使用者指南

# AWS Well-Architected Tool

# AWS Well-Architected Tool: 使用者指南

# Table of Contents

您可以使用 Jira AWS Well-Architected Tool 連接器將您的 Jira 帳戶與其連結 AWS Well-Architected Tool，並在工作負載和 Jira 專案之間同步改進項目。

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。

# 什麼是 AWS Well-Architected Tool？

AWS Well-Architected Tool(AWS WA Tool) 是雲端中的一項服務，可提供一致的程序，讓您使用AWS最佳實務來衡量架構。 AWS WA Tool在整個產品生命週期中協助您：

- 協助記錄您所做的決定
- 根據最佳實務提供改善工作負載的建議
- 引導您讓工作負載更可靠、安全、有效率且經濟實惠

您可以使用 AWS WA Tool AWS Well-Architected 的框架中的最佳做法來記錄和衡量工作負載。這些最佳做法是由AWS解決方案架構師根據他們在各種企業中建置解決方案的多年經驗所開發。這個架構會提供衡量架構的一致方法，並引導使用者實作能夠隨需求擴展的設計。

除了AWS最佳做法外，您還可以使用自訂鏡頭，使用自己的最佳實務來測量您的工作負載。您可以針對特定技術量身打造自訂鏡頭中的問題，或協助您滿足組織內的治理需求。訂製鏡頭延伸了鏡AWS頭所提供的導引。

與之整合AWS Trusted Advisor並AWS Service Catalog AppRegistry幫助您更輕鬆地發現回答 Well-Architected 評論問題所需的資訊。

這項服務適用於從事技術產品開發的人員，例如首席技術官（CTO），架構師，開發人員和運營團隊成員。 AWS客戶用AWS WA Tool來記錄其架構、提供產品發佈治理，以及瞭解和管理其技術組合中的風險。

主題



## AWSWell-Architected 的框架

AWSWell-Architected 的架構會記錄一組基礎問題，讓您瞭解特定架構如何與雲端最佳實務一致。這個架構會提供一致的方法，讓您可依據現代雲端系統中預期的特質來評估系統。該架構會根據您系統架構的狀態來建議達到這些特質所需進行的改善。

透過使用該架構，您可以了解在雲端中設計和操作可靠、安全、有效率、經濟實惠系統的架構最佳實務。其可讓您根據最佳實務以一致的方式來衡量架構，並找出需要改善的區域。該框架基於六大支柱：卓越營運、安全性、可靠性、效能效率、成本最佳化和永續性。

設計工作負載時，您必須根據業務需求在這幾個要件中做出取捨。這些業務決策有助於您了解工程設計的優先順序。在開發環境中，您可能需要在犧牲可靠性的情況下進行最佳化，藉此降低成本。在關鍵任務解決方案中，您可能會將可靠性最佳化，並接受成本提高。在電子商務解決方案，您可能會將效能放在較高的優先順序，因為客戶滿意度可以帶來更高的收入。安全性和操作效能通常不會因其他要件而被犧牲。

有關框架的更多信息，請訪問 AWSWell-Architected 的網站。

# 定義

在AWS WA Tool和 AWS Well-Architected 的框架中：

- 工作負載會識別一組可提供商業價值的元件。工作負載通常是商業和技術領導者用以溝通詳細資訊的層級。工作負載的例子包含行銷網站、電子商務網站、行動應用程式後端系統與分析平台。工作負載會因架構的複雜程度而有所不同。它們可能如靜態網站一般簡單，也可能如具有多個資料存放區和許多元件的微型服務架構一般複雜。
- 里程碑標誌著您架構在整個產品生命週期（設計、測試、上線和生產）的發展過程中的關鍵變化。
- 鏡頭可讓您根據最佳實務，以一致的方式來衡量架構，並找出需要改善的區域。

  除了提供的鏡頭之外AWS，您還可以創建和使用自己的鏡頭，或使用與您共享的鏡頭。
- 高風險問題 (HRI) 是架構和營運選擇，AWS發現可能會對企業造成重大負面影響。這些 HRI 可能會影響組織營運、資產和個人。
- 中度風險問題 (MRI) 是架構和營運選擇，發現可能會對業務產生負面影響，但其程度低於 HRI。AWS

