Example Translator.java

```

package com.mycompany.testing.mytesthook;

import com.mycompany.testing.mytesthook.model.aws.s3.bucket.AwsS3Bucket;
import com.mycompany.testing.mytesthook.model.aws.sqs.queue.AwsSqsQueue;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.sqs.SqsClient;

```

```
import software.amazon.cloudformation.exceptions.UnsupportedTargetException;
import software.amazon.cloudformation.proxy.AmazonWebServicesClientProxy;
import software.amazon.cloudformation.proxy.Logger;
import software.amazon.cloudformation.proxy.ProgressEvent;
import software.amazon.cloudformation.proxy.ProxyClient;
import software.amazon.cloudformation.proxy.hook.HookHandlerRequest;
import software.amazon.cloudformation.proxy.hook.targetmodel.HookTargetModel;

public abstract class BaseHookHandlerStd extends BaseHookHandler<CallbackContext,
    TypeConfigurationModel> {
    public static final String HOOK_TYPE_NAME = "MyCompany::Testing::MyTestHook";

    protected Logger logger;

    @Override
    public ProgressEvent<HookTargetModel, CallbackContext> handleRequest(
        final AmazonWebServicesClientProxy proxy,
        final HookHandlerRequest request,
        final CallbackContext callbackContext,
        final Logger logger,
        final TypeConfigurationModel typeConfiguration
    ) {
        this.logger = logger;

        final String targetName = request.getHookContext().getTargetName();

        final ProgressEvent<HookTargetModel, CallbackContext> result;
        if (AwsS3Bucket.TYPE_NAME.equals(targetName)) {
            result = handleS3BucketRequest(
                proxy,
                request,
                callbackContext != null ? callbackContext : new
                CallbackContext(),
                proxy.newProxy(ClientBuilder::createS3Client),
                typeConfiguration
            );
        } else if (AwsSqsQueue.TYPE_NAME.equals(targetName)) {
            result = handleSqsQueueRequest(
                proxy,
                request,
                callbackContext != null ? callbackContext : new
                CallbackContext(),
                proxy.newProxy(ClientBuilder::createSqsClient),
```

```
        typeConfiguration
    );
} else {
    throw new UnsupportedTargetException(targetName);
}

log(
    String.format(
        "Result for [%s] invocation for target [%s] returned status [%s]
with message [%s]",
        request.getHookContext().getInvocationPoint(),
        targetName,
        result.getStatus(),
        result.getMessage()
    )
);

return result;
}

protected abstract ProgressEvent<HookTargetModel, CallbackContext>
handleS3BucketRequest(
    final AmazonWebServicesClientProxy proxy,
    final HookHandlerRequest request,
    final CallbackContext callbackContext,
    final ProxyClient<S3Client> proxyClient,
    final TypeConfigurationModel typeConfiguration
);

protected abstract ProgressEvent<HookTargetModel, CallbackContext>
handleSqsQueueRequest(
    final AmazonWebServicesClientProxy proxy,
    final HookHandlerRequest request,
    final CallbackContext callbackContext,
    final ProxyClient<SqsClient> proxyClient,
    final TypeConfigurationModel typeConfiguration
);

protected void log(final String message) {
    if (logger != null) {
        logger.log(message);
    } else {
        System.out.println(message);
    }
}
```



```
}  
}
```

實作preCreate處理常式

preCreate 處理常式會驗證 AWS::S3::Bucket 或 AWS::SQS::Queue 資源的伺服器端加密設定。

- 對於 AWS::S3::Bucket 資源，勾點只有在下列情況為 true 時才會傳遞：
 - Amazon S3 儲存貯體加密已設定。
 - 已啟用儲存貯體的 Amazon S3 儲存貯體金鑰。
 - Amazon S3 儲存貯體的加密演算法集是所需的正確演算法。
 - AWS Key Management Service 金鑰 ID 已設定。
- 對於 AWS::SQS::Queue 資源，勾點只會在下列情況為 true 時傳遞：
 - AWS Key Management Service 金鑰 ID 已設定。

編碼preCreate處理常式

1. 在您的 IDE 中，開啟 PreCreateHookHandler.java 位於 src/main/java/software/mycompany/testing/mytesthook 資料夾的檔案。
2. 使用下列程式碼取代 PreCreateHookHandler.java 檔案的整個內容。

```
package com.mycompany.testing.mytesthook;  
  
import com.mycompany.testing.mytesthook.model.aws.s3.bucket.AwsS3Bucket;  
import com.mycompany.testing.mytesthook.model.aws.s3.bucket.AwsS3BucketTargetModel;  
import com.mycompany.testing.mytesthook.model.aws.s3.bucket.BucketEncryption;  
import  
    com.mycompany.testing.mytesthook.model.aws.s3.bucket.ServerSideEncryptionByDefault;  
import  
    com.mycompany.testing.mytesthook.model.aws.s3.bucket.ServerSideEncryptionRule;  
import com.mycompany.testing.mytesthook.model.aws.sqs.queue.AwsSqsQueue;  
import com.mycompany.testing.mytesthook.model.aws.sqs.queue.AwsSqsQueueTargetModel;  
import org.apache.commons.collections.CollectionUtils;  
import org.apache.commons.lang3.StringUtils;  
import software.amazon.cloudformation.exceptions.UnsupportedTargetException;  
import software.amazon.cloudformation.proxy.HandlerErrorCode;  
import software.amazon.cloudformation.proxy.Logger;  
import software.amazon.cloudformation.proxy.AmazonWebServicesClientProxy;
```

```
import software.amazon.cloudformation.proxy.hook.HookStatus;
import software.amazon.cloudformation.proxy.hook.HookProgressEvent;
import software.amazon.cloudformation.proxy.hook.HookHandlerRequest;
import
    software.amazon.cloudformation.proxy.hook.targetmodel.ResourceHookTargetModel;

import java.util.List;

public class PreCreateHookHandler extends BaseHookHandler<TypeConfigurationModel,
    CallbackContext> {

    @Override
    public HookProgressEvent<CallbackContext> handleRequest(
        final AmazonWebServicesClientProxy proxy,
        final HookHandlerRequest request,
        final CallbackContext callbackContext,
        final Logger logger,
        final TypeConfigurationModel typeConfiguration) {

        final String targetName = request.getHookContext().getTargetName();
        if ("AWS::S3::Bucket".equals(targetName)) {
            final ResourceHookTargetModel<AwsS3Bucket> targetModel =
request.getHookContext().getTargetModel(AwsS3BucketTargetModel.class);

            final AwsS3Bucket bucket = targetModel.getResourceProperties();
            final String encryptionAlgorithm =
typeConfiguration.getEncryptionAlgorithm();

            return validateS3BucketEncryption(bucket, encryptionAlgorithm);

        } else if ("AWS::SQS::Queue".equals(targetName)) {
            final ResourceHookTargetModel<AwsSqsQueue> targetModel =
request.getHookContext().getTargetModel(AwsSqsQueueTargetModel.class);

            final AwsSqsQueue queue = targetModel.getResourceProperties();
            return validateSQSQueueEncryption(queue);
        } else {
            throw new UnsupportedTargetException(targetName);
        }
    }

    private HookProgressEvent<CallbackContext> validateS3BucketEncryption(final
    AwsS3Bucket bucket, final String requiredEncryptionAlgorithm) {
        HookStatus resultStatus = null;
    }
}
```

```
String resultMessage = null;

if (bucket != null) {
    final BucketEncryption bucketEncryption = bucket.getBucketEncryption();
    if (bucketEncryption != null) {
        final List<ServerSideEncryptionRule> serverSideEncryptionRules =
bucketEncryption.getServerSideEncryptionConfiguration();
        if (CollectionUtils.isNotEmpty(serverSideEncryptionRules)) {
            for (final ServerSideEncryptionRule rule :
serverSideEncryptionRules) {
                final Boolean bucketKeyEnabled =
rule.getBucketKeyEnabled();
                if (bucketKeyEnabled) {
                    final ServerSideEncryptionByDefault
serverSideEncryptionByDefault = rule.getServerSideEncryptionByDefault();

                    final String encryptionAlgorithm =
serverSideEncryptionByDefault.getSSEAlgorithm();
                    final String kmsKeyId =
serverSideEncryptionByDefault.getKMSTMasterKeyID(); // "KMSTMasterKeyID" is name of
the property for an AWS::S3::Bucket;

                    if (!StringUtils.equals(encryptionAlgorithm,
requiredEncryptionAlgorithm) && StringUtils.isBlank(kmsKeyId)) {
                        resultStatus = HookStatus.FAILED;
                        resultMessage = "KMS Key ID not set
and SSE Encryption Algorithm is incorrect for bucket with name: " +
bucket.getBucketName();
                    } else if (!StringUtils.equals(encryptionAlgorithm,
requiredEncryptionAlgorithm)) {
                        resultStatus = HookStatus.FAILED;
                        resultMessage = "SSE Encryption Algorithm is
incorrect for bucket with name: " + bucket.getBucketName();
                    } else if (StringUtils.isBlank(kmsKeyId)) {
                        resultStatus = HookStatus.FAILED;
                        resultMessage = "KMS Key ID not set for bucket with
name: " + bucket.getBucketName();
                    } else {
                        resultStatus = HookStatus.SUCCESS;
                        resultMessage = "Successfully invoked
PreCreateHookHandler for target: AWS::S3::Bucket";
                    }
                } else {
                    resultStatus = HookStatus.FAILED;
                }
            }
        }
    }
}
```

```
                resultMessage = "Bucket key not enabled for bucket with
name: " + bucket.getBucketName();
            }

            if (resultStatus == HookStatus.FAILED) {
                break;
            }
        } else {
            resultStatus = HookStatus.FAILED;
            resultMessage = "No SSE Encryption configurations for bucket
with name: " + bucket.getBucketName();
        }
    } else {
        resultStatus = HookStatus.FAILED;
        resultMessage = "Bucket Encryption not enabled for bucket with
name: " + bucket.getBucketName();
    }
} else {
    resultStatus = HookStatus.FAILED;
    resultMessage = "Resource properties for S3 Bucket target model are
empty";
}

return HookProgressEvent.<CallbackContext>builder()
    .status(resultStatus)
    .message(resultMessage)
    .errorCode(resultStatus == HookStatus.FAILED ?
HandlerErrorCode.ResourceConflict : null)
    .build();
}

private HookProgressEvent<CallbackContext> validateSQSQueueEncryption(final
AwsSqsQueue queue) {
    if (queue == null) {
        return HookProgressEvent.<CallbackContext>builder()
            .status(HookStatus.FAILED)
            .message("Resource properties for SQS Queue target model are
empty")
            .errorCode(HandlerErrorCode.ResourceConflict)
            .build();
    }
}
```

```
        final String kmsKeyId = queue.getKmsMasterKeyId(); // "KmsMasterKeyId" is
name of the property for an AWS::SQS::Queue
        if (StringUtils.isBlank(kmsKeyId)) {
            return HookProgressEvent.<CallbackContext>builder()
                .status(HookStatus.FAILED)
                .message("Server side encryption turned off for queue with
name: " + queue.getQueueName())
                .errorCode(HandlerErrorCode.ResourceConflict)
                .build();
        }

        return HookProgressEvent.<CallbackContext>builder()
            .status(HookStatus.SUCCESS)
            .message("Successfully invoked PreCreateHookHandler for target:
AWS::SQS::Queue")
            .build();
    }
}
```

更新preCreate測試

1. 在 IDE 中，開啟PreCreateHandlerTest.java位於 src/test/java/software/mycompany/testing/mytesthook 資料夾的檔案。
2. 使用下列程式碼取代PreCreateHandlerTest.java檔案的整個內容。

```
package com.mycompany.testing.mytesthook;

import com.google.common.collect.ImmutableMap;
import com.mycompany.testing.mytesthook.model.aws.s3.bucket.AwsS3Bucket;
import com.mycompany.testing.mytesthook.model.aws.s3.bucket.BucketEncryption;
import
    com.mycompany.testing.mytesthook.model.aws.s3.bucket.ServerSideEncryptionByDefault;
import
    com.mycompany.testing.mytesthook.model.aws.s3.bucket.ServerSideEncryptionRule;
import com.mycompany.testing.mytesthook.model.aws.sqs.queue.AwsSqsQueue;
import org.junit.jupiter.api.BeforeEach;
import org.junit.jupiter.api.Test;
import org.junit.jupiter.api.extension.ExtendWith;
import org.mockito.Mock;
import org.mockito.junit.jupiter.MockitoExtension;
import software.amazon.cloudformation.exceptions.UnsupportedTargetException;
import software.amazon.cloudformation.proxy.AmazonWebServicesClientProxy;
```

```
import software.amazon.cloudformation.proxy.HandlerErrorCode;
import software.amazon.cloudformation.proxy.Logger;
import software.amazon.cloudformation.proxy.hook.HookContext;
import software.amazon.cloudformation.proxy.hook.HookHandlerRequest;
import software.amazon.cloudformation.proxy.hook.HookProgressEvent;
import software.amazon.cloudformation.proxy.hook.HookStatus;
import software.amazon.cloudformation.proxy.hook.targetmodel.HookTargetModel;

import java.util.Collections;
import java.util.Map;

import static org.assertj.core.api.Assertions.assertThat;
import static org.assertj.core.api.Assertions.assertThatExceptionOfType;
import static org.mockito.Mockito.mock;

@ExtendWith(MockitoExtension.class)
public class PreCreateHookHandlerTest {

    @Mock
    private AmazonWebServicesClientProxy proxy;

    @Mock
    private Logger logger;

    @BeforeEach
    public void setup() {
        proxy = mock(AmazonWebServicesClientProxy.class);
        logger = mock(Logger.class);
    }

    @Test
    public void handleRequest_awsSqsQueueSuccess() {
        final PreCreateHookHandler handler = new PreCreateHookHandler();

        final AwsSqsQueue queue = buildSqsQueue("MyQueue", "KmsKey");
        final HookTargetModel targetModel = createHookTargetModel(queue);
        final TypeConfigurationModel typeConfiguration =
TypeConfigurationModel.builder().encryptionAlgorithm("AES256").build();

        final HookHandlerRequest request = HookHandlerRequest.builder()

        .hookContext(HookContext.builder().targetName("AWS::SQS::Queue").targetModel(targetModel)
        .build());
    }
}
```

```
        final HookProgressEvent<CallbackContext> response =
handler.handleRequest(proxy, request, null, logger, typeConfiguration);
        assertResponse(response, HookStatus.SUCCESS, "Successfully invoked
PreCreateHookHandler for target: AWS::SQS::Queue");
    }

    @Test
    public void handleRequest_awsS3BucketSuccess() {
        final PreCreateHookHandler handler = new PreCreateHookHandler();

        final AwsS3Bucket bucket = buildAwsS3Bucket("amzn-s3-demo-bucket", true,
"AES256", "KmsKey");
        final HookTargetModel targetModel = createHookTargetModel(bucket);
        final TypeConfigurationModel typeConfiguration =
TypeConfigurationModel.builder().encryptionAlgorithm("AES256").build();

        final HookHandlerRequest request = HookHandlerRequest.builder()

.hookContext(HookContext.builder().targetName("AWS::S3::Bucket").targetModel(targetModel)
        .build());

        final HookProgressEvent<CallbackContext> response =
handler.handleRequest(proxy, request, null, logger, typeConfiguration);
        assertResponse(response, HookStatus.SUCCESS, "Successfully invoked
PreCreateHookHandler for target: AWS::S3::Bucket");
    }

    @Test
    public void handleRequest_awsS3BucketFail_bucketKeyNotEnabled() {
        final PreCreateHookHandler handler = new PreCreateHookHandler();

        final AwsS3Bucket bucket = buildAwsS3Bucket("amzn-s3-demo-bucket", false,
"AES256", "KmsKey");
        final HookTargetModel targetModel = createHookTargetModel(bucket);
        final TypeConfigurationModel typeConfiguration =
TypeConfigurationModel.builder().encryptionAlgorithm("AES256").build();

        final HookHandlerRequest request = HookHandlerRequest.builder()

.hookContext(HookContext.builder().targetName("AWS::S3::Bucket").targetModel(targetModel)
        .build());

        final HookProgressEvent<CallbackContext> response =
handler.handleRequest(proxy, request, null, logger, typeConfiguration);
```

```
        assertResponse(response, HookStatus.FAILED, "Bucket key not enabled for
bucket with name: amzn-s3-demo-bucket");
    }

    @Test
    public void handleRequest_awsS3BucketFail_incorrectSSEEncryptionAlgorithm() {
        final PreCreateHookHandler handler = new PreCreateHookHandler();

        final AwsS3Bucket bucket = buildAwsS3Bucket("amzn-s3-demo-bucket", true,
"SHA512", "KmsKey");
        final HookTargetModel targetModel = createHookTargetModel(bucket);
        final TypeConfigurationModel typeConfiguration =
TypeConfigurationModel.builder().encryptionAlgorithm("AES256").build();

        final HookHandlerRequest request = HookHandlerRequest.builder()

.hookContext(HookContext.builder().targetName("AWS::S3::Bucket").targetModel(targetModel)
        .build());

        final HookProgressEvent<CallbackContext> response =
handler.handleRequest(proxy, request, null, logger, typeConfiguration);
        assertResponse(response, HookStatus.FAILED, "SSE Encryption Algorithm is
incorrect for bucket with name: amzn-s3-demo-bucket");
    }

    @Test
    public void handleRequest_awsS3BucketFail_kmsKeyIdNotSet() {
        final PreCreateHookHandler handler = new PreCreateHookHandler();

        final AwsS3Bucket bucket = buildAwsS3Bucket("amzn-s3-demo-bucket", true,
"AES256", null);
        final HookTargetModel targetModel = createHookTargetModel(bucket);
        final TypeConfigurationModel typeConfiguration =
TypeConfigurationModel.builder().encryptionAlgorithm("AES256").build();

        final HookHandlerRequest request = HookHandlerRequest.builder()

.hookContext(HookContext.builder().targetName("AWS::S3::Bucket").targetModel(targetModel)
        .build());

        final HookProgressEvent<CallbackContext> response =
handler.handleRequest(proxy, request, null, logger, typeConfiguration);
        assertResponse(response, HookStatus.FAILED, "KMS Key ID not set for bucket
with name: amzn-s3-demo-bucket");
    }
}
```



```
}

@Test
public void handleRequest_awsSqsQueueFail_serverSideEncryptionOff() {
    final PreCreateHookHandler handler = new PreCreateHookHandler();

    final AwsSqsQueue queue = buildSqsQueue("MyQueue", null);
    final HookTargetModel targetModel = createHookTargetModel(queue);
    final TypeConfigurationModel typeConfiguration =
TypeConfigurationModel.builder().encryptionAlgorithm("AES256").build();

    final HookHandlerRequest request = HookHandlerRequest.builder()

.hookContext(HookContext.builder().targetName("AWS::SQS::Queue").targetModel(targetModel)
    .build());

    final HookProgressEvent<CallbackContext> response =
handler.handleRequest(proxy, request, null, logger, typeConfiguration);
    assertResponse(response, HookStatus.FAILED, "Server side encryption turned
off for queue with name: MyQueue");
}

@Test
public void handleRequest_unsupportedTarget() {
    final PreCreateHookHandler handler = new PreCreateHookHandler();

    final Map<String, Object> unsupportedTarget =
ImmutableMap.of("ResourceName", "MyUnsupportedTarget");
    final HookTargetModel targetModel =
createHookTargetModel(unsupportedTarget);
    final TypeConfigurationModel typeConfiguration =
TypeConfigurationModel.builder().encryptionAlgorithm("AES256").build();

    final HookHandlerRequest request = HookHandlerRequest.builder()

.hookContext(HookContext.builder().targetName("AWS::Unsupported::Target").targetModel(targ
    .build());

    assertThatExceptionOfType(UnsupportedTargetException.class)
        .isThrownBy(() -> handler.handleRequest(proxy, request, null,
logger, typeConfiguration))
        .withMessageContaining("Unsupported target")
        .withMessageContaining("AWS::Unsupported::Target")
}
```

```
        .satisfies(e ->
assertThat(e.getErrorCode()).isEqualTo(HandlerErrorCode.InvalidRequest));
    }

    private void assertResponse(final HookProgressEvent<CallbackContext> response,
final HookStatus expectedStatus, final String expectedErrorMsg) {
        assertThat(response).isNotNull();
        assertThat(response.getStatus()).isEqualTo(expectedStatus);
        assertThat(response.getCallbackContext()).isNull();
        assertThat(response.getCallbackDelaySeconds()).isEqualTo(0);
        assertThat(response.getMessage()).isNotNull();
        assertThat(response.getMessage()).isEqualTo(expectedErrorMsg);
    }

    private HookTargetModel createHookTargetModel(final Object resourceProperties)
{
        return HookTargetModel.of(ImmutableMap.of("ResourceProperties",
resourceProperties));
    }

    @SuppressWarnings("SameParameterValue")
    private AwsSqsQueue buildSqsQueue(final String queueName, final String
kmsKeyId) {
        return AwsSqsQueue.builder()
            .queueName(queueName)
            .kmsMasterKeyId(kmsKeyId) // "KmsMasterKeyId" is name of the
property for an AWS::SQS::Queue
            .build();
    }

    @SuppressWarnings("SameParameterValue")
    private AwsS3Bucket buildAwsS3Bucket(
        final String bucketName,
        final Boolean bucketKeyEnabled,
        final String sseAlgorithm,
        final String kmsKeyId
    ) {
        return AwsS3Bucket.builder()
            .bucketName(bucketName)
            .bucketEncryption(
                BucketEncryption.builder()
                    .serverSideEncryptionConfiguration(
                        Collections.singletonList(
                            ServerSideEncryptionRule.builder()