  如需其他資訊，請參閱 高風險問題 (HRI) 及中等風險問題 (MRI)。

# 開始使用 AWS Well-Architected Tool

本節說明如何開始使用 AWS WA Tool。

主題



## 提供使用者、群組或角色的存取權 AWS WA Tool

在此步驟中，您授與存取權 AWS WA Tool。

提供存取權 AWS WA Tool

1. 若要提供存取權，請新增權限至您的使用者、群組或角色：

   - 使用者和群組位於 AWS IAM Identity Center：

     建立權限合集。請按照 AWS IAM Identity Center 使用者指南 中的 建立權限合集 說明進行操作。

   - 透過身分提供者在 IAM 中管理的使用者：

     建立聯合身分的角色。請按照 IAM 使用者指南 的 為第三方身分提供者 (聯合) 建立角色 中的指示進行操作。

   - IAM 使用者：

     - 建立您的使用者可擔任的角色。請按照 IAM 使用者指南 的 為 IAM 使用者建立角色 中的指示進行操作。
     - (不建議) 將政策直接附加至使用者，或將使用者新增至使用者群組。請遵循 IAM 使用者指南的新增許可到使用者 (主控台)中的指示。

2. 若要授與完全控制權，請將受WellArchitectedConsoleFullAccess管理的原則套用至權限集或角色。

「完整」存取權可讓主參與者執行中的所有動作 AWS WA Tool。定義工作負載、刪除工作負載、檢視工作負載、更新工作負載、共用工作負載、建立自訂鏡頭以及共用自訂鏡頭時，都需要此存取權。

3. 若要授與唯讀存取權，請將受WellArchitectedConsoleReadOnlyAccess管理的原則套用至權限集或角色。具有此角色的主參與者只能檢視資源。

如需這些原則的詳細資訊，請參閱AWS 受管理的政策 AWS Well-Architected Tool。

# 啟用其他服 AWS 務的支援

啟動組織存取權限 AWS WA Tool 以收集組織結構的相關資訊，以便更輕鬆地共用資源 (the section called “在其中啟用資源共用 AWS Organizations”如需詳細資訊，請參閱)。啟用 Discovery 支援會從AWS Trusted AdvisorAWS Service Catalog AppRegistry、和相關資源 (例如資源集合中的 AWS CloudFormation 堆疊) 收集 AppRegistry 資訊，以協助您更輕鬆地探索回答 Well-Architected 檢閱問題所需的資訊，並針對工作負載量身打造 Trusted Advisor 檢查。

啟用支援或啟用 Discovery 支援會自動為您的帳戶建立服務連結角色。 AWS Organizations

若要開啟對 AWS WA Tool 可與之互動的其他服務的支援，請瀏覽至 [設定]。

1. 若要從中收集資訊 AWS Organizations，請開啟啟用 AWS Organizations 支援。
2. 開啟啟動探索支援以從其他 AWS 服務和資源收集資訊。
3. 選取 [檢視角色權限] 以檢視服務連結的角色權限或信任關係原則。
4. 選取 [儲存設定]。

## AppRegistry 針對工作負載啟動

使用 AppRegistry 是選擇性的， AWS 商業和企業 Support 客戶可以根據每個工作負載來啟用它。

每當開啟探查支援並 AppRegistry 與新的或現有的工作負載產生關聯時，都 AWS WA Tool 會建立服務管理的屬性群組。中的屬性群組「中繼資料」 AppRegistry 包含工作負載 ARN、工作負載名稱以及與工作負載相關聯的風險。

- 開啟探查支援時，只要工作負載發生變更，就會更新屬性群組。
- 關閉探查支援或從工作負載中移除應用程式時，會從中移除工作負載資訊 AWS Service Catalog。

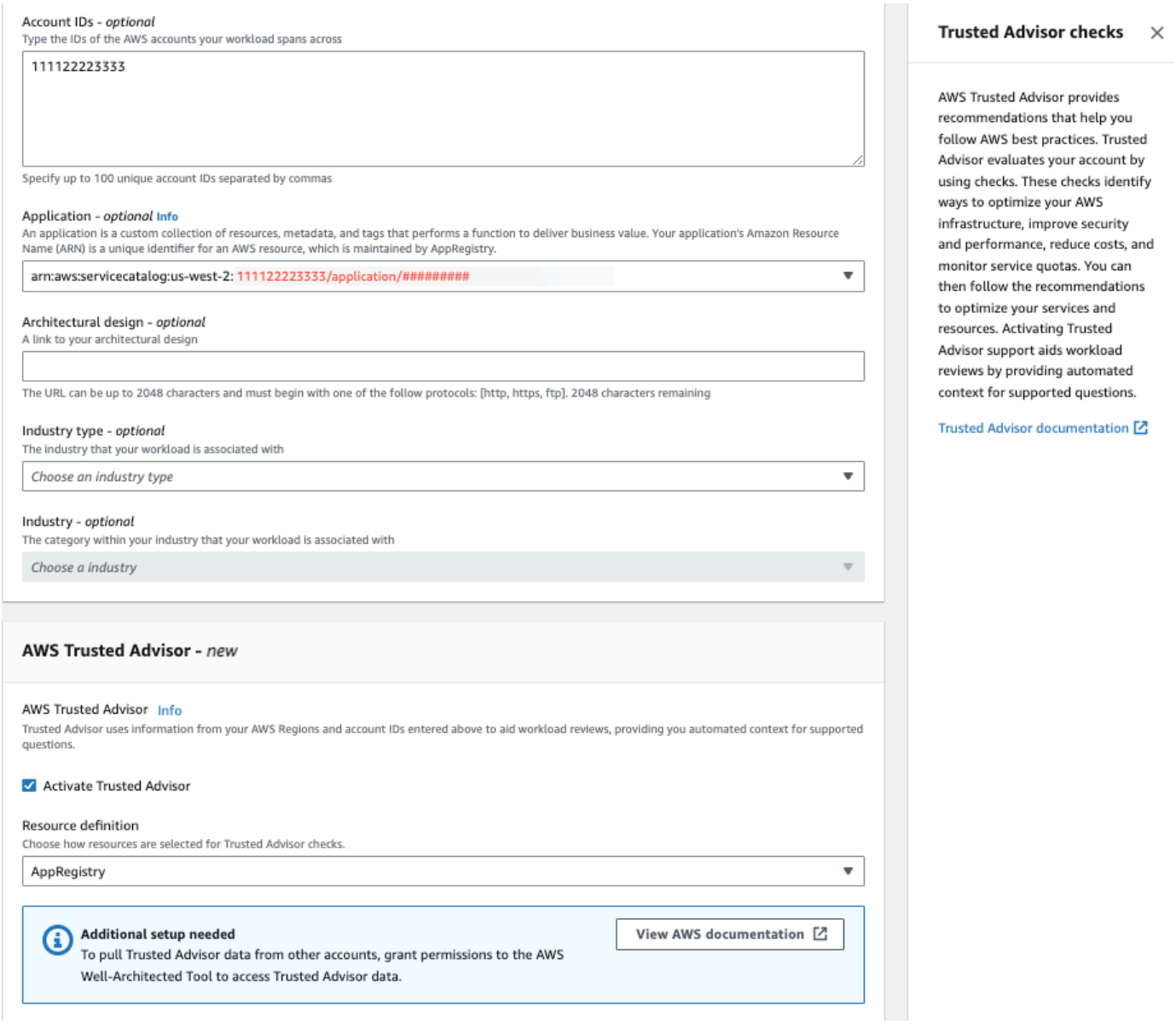
如果您希望 AppRegistry 應用程式驅動從中擷取的資料 Trusted Advisor，請將您的工作負載資源定義設定為AppRegistry或全部。遵循中的指導方針，為應用程式中擁有資源的所有帳號建立角色the section called “ Trusted Advisor 在 IAM 中啟用”。