```

```

        .bucketKeyEnabled(bucketKeyEnabled)
        .serverSideEncryptionByDefault(
            ServerSideEncryptionByDefault.builder()
                .sSEAlgorithm(sseAlgorithm)
                .kMSMasterKeyID(kmsKeyId) //
                "KMSMasterKeyID" is name of the property for an AWS::S3::Bucket
                .build()
            ).build()
        )
    ).build()
).build();
}
}

```

實作preUpdate處理常式

實作preUpdate處理常式，其會在處理常式中所有指定目標的更新操作之前啟動。preUpdate 處理常式會完成下列項目：

- 對於 AWS::S3::Bucket 資源，勾點只有在下列情況為 true 時才會傳遞：
 - Amazon S3 儲存貯體的儲存貯體加密演算法尚未修改。

編碼preUpdate處理常式

1. 在您的 IDE 中，開啟PreUpdateHookHandler.java位於 src/main/java/software/mycompany/testing/mytesthook 資料夾的檔案。
2. 使用下列程式碼取代PreUpdateHookHandler.java檔案的整個內容。

```

package com.mycompany.testing.mytesthook;

import com.mycompany.testing.mytesthook.model.aws.s3.bucket.AwsS3Bucket;
import com.mycompany.testing.mytesthook.model.aws.s3.bucket.AwsS3BucketTargetModel;
import
    com.mycompany.testing.mytesthook.model.aws.s3.bucket.ServerSideEncryptionRule;
import org.apache.commons.lang3.StringUtils;
import software.amazon.cloudformation.exceptions.UnsupportedTargetException;
import software.amazon.cloudformation.proxy.HandlerErrorCode;
import software.amazon.cloudformation.proxy.Logger;
import software.amazon.cloudformation.proxy.AmazonWebServicesClientProxy;
import software.amazon.cloudformation.proxy.hook.HookStatus;

```

```
import software.amazon.cloudformation.proxy.hook.HookProgressEvent;
import software.amazon.cloudformation.proxy.hook.HookHandlerRequest;
import
    software.amazon.cloudformation.proxy.hook.targetmodel.ResourceHookTargetModel;

import java.util.List;

public class PreUpdateHookHandler extends BaseHookHandler<TypeConfigurationModel,
    CallbackContext> {

    @Override
    public HookProgressEvent<CallbackContext> handleRequest(
        final AmazonWebServicesClientProxy proxy,
        final HookHandlerRequest request,
        final CallbackContext callbackContext,
        final Logger logger,
        final TypeConfigurationModel typeConfiguration) {

        final String targetName = request.getHookContext().getTargetName();
        if ("AWS::S3::Bucket".equals(targetName)) {
            final ResourceHookTargetModel<AwsS3Bucket> targetModel =
                request.getHookContext().getTargetModel(AwsS3BucketTargetModel.class);

            final AwsS3Bucket bucketProperties =
                targetModel.getResourceProperties();
            final AwsS3Bucket previousBucketProperties =
                targetModel.getPreviousResourceProperties();

            return validateBucketEncryptionRulesNotUpdated(bucketProperties,
                previousBucketProperties);
        } else {
            throw new UnsupportedTargetException(targetName);
        }
    }

    private HookProgressEvent<CallbackContext>
        validateBucketEncryptionRulesNotUpdated(final AwsS3Bucket resourceProperties,
            final AwsS3Bucket previousResourceProperties) {
        final List<ServerSideEncryptionRule> bucketEncryptionConfigs =
            resourceProperties.getBucketEncryption().getServerSideEncryptionConfiguration();
        final List<ServerSideEncryptionRule> previousBucketEncryptionConfigs =
            previousResourceProperties.getBucketEncryption().getServerSideEncryptionConfiguration();
    }
}
```

```
        if (bucketEncryptionConfigs.size() !=
previousBucketEncryptionConfigs.size()) {
            return HookProgressEvent.<CallbackContext>builder()
                .status(HookStatus.FAILED)
                .errorCode(HandlerErrorCode.NotUpdatable)
                .message(
                    String.format(
                        "Current number of bucket encryption configs does not
match previous. Current has %d configs while previously there were %d configs",
                        bucketEncryptionConfigs.size(),
                        previousBucketEncryptionConfigs.size()
                    )
                )
                .build();
        }

        for (int i = 0; i < bucketEncryptionConfigs.size(); ++i) {
            final String currentEncryptionAlgorithm =
bucketEncryptionConfigs.get(i).getServerSideEncryptionByDefault().getSSEAlgorithm();
            final String previousEncryptionAlgorithm =
previousBucketEncryptionConfigs.get(i).getServerSideEncryptionByDefault().getSSEAlgorithm()

            if (!StringUtils.equals(currentEncryptionAlgorithm,
previousEncryptionAlgorithm)) {
                return HookProgressEvent.<CallbackContext>builder()
                    .status(HookStatus.FAILED)
                    .errorCode(HandlerErrorCode.NotUpdatable)
                    .message(
                        String.format(
                            "Bucket Encryption algorithm can not be changed once
set. The encryption algorithm was changed to '%s' from '%s'.",
                            currentEncryptionAlgorithm,
                            previousEncryptionAlgorithm
                        )
                    )
                    .build();
            }
        }

        return HookProgressEvent.<CallbackContext>builder()
            .status(HookStatus.SUCCESS)
            .message("Successfully invoked PreUpdateHookHandler for target:
AWS::SQS::Queue")
            .build();
    }
}
```

```
}
```

更新preUpdate測試

1. 在 IDE 中，開啟 `src/main/java/com/mycompany/testing/mytesthook` 資料夾中的 `PreUpdateHandlerTest.java` 檔案。
2. 使用下列程式碼取代 `PreUpdateHandlerTest.java` 檔案的整個內容。

```
package com.mycompany.testing.mytesthook;

import com.google.common.collect.ImmutableMap;
import com.mycompany.testing.mytesthook.model.aws.s3.bucket.AwsS3Bucket;
import com.mycompany.testing.mytesthook.model.aws.s3.bucket.BucketEncryption;
import
    com.mycompany.testing.mytesthook.model.aws.s3.bucket.ServerSideEncryptionByDefault;
import
    com.mycompany.testing.mytesthook.model.aws.s3.bucket.ServerSideEncryptionRule;
import org.junit.jupiter.api.BeforeEach;
import org.junit.jupiter.api.Test;
import org.junit.jupiter.api.extension.ExtendWith;
import org.mockito.Mock;
import org.mockito.junit.jupiter.MockitoExtension;
import software.amazon.cloudformation.exceptions.UnsupportedTargetException;
import software.amazon.cloudformation.proxy.AmazonWebServicesClientProxy;
import software.amazon.cloudformation.proxy.HandlerErrorCode;
import software.amazon.cloudformation.proxy.Logger;
import software.amazon.cloudformation.proxy.hook.HookContext;
import software.amazon.cloudformation.proxy.hook.HookHandlerRequest;
import software.amazon.cloudformation.proxy.hook.HookProgressEvent;
import software.amazon.cloudformation.proxy.hook.HookStatus;
import software.amazon.cloudformation.proxy.hook.targetmodel.HookTargetModel;

import java.util.Arrays;
import java.util.stream.Stream;

import static org.assertj.core.api.Assertions.assertThat;
import static org.assertj.core.api.Assertions.assertThatExceptionOfType;
import static org.mockito.Mockito.mock;

@ExtendWith(MockitoExtension.class)
public class PreUpdateHookHandlerTest {
```

```
@Mock
private AmazonWebServicesClientProxy proxy;

@Mock
private Logger logger;

@BeforeEach
public void setup() {
    proxy = mock(AmazonWebServicesClientProxy.class);
    logger = mock(Logger.class);
}

@Test
public void handleRequest_awsS3BucketSuccess() {
    final PreUpdateHookHandler handler = new PreUpdateHookHandler();

    final ServerSideEncryptionRule serverSideEncryptionRule =
buildServerSideEncryptionRule("AES256");
    final AwsS3Bucket resourceProperties = buildAwsS3Bucket("amzn-s3-demo-
bucket", serverSideEncryptionRule);
    final AwsS3Bucket previousResourceProperties = buildAwsS3Bucket("amzn-s3-
demo-bucket", serverSideEncryptionRule);
    final HookTargetModel targetModel =
createHookTargetModel(resourceProperties, previousResourceProperties);
    final TypeConfigurationModel typeConfiguration =
TypeConfigurationModel.builder().encryptionAlgorithm("AES256").build();

    final HookHandlerRequest request = HookHandlerRequest.builder()

.hookContext(HookContext.builder().targetName("AWS::S3::Bucket").targetModel(targetModel)
    .build());

    final HookProgressEvent<CallbackContext> response =
handler.handleRequest(proxy, request, null, logger, typeConfiguration);
    assertResponse(response, HookStatus.SUCCESS, "Successfully invoked
PreUpdateHookHandler for target: AWS::SQS::Queue");
}

@Test
public void handleRequest_awsS3BucketFail_bucketEncryptionConfigsDontMatch() {
    final PreUpdateHookHandler handler = new PreUpdateHookHandler();

    final ServerSideEncryptionRule[] serverSideEncryptionRules =
Stream.of("AES256", "SHA512", "AES32")
```

```
        .map(this::buildServerSideEncryptionRule)
        .toArray(ServerSideEncryptionRule[]::new);

        final AwsS3Bucket resourceProperties = buildAwsS3Bucket("amzn-s3-demo-
bucket", serverSideEncryptionRules[0]);
        final AwsS3Bucket previousResourceProperties = buildAwsS3Bucket("amzn-s3-
demo-bucket", serverSideEncryptionRules);
        final HookTargetModel targetModel =
createHookTargetModel(resourceProperties, previousResourceProperties);
        final TypeConfigurationModel typeConfiguration =
TypeConfigurationModel.builder().encryptionAlgorithm("AES256").build();

        final HookHandlerRequest request = HookHandlerRequest.builder()

.hookContext(HookContext.builder().targetName("AWS::S3::Bucket").targetModel(targetModel)
        .build());

        final HookProgressEvent<CallbackContext> response =
handler.handleRequest(proxy, request, null, logger, typeConfiguration);
        assertResponse(response, HookStatus.FAILED, "Current number of bucket
encryption configs does not match previous. Current has 1 configs while previously
there were 3 configs");
    }

    @Test
    public void
handleRequest_awsS3BucketFail_bucketEncryptionAlgorithmDoesNotMatch() {
        final PreUpdateHookHandler handler = new PreUpdateHookHandler();

        final AwsS3Bucket resourceProperties = buildAwsS3Bucket("amzn-s3-demo-
bucket", buildServerSideEncryptionRule("SHA512"));
        final AwsS3Bucket previousResourceProperties = buildAwsS3Bucket("amzn-s3-
demo-bucket", buildServerSideEncryptionRule("AES256"));
        final HookTargetModel targetModel =
createHookTargetModel(resourceProperties, previousResourceProperties);
        final TypeConfigurationModel typeConfiguration =
TypeConfigurationModel.builder().encryptionAlgorithm("AES256").build();

        final HookHandlerRequest request = HookHandlerRequest.builder()

.hookContext(HookContext.builder().targetName("AWS::S3::Bucket").targetModel(targetModel)
        .build());
```



```

        final HookProgressEvent<CallbackContext> response =
handler.handleRequest(proxy, request, null, logger, typeConfiguration);
        assertResponse(response, HookStatus.FAILED, String.format("Bucket
Encryption algorithm can not be changed once set. The encryption algorithm was
changed to '%s' from '%s'.", "SHA512", "AES256"));
    }

@Test
public void handleRequest_unsupportedTarget() {
    final PreUpdateHookHandler handler = new PreUpdateHookHandler();

    final Object resourceProperties = ImmutableMap.of("FileSizeLimit", 256);
    final Object previousResourceProperties = ImmutableMap.of("FileSizeLimit",
512);
    final HookTargetModel targetModel =
createHookTargetModel(resourceProperties, previousResourceProperties);
    final TypeConfigurationModel typeConfiguration =
TypeConfigurationModel.builder().encryptionAlgorithm("AES256").build();

    final HookHandlerRequest request = HookHandlerRequest.builder()

.hookContext(HookContext.builder().targetName("AWS::Unsupported::Target").targetModel(targetModel)
.build());

    assertThatExceptionOfType(UnsupportedTargetException.class)
        .isThrownBy(() -> handler.handleRequest(proxy, request, null,
logger, typeConfiguration))
        .withMessageContaining("Unsupported target")
        .withMessageContaining("AWS::Unsupported::Target")
        .satisfies(e ->
assertThat(e.getErrorCode()).isEqualTo(HandlerErrorCode.InvalidRequest));
}

private void assertResponse(final HookProgressEvent<CallbackContext> response,
final HookStatus expectedStatus, final String expectedErrorMsg) {
    assertThat(response).isNotNull();
    assertThat(response.getStatus()).isEqualTo(expectedStatus);
    assertThat(response.getCallbackContext()).isNull();
    assertThat(response.getCallbackDelaySeconds()).isEqualTo(0);
    assertThat(response.getMessage()).isNotNull();
    assertThat(response.getMessage()).isEqualTo(expectedErrorMsg);
}

```

```
private HookTargetModel createHookTargetModel(final Object resourceProperties,
final Object previousResourceProperties) {
    return HookTargetModel.of(
        ImmutableMap.of(
            "ResourceProperties", resourceProperties,
            "PreviousResourceProperties", previousResourceProperties
        )
    );
}

@SuppressWarnings("SameParameterValue")
private AwsS3Bucket buildAwsS3Bucket(
    final String bucketName,
    final ServerSideEncryptionRule ...serverSideEncryptionRules
) {
    return AwsS3Bucket.builder()
        .bucketName(bucketName)
        .bucketEncryption(
            BucketEncryption.builder()
                .serverSideEncryptionConfiguration(
                    Arrays.asList(serverSideEncryptionRules)
                ).build()
        ).build();
}

private ServerSideEncryptionRule buildServerSideEncryptionRule(final String
encryptionAlgorithm) {
    return ServerSideEncryptionRule.builder()
        .bucketKeyEnabled(true)
        .serverSideEncryptionByDefault(
            ServerSideEncryptionByDefault.builder()
                .sSEAlgorithm(encryptionAlgorithm)
                .build()
        ).build();
}
}
```

實作preDelete處理常式

實作preDelete處理常式，其會在處理常式中所有指定目標的刪除操作之前啟動。preDelete 處理常式會完成下列項目：

- 對於 `AWS::S3::Bucket` 資源，勾點只有在下列情況為 `true` 時才會傳遞：
 - 驗證刪除資源後，帳戶是否將存在最低必要投訴資源。
 - 最低必要投訴資源數量是在 Hook 的類型組態中設定。

編碼 `preDelete` 處理常式

1. 在 IDE 中，開啟 `src/main/java/com/mycompany/testing/mytesthook` 資料夾中的 `PreDeleteHookHandler.java` 檔案。
2. 使用下列程式碼取代 `PreDeleteHookHandler.java` 檔案的整個內容。

```
package com.mycompany.testing.mytesthook;

import com.google.common.annotations.VisibleForTesting;
import com.mycompany.testing.mytesthook.model.aws.s3.bucket.AwsS3Bucket;
import com.mycompany.testing.mytesthook.model.aws.s3.bucket.AwsS3BucketTargetModel;
import com.mycompany.testing.mytesthook.model.aws.sqs.queue.AwsSqsQueue;
import com.mycompany.testing.mytesthook.model.aws.sqs.queue.AwsSqsQueueTargetModel;
import org.apache.commons.lang3.StringUtils;
import org.apache.commons.lang3.math.NumberUtils;
import software.amazon.awssdk.services.cloudformation.CloudFormationClient;
import
    software.amazon.awssdk.services.cloudformation.model.CloudFormationException;
import
    software.amazon.awssdk.services.cloudformation.model.DescribeStackResourceRequest;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.Bucket;
import software.amazon.awssdk.services.s3.model.S3Exception;
import software.amazon.awssdk.services.sqs.SqsClient;
import software.amazon.awssdk.services.sqs.model.GetQueueAttributesRequest;
import software.amazon.awssdk.services.sqs.model.GetQueueUrlRequest;
import software.amazon.awssdk.services.sqs.model.ListQueuesRequest;
import software.amazon.awssdk.services.sqs.model.ListQueuesResponse;
import software.amazon.awssdk.services.sqs.model.QueueAttributeName;
import software.amazon.awssdk.services.sqs.model.SqsException;
import software.amazon.cloudformation.exceptions.CfnGeneralServiceException;
import software.amazon.cloudformation.proxy.AmazonWebServicesClientProxy;
import software.amazon.cloudformation.proxy.HandlerErrorCode;
import software.amazon.cloudformation.proxy.OperationStatus;
import software.amazon.cloudformation.proxy.ProgressEvent;
import software.amazon.cloudformation.proxy.ProxyClient;
import software.amazon.cloudformation.proxy.hook.HookContext;
```

```
import software.amazon.cloudformation.proxy.hook.HookHandlerRequest;
import software.amazon.cloudformation.proxy.hook.targetmodel.HookTargetModel;
import
    software.amazon.cloudformation.proxy.hook.targetmodel.ResourceHookTargetModel;

import java.util.ArrayList;
import java.util.Collection;
import java.util.HashSet;
import java.util.List;
import java.util.Objects;
import java.util.stream.Collectors;

public class PreDeleteHookHandler extends BaseHookHandlerStd {

    private ProxyClient<S3Client> s3Client;
    private ProxyClient<SqsClient> sqsClient;

    @Override
    protected ProgressEvent<HookTargetModel, CallbackContext>
    handleS3BucketRequest(
        final AmazonWebServicesClientProxy proxy,
        final HookHandlerRequest request,
        final CallbackContext callbackContext,
        final ProxyClient<S3Client> proxyClient,
        final TypeConfigurationModel typeConfiguration
    ) {
        final HookContext hookContext = request.getHookContext();
        final String targetName = hookContext.getTargetName();
        if (!AwsS3Bucket.TYPE_NAME.equals(targetName)) {
            throw new RuntimeException(String.format("Request target type [%s] is
not 'AWS::S3::Bucket'", targetName));
        }
        this.s3Client = proxyClient;

        final String encryptionAlgorithm =
typeConfiguration.getEncryptionAlgorithm();
        final int minBuckets =
NumberUtils.toInt(typeConfiguration.getMinBuckets());

        final ResourceHookTargetModel<AwsS3Bucket> targetModel =
hookContext.getTargetModel(AwsS3BucketTargetModel.class);
        final List<String> buckets = listBuckets().stream()
            .filter(b -> !StringUtils.equals(b,
targetModel.getResourceProperties().getBucketName()))
```

```

        .collect(Collectors.toList());

final List<String> compliantBuckets = new ArrayList<>();
for (final String bucket : buckets) {
    if (getBucketSSEAlgorithm(bucket).contains(encryptionAlgorithm)) {
        compliantBuckets.add(bucket);
    }

    if (compliantBuckets.size() >= minBuckets) {
        return ProgressEvent.<HookTargetModel, CallbackContext>builder()
            .status(OperationStatus.SUCCESS)
            .message("Successfully invoked PreDeleteHookHandler for
target: AWS::S3::Bucket")
            .build();
    }
}

return ProgressEvent.<HookTargetModel, CallbackContext>builder()
    .status(OperationStatus.FAILED)
    .errorCode(HandlerErrorCode.NonCompliant)
    .message(String.format("Failed to meet minimum of [%d] encrypted
buckets.", minBuckets))
    .build();
}

@Override
protected ProgressEvent<HookTargetModel, CallbackContext>
handleSqsQueueRequest(
    final AmazonWebServicesClientProxy proxy,
    final HookHandlerRequest request,
    final CallbackContext callbackContext,
    final ProxyClient<SqsClient> proxyClient,
    final TypeConfigurationModel typeConfiguration
) {
    final HookContext hookContext = request.getHookContext();
    final String targetName = hookContext.getTargetName();
    if (!AwsSqsQueue.TYPE_NAME.equals(targetName)) {
        throw new RuntimeException(String.format("Request target type [%s] is
not 'AWS::SQS::Queue'", targetName));
    }
    this.sqsClient = proxyClient;
    final int minQueues = NumberUtils.toInt(typeConfiguration.getMinQueues());

```

```
final ResourceHookTargetModel<AwsSqsQueue> targetModel =
hookContext.getTargetModel(AwsSqsQueueTargetModel.class);

final String queueName =
Objects.toString(targetModel.getResourceProperties().get("QueueName"), null);

String targetQueueUrl = null;
if (queueName != null) {
    try {
        targetQueueUrl = sqsClient.injectCredentialsAndInvokeV2(
            GetQueueUrlRequest.builder().queueName(
                queueName
            ).build(),
            sqsClient.client()::getQueueUrl
        ).queueUrl();
    } catch (SqsException e) {
        log(String.format("Error while calling GetQueueUrl API for queue
name [%s]: %s", queueName, e.getMessage()));
    }
} else {
    log("Queue name is empty, attempting to get queue's physical ID");
    try {
        final ProxyClient<CloudFormationClient> cfnClient =
proxy.newProxy(ClientBuilder::createCloudFormationClient);
        targetQueueUrl = cfnClient.injectCredentialsAndInvokeV2(
            DescribeStackResourceRequest.builder()
                .stackName(hookContext.getTargetLogicalId())
                .logicalResourceId(hookContext.getTargetLogicalId())
                .build(),
            cfnClient.client()::describeStackResource
        ).stackResourceDetail().physicalResourceId();
    } catch (CloudFormationException e) {
        log(String.format("Error while calling DescribeStackResource API
for queue name: %s", e.getMessage()));
    }
}

// Creating final variable for the filter lambda
final String finalTargetQueueUrl = targetQueueUrl;

final List<String> compliantQueues = new ArrayList<>();

String nextToken = null;
```

```
do {
    final ListQueuesRequest req =
Translator.createListQueuesRequest(nextToken);
    final ListQueuesResponse res =
sqsClient.injectCredentialsAndInvokeV2(req, sqsClient.client()::listQueues);
    final List<String> queueUrls = res.queueUrls().stream()
        .filter(q -> !StringUtils.equals(q, finalTargetQueueUrl))
        .collect(Collectors.toList());

    for (final String queueUrl : queueUrls) {
        if (isQueueEncrypted(queueUrl)) {
            compliantQueues.add(queueUrl);
        }

        if (compliantQueues.size() >= minQueues) {
            return ProgressEvent.<HookTargetModel,
CallbackContext>builder()
                .status(OperationStatus.SUCCESS)
                .message("Successfully invoked PreDeleteHookHandler for
target: AWS::SQS::Queue")
                .build();
        }
        nextToken = res.nextToken();
    }
} while (nextToken != null);

return ProgressEvent.<HookTargetModel, CallbackContext>builder()
    .status(OperationStatus.FAILED)
    .errorCode(HandlerErrorCode.NonCompliant)
    .message(String.format("Failed to meet minimum of [%d] encrypted
queues.", minQueues))
    .build();
}

private List<String> listBuckets() {
    try {
        return
s3Client.injectCredentialsAndInvokeV2(Translator.createListBucketsRequest(),
s3Client.client()::listBuckets)
            .buckets()
            .stream()
            .map(Bucket::name)
            .collect(Collectors.toList());
    } catch (S3Exception e) {
```

```
        throw new CfnGeneralServiceException("Error while calling S3
ListBuckets API", e);
    }
}

@VisibleForTesting
Collection<String> getBucketSSEAlgorithm(final String bucket) {
    try {
        return
s3Client.injectCredentialsAndInvokeV2(Translator.createGetBucketEncryptionRequest(bucket),
s3Client.client()::getBucketEncryption)
            .serverSideEncryptionConfiguration()
            .rules()
            .stream()
            .filter(r ->
Objects.nonNull(r.applyServerSideEncryptionByDefault()))
            .map(r ->
r.applyServerSideEncryptionByDefault().sseAlgorithmAsString())
            .collect(Collectors.toSet());
    } catch (S3Exception e) {
        return new HashSet<>();
    }
}

@VisibleForTesting
boolean isQueueEncrypted(final String queueUrl) {
    try {
        final GetQueueAttributesRequest request =
GetQueueAttributesRequest.builder()
            .queueUrl(queueUrl)
            .attributeNames(QueueAttributeName.KMS_MASTER_KEY_ID)
            .build();
        final String kmsKeyId = sqsClient.injectCredentialsAndInvokeV2(request,
sqsClient.client()::getQueueAttributes)
            .attributes()
            .get(QueueAttributeName.KMS_MASTER_KEY_ID);

        return StringUtils.isNotBlank(kmsKeyId);
    } catch (SqsException e) {
        throw new CfnGeneralServiceException("Error while calling SQS
GetQueueAttributes API", e);
    }
}
```



```
}
```

更新preDelete處理常式

1. 在 IDE 中，開啟 `src/main/java/com/mycompany/testing/mytesthook` 資料夾中的 `PreDeleteHookHandler.java` 檔案。
2. 使用下列程式碼取代 `PreDeleteHookHandler.java` 檔案的整個內容。

```
package com.mycompany.testing.mytesthook;

import com.google.common.collect.ImmutableList;
import com.google.common.collect.ImmutableMap;
import com.mycompany.testing.mytesthook.model.aws.s3.bucket.AwsS3Bucket;
import org.junit.jupiter.api.BeforeEach;
import org.junit.jupiter.api.Test;
import org.junit.jupiter.api.extension.ExtendWith;
import org.mockito.Mock;
import org.mockito.Mockito;
import org.mockito.junit.jupiter.MockitoExtension;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.Bucket;
import software.amazon.awssdk.services.s3.model.GetBucketEncryptionRequest;
import software.amazon.awssdk.services.s3.model.GetBucketEncryptionResponse;
import software.amazon.awssdk.services.s3.model.ListBucketsRequest;
import software.amazon.awssdk.services.s3.model.ListBucketsResponse;
import software.amazon.awssdk.services.s3.model.S3Exception;
import software.amazon.awssdk.services.s3.model.ServerSideEncryptionByDefault;
import software.amazon.awssdk.services.s3.model.ServerSideEncryptionConfiguration;
import software.amazon.awssdk.services.s3.model.ServerSideEncryptionRule;
import software.amazon.awssdk.services.sqs.SqsClient;
import software.amazon.awssdk.services.sqs.model.GetQueueAttributesRequest;
import software.amazon.awssdk.services.sqs.model.GetQueueAttributesResponse;
import software.amazon.awssdk.services.sqs.model.GetQueueUrlRequest;
import software.amazon.awssdk.services.sqs.model.GetQueueUrlResponse;
import software.amazon.awssdk.services.sqs.model.ListQueuesRequest;
import software.amazon.awssdk.services.sqs.model.ListQueuesResponse;
import software.amazon.awssdk.services.sqs.model.QueueAttributeName;
import software.amazon.cloudformation.proxy.Logger;
import software.amazon.cloudformation.proxy.OperationStatus;
import software.amazon.cloudformation.proxy.ProgressEvent;
import software.amazon.cloudformation.proxy.hook.HookContext;
import software.amazon.cloudformation.proxy.hook.HookHandlerRequest;
```

```
import software.amazon.cloudformation.proxy.hook.targetmodel.HookTargetModel;

import java.util.Arrays;
import java.util.Collection;
import java.util.HashMap;
import java.util.List;
import java.util.stream.Collectors;

import static org.mockito.ArgumentMatchers.any;
import static org.mockito.Mockito.mock;
import static org.mockito.Mockito.never;
import static org.mockito.Mockito.times;
import static org.mockito.Mockito.verify;
import static org.mockito.Mockito.when;

@ExtendWith(MockitoExtension.class)
public class PreDeleteHookHandlerTest extends AbstractTestBase {

    @Mock private S3Client s3Client;
    @Mock private SqsClient sqsClient;
    @Mock private Logger logger;

    @BeforeEach
    public void setup() {
        s3Client = mock(S3Client.class);
        sqsClient = mock(SqsClient.class);
        logger = mock(Logger.class);
    }

    @Test
    public void handleRequest_awsS3BucketSuccess() {
        final PreDeleteHookHandler handler = Mockito.spy(new
PreDeleteHookHandler());

        final List<Bucket> bucketList = ImmutableList.of(
            Bucket.builder().name("bucket1").build(),
            Bucket.builder().name("bucket2").build(),
            Bucket.builder().name("toBeDeletedBucket").build(),
            Bucket.builder().name("bucket3").build(),
            Bucket.builder().name("bucket4").build(),
            Bucket.builder().name("bucket5").build()
        );

        final ListBucketsResponse mockResponse =
ListBucketsResponse.builder().buckets(bucketList).build();
```

```

when(s3Client.listBuckets(any(ListBucketsRequest.class))).thenReturn(mockResponse);
    when(s3Client.getBucketEncryption(any(GetBucketEncryptionRequest.class)))
        .thenReturn(buildGetBucketEncryptionResponse("AES256"))
        .thenReturn(buildGetBucketEncryptionResponse("AES256", "aws:kms"))
        .thenThrow(S3Exception.builder().message("No Encrypt").build())
        .thenReturn(buildGetBucketEncryptionResponse("aws:kms"))
        .thenReturn(buildGetBucketEncryptionResponse("AES256"));
    setServiceClient(s3Client);

    final TypeConfigurationModel typeConfiguration =
TypeConfigurationModel.builder()
    .encryptionAlgorithm("AES256")
    .minBuckets("3")
    .build();

    final HookHandlerRequest request = HookHandlerRequest.builder()
        .hookContext(
            HookContext.builder()
                .targetName("AWS::S3::Bucket")
                .targetModel(
                    createHookTargetModel(
                        AwsS3Bucket.builder()
                            .bucketName("toBeDeletedBucket")
                            .build()
                    )
                )
            )
        .build();

    final ProgressEvent<HookTargetModel, CallbackContext> response =
handler.handleRequest(proxy, request, null, logger, typeConfiguration);

    verify(s3Client,
times(5)).getBucketEncryption(any(GetBucketEncryptionRequest.class));
    verify(handler, never()).getBucketSSEAlgorithm("toBeDeletedBucket");

    assertResponse(response, OperationStatus.SUCCESS, "Successfully invoked
PreDeleteHookHandler for target: AWS::S3::Bucket");
}

@Test
public void handleRequest_awsSqsQueueSuccess() {