## AWS Trusted Advisor 針對工作負載啟動

與整合 AWS Trusted Advisor 是選擇性的，而且可以針對 AWS 商業和企業 Support 客戶根據每個工作負載啟動。無需整合 Trusted Advisor 成本 AWS WA Tool，但如需 Trusted Advisor 定價詳細資訊，請參閱 Sup AWS port 方案。

啟動工作負載的 Trusted Advisor

1. 若要啟動 Trusted Advisor，工作負載擁有者可以使用 AWS WA Tool 來更新現有工作負載，或透過選擇定義工作負載來建立新的工作負載。
2. 在「帳號 ID」欄位 Trusted Advisor 中輸入使用的帳號 ID，在「應用程式」欄位中選取應用程式 ARN，或同時選取兩者來啟動 Trusted Advisor。
3. 在AWS Trusted Advisor區段中，選取「啟動」 Trusted Advisor。




4. 將建立 IAM 服務角色的通知會顯示第一次針 Trusted Advisor 對工作負載啟用。選擇檢視權限會顯示 IAM 角色許可。您可以檢視角色名稱，以及在 IAM 中為您自動建立的許可和信任關係 JSON。建立角色後，對於後續啟動的工作負載 Trusted Advisor，只會顯示「需要其他設定」的通知。
5. 在資源定義下拉式清單中，您可以選取工作負載中繼資料 AppRegistry，或選取全部。資源定義選項可定義從哪些資料 AWS WA Tool 擷取，以便在工作負載檢閱中提供對應 Trusted Advisor 至 Well-Architected 最佳做法的狀態檢查。

   工作負載中繼資料 — 工作負載由帳號 ID 定義，並在工作負載中 AWS 區域 指定。

   AppRegistry— 工作負載由與工作負載關聯的 AppRegistry 應用程式中存在的資源 (例如 AWS CloudFormation 堆疊) 定義。

全部 — 工作負載由工作負載中繼資料和 AppRegistry 資源定義。

6. 選擇下一步。
7. 將 AWS Well-Architected 的架構套用至您的工作負載，然後選擇定義工作負載。 Trusted Advisor 檢查僅與 AWS Well-Architected 的框架相關聯，而不是其他鏡頭。

定 AWS WA Tool 期從 Trusted Advisor 使用 IAM 中建立的角色取得資料。系統會為工作負載擁有者自動建立 IAM 角色。不過，若要檢視 Trusted Advisor 資訊，工作負載上任何關聯帳戶的擁有者必須前往 IAM 並建立角色，請參閱以取得???詳細資訊。如果此角色不存在，則 AWS WA Tool 無法取得該帳號的 Trusted Advisor 資訊並顯示錯誤。

如需在 AWS Identity and Access Management (IAM) 中建立角色的詳細資訊，請參閱《IAM 使用者指南》中的為 AWS 服務建立角色 (主控台)。

## 在 IAM 中啟用 Trusted Advisor 工作負載

> **Note**
>
> 工作負載擁有者應在建立工作負 Trusted Advisor 載之前啟動其帳戶的探查支援。選擇啟動探查支援可建立工作負載擁有者所需的角色。對所有其他關聯帳戶使用下列步驟。