```

```
final PreDeleteHookHandler handler = Mockito.spy(new
PreDeleteHookHandler());

final List<String> queueUrls = ImmutableList.of(
    "https://queue1.queue",
    "https://queue2.queue",
    "https://toBeDeletedQueue.queue",
    "https://queue3.queue",
    "https://queue4.queue",
    "https://queue5.queue"
);

when(sqsClient.getQueueUrl(any(GetQueueUrlRequest.class)))
    .thenReturn(GetQueueUrlResponse.builder().queueUrl("https://
toBeDeletedQueue.queue").build());
when(sqsClient.listQueues(any(ListQueuesRequest.class)))

.thenReturn(ListQueuesResponse.builder().queueUrls(queueUrls).build());
when(sqsClient.getQueueAttributes(any(GetQueueAttributesRequest.class)))

.thenReturn(GetQueueAttributesResponse.builder().attributes(ImmutableMap.of(QueueAttribute
"kmsKeyId")).build())
    .thenReturn(GetQueueAttributesResponse.builder().attributes(new
HashMap<>()).build())

.thenReturn(GetQueueAttributesResponse.builder().attributes(ImmutableMap.of(QueueAttribute
"kmsKeyId")).build())
    .thenReturn(GetQueueAttributesResponse.builder().attributes(new
HashMap<>()).build())

.thenReturn(GetQueueAttributesResponse.builder().attributes(ImmutableMap.of(QueueAttribute
"kmsKeyId")).build());
setServiceClient(sqsClient);

final TypeConfigurationModel typeConfiguration =
TypeConfigurationModel.builder()
    .minQueues("3")
    .build();

final HookHandlerRequest request = HookHandlerRequest.builder()
    .hookContext(
        HookContext.builder()
            .targetName("AWS::SQS::Queue")
            .targetModel(
```

```
        createHookTargetModel(
            ImmutableMap.of("QueueName", "toBeDeletedQueue")
        )
    )
    .build()
    .build();

    final ProgressEvent<HookTargetModel, CallbackContext> response =
handler.handleRequest(proxy, request, null, logger, typeConfiguration);

    verify(sqsClient,
times(5)).getQueueAttributes(any(GetQueueAttributesRequest.class));
    verify(handler, never()).isQueueEncrypted("toBeDeletedQueue");

    assertResponse(response, OperationStatus.SUCCESS, "Successfully invoked
PreDeleteHookHandler for target: AWS::SQS::Queue");
}

@Test
public void handleRequest_awsS3BucketFailed() {
    final PreDeleteHookHandler handler = Mockito.spy(new
PreDeleteHookHandler());

    final List<Bucket> bucketList = ImmutableList.of(
        Bucket.builder().name("bucket1").build(),
        Bucket.builder().name("bucket2").build(),
        Bucket.builder().name("toBeDeletedBucket").build(),
        Bucket.builder().name("bucket3").build(),
        Bucket.builder().name("bucket4").build(),
        Bucket.builder().name("bucket5").build()
    );
    final ListBucketsResponse mockResponse =
ListBucketsResponse.builder().buckets(bucketList).build();

when(s3Client.listBuckets(any(ListBucketsRequest.class))).thenReturn(mockResponse);
when(s3Client.getBucketEncryption(any(GetBucketEncryptionRequest.class)))
    .thenReturn(buildGetBucketEncryptionResponse("AES256"))
    .thenReturn(buildGetBucketEncryptionResponse("AES256", "aws:kms"))
    .thenThrow(S3Exception.builder().message("No Encrypt").build())
    .thenReturn(buildGetBucketEncryptionResponse("aws:kms"))
    .thenReturn(buildGetBucketEncryptionResponse("AES256"));
setServiceClient(s3Client);
```

```
    final TypeConfigurationModel typeConfiguration =
TypeConfigurationModel.builder()
    .encryptionAlgorithm("AES256")
    .minBuckets("10")
    .build();

    final HookHandlerRequest request = HookHandlerRequest.builder()
    .hookContext(
        HookContext.builder()
            .targetName("AWS::S3::Bucket")
            .targetModel(
                createHookTargetModel(
                    AwsS3Bucket.builder()
                        .bucketName("toBeDeletedBucket")
                        .build()
                )
            )
        .build())
    .build();

    final ProgressEvent<HookTargetModel, CallbackContext> response =
handler.handleRequest(proxy, request, null, logger, typeConfiguration);

    verify(s3Client,
times(5)).getBucketEncryption(any(GetBucketEncryptionRequest.class));
    verify(handler, never()).getBucketSSEAlgorithm("toBeDeletedBucket");

    assertResponse(response, OperationStatus.FAILED, "Failed to meet minimum of
[10] encrypted buckets.");
}

@Test
public void handleRequest_awsSqsQueueFailed() {
    final PreDeleteHookHandler handler = Mockito.spy(new
PreDeleteHookHandler());

    final List<String> queueUrls = ImmutableList.of(
        "https://queue1.queue",
        "https://queue2.queue",
        "https://toBeDeletedQueue.queue",
        "https://queue3.queue",
        "https://queue4.queue",
        "https://queue5.queue"
```

```

);

    when(sqsClient.getQueueUrl(any(GetQueueUrlRequest.class)))
        .thenReturn(GetQueueUrlResponse.builder().queueUrl("https://
toBeDeletedQueue.queue").build());
    when(sqsClient.listQueues(any(ListQueuesRequest.class)))

.thenReturn(ListQueuesResponse.builder().queueUrls(queueUrls).build());
    when(sqsClient.getQueueAttributes(any(GetQueueAttributesRequest.class)))

.thenReturn(GetQueueAttributesResponse.builder().attributes(ImmutableMap.of(QueueAttribute
"kmsKeyId")).build())
        .thenReturn(GetQueueAttributesResponse.builder().attributes(new
HashMap<>()).build())

.thenReturn(GetQueueAttributesResponse.builder().attributes(ImmutableMap.of(QueueAttribute
"kmsKeyId")).build())
        .thenReturn(GetQueueAttributesResponse.builder().attributes(new
HashMap<>()).build())

.thenReturn(GetQueueAttributesResponse.builder().attributes(ImmutableMap.of(QueueAttribute
"kmsKeyId")).build());
    setServiceClient(sqsClient);

    final TypeConfigurationModel typeConfiguration =
TypeConfigurationModel.builder()
        .minQueues("10")
        .build();

    final HookHandlerRequest request = HookHandlerRequest.builder()
        .hookContext(
            HookContext.builder()
                .targetName("AWS::SQS::Queue")
                .targetModel(
                    createHookTargetModel(
                        ImmutableMap.of("QueueName", "toBeDeletedQueue")
                    )
                )
                .build()
        )
        .build();

    final ProgressEvent<HookTargetModel, CallbackContext> response =
handler.handleRequest(proxy, request, null, logger, typeConfiguration);

```

```
        verify(sqsClient,
times(5)).getQueueAttributes(any(GetQueueAttributesRequest.class));
        verify(handler, never()).isQueueEncrypted("toBeDeletedQueue");

        assertResponse(response, OperationStatus.FAILED, "Failed to meet minimum of
[10] encrypted queues.");
    }

    private GetBucketEncryptionResponse buildGetBucketEncryptionResponse(final
String ...sseAlgorithm) {
        return buildGetBucketEncryptionResponse(
            Arrays.stream(sseAlgorithm)
                .map(a ->
ServerSideEncryptionRule.builder().applyServerSideEncryptionByDefault(
                    ServerSideEncryptionByDefault.builder()
                        .sseAlgorithm(a)
                        .build()
                    ).build()
                )
            .collect(Collectors.toList())
        );
    }

    private GetBucketEncryptionResponse buildGetBucketEncryptionResponse(final
Collection<ServerSideEncryptionRule> rules) {
        return GetBucketEncryptionResponse.builder()
            .serverSideEncryptionConfiguration(
                ServerSideEncryptionConfiguration.builder().rules(
                    rules
                ).build()
            ).build();
    }
}
```

使用 Python 建立自訂 AWS CloudFormation 勾點的模型

建立自訂 AWS CloudFormation 勾點的模型需要建立定義勾點、其屬性及其屬性的結構描述。本教學課程將逐步引導您使用 Python 建立自訂勾點的模型。

步驟 1：產生勾點專案套件

產生您的 Hook 專案套件。CloudFormation CLI 會建立空的處理常式函數，其對應至目標生命週期中的特定 Hook 動作，如 Hook 規格所定義。

```
cfn generate
```

命令會傳回下列輸出：

```
Generated files for MyCompany::Testing::MyTestHook
```

Note

確保您的 Lambda 執行時間是 up-to-date，以避免使用已棄用版本。如需詳細資訊，請參閱 [更新資源類型和勾點的 Lambda 執行時間](#)。

步驟 2：新增勾點處理常式

將您自己的 Hook 處理常式執行時間程式碼新增至您選擇實作的處理常式。例如，您可以新增下列程式碼進行記錄。

```
LOG.setLevel(logging.INFO)
LOG.info("Internal testing Hook triggered for target: " +
        request.hookContext.targetName);
```

CloudFormation CLI 會從產生 src/models.py 檔案 [組態結構描述](#)。

Example models.py

```
import sys
from dataclasses import dataclass
from inspect import getmembers, isclass
from typing import (
    AbstractSet,
    Any,
    Generic,
    Mapping,
    MutableMapping,
    Optional,
    Sequence,
```

```
    Type,
    TypeVar,
)

from cloudformation_cli_python_lib.interface import (
    BaseModel,
    BaseHookHandlerRequest,
)
from cloudformation_cli_python_lib.recast import recast_object
from cloudformation_cli_python_lib.utils import deserialize_list

T = TypeVar("T")

def set_or_none(value: Optional[Sequence[T]]) -> Optional[AbstractSet[T]]:
    if value:
        return set(value)
    return None

@dataclass
class HookHandlerRequest(BaseHookHandlerRequest):
    pass

@dataclass
class TypeConfigurationModel(BaseModel):
    limitSize: Optional[str]
    cidr: Optional[str]
    encryptionAlgorithm: Optional[str]

    @classmethod
    def _deserialize(
        cls: Type["_TypeConfigurationModel"],
        json_data: Optional[Mapping[str, Any]],
    ) -> Optional["_TypeConfigurationModel"]:
        if not json_data:
            return None
        return cls(
            limitSize=json_data.get("limitSize"),
            cidr=json_data.get("cidr"),
            encryptionAlgorithm=json_data.get("encryptionAlgorithm"),
        )
```

```
_TypeConfigurationModel = TypeConfigurationModel
```

步驟 3：實作勾點處理常式

透過產生的 Python 資料類別，您可以撰寫實際實作勾點功能的處理常式。在此範例中，您將實作處理常式的 `preUpdate`、`preCreate` 和 `preDelete` 呼叫點。

主題

- [實作 `preCreate` 處理常式](#)
- [實作 `preUpdate` 處理常式](#)
- [實作 `preDelete` 處理常式](#)
- [實作勾點處理常式](#)

實作 `preCreate` 處理常式

`preCreate` 處理常式會驗證 `AWS::S3::Bucket` 或 `AWS::SQS::Queue` 資源的伺服器端加密設定。

- 對於 `AWS::S3::Bucket` 資源，勾點只有在下列情況為 `true` 時才會通過。
 - Amazon S3 儲存貯體加密已設定。
 - 已啟用儲存貯體的 Amazon S3 儲存貯體金鑰。
 - Amazon S3 儲存貯體的加密演算法集是所需的正確演算法。
 - AWS Key Management Service 金鑰 ID 已設定。
- 對於 `AWS::SQS::Queue` 資源，勾點只有在下列情況為 `true` 時才會通過。
 - AWS Key Management Service 金鑰 ID 已設定。

實作 `preUpdate` 處理常式

實作 `preUpdate` 處理常式，其會在處理常式中所有指定目標的更新操作之前啟動。`preUpdate` 處理常式會完成下列項目：

- 對於 `AWS::S3::Bucket` 資源，勾點只會在下列情況為 `true` 時傳遞：
 - Amazon S3 儲存貯體的儲存貯體加密演算法尚未修改。

實作 preDelete 處理常式

實作preDelete處理常式，其會在處理常式中所有指定目標的刪除操作之前啟動。preDelete 處理常式會完成下列項目：

- 對於 `AWS::S3::Bucket` 資源，勾點只會在下列情況為 true 時傳遞：
 - 驗證刪除資源後，帳戶是否將存在最低必要合規資源。
 - 所需的最低合規資源數量是在 Hook 的組態中設定。

實作勾點處理常式

1. 在您的 IDE 中，開啟 `handlers.py` 位於 `src` 資料夾的檔案。
2. 使用下列程式碼取代 `handlers.py` 檔案的整個內容。

Example handlers.py

```
import logging
from typing import Any, MutableMapping, Optional
import boto3

from cloudformation_cli_python_lib import (
    BaseHookHandlerRequest,
    HandlerErrorCode,
    Hook,
    HookInvocationPoint,
    OperationStatus,
    ProgressEvent,
    SessionProxy,
    exceptions,
)

from .models import HookHandlerRequest, TypeConfigurationModel

# Use this logger to forward log messages to CloudWatch Logs.
LOG = logging.getLogger(__name__)
TYPE_NAME = "MyCompany::Testing::MyTestHook"

LOG.setLevel(logging.INFO)

hook = Hook(TYPE_NAME, TypeConfigurationModel)
test_entrypoint = hook.test_entrypoint
```

```

def _validate_s3_bucket_encryption(
    bucket: MutableMapping[str, Any], required_encryption_algorithm: str
) -> ProgressEvent:
    status = None
    message = ""
    error_code = None

    if bucket:
        bucket_name = bucket.get("BucketName")

        bucket_encryption = bucket.get("BucketEncryption")
        if bucket_encryption:
            server_side_encryption_rules = bucket_encryption.get(
                "ServerSideEncryptionConfiguration"
            )
            if server_side_encryption_rules:
                for rule in server_side_encryption_rules:
                    bucket_key_enabled = rule.get("BucketKeyEnabled")
                    if bucket_key_enabled:
                        server_side_encryption_by_default = rule.get(
                            "ServerSideEncryptionByDefault"
                        )

                        encryption_algorithm =
server_side_encryption_by_default.get(
                            "SSEAlgorithm"
                        )
                        kms_key_id = server_side_encryption_by_default.get(
                            "KMSMasterKeyID"
                        ) # "KMSMasterKeyID" is name of the property for an
AWS::S3::Bucket

                        if encryption_algorithm == required_encryption_algorithm:
                            if encryption_algorithm == "aws:kms" and not
kms_key_id:
                                status = OperationStatus.FAILED
                                message = f"KMS Key ID not set for bucket with
name: f{bucket_name}"
                            else:
                                status = OperationStatus.SUCCESS
                                message = f"Successfully invoked
PreCreateHookHandler for AWS::S3::Bucket with name: {bucket_name}"

```

```

        else:
            status = OperationStatus.FAILED
            message = f"SSE Encryption Algorithm is incorrect for
bucket with name: {bucket_name}"
        else:
            status = OperationStatus.FAILED
            message = f"Bucket key not enabled for bucket with name:
{bucket_name}"

        if status == OperationStatus.FAILED:
            break
    else:
        status = OperationStatus.FAILED
        message = f"No SSE Encryption configurations for bucket with name:
{bucket_name}"
    else:
        status = OperationStatus.FAILED
        message = (
            f"Bucket Encryption not enabled for bucket with name:
{bucket_name}"
        )
    else:
        status = OperationStatus.FAILED
        message = "Resource properties for S3 Bucket target model are empty"

    if status == OperationStatus.FAILED:
        error_code = HandlerErrorCode.NonCompliant

    return ProgressEvent(status=status, message=message, errorCode=error_code)

def _validate_sqs_queue_encryption(queue: MutableMapping[str, Any]) ->
ProgressEvent:
    if not queue:
        return ProgressEvent(
            status=OperationStatus.FAILED,
            message="Resource properties for SQS Queue target model are empty",
            errorCode=HandlerErrorCode.NonCompliant,
        )
    queue_name = queue.get("QueueName")

    kms_key_id = queue.get(
        "KmsMasterKeyId"
    ) # "KmsMasterKeyId" is name of the property for an AWS::SQS::Queue

```

```

    if not kms_key_id:
        return ProgressEvent(
            status=OperationStatus.FAILED,
            message=f"Server side encryption turned off for queue with name:
{queue_name}",
            errorCode=HandlerErrorCode.NonCompliant,
        )

    return ProgressEvent(
        status=OperationStatus.SUCCESS,
        message=f"Successfully invoked PreCreateHookHandler for
targetAWS::SQS::Queue with name: {queue_name}",
    )

@hook.handler(HookInvocationPoint.CREATE_PRE_PROVISION)
def pre_create_handler(
    session: Optional[SessionProxy],
    request: HookHandlerRequest,
    callback_context: MutableMapping[str, Any],
    type_configuration: TypeConfigurationModel,
) -> ProgressEvent:
    target_name = request.hookContext.targetName
    if "AWS::S3::Bucket" == target_name:
        return _validate_s3_bucket_encryption(
            request.hookContext.targetModel.get("resourceProperties"),
            type_configuration.encryptionAlgorithm,
        )
    elif "AWS::SQS::Queue" == target_name:
        return _validate_sqs_queue_encryption(
            request.hookContext.targetModel.get("resourceProperties")
        )
    else:
        raise exceptions.InvalidRequest(f"Unknown target type: {target_name}")

def _validate_bucket_encryption_rules_not_updated(
    resource_properties, previous_resource_properties
) -> ProgressEvent:
    bucket_encryption_configs = resource_properties.get("BucketEncryption",
{}).get(
        "ServerSideEncryptionConfiguration", []
    )
    previous_bucket_encryption_configs = previous_resource_properties.get(

```

```
        "BucketEncryption", {}
    ).get("ServerSideEncryptionConfiguration", [])

    if len(bucket_encryption_configs) != len(previous_bucket_encryption_configs):
        return ProgressEvent(
            status=OperationStatus.FAILED,
            message=f"Current number of bucket encryption configs does not
match previous. Current has {str(len(bucket_encryption_configs))} configs while
previously there were {str(len(previous_bucket_encryption_configs))} configs",
            errorCode=HandlerErrorCode.NonCompliant,
        )

    for i in range(len(bucket_encryption_configs)):
        current_encryption_algorithm = (
            bucket_encryption_configs[i]
            .get("ServerSideEncryptionByDefault", {})
            .get("SSEAlgorithm")
        )
        previous_encryption_algorithm = (
            previous_bucket_encryption_configs[i]
            .get("ServerSideEncryptionByDefault", {})
            .get("SSEAlgorithm")
        )

        if current_encryption_algorithm != previous_encryption_algorithm:
            return ProgressEvent(
                status=OperationStatus.FAILED,
                message=f"Bucket Encryption algorithm can not be changed once
set. The encryption algorithm was changed to {current_encryption_algorithm} from
{previous_encryption_algorithm}.",
                errorCode=HandlerErrorCode.NonCompliant,
            )

    return ProgressEvent(
        status=OperationStatus.SUCCESS,
        message="Successfully invoked PreUpdateHookHandler for target:
AWS::SQS::Queue",
    )

def _validate_queue_encryption_not_disabled(
    resource_properties, previous_resource_properties
) -> ProgressEvent:
    if previous_resource_properties.get(
```



```
        "KmsMasterKeyId"
    ) and not resource_properties.get("KmsMasterKeyId"):
        return ProgressEvent(
            status=OperationStatus.FAILED,
            errorCode=HandlerErrorCode.NonCompliant,
            message="Queue encryption can not be disable",
        )
    else:
        return ProgressEvent(status=OperationStatus.SUCCESS)

@hook.handler(HookInvocationPoint.UPDATE_PRE_PROVISION)
def pre_update_handler(
    session: Optional[SessionProxy],
    request: BaseHookHandlerRequest,
    callback_context: MutableMapping[str, Any],
    type_configuration: MutableMapping[str, Any],
) -> ProgressEvent:
    target_name = request.hookContext.targetName
    if "AWS::S3::Bucket" == target_name:
        resource_properties =
request.hookContext.targetModel.get("resourceProperties")
        previous_resource_properties = request.hookContext.targetModel.get(
            "previousResourceProperties"
        )

        return _validate_bucket_encryption_rules_not_updated(
            resource_properties, previous_resource_properties
        )
    elif "AWS::SQS::Queue" == target_name:
        resource_properties =
request.hookContext.targetModel.get("resourceProperties")
        previous_resource_properties = request.hookContext.targetModel.get(
            "previousResourceProperties"
        )

        return _validate_queue_encryption_not_disabled(
            resource_properties, previous_resource_properties
        )
    else:
        raise exceptions.InvalidRequest(f"Unknown target type: {target_name}")
```

繼續進行下一個主題向 [註冊自訂勾點 AWS CloudFormation](#)。

向 註冊自訂勾點 AWS CloudFormation

建立自訂勾點後，您需要向 註冊它 AWS CloudFormation ，以便使用它。在本節中，您將了解如何封裝和註冊您的勾點，以便在 中使用 AWS 帳戶。

封裝勾點 (Java)

如果您已使用 Java 開發 Hook ，請使用 Maven 來封裝它。

在 Hook 專案的 目錄中，執行下列命令來建置您的 Hook、執行單位測試，並將您的專案封裝為檔案JAR，供您將 Hook 提交至 CloudFormation 登錄檔。

```
mvn clean package
```

註冊自訂勾點

註冊勾點

1. (選用) 透過提交 [configure](#)操作us-west-2，將預設 AWS 區域 名稱設定為。

```
$ aws configure
AWS Access Key ID [None]: <Your Access Key ID>
AWS Secret Access Key [None]: <Your Secret Key>
Default region name [None]: us-west-2
Default output format [None]: json
```

2. (選用) 下列命令會建置和封裝您的 Hook 專案，而無須註冊。

```
$ cfn submit --dry-run
```

3. 使用 CloudFormation CLI [submit](#)操作註冊您的勾點。

```
$ cfn submit --set-default
```

該命令會傳回下列命令。

```
{'ProgressStatus': 'COMPLETE'}
```

結果：您已成功註冊您的勾點。

驗證勾點可在您的帳戶中存取

確認您的勾點在您提交勾點的 AWS 帳戶 和 區域中可用。

1. 若要驗證您的勾點，請使用 [list-types](#) 命令列出新註冊的勾點，並傳回其摘要說明。

```
$ aws cloudformation list-types
```

命令會傳回下列輸出，也會顯示您可以在 AWS 帳戶 和 區域中啟用的公開可用勾點。

```
{
  "TypeSummaries": [
    {
      "Type": "HOOK",
      "TypeName": "MyCompany::Testing::MyTestHook",
      "DefaultVersionId": "00000001",
      "TypeArn": "arn:aws:cloudformation:us-west-2:ACCOUNT_ID/type/hook/MyCompany-Testing-MyTestHook",
      "LastUpdated": "2021-08-04T23:00:03.058000+00:00",
      "Description": "Verifies S3 bucket and SQS queues properties before creating or updating"
    }
  ]
}
```

2. TypeArn 從 Hook 的 list-type 輸出擷取 並儲存。

```
export HOOK_TYPE_ARN=arn:aws:cloudformation:us-west-2:ACCOUNT_ID/type/hook/MyCompany-Testing-MyTestHook
```

若要了解如何發佈勾點以供公開使用，請參閱 [公開發佈勾點](#)。

設定勾點

開發並註冊 Hook 之後，您可以將 Hook 發佈到登錄檔，AWS 帳戶 以在 中設定 Hook。

- 若要在帳戶中設定勾點，請使用 [SetTypeConfiguration](#) 操作。此操作會啟用勾點結構描述 properties 區段中定義的勾點屬性。在下列範例中，minBuckets 屬性會在組態 1 中設為 。

Note

透過在帳戶中啟用勾點，您授權勾點使用您定義的許可 AWS 帳戶。CloudFormation 會先移除非必要許可，再將許可傳遞給勾點。CloudFormation 建議客戶或 Hook 使用者檢閱 Hook 許可，並注意在您的帳戶中啟用 Hooks 之前允許 Hooks 的哪些許可。

指定相同帳戶中已註冊的 Hook 延伸模組的組態資料，以及 AWS 區域。

```
$ aws cloudformation set-type-configuration --region us-west-2
  --configuration '{"CloudFormationConfiguration":{"HookConfiguration":
{"HookInvocationStatus":"ENABLED","FailureMode":"FAIL","Properties":{"minBuckets":
"1","minQueues": "1", "encryptionAlgorithm": "aws:kms"}}}}'
  --type-arn $HOOK_TYPE_ARN
```

Important

若要讓您的 Hook 主動檢查堆疊的組態，您必須在帳戶中註冊和啟用 Hook 之後，在 HookConfiguration 區段 HookInvocationStatusENABLED 中將設定為。

在處理常式中存取 AWS APIs

如果您的 Hooks 在其任何處理常式中使用 AWS API，CFN-CLI 會自動建立 IAM 執行角色範本 `hook-role.yaml`。`hook-role.yaml` 範本是根據 Hook 結構描述中處理常式區段中每個處理常式指定的許可。如果在 [generate](#) 操作期間未使用 `--role-arn` 旗標，此堆疊中的角色將佈建並用作勾點的執行角色。

如需詳細資訊，請參閱 [從資源類型存取 AWS APIs](#)。

hook-role.yaml 範本

Note

如果您選擇建立自己的執行角色，我們強烈建議您只允許列出 `hooks.cloudformation.amazonaws.com` 和 `resources.cloudformation.amazonaws.com`，以練習最低權限原則。

下列範本使用 IAM、Amazon S3 和 Amazon SQS 許可。

```
AWSTemplateFormatVersion: 2010-09-09
Description: >
  This CloudFormation template creates a role assumed by CloudFormation during
  Hook operations on behalf of the customer.
Resources:
  ExecutionRole:
    Type: 'AWS::IAM::Role'
    Properties:
      MaxSessionDuration: 8400
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - resources.cloudformation.amazonaws.com
                - hooks.cloudformation.amazonaws.com
            Action: 'sts:AssumeRole'
            Condition:
              StringEquals:
                aws:SourceAccount: !Ref AWS::AccountId
              StringLike:
                aws:SourceArn: !Sub arn:${AWS::Partition}:cloudformation:
${AWS::Region}:${AWS::AccountId}:type/hook/MyCompany-Testing-MyTestHook/*
            Path: /
    Policies:
      - PolicyName: HookTypePolicy
        PolicyDocument:
          Version: 2012-10-17
          Statement:
            - Effect: Allow
              Action:
                - 's3:GetEncryptionConfiguration'
                - 's3:ListBucket'
                - 's3:ListAllMyBuckets'
                - 'sqs:GetQueueAttributes'
                - 'sqs:GetQueueUrl'
                - 'sqs:ListQueues'
              Resource: '*'
Outputs:
  ExecutionRoleArn:
    Value: !GetAtt
```

- ExecutionRole
- Arn

在中測試自訂勾點 AWS 帳戶

現在您已將對應至調用點的處理常式函數編碼，現在是測試 CloudFormation 堆疊上的自訂掛鉤的時候了。

FAIL 如果 CloudFormation 範本未佈建具有下列項目的 S3 儲存貯體，則勾點失敗模式會設為：

- Amazon S3 儲存貯體加密已設定。
- 已啟用儲存貯體的 Amazon S3 儲存貯體金鑰。
- Amazon S3 儲存貯體的加密演算法集是所需的正確演算法。
- AWS Key Management Service 金鑰 ID 已設定。

在下列範例中，建立名為 `my-hook-stack` 的範本，`my-failed-bucket-stack.yml` 其堆疊名稱為 `my-hook-stack`，該範本會失敗堆疊組態，並在資源佈建之前停止。

透過佈建堆疊來測試勾點

範例 1：佈建堆疊

佈建不合規的堆疊

1. 撰寫指定 S3 儲存貯體的範本。例如：`my-failed-bucket-stack.yml`。

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  S3Bucket:
    Type: 'AWS::S3::Bucket'
    Properties: {}
```

2. 建立堆疊，並在 AWS Command Line Interface () 中指定您的範本 AWS CLI。在下列範例中，將堆疊名稱指定為 `my-hook-stack`，`my-failed-bucket-stack.yml` 範本名稱指定為 `my-failed-bucket-stack.yml`。

```
$ aws cloudformation create-stack \
  --stack-name my-hook-stack \
  --template-body file:///my-failed-bucket-stack.yml
```

3. (選用) 透過指定堆疊名稱來檢視堆疊進度。在下列範例中，指定堆疊名稱 `my-hook-stack`。

```
$ aws cloudformation describe-stack-events \  
  --stack-name my-hook-stack
```

使用 `describe-stack-events` 操作來查看建立儲存貯體時的勾點失敗。以下是 命令的範例輸出。

```
{  
  "StackEvents": [  
    ...  
    {  
      "StackId": "arn:aws:cloudformation:us-west-2:ACCOUNT_ID:stack/my-hook-  
stack/2c693970-f57e-11eb-a0fb-061a2a83f0b9",  
      "EventId": "S3Bucket-CREATE_FAILED-2021-08-04T23:47:03.305Z",  
      "StackName": "my-hook-stack",  
      "LogicalResourceId": "S3Bucket",  
      "PhysicalResourceId": "",  
      "ResourceType": "AWS::S3::Bucket",  
      "Timestamp": "2021-08-04T23:47:03.305000+00:00",  
      "ResourceStatus": "CREATE_FAILED",  
      "ResourceStatusReason": "The following hook(s) failed:  
[MyCompany::Testing::MyTestHook]",  
      "ResourceProperties": "{}",  
      "ClientRequestToken": "Console-CreateStack-abe71ac2-ade4-  
a762-0499-8d34d91d6a92"  
    },  
    ...  
  ]  
}
```

結果：Hook 調用失敗堆疊組態，並停止資源佈建。

使用 CloudFormation 範本傳遞勾點驗證

1. 若要建立堆疊並通過勾點驗證，請更新範本，讓您的資源使用加密的 S3 儲存貯體。此範例使用範本 `my-encrypted-bucket-stack.yml`。

```
AWSTemplateFormatVersion: 2010-09-09  
Description: |  
  This CloudFormation template provisions an encrypted S3 Bucket  
Resources:
```

```

EncryptedS3Bucket:
  Type: 'AWS::S3::Bucket'
  Properties:
    BucketName: !Sub 'encryptedbucket-${AWS::Region}-${AWS::AccountId}'
    BucketEncryption:
      ServerSideEncryptionConfiguration:
        - ServerSideEncryptionByDefault:
            SSEAlgorithm: 'aws:kms'
            KMSMasterKeyID: !Ref EncryptionKey
            BucketKeyEnabled: true
    EncryptionKey:
      Type: 'AWS::KMS::Key'
      DeletionPolicy: Retain
      Properties:
        Description: KMS key used to encrypt the resource type artifacts
        EnableKeyRotation: true
        KeyPolicy:
          Version: 2012-10-17
          Statement:
            - Sid: Enable full access for owning account
              Effect: Allow
              Principal:
                AWS: !Ref 'AWS::AccountId'
              Action: 'kms:*'
              Resource: '*'
Outputs:
  EncryptedBucketName:
    Value: !Ref EncryptedS3Bucket

```

Note

不會針對略過的資源叫用勾點。

2. 建立堆疊並指定您的範本。在此範例中，堆疊名稱為 `my-encrypted-bucket-stack`。

```

$ aws cloudformation create-stack \
  --stack-name my-encrypted-bucket-stack \
  --template-body file:///my-encrypted-bucket-stack.yml \

```

3. (選用) 透過指定堆疊名稱來檢視堆疊進度。

```

$ aws cloudformation describe-stack-events \

```



```
--stack-name my-encrypted-bucket-stack
```

使用 `describe-stack-events` 命令來檢視回應。以下是 `describe-stack-events` 命令的範例。

```
{
  "StackEvents": [
    ...
    {
      "StackId": "arn:aws:cloudformation:us-west-2:ACCOUNT_ID:stack/my-encrypted-bucket-stack/82a97150-f57a-11eb-8eb2-06a6bdcc7779",
      "EventId": "EncryptedS3Bucket-CREATE_COMPLETE-2021-08-04T23:23:20.973Z",
      "StackName": "my-encrypted-bucket-stack",
      "LogicalResourceId": "EncryptedS3Bucket",
      "PhysicalResourceId": "encryptedbucket-us-west-2-ACCOUNT_ID",
      "ResourceType": "AWS::S3::Bucket",
      "Timestamp": "2021-08-04T23:23:20.973000+00:00",
      "ResourceStatus": "CREATE_COMPLETE",
      "ResourceProperties": "{\"BucketName\": \"encryptedbucket-us-west-2-071617338693\", \"BucketEncryption\": {\"ServerSideEncryptionConfiguration\": [{\"BucketKeyEnabled\": \"true\", \"ServerSideEncryptionByDefault\": {\"SSEAlgorithm\": \"aws:kms\", \"KMSMasterKeyID\": \"ENCRYPTION_KEY_ARN\"}}]}}",
      "ClientRequestToken": "Console-CreateStack-39df35ac-ca00-b7f6-5661-4e917478d075"
    },
    {
      "StackId": "arn:aws:cloudformation:us-west-2:ACCOUNT_ID:stack/my-encrypted-bucket-stack/82a97150-f57a-11eb-8eb2-06a6bdcc7779",
      "EventId": "EncryptedS3Bucket-CREATE_IN_PROGRESS-2021-08-04T23:22:59.410Z",
      "StackName": "my-encrypted-bucket-stack",
      "LogicalResourceId": "EncryptedS3Bucket",
      "PhysicalResourceId": "encryptedbucket-us-west-2-ACCOUNT_ID",
      "ResourceType": "AWS::S3::Bucket",
      "Timestamp": "2021-08-04T23:22:59.410000+00:00",
      "ResourceStatus": "CREATE_IN_PROGRESS",
      "ResourceStatusReason": "Resource creation Initiated",
      "ResourceProperties": "{\"BucketName\": \"encryptedbucket-us-west-2-071617338693\", \"BucketEncryption\": {\"ServerSideEncryptionConfiguration\": [{\"BucketKeyEnabled\": \"true\", \"ServerSideEncryptionByDefault\": {\"SSEAlgorithm\": \"aws:kms\", \"KMSMasterKeyID\": \"ENCRYPTION_KEY_ARN\"}}]}}",

```

```

        "ClientRequestToken": "Console-CreateStack-39df35ac-ca00-
b7f6-5661-4e917478d075"
      },
      {
        "StackId": "arn:aws:cloudformation:us-west-2:ACCOUNT_ID:stack/my-
encrypted-bucket-stack/82a97150-f57a-11eb-8eb2-06a6bdcc7779",
        "EventId": "EncryptedS3Bucket-6516081f-c1f2-4bfe-a0f0-cefa28679994",
        "StackName": "my-encrypted-bucket-stack",
        "LogicalResourceId": "EncryptedS3Bucket",
        "PhysicalResourceId": "",
        "ResourceType": "AWS::S3::Bucket",
        "Timestamp": "2021-08-04T23:22:58.349000+00:00",
        "ResourceStatus": "CREATE_IN_PROGRESS",
        "ResourceStatusReason": "Hook invocations complete. Resource creation
initiated",
        "ClientRequestToken": "Console-CreateStack-39df35ac-ca00-
b7f6-5661-4e917478d075"
      },
      ...
    ]
  }

```

結果：CloudFormation 已成功建立堆疊。Hook 的邏輯驗證AWS::S3::Bucket資源在佈建資源之前包含伺服器端加密。

範例 2：佈建堆疊

佈建不合規的堆疊

1. 撰寫指定 S3 儲存貯體的範本。例如 aes256-bucket.yml。