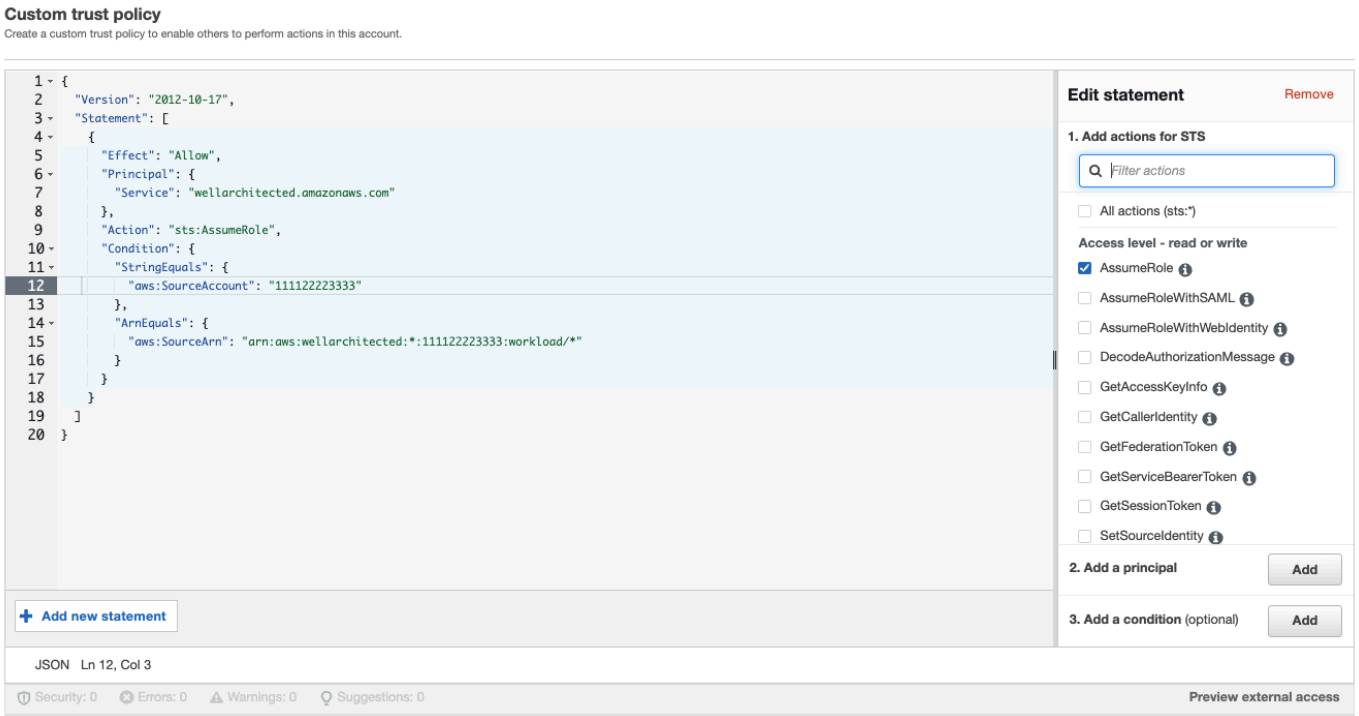
已啟動之工作負載的關聯帳戶擁有者 Trusted Advisor 必須在 IAM 中建立角色，才能查看中的 Trusted Advisor 資訊 AWS WA Tool。

若要在 IAM 中建立 AWS WA Tool 要取得資訊的角色 Trusted Advisor

1. 登入 AWS Management Console 並開啟 IAM 主控台，位於https://console.aws.amazon.com/iam/。
2. 在 IAM 主控台的導覽窗格中，選擇 [角色]，然後選擇 [建立角色]。
3. 在 [信任的實體類型] 下，選擇 [自訂信任
4. 將下列自訂信任政策複製並貼到 IAM 主控台的 JSON 欄位中，如下圖所示。*WORKLOAD_OWNER_ACCOUNT_ID*以工作負載擁有者的帳戶 ID 取代，然後選擇 [下一步]。

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

```
      "Effect": "Allow",
      "Principal": {
        "Service": "wellarchitected.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "WORKLOAD_OWNER_ACCOUNT_ID"
        },
        "ArnEquals": {
          "aws:SourceArn":
 "arn:aws:wellarchitected:*:WORKLOAD_OWNER_ACCOUNT_ID:workload/*"
        }
      }
    }
  ]
}
```




> **Note**
>
> 先前自訂信任原則的條件區塊aws:sourceArn中的是"arn:aws:wellarchitected:*:*WORKLOAD_OWNER_ACCOUNT_ID*:workload/

*"，這是一般條件，說明此角色可用於所有工作 AWS WA Tool 負載擁有者的工作負載。但是，存取範圍可以縮小為特定工作負載 ARN 或一組工作負載 ARN。若要指定多個 ARN，請參閱下列範例信任原則。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "wellarchitected.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "WORKLOAD_OWNER_ACCOUNT_ID"
                },
                "ArnEquals": {
                    "aws:SourceArn": [