```

AWSTemplateFormatVersion: 2010-09-09
Description: |
  This CloudFormation template provisions an encrypted S3 Bucket
Resources:
  EncryptedS3Bucket:
    Type: 'AWS::S3::Bucket'
    Properties:
      BucketName: !Sub 'encryptedbucket-${AWS::Region}-${AWS::AccountId}'
      BucketEncryption:
        ServerSideEncryptionConfiguration:
          - ServerSideEncryptionByDefault:

```

```

        SSEAlgorithm: AES256
        BucketKeyEnabled: true
Outputs:
  EncryptedBucketName:
    Value: !Ref EncryptedS3Bucket

```

2. 建立堆疊，並在 中指定您的範本 AWS CLI。在下列範例中，將堆疊名稱指定為 `my-hook-stack` 範本名稱指定為 `aes256-bucket.yml`。

```

$ aws cloudformation create-stack \
  --stack-name my-hook-stack \
  --template-body file://aes256-bucket.yml

```

3. (選用) 透過指定堆疊名稱來檢視堆疊進度。在下列範例中，指定堆疊名稱 `my-hook-stack`。

```

$ aws cloudformation describe-stack-events \
  --stack-name my-hook-stack

```

使用 `describe-stack-events` 操作來查看建立儲存貯體時的勾點失敗。以下是 命令的範例輸出。

```

{
  "StackEvents": [
    ...
    {
      "StackId": "arn:aws:cloudformation:us-west-2:ACCOUNT_ID:stack/my-hook-stack/2c693970-f57e-11eb-a0fb-061a2a83f0b9",
      "EventId": "S3Bucket-CREATE_FAILED-2021-08-04T23:47:03.305Z",
      "StackName": "my-hook-stack",
      "LogicalResourceId": "S3Bucket",
      "PhysicalResourceId": "",
      "ResourceType": "AWS::S3::Bucket",
      "Timestamp": "2021-08-04T23:47:03.305000+00:00",
      "ResourceStatus": "CREATE_FAILED",
      "ResourceStatusReason": "The following hook(s) failed:
[MyCompany::Testing::MyTestHook]",
      "ResourceProperties": "{}",
      "ClientRequestToken": "Console-CreateStack-abe71ac2-ade4-a762-0499-8d34d91d6a92"
    },
    ...
  ]
}

```

```
}
```

結果：Hook 調用失敗堆疊組態，並停止資源佈建。由於 S3 儲存貯體加密設定不正確，堆疊失敗。此儲存貯體使用 `aws:kms` 時，需要勾點類型組態 `AES256`。

使用 CloudFormation 範本傳遞勾點驗證

1. 若要建立堆疊並通過勾點驗證，請更新範本，讓您的資源使用加密的 S3 儲存貯體。此範例使用範本 `kms-bucket-and-queue.yml`。

```
AWSTemplateFormatVersion: 2010-09-09
Description: |
  This CloudFormation template provisions an encrypted S3 Bucket
Resources:
  EncryptedS3Bucket:
    Type: 'AWS::S3::Bucket'
    Properties:
      BucketName: !Sub 'encryptedbucket-${AWS::Region}-${AWS::AccountId}'
      BucketEncryption:
        ServerSideEncryptionConfiguration:
          - ServerSideEncryptionByDefault:
              SSEAlgorithm: 'aws:kms'
              KMSMasterKeyID: !Ref EncryptionKey
            BucketKeyEnabled: true
  EncryptedQueue:
    Type: 'AWS::SQS::Queue'
    Properties:
      QueueName: 'encryptedqueue-${AWS::Region}-${AWS::AccountId}'
      KmsMasterKeyId: !Ref EncryptionKey
  EncryptionKey:
    Type: 'AWS::KMS::Key'
    DeletionPolicy: Retain
    Properties:
      Description: KMS key used to encrypt the resource type artifacts
      EnableKeyRotation: true
      KeyPolicy:
        Version: 2012-10-17
        Statement:
          - Sid: Enable full access for owning account
            Effect: Allow
            Principal:
              AWS: !Ref 'AWS::AccountId'
```

```

        Action: 'kms:*'
        Resource: '*'
Outputs:
  EncryptedBucketName:
    Value: !Ref EncryptedS3Bucket
  EncryptedQueueName:
    Value: !Ref EncryptedQueue

```

Note

不會針對略過的資源叫用勾點。

2. 建立堆疊並指定您的範本。在此範例中，堆疊名稱為 `my-encrypted-bucket-stack`。

```

$ aws cloudformation create-stack \
  --stack-name my-encrypted-bucket-stack \
  --template-body file://kms-bucket-and-queue.yml

```

3. (選用) 透過指定堆疊名稱來檢視堆疊進度。

```

$ aws cloudformation describe-stack-events \
  --stack-name my-encrypted-bucket-stack

```

使用 `describe-stack-events` 命令來檢視回應。以下是 `describe-stack-events` 命令的範例。

```

{
  "StackEvents": [
    ...
    {
      "StackId": "arn:aws:cloudformation:us-west-2:ACCOUNT_ID:stack/my-encrypted-bucket-stack/82a97150-f57a-11eb-8eb2-06a6bdcc7779",
      "EventId": "EncryptedS3Bucket-CREATE_COMPLETE-2021-08-04T23:23:20.973Z",
      "StackName": "my-encrypted-bucket-stack",
      "LogicalResourceId": "EncryptedS3Bucket",
      "PhysicalResourceId": "encryptedbucket-us-west-2-ACCOUNT_ID",
      "ResourceType": "AWS::S3::Bucket",
      "Timestamp": "2021-08-04T23:23:20.973000+00:00",
      "ResourceStatus": "CREATE_COMPLETE",

```

```

        "ResourceProperties": "{\"BucketName\": \"encryptedbucket-us-
west-2-071617338693\", \"BucketEncryption\": {\"ServerSideEncryptionConfiguration\":
[ {\"BucketKeyEnabled\": \"true\", \"ServerSideEncryptionByDefault\": {\"SSEAlgorithm
\": \"aws:kms\", \"KMSMasterKeyID\": \"ENCRYPTION_KEY_ARM\"} } ] } }\",
        \"ClientRequestToken\": \"Console-CreateStack-39df35ac-ca00-
b7f6-5661-4e917478d075\"
    },
    {
        \"StackId\": \"arn:aws:cloudformation:us-west-2:ACCOUNT_ID:stack/my-
encrypted-bucket-stack/82a97150-f57a-11eb-8eb2-06a6bdcc7779\",
        \"EventId\": \"EncryptedS3Bucket-
CREATE_IN_PROGRESS-2021-08-04T23:22:59.410Z\",
        \"StackName\": \"my-encrypted-bucket-stack\",
        \"LogicalResourceId\": \"EncryptedS3Bucket\",
        \"PhysicalResourceId\": \"encryptedbucket-us-west-2-ACCOUNT_ID\",
        \"ResourceType\": \"AWS::S3::Bucket\",
        \"Timestamp\": \"2021-08-04T23:22:59.410000+00:00\",
        \"ResourceStatus\": \"CREATE_IN_PROGRESS\",
        \"ResourceStatusReason\": \"Resource creation Initiated\",
        \"ResourceProperties\": \"{\\\"BucketName\\\": \\\"encryptedbucket-us-
west-2-071617338693\\\", \\\"BucketEncryption\\\": {\\\"ServerSideEncryptionConfiguration\\\":
[ {\\\"BucketKeyEnabled\\\": \\\"true\\\", \\\"ServerSideEncryptionByDefault\\\": {\\\"SSEAlgorithm
\\\": \\\"aws:kms\\\", \\\"KMSMasterKeyID\\\": \\\"ENCRYPTION_KEY_ARM\\\"} } ] } }\",
        \"ClientRequestToken\": \"Console-CreateStack-39df35ac-ca00-
b7f6-5661-4e917478d075\"
    },
    {
        \"StackId\": \"arn:aws:cloudformation:us-west-2:ACCOUNT_ID:stack/my-
encrypted-bucket-stack/82a97150-f57a-11eb-8eb2-06a6bdcc7779\",
        \"EventId\": \"EncryptedS3Bucket-6516081f-c1f2-4bfe-a0f0-cefa28679994\",
        \"StackName\": \"my-encrypted-bucket-stack\",
        \"LogicalResourceId\": \"EncryptedS3Bucket\",
        \"PhysicalResourceId\": \"\",
        \"ResourceType\": \"AWS::S3::Bucket\",
        \"Timestamp\": \"2021-08-04T23:22:58.349000+00:00\",
        \"ResourceStatus\": \"CREATE_IN_PROGRESS\",
        \"ResourceStatusReason\": \"Hook invocations complete. Resource creation
initiated\",
        \"ClientRequestToken\": \"Console-CreateStack-39df35ac-ca00-
b7f6-5661-4e917478d075\"
    },
    ...
]

```

```
}
```

結果：CloudFormation 已成功建立堆疊。Hook 的邏輯驗證AWS::S3::Bucket資源在佈建資源之前包含伺服器端加密。

更新自訂勾點

更新自訂勾點允許在 CloudFormation 登錄檔中提供勾點中的修訂。

若要更新自訂勾點，請透過 CloudFormation CLI [submit](#)操作將您的修訂提交至 CloudFormation 登錄檔。

```
$ cfn submit
```

若要在帳戶中指定預設的 Hook 版本，請使用 [set-type-default-version](#)命令並指定類型、類型名稱和版本 ID。

```
$ aws cloudformation set-type-default-version \  
  --type HOOK \  
  --type-name MyCompany::Testing::MyTestHook \  
  --version-id 00000003
```

若要擷取有關 Hook 版本的資訊，請使用 [list-type-versions](#)。

```
$ aws cloudformation list-type-versions \  
  --type HOOK \  
  --type-name "MyCompany::Testing::MyTestHook"
```

從 CloudFormation 登錄檔取消註冊自訂勾點

取消註冊自訂 Hook 會將延伸模組或延伸模組版本標記為 CloudFormation 登錄DEPRECATED檔中的，這會將其從作用中使用中移除。一旦棄用，自訂勾點就無法在 CloudFormation 操作中使用。

Note

取消註冊勾點之前，您必須個別取消註冊該延伸模組的所有先前作用中版本。如需詳細資訊，請參閱[DeregisterType](#)。

若要取消註冊勾點，請使用 [deregister-type](#) 操作並指定您的勾點 ARN。

```
$ aws cloudformation deregister-type \  
  --arn HOOK_TYPE_ARN
```

此命令不會產生輸出。

公開發佈勾點

若要開發公有第三方勾點，請將您的勾點開發為私有延伸。然後，在您要公開使用延伸模組的每個 AWS 區域中：

1. 在 CloudFormation 登錄檔中將 Hook 註冊為私有延伸。
2. 測試您的勾點，以確保其符合在 CloudFormation 登錄檔中發佈的所有必要要求。
3. 將您的勾點發佈至 CloudFormation 登錄檔。

Note

在指定區域中發佈任何延伸之前，您必須先註冊為該區域中的延伸發佈者。若要同時在多個區域中執行此操作，請參閱《AWS CloudFormation CLI 使用者指南》中的[使用 StackSets 在多個區域中發佈擴充](#)功能。

開發並註冊 Hook 之後，您可以將它發佈到 CloudFormation 登錄檔做為第三方公有延伸，讓一般 CloudFormation 使用者公開使用。

公有第三方勾點可讓您提供 CloudFormation 使用者在佈建之前主動檢查 AWS 資源的組態。與私有勾點一樣，公有勾點的處理方式與 CloudFormation AWS 中發佈的任何勾點相同。

發佈到登錄檔的勾點，可供發佈其 AWS 區域所在中的所有 CloudFormation 使用者查看。然後，使用者可以在其帳戶中啟用您的擴充功能，以便在其範本中使用。如需詳細資訊，請參閱 AWS CloudFormation 《使用者指南》中的[使用 CloudFormation 登錄檔的第三方公有延伸](#)模組。

測試自訂勾點以供公開使用

若要發佈已註冊的自訂勾點，它必須通過為其定義的所有測試要求。以下是將自訂勾點發佈為第三方延伸模組之前所需的需求清單。

每個處理常式和目標都會經過兩次測試。一次用於 SUCCESS，一次用於 FAILED。

- 針對SUCCESS回應案例：
 - 狀態必須為 SUCCESS。
 - 不得傳回錯誤碼。
 - 如果指定，回呼延遲應設為0秒。
- 對於FAILED回應案例：
 - 狀態必須為 FAILED。
 - 必須傳回錯誤碼。
 - 必須有訊息作為回應。
 - 如果指定，回呼延遲應設為0秒。
- 對於IN_PROGRESS回應案例：
 - 不得傳回錯誤碼。
 - Result 欄位不得設定為回應。

指定用於合約測試的輸入資料

根據預設，會使用您於 Hook 結構描述中定義的模式所產生的輸入屬性 CloudFormation 來執行合約測試。不過，大多數勾點都足夠複雜，因此預先建立或預先更新佈建堆疊的輸入屬性需要了解佈建的資源。若要解決此問題，您可以指定執行其合約測試 CloudFormation 時使用的輸入。

CloudFormation 提供兩種方式，可讓您指定輸入資料，以便在執行合約測試時使用：

- 覆寫檔案

使用 overrides 檔案提供輕量方式，可指定特定屬性的輸入資料 CloudFormation，以便在 preCreate、preUpdate和 preDelete操作測試期間使用。

- 輸入檔案

在以下情況下，您也可以使用多個input檔案來指定合約測試輸入資料：

- 您想要或需要為建立、更新和刪除操作指定不同的輸入資料，或測試的無效資料。
- 您想要指定多個不同的輸入資料集。

使用覆寫檔案指定輸入資料

以下是使用 overrides 檔案的 Amazon S3 Hook 輸入資料範例。

```
{
  "CREATE_PRE_PROVISION": {
    "AWS::S3::Bucket": {
      "resourceProperties": {
        "/BucketName": "encryptedbucket-us-west-2-contractor",
        "/BucketEncryption/ServerSideEncryptionConfiguration": [
          {
            "BucketKeyEnabled": true,
            "ServerSideEncryptionByDefault": {
              "KMSMasterKeyID": "KMS-KEY-ARN",
              "SSEAlgorithm": "aws:kms"
            }
          }
        ]
      }
    },
    "AWS::SQS::Queue": {
      "resourceProperties": {
        "/QueueName": "MyQueueContract",
        "/KmsMasterKeyId": "hellocontract"
      }
    }
  },
  "UPDATE_PRE_PROVISION": {
    "AWS::S3::Bucket": {
      "resourceProperties": {
        "/BucketName": "encryptedbucket-us-west-2-contractor",
        "/BucketEncryption/ServerSideEncryptionConfiguration": [
          {
            "BucketKeyEnabled": true,
            "ServerSideEncryptionByDefault": {
              "KMSMasterKeyID": "KMS-KEY-ARN",
              "SSEAlgorithm": "aws:kms"
            }
          }
        ]
      },
      "previousResourceProperties": {
        "/BucketName": "encryptedbucket-us-west-2-contractor",
        "/BucketEncryption/ServerSideEncryptionConfiguration": [
          {
            "BucketKeyEnabled": true,
            "ServerSideEncryptionByDefault": {
```



```
}
```

使用輸入檔案指定輸入資料

使用 `input` 檔案來指定不同類型的輸入資料 CloudFormation，以供使用 `:preCreate` 輸入、`preUpdate` 輸入和無效輸入。每種類型的資料都會在個別的檔案中指定。您也可以為合約測試指定多組輸入資料。

若要指定 CloudFormation 要在合約測試中使用的 `input` 檔案，請將 `inputs` 資料夾新增至 Hooks 專案的根目錄。然後新增您的輸入檔案。

使用以下命名慣例指定檔案包含的輸入資料類型，其中 *n* 是整數：

- `inputs_n_pre_create.json`：使用檔案搭配 `preCreate` 處理常式來指定用於建立資源的輸入。
- `inputs_n_pre_update.json`：使用檔案搭配 `preUpdate` 處理常式來指定用於更新資源的輸入。
- `inputs_n_pre_delete.json`：使用檔案搭配 `preDelete` 處理常式來指定用於刪除資源的輸入。
- `inputs_n_invalid.json`：用於指定無效的輸入進行測試。

若要為合約測試指定多組輸入資料，請遞增檔案名稱中的整數，以排序您的輸入資料集。例如，您的第一組輸入檔案應該命名為 `inputs_1_pre_create.json`、`inputs_1_pre_update.json` 和 `inputs_1_pre_invalid.json`。您的下一組將命名為 `inputs_2_pre_create.json`、`inputs_2_pre_update.json` 和 `inputs_2_pre_invalid.json`，以此類推。

每個輸入檔案都是 JSON 檔案，僅包含用於測試的資源屬性。

以下是 `inputs` 使用輸入檔案 Amazon S3 指定輸入資料的範例目錄。

`inputs_1_pre_create.json`

以下是 `inputs_1_pre_create.json` 合約測試的範例。

```
{
  "AWS::S3::Bucket": {
    "resourceProperties": {
      "AccessControl": "BucketOwnerFullControl",
      "AnalyticsConfigurations": [],
      "BucketEncryption": {
        "ServerSideEncryptionConfiguration": [
          {
```

```
        "BucketKeyEnabled": true,
        "ServerSideEncryptionByDefault": {
            "KMSMasterKeyID": "KMS-KEY-ARN",
            "SSEAlgorithm": "aws:kms"
        }
    ]
},
"BucketName": "encryptedbucket-us-west-2"
}
},
"AWS::SQS::Queue": {
    "resourceProperties": {
        "QueueName": "MyQueue",
        "KmsMasterKeyId": "KMS-KEY-ARN"
    }
}
}
```

inputs_1_pre_update.json

以下是inputs_1_pre_update.json合約測試的範例。

```
{
  "AWS::S3::Bucket": {
    "resourceProperties": {
      "BucketEncryption": {
        "ServerSideEncryptionConfiguration": [
          {
            "BucketKeyEnabled": true,
            "ServerSideEncryptionByDefault": {
              "KMSMasterKeyID": "KMS-KEY-ARN",
              "SSEAlgorithm": "aws:kms"
            }
          }
        ]
      },
      "BucketName": "encryptedbucket-us-west-2"
    },
    "previousResourceProperties": {
      "BucketEncryption": {
        "ServerSideEncryptionConfiguration": [
          {
            "BucketKeyEnabled": true,
```

```

        "ServerSideEncryptionByDefault": {
            "KMSMasterKeyID": "KMS-KEY-ARN",
            "SSEAlgorithm": "aws:kms"
        }
    ]
},
"BucketName": "encryptedbucket-us-west-2"
}
}
}

```

inputs_1_invalid.json

以下是inputs_1_invalid.json合約測試的範例。

```

{
  "AWS::S3::Bucket": {
    "resourceProperties": {
      "AccessControl": "BucketOwnerFullControl",
      "AnalyticsConfigurations": [],
      "BucketEncryption": {
        "ServerSideEncryptionConfiguration": [
          {
            "ServerSideEncryptionByDefault": {
              "SSEAlgorithm": "AES256"
            }
          }
        ]
      },
      "BucketName": "encryptedbucket-us-west-2"
    }
  },
  "AWS::SQS::Queue": {
    "resourceProperties": {
      "NotValid": "The property of this resource is not valid."
    }
  }
}

```

inputs_1_invalid_pre_update.json

以下是inputs_1_invalid_pre_update.json合約測試的範例。

```
{
  "AWS::S3::Bucket": {
    "resourceProperties": {
      "BucketEncryption": {
        "ServerSideEncryptionConfiguration": [
          {
            "BucketKeyEnabled": true,
            "ServerSideEncryptionByDefault": {
              "KMSEncryption": {
                "KMSMasterKeyID": "KMS-KEY-ARN",
                "SSEAlgorithm": "AES256"
              }
            }
          }
        ]
      },
      "BucketName": "encryptedbucket-us-west-2"
    },
    "previousResourceProperties": {
      "BucketEncryption": {
        "ServerSideEncryptionConfiguration": [
          {
            "BucketKeyEnabled": true,
            "ServerSideEncryptionByDefault": {
              "KMSEncryption": {
                "KMSMasterKeyID": "KMS-KEY-ARN",
                "SSEAlgorithm": "aws:kms"
              }
            }
          }
        ]
      },
      "BucketName": "encryptedbucket-us-west-2"
    }
  }
}
```

如需詳細資訊，請參閱《AWS CloudFormation CLI 使用者指南》中的[發佈擴充功能以供公眾使用](#)。

AWS CloudFormation 勾點的結構描述語法參考

本節說明您用來開發 AWS CloudFormation Hooks 的結構描述語法。

勾點包含由 JSON 結構描述和勾點處理常式表示的勾點規格。建立自訂勾點的第一步是建立定義勾點、其屬性及其屬性的結構描述模型。當您使用 CloudFormation CLI [init](#) 命令初始化自訂 Hook 專案時，會為您建立 Hook 結構描述檔案。使用此結構描述檔案作為定義自訂勾點形狀和語意的起點。

結構描述語法

下列結構描述是勾點的結構。

```
{
  "typeName": "string",
  "description": "string",
  "sourceUrl": "string",
  "documentationUrl": "string",
  "definitions": {
    "definitionName": {
      . . .
    }
  },
  "typeConfiguration": {
    "properties": {
      "propertyName": {
        "description": "string",
        "type": "string",
        . . .
      },
    },
  },
  "required": [
    "propertyName"
    . . .
  ],
  "additionalProperties": false
},
"handlers": {
  "preCreate": {
    "targetNames": [
    ],
    "permissions": [
    ]
  },
  "preUpdate": {
    "targetNames": [
    ],
    "permissions": [
    ]
  },
  "preDelete": {
    "targetNames": [
    ],
  },
}
```



```

        "permissions": [
        ]
    },
    "additionalProperties": false
}

```

typeName

勾點的唯一名稱。為 Hook 指定三個部分的命名空間，建議模式為 `Organization::Service::Hook`。

Note

下列組織命名空間已保留，無法用於您的勾點類型名稱：

- Alexa
- AMZN
- Amazon
- ASK
- AWS
- Custom
- Dev

必要：是

模式：`^[a-zA-Z0-9]{2,64}::[a-zA-Z0-9]{2,64}::[a-zA-Z0-9]{2,64}$`

下限：10

上限：196

description

CloudFormation 主控台中顯示的勾點簡短描述。

必要：是

sourceUrl

如果為公有，則 Hook 原始碼的 URL。

必要：否

上限：4096

documentationUrl

提供勾點詳細文件的頁面 URL。

必要：是

模式：`^https\:\/\/[0-9a-zA-Z]([-.\w]*[0-9a-zA-Z])(\:[0-9]*)*([\?/#].*)?$`

上限：4096

Note

雖然 Hook 結構描述應包含完整且準確的屬性描述，但您可以使用 `documentationUrl` 屬性為使用者提供更多詳細資訊，包括範例、使用案例和其他詳細資訊。

definitions

使用 `definitions` 區塊提供共用的 Hook 屬性結構描述。

使用 `definitions` 區段來定義結構描述元素的最佳實務，可用於勾點類型結構描述中的多個點。然後，您可以使用 JSON 指標，在勾點類型結構描述的適當位置參考該元素。

必要：否

typeConfiguration

Hook 組態資料的定義。

必要：是

properties

勾點的屬性。勾點的所有屬性都必須在結構描述中表示。將勾點結構描述屬性與勾點類型組態屬性對齊。

Note

不允許巢狀屬性。反之，請在 `definitions` 元素中定義任何巢狀屬性，並使用 `$ref` 指標在所需的屬性中參考它們。

additionalProperties

`additionalProperties` 必須設定為 `false`。勾點的所有屬性都必須在結構描述中表示：不允許任意輸入。

必要：是

有效值：`false`

handlers

處理常式會指定可啟動結構描述中定義的勾點的操作，例如勾點叫用點。例如，`preUpdate`在處理常式中所有指定目標的更新操作之前，會叫用處理常式。

有效值：`preCreate` | `preUpdate` | `preDelete`

Note

必須至少為處理常式指定一個值。

Important

導致狀態的堆疊操作`UpdateCleanup`不會叫用勾點。例如，在以下兩個案例中，不會叫用 Hook 的`preDelete`處理常式：

- 從範本中移除一個資源後，堆疊會更新。
- 會刪除具有更新類型取代的資源。

targetNames

Hook 目標的類型名稱字串陣列。例如，如果`preCreate`處理常式有 `AWS::S3::Bucket`目標，則 Hook 會在預先佈建階段針對 Amazon S3 儲存貯體執行。

- `TargetName`

為每個實作的處理常式指定至少一個目標名稱。

模式：`^[a-zA-Z0-9]{2,64}::[a-zA-Z0-9]{2,64}::[a-zA-Z0-9]{2,64}$`

下限：1

必要：是

⚠ Warning

SSM SecureString 和 Secrets Manager 動態參考在傳遞至 Hooks 之前不會解析。

permissions

字串陣列，指定呼叫處理常式所需的 AWS 許可。

必要：是

additionalProperties

additionalProperties 必須設定為 false。勾點的所有屬性都必須在結構描述中表示：不允許任意輸入。

必要：是

有效值：false

勾點結構描述範例

範例 1

Java 和 Python 演練使用以下程式碼範例。以下是名為 mycompany-testing-mytesthook.json 的勾點的範例結構。

```
{
  "typeName": "MyCompany::Testing::MyTestHook",
  "description": "Verifies S3 bucket and SQS queues properties before create and update",
  "sourceUrl": "https://mycorp.com/my-repo.git",
  "documentationUrl": "https://mycorp.com/documentation",
  "typeConfiguration": {
    "properties": {
      "minBuckets": {
        "description": "Minimum number of compliant buckets",
        "type": "string"
      },
      "minQueues": {
        "description": "Minimum number of compliant queues",
```

```
        "type":"string"
    },
    "encryptionAlgorithm":{
        "description":"Encryption algorithm for SSE",
        "default":"AES256",
        "type":"string"
    }
},
"required":[

],
"additionalProperties":false
},
"handlers":{
    "preCreate":{
        "targetNames":[
            "AWS::S3::Bucket",
            "AWS::SQS::Queue"
        ],
        "permissions":[

        ]
    },
    "preUpdate":{
        "targetNames":[
            "AWS::S3::Bucket",
            "AWS::SQS::Queue"
        ],
        "permissions":[

        ]
    },
    "preDelete":{
        "targetNames":[
            "AWS::S3::Bucket",
            "AWS::SQS::Queue"
        ],
        "permissions":[
            "s3:ListBucket",
            "s3:ListAllMyBuckets",
            "s3:GetEncryptionConfiguration",
            "sqs:ListQueues",
            "sqs:GetQueueAttributes",
            "sqs:GetQueueUrl"
        ]
    }
}
```

```

    ]
  }
},
"additionalProperties":false
}

```

範例 2

下列範例是使用 STACK和 CAHNGE_SET 的結構描述targetNames，以堆疊範本和變更集操作為目標。

```

{
  "typeName":"MyCompany::Testing::MyTestHook",
  "description":"Verifies Stack and Change Set properties before create and update",
  "sourceUrl":"https://mycorp.com/my-repo.git",
  "documentationUrl":"https://mycorp.com/documentation",
  "typeConfiguration":{
    "properties":{
      "minBuckets":{
        "description":"Minimum number of compliant buckets",
        "type":"string"
      },
      "minQueues":{
        "description":"Minimum number of compliant queues",
        "type":"string"
      },
      "encryptionAlgorithm":{
        "description":"Encryption algorithm for SSE",
        "default":"AES256",
        "type":"string"
      }
    },
    "required":[
    ],
    "additionalProperties":false
  },
  "handlers":{
    "preCreate":{
      "targetNames":[
        "STACK",
        "CHANGE_SET"
      ],
      "permissions":[

```

```
    ]
  },
  "preUpdate":{
    "targetNames":[
      "STACK"
    ],
    "permissions":[
    ]
  },
  "preDelete":{
    "targetNames":[
      "STACK"
    ],
    "permissions":[
    ]
  }
},
"additionalProperties":false
}
```

停用和啟用 AWS CloudFormation 勾點

本主題說明如何停用，然後重新啟用 勾點，暫時防止其在您的帳戶中處於作用中狀態。當您需要在不受 Hooks 干擾的情況下調查問題時，停用 Hooks 非常有用。

在帳戶中停用和啟用勾點（主控台）

在帳戶中停用勾點

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/cloudformation> 開啟 AWS CloudFormation 主控台。
2. 在畫面頂端的導覽列上，選擇 AWS 區域 勾點所在的。
3. 從導覽窗格中，選擇勾點。
4. 選擇您要停用的勾點名稱。
5. 在勾點詳細資訊頁面的勾點名稱右側，選擇停用按鈕。
6. 出現確認提示時，請選擇停用勾點。

重新啟用先前停用的勾點

1. 登入 AWS Management Console，並在 <https://console.aws.amazon.com/cloudformation> 開啟 AWS CloudFormation 主控台。
2. 在畫面頂端的導覽列上，選擇 AWS 區域 勾點所在的。
3. 從導覽窗格中，選擇勾點。
4. 選擇您要啟用的勾點名稱。
5. 在勾點詳細資訊頁面的勾點名稱右側，選擇啟用按鈕。
6. 出現確認提示時，請選擇啟用勾點。

在帳戶中停用和啟用勾點 (AWS CLI)

⚠ Important

停用和啟用勾點的 AWS CLI 命令會將整個勾點組態取代為 `--configuration` 選項中指定的值。為了避免意外的變更，您必須包含執行這些命令時想要保留的所有現有設定。若要檢視目前的組態資料，請使用 [describe-type](#) 命令。

停用勾點

使用下列 [set-type-configuration](#) 命令並指定 `HookInvocationStatus` 做為 `DISABLED` 來停用勾點。將預留位置取代為您的特定值。

```
aws cloudformation set-type-configuration \  
  --configuration '{"CloudFormationConfiguration":{"HookConfiguration":  
{"HookInvocationStatus": "DISABLED", "FailureMode": "FAIL",  
"TargetOperations": ["STACK", "RESOURCE", "CHANGE_SET"], "Properties":{}}}}' \  
  --type-arn "arn:aws:cloudformation:us-west-2:123456789012:type/hook/MyTestHook" \  
  --region us-west-2
```

重新啟用先前停用的勾點

使用下列 [set-type-configuration](#) 命令並指定 `HookInvocationStatus` 為 `ENABLED` 以重新啟用勾點。將預留位置取代為您的特定值。

```
aws cloudformation set-type-configuration \  
  --configuration '{"CloudFormationConfiguration":{"HookConfiguration":  
{"HookInvocationStatus": "ENABLED", "FailureMode": "FAIL",  
"TargetOperations": ["STACK", "RESOURCE", "CHANGE_SET"], "Properties":{}}}}' \  
  --type-arn "arn:aws:cloudformation:us-west-2:123456789012:type/hook/MyTestHook" \  
  --region us-west-2
```

如需詳細資訊，請參閱 [勾點組態結構描述語法參考](#)。

勾點組態結構描述語法參考

本節概述用於設定勾點的結構描述語法。CloudFormation 在中叫用勾點時，會在執行時間使用此組態結構描述 AWS 帳戶。

若要讓勾點主動檢查堆疊的組態，請在您的帳戶中註冊並啟用勾點ENABLED之後，將 HookInvocationStatus 設定為。

主題

- [勾點組態結構描述屬性](#)
- [勾點組態範例](#)
- [AWS CloudFormation 勾點堆疊層級篩選條件](#)
- [AWS CloudFormation 勾點目標篩選條件](#)
- [使用萬用字元搭配 Hook 目標名稱](#)

Note

Hook 組態可儲存的最大資料量為 300 KB。這是對 [SetTypeConfiguration](#) 操作的 Configuration 請求參數施加的所有限制之外的。

勾點組態結構描述屬性

下列結構描述是勾點組態結構描述的結構。

```
{
  "CloudFormationConfiguration": {
    "HookConfiguration": {
      "HookInvocationStatus": "ENABLED",
      "TargetOperations": "STACK",
      "FailureMode": "FAIL",
      "Properties": {
        ...
      }
    }
  }
}
```

HookConfiguration

勾點組態支援在堆疊層級、失敗模式和勾點屬性值啟用或停用勾點。

Hook 組態支援下列屬性。

HookInvocationStatus

指定勾點是 ENABLED 還是 DISABLED。

有效值：ENABLED | DISABLED

TargetOperations

指定要執行勾點的操作類型。

有效值：STACK | RESOURCE | CHANGE_SET | CLOUD_CONTROL

TargetStacks

可用於回溯相容性。請 *HookInvocationStatus* 改用。

如果模式設定為 ALL，則勾點會在 UPDATE、CREATE 或 DELETE 資源操作期間套用至您帳戶中的所有堆疊。

如果模式設定為 NONE，則勾點不會套用至您帳戶中的堆疊。

有效值：ALL | NONE

FailureMode

此欄位會告知服務如何處理勾點故障。

- 如果模式設定為 FAIL，且勾點失敗，則失敗組態會停止佈建資源並復原堆疊。
- 如果模式設定為 WARN 且勾點失敗，則警告組態允許佈建繼續出現警告訊息。

有效值：FAIL | WARN

Properties

指定勾點執行時間屬性。這些應符合 Hooks 結構描述支援的屬性形狀。

勾點組態範例

如需從 設定勾點的範例 AWS CLI，請參閱下列各節：

- [啟用 Guard Hook \(AWS CLI\)](#)
- [啟用 Lambda Hook \(AWS CLI\)](#)

AWS CloudFormation 勾點堆疊層級篩選條件

您可以新增堆疊層級篩選條件至 CloudFormation Hooks，以根據堆疊名稱和角色鎖定特定堆疊。當您有多個具有相同資源類型的堆疊，但勾點適用於特定堆疊時，這很有用。

本節說明這些篩選條件的運作方式，並提供您可以遵循的範例。

沒有堆疊層級篩選的勾點組態基本結構如下所示：

```
{
  "CloudFormationConfiguration": {
    "HookConfiguration": {
      "HookInvocationStatus": "ENABLED",
      "TargetOperations": [
        "STACK",
        "RESOURCE"
      ],
      "FailureMode": "WARN",
      "Properties": {}
    }
  }
}
```

如需 HookConfiguration 語法的詳細資訊，請參閱 [勾點組態結構描述語法參考](#)。

若要使用堆疊層級篩選條件，請在下新增 StackFilters 金鑰 HookConfiguration。

StackFilters 金鑰有一個必要成員，並且有兩個選用成員。

- FilteringCriteria (必要)
- StackNames (選用)
- StackRoles (選用)

StackNames 或 StackRoles 屬性是選用的。但是，您必須指定這些屬性中至少其中一種屬性。

如果您建立鎖定 [Cloud Control API](#) 操作的勾點，則會忽略所有堆疊層級篩選條件。

FilteringCriteria

FilteringCriteria 是指定篩選行為的必要參數。它可以設定為 ALL 或 ANY。

- ALL 如果所有篩選條件都相符，會叫用勾點。
- ANY 如果符合任何一個篩選條件，會叫用勾點。

StackNames

若要在 Hooks 組態中將一或多個堆疊名稱指定為篩選條件，請使用下列 JSON 結構：