 "arn:aws:wellarchitected:REGION:WORKLOAD_OWNER_ACCOUNT_ID:workload/
WORKLOAD_ID_1",

 "arn:aws:wellarchitected:REGION:WORKLOAD_OWNER_ACCOUNT_ID:workload/
WORKLOAD_ID_2"
                    ]
                }
            }
        }
    ]
}
```

5. 在 [新增權限] 頁面上，對於 [權限] 原則，選擇 [建立原則] 以授與讀 AWS WA Tool 取資料的存取權 Trusted Advisor。選取 [建立原則] 會開啟新視窗。

> **Note**
>
> 此外，您可以選擇在建立角色期間略過建立權限，並在建立角色後建立內嵌原則。在成功的角色建立訊息中選擇 [檢視角色]，然後從 [權限] 索引標籤的 [新增權限] 下拉式清單中選取 [建立

6. 將下列權限原則複製並貼到 JSON 欄位中。在 `Resource` ARN 中，以您自己*YOUR_ACCOUNT_ID*的帳戶 ID 取代，指定 [地區] 或 [星號] (*)，然後選擇 [下一步:標籤]。

   如需有關 ARN 格式的詳細資訊，請參閱《AWS 一般參考指南》中的 Amazon Resource Name (ARN)。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:DescribeCheckRefreshStatuses",
                "trustedadvisor:DescribeCheckSummaries",
                "trustedadvisor:DescribeRiskResources",
                "trustedadvisor:DescribeAccount",
                "trustedadvisor:DescribeRisk",
                "trustedadvisor:DescribeAccountAccess",
                "trustedadvisor:DescribeRisks",
                "trustedadvisor:DescribeCheckItems"
            ],
            "Resource": [
              "arn:aws:trustedadvisor:*:YOUR_ACCOUNT_ID:checks/*"
            ]
        }
    ]
}
```

7. 如果 Trusted Advisor 針對工作負載啟動，且 [資源定義] 設定為AppRegistry或 [全部]，則在連結至工作負載的 AppRegistry 應用程式中擁有資源的所有帳號都必須將下列權限新增至其 Trusted Advisor 角色的權限原則。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DiscoveryPermissions",
            "Effect": "Allow",
            "Action": [
                "servicecatalog:ListAssociatedResources",
                "tag:GetResources",
                "servicecatalog:GetApplication",
```

```
                "resource-groups:ListGroupResources",
                "cloudformation:DescribeStacks",
                "cloudformation:ListStackResources"
            ],
            "Resource": "*"
        }
    ]
}
```

8. (選用) 新增標籤。選擇下一步：檢閱。
9. 檢閱策略，為其命名，然後選取建立策略。
10. 在角色的 [新增權限] 頁面上，選取您剛建立的原則名稱，然後選取 [下一步]。
11. 輸入角色名稱，此名稱必須使用下列語法：`WellArchitectedRoleForTrustedAdvisor-`*`WORKLOAD_OWNER_ACCOUNT_ID`*並選擇 [建立角色]。*`WORKLOAD_OWNER_ACCOUNT_ID`*以工作負載擁有者的帳戶 ID 取代。

    您應該會在頁面頂端看到成功訊息，通知您已建立角色。
12. 若要檢視角色和相關聯的權限原則，請在 [存取管理] 下的左側導覽窗格中，選擇 [角色] 並搜尋`WellArchitectedRoleForTrustedAdvisor-`*`WORKLOAD_OWNER_ACCOUNT_ID`*名稱。選取角色的名稱，以確認「權限」和「信任」關係是否正確。

## 停用 Trusted Advisor 工作負載

停用工作負載的 Trusted Advisor

您可以 AWS WA Tool 透過編輯工作負載並取消 Trusted Advisor 選取啟用來停用任何工作負載。Trusted Advisor如需編輯工作負載的詳細資訊，請參閱the section called “編輯工作負載”。

停用 Trusted Advisor AWS WA Tool 不會刪除 IAM 中建立的角色。從 IAM 刪除角色需要單獨的清理措施。相關帳戶的工作負載擁