```
"StackNames": {
  "Include": [
    "string"
  ],
  "Exclude": [
    "string"
  ]
}
```

您必須指定下列其中一項：

- Include：要包含的堆疊名稱清單。只有此清單中指定的堆疊會叫用勾點。
 - 類型：字串陣列
 - 項目上限：50
 - 最小項目：1
- Exclude：要排除的堆疊名稱清單。除了此處列出的堆疊之外，所有堆疊都會叫用勾點。
 - 類型：字串陣列
 - 項目上限：50
 - 最小項目：1

Include 和 Exclude 陣列中的每個堆疊名稱都必須遵守下列模式和長度要求：

- 模式：`^[a-zA-Z][-a-zA-Z0-9]*$`
- 長度上限：128

StackRoles

若要在勾點組態中將一或多個 [IAM 角色](#) 指定為篩選條件，請使用下列 JSON 結構：

```
"StackRoles": {
  "Include": [
    "string"
  ],
  "Exclude": [
    "string"
  ]
}
```

您必須指定下列其中一項：

- **Include**：IAM 角色 ARNs 的清單，指向與這些角色相關聯的目標堆疊。只有這些角色啟動的堆疊操作才會叫用勾點。
 - 類型：字串陣列
 - 項目上限：50
 - 最小項目：1
- **Exclude**：您要排除之堆疊的 IAM 角色 ARNs 清單。除了由指定角色啟動的以外，所有堆疊都會叫用勾點。
 - 類型：字串陣列
 - 項目上限：50
 - 最小項目：1

Include 和 Exclude 陣列中的每個堆疊角色都必須遵守下列模式和長度要求：

- 模式：arn:.*:iam::[0-9]{12}:role/.+
- 長度上限：256

Include 和 Exclude

每個篩選條件 (StackNames 和 StackRoles) 都有 Include 清單和 Exclude 清單。使用 StackNames 做為範例，勾點只會在 Include 清單中指定的堆疊上調用。如果只指定 Exclude 清

單中的堆疊名稱，則只會在不在Exclude清單中的堆疊上叫用掛鉤。如果同時指定 Exclude Include和，Hook 會鎖定Include清單中的內容，而不是Exclude清單中的內容。

例如，假設您有四個堆疊：A、B、C 和 D。

- "Include": ["A","B"] 在 A 和 B 上叫用勾點。
- "Exclude": ["B"] 在 A、C 和 D 上叫用勾點。
- "Include": ["A","B","C"], "Exclude": ["A","D"] 勾點在 B 和 C 上調用。
- "Include": ["A","B","C"], "Exclude": ["A","B","C"] 任何堆疊上都不會叫用勾點。

堆疊層級篩選條件的範例

本節提供您可以遵循的範例，以為 AWS CloudFormation 勾點建立堆疊層級篩選條件。

範例 1：包含特定堆疊

下列範例會指定Include清單。鉤子只會在名為 stack-test-1、 stack-test-2和 的堆疊上叫用stack-test-3。

```
{
  "CloudFormationConfiguration": {
    "HookConfiguration": {
      "HookInvocationStatus": "ENABLED",
      "TargetOperations": [
        "STACK",
        "RESOURCE"
      ],
      "FailureMode": "WARN",
      "Properties": {},
      "StackFilters": {
        "FilteringCriteria": "ALL",
        "StackNames": {
          "Include": [
            "stack-test-1",
            "stack-test-2",
            "stack-test-3"
          ]
        }
      }
    }
  }
}
```

```

}
}

```

範例 2：排除特定堆疊

如果堆疊名稱改為新增至Exclude清單，則會在未命名為 stack-test-1、stack-test-2或的任何堆疊上叫用勾點stack-test-3。

```

{
  "CloudFormationConfiguration": {
    "HookConfiguration": {
      "HookInvocationStatus": "ENABLED",
      "TargetOperations": [
        "STACK",
        "RESOURCE"
      ],
      "FailureMode": "WARN",
      "Properties": {},
      "StackFilters": {
        "FilteringCriteria": "ALL",
        "StackNames": {
          "Exclude": [
            "stack-test-1",
            "stack-test-2",
            "stack-test-3"
          ]
        }
      }
    }
  }
}

```

範例 3：合併包含和排除

如果未指定 Include和 Exclude清單，則只會在不在Exclude清單中Include的堆疊上叫用勾點。在下列範例中，勾點只會在 上叫用stack-test-3。

```

{
  "CloudFormationConfiguration": {
    "HookConfiguration": {
      "HookInvocationStatus": "ENABLED",
      "TargetOperations": [

```



```

    "STACK",
    "RESOURCE"
  ],
  "FailureMode": "WARN",
  "Properties": {},
  "StackFilters": {
    "FilteringCriteria": "ALL",
    "StackNames": {
      "Include": [
        "stack-test-1",
        "stack-test-2",
        "stack-test-3"
      ],
      "Exclude": [
        "stack-test-1",
        "stack-test-2"
      ]
    }
  }
}
}
}
}
}

```

範例 4：結合堆疊名稱和角色與ALL條件

下列勾點包含三個堆疊名稱和一個堆疊角色。由於 `FilteringCriteria` 指定為 `ALL`，所以僅針對同時具有相符堆疊名稱和相符堆疊角色的堆疊叫用勾點。

```

{
  "CloudFormationConfiguration": {
    "HookConfiguration": {
      "HookInvocationStatus": "ENABLED",
      "TargetOperations": [
        "STACK",
        "RESOURCE"
      ],
      "FailureMode": "WARN",
      "Properties": {},
      "StackFilters": {
        "FilteringCriteria": "ALL",
        "StackNames": {
          "Include": [
            "stack-test-1",

```

```
        "stack-test-2",
        "stack-test-3"
    ]
  },
  "StackRoles": {
    "Include": ["arn:aws:iam::123456789012:role/hook-role"]
  }
}
}
```

範例 5：結合堆疊名稱和角色與ANY條件

下列勾點包含三個堆疊名稱和一個堆疊角色。由於 `FilteringCriteria` 指定為 `ANY`，所以針對具有相符堆疊名稱或相符堆疊角色的堆疊，會叫用勾點。

```
{
  "CloudFormationConfiguration": {
    "HookConfiguration": {
      "HookInvocationStatus": "ENABLED",
      "TargetOperations": [
        "STACK",
        "RESOURCE"
      ],
      "FailureMode": "WARN",
      "Properties": {},
      "StackFilters": {
        "FilteringCriteria": "ANY",
        "StackNames": {
          "Include": [
            "stack-test-1",
            "stack-test-2",
            "stack-test-3"
          ]
        }
      }
    },
    "StackRoles": {
      "Include": ["arn:aws:iam::123456789012:role/hook-role"]
    }
  }
}
```

AWS CloudFormation 勾點目標篩選條件

本主題提供設定 AWS CloudFormation Hooks 目標篩選條件的指引。您可以使用目標篩選條件來更精細地控制您的勾點被調用的時間和資源。您可以設定篩選條件，範圍從簡單的資源類型目標到更複雜的資源類型、動作和調用點組合。

若要在勾點組態中將一或多個堆疊名稱指定為篩選條件，請在下新增TargetFilters金鑰HookConfiguration。

TargetFilters 支援下列屬性。

TargetNames

指定要目標的資源類型名稱的字串陣列。如需範例，請參閱「[範例 1：基本目標篩選條件](#)」。

目標名稱支援具體目標名稱和完整的萬用字元比對。如需詳細資訊，請參閱[使用萬用字元搭配 Hook 目標名稱](#)。

模式：`^[a-zA-Z0-9]{2,64}::[a-zA-Z0-9]{2,64}::[a-zA-Z0-9]{2,64}$`

上限：50

Actions

字串陣列，指定您在 中列出之目標的目標動作TargetNames。

有效值：CREATE | UPDATE | DELETE

Note

使用 RESOURCE、STACK和 CLOUD_CONTROL Hook 目標時，所有目標動作都適用。使用 CHANGE_SET Hook 目標時，只有 CREATE動作適用。

InvocationPoints

字串陣列，指定您在 中列出之目標的叫用點TargetNames。

有效值：PRE_PROVISION

Targets

物件陣列，指定要用於目標篩選的目標清單。

目標陣列中的每個目標都有下列屬性。

TargetNames

要目標的資源類型名稱。

Actions

指定目標的動作。

有效值：CREATE | UPDATE | DELETE

InvocationPoints

指定目標的調用點。

有效值：PRE_PROVISION

Note

您無法同時包含Targets物件陣列和 Actions、TargetNames或 InvocationPoints陣列。如果您想要使用這三個項目 和 Targets，您必須在Targets物件陣列中包含它們。如需範例，請參閱「[範例 2：使用Targets物件陣列](#)」。

目標篩選條件的範例

本節提供您可以遵循的範例，以建立 AWS CloudFormation Hooks 的目標篩選條件。

範例 1：基本目標篩選條件

若要建立著重於特定資源類型的基本目標篩選條件，請使用 TargetFilters 物件搭配 TargetNames陣列。下列目標篩選條件組態會在 S3 儲存貯體和 DynamoDB 資料表上的所有操作上叫用勾點。

```
{
  "CloudFormationConfiguration": {
    "HookConfiguration": {
      "HookInvocationStatus": "ENABLED",
      "TargetOperations": [
        "STACK",
        "RESOURCE"
      ]
    }
  }
}
```

```

    ],
    "FailureMode": "WARN",
    "Properties": {},
    "TargetFilters": {
      "TargetNames": [
        "AWS::S3::Bucket",
        "AWS::DynamoDB::Table"
      ]
    }
  }
}
}
}
}

```

範例 2：使用Targets物件陣列

對於更進階的篩選條件，您可以使用Targets物件陣列來列出特定目標、動作和調用點組合。下列目標篩選條件組態會在 S3 儲存貯體CREATE和 DynamoDB 資料表上調用 Hook 之前和UPDATE操作。

```

{
  "CloudFormationConfiguration": {
    "HookConfiguration": {
      "HookInvocationStatus": "ENABLED",
      "TargetOperations": [
        "STACK",
        "RESOURCE"
      ],
    },
    "FailureMode": "WARN",
    "Properties": {},
    "TargetFilters": {
      "Targets": [
        {
          "TargetName": "AWS::S3::Bucket",
          "Action": "CREATE",
          "InvocationPoint": "PRE_PROVISION"
        },
        {
          "TargetName": "AWS::S3::Bucket",
          "Action": "UPDATE",
          "InvocationPoint": "PRE_PROVISION"
        },
        {
          "TargetName": "AWS::DynamoDB::Table",
          "Action": "CREATE",

```

```

        "InvocationPoint": "PRE_PROVISION"
      },
      {
        "TargetName": "AWS::DynamoDB::Table",
        "Action": "UPDATE",
        "InvocationPoint": "PRE_PROVISION"
      }
    ]
  }
}
}
}
}

```

使用萬用字元搭配 Hook 目標名稱

您可以使用萬用字元做為目標名稱的一部分。您可以在 Hook 目標名稱中使用萬用字元 (* 和 ?)。星號 (*) 代表字元的任意組合。問號 (?) 代表任何單一字元。您可以在目標名稱中使用多個 * 和 ? 字元。

Example : Hook 結構描述中目標名稱萬用字元的範例

下列範例以 Amazon S3 支援的所有資源類型為目標。

```

{
  ...
  "handlers": {
    "preCreate": {
      "targetNames": [
        "AWS::S3::*"
      ],
      "permissions": []
    }
  }
}
...
}

```

下列範例符合名稱中具有「Bucket」的所有資源類型。

```

{
  ...
  "handlers": {
    "preCreate": {
      "targetNames": [

```

```

        "AWS::*::Bucket*"
    ],
    "permissions": []
}
}
...
}

```

AWS::*::Bucket* 可能會解析為下列任何具體資源類型：

- AWS::Lightsail::Bucket
- AWS::S3::Bucket
- AWS::S3::BucketPolicy
- AWS::S3Outpost::Bucket
- AWS::S3Outpost::BucketPolicy

Example：Hook 組態結構描述中目標名稱萬用字元的範例

下列範例組態會叫用 勾點，用於所有 Amazon S3 資源類型的CREATE操作，以及所有具名資料表資源類型的UPDATE操作，例如 AWS::DynamoDB::Table或 AWS::Glue::Table。

```

{
  "CloudFormationConfiguration": {
    "HookConfiguration": {
      "TargetStacks": "ALL",
      "FailureMode": "FAIL",
      "Properties": {},
      "TargetFilters": {
        "Targets": [
          {
            "TargetName": "AWS::S3::*",
            "Action": "CREATE",
            "InvocationPoint": "PRE_PROVISION"
          },
          {
            "TargetName": "AWS::*::Table",
            "Action": "UPDATE",
            "InvocationPoint": "PRE_PROVISION"
          }
        ]
      }
    }
  }
}

```

```

    }
  }
}

```

下列範例組態會叫用所有 Amazon S3 資源類型的 和 CREATEUPDATE 操作的勾點，以及所有具名資料表資源類型的 CREATE 和 UPDATE 操作，例如 AWS::DynamoDB::Table 或 AWS::Glue::Table。

```

{
  "CloudFormationConfiguration": {
    "HookConfiguration": {
      "TargetStacks": "ALL",
      "FailureMode": "FAIL",
      "Properties": {},
      "TargetFilters": {
        "TargetNames": [
          "AWS::S3::*",
          "AWS::*::Table"
        ],
        "Actions": [
          "CREATE",
          "UPDATE"
        ],
        "InvocationPoints": [
          "PRE_PROVISION"
        ]
      }
    }
  }
}

```


使用 CloudFormation 範本建立勾點

此頁面提供 Hooks 的範例 CloudFormation 範本和技術參考主題的連結。

透過使用 CloudFormation 範本建立勾點，您可以重複使用範本來一致且重複地設定勾點。此方法可讓您定義勾點一次，然後在多個 AWS 帳戶和區域中逐一佈建相同的勾點。

CloudFormation 為 Guard 和 Lambda Hook 建立提供下列專用資源類型。

任務	解決方案	連結
建立 Guard Hook	使用 <code>AWS::CloudFormation::GuardHook</code> 資源類型來建立和啟用 Guard Hook。	範本範例 技術參考
建立 Lambda 勾點	使用 <code>AWS::CloudFormation::LambdaHook</code> 資源類型來建立和啟用 Lambda Hook。	範本範例 技術參考

CloudFormation 也提供下列資源類型，您可以在堆疊範本中用於建立自訂勾點。

任務	解決方案	連結
設定勾點的預設版本	使用 <code>AWS::CloudFormation::HookDefaultVersion</code> 資源類型來指定自訂勾點的預設版本。	範例範本 技術參考
設定勾點的組態	使用 <code>AWS::CloudFormation::HookTypeConfig</code> 資源類型來指定自訂勾點的組態。	範例範本 技術參考
註冊勾點	使用 <code>AWS::CloudFormation::HookVersion</code> 資源類型將新版或第一個版本的自訂勾點發佈至 CloudFormation 登錄檔。	範例範本 技術參考
公開發佈勾點	使用 <code>AWS::CloudFormation::PublicTypeVersion</code> 資源	技術參考

任務	解決方案	連結
	類型來測試和發佈已註冊的自訂勾點做為公有第三方勾點。	
將您的帳戶註冊為發佈者	使用 <code>AWS::CloudFormation::Publisher</code> 資源類型，在 CloudFormation 登錄檔中將您的帳戶註冊為公有擴充功能（勾點、模組和資源類型）的發佈者。	技術參考
啟用公有、第三方勾點	AWS::CloudFormation::TypeActivation 資源類型與 AWS::CloudFormation::HookTypeConfig 資源類型搭配使用，以啟用您帳戶中的公有第三方自訂勾點。	技術參考

AWS CloudFormation Hooks 使用者指南的文件歷史記錄

下表說明自上次發佈 AWS CloudFormation Hooks 以來文件的重要變更。如需有關此文件更新的通知，您可以訂閱 RSS 訂閱源。

- 文件最近更新時間：2023 年 12 月 8 日。

變更	描述	日期
堆疊層級勾點	掛鉤現在在堆疊層級受到支援，可讓客戶使用 CloudFormation Hooks 來評估新的範本，並可能封鎖堆疊操作以繼續。	2024 年 11 月 13 日
AWS Cloud Control API 勾點整合	勾點現在已與 Cloud Control API 整合，可讓客戶使用 CloudFormation Hooks 在佈建之前主動檢查資源的組態。如果找到不合規的資源，勾點會失敗操作並防止佈建資源，或發出警告並允許佈建操作繼續。	2024 年 11 月 13 日
AWS CloudFormation Guard 勾點	AWS CloudFormation Guard 是開放原始碼和一般用途網域特定語言 (DSL)，可用來撰寫 policy-as-code。Guard Hooks 可以評估 Cloud Control API 和 CloudFormation 操作，以在佈建之前檢查資源的組態。如果找到不合規的資源，勾點會失敗操作並防止佈建資源，或發出警告並允許佈建操作繼續。	2024 年 11 月 13 日
AWS Lambda 勾點	AWS CloudFormation Lambda Hooks 可讓您針對自訂自訂程式碼評估 CloudFormation 和	2024 年 11 月 13 日

Cloud Control API 操作。您的勾點可能會封鎖操作以繼續，或向發起人發出警告，並允許操作繼續。

[Hooks 使用者指南](#)

AWS CloudFormation Hooks 使用者指南的初始版本。更新包括新的簡介、入門演練、概念和術語、堆疊層級篩選，以及有關先決條件、設定和 CloudFormation Hooks 開發的更新主題。

2023 年 12 月 8 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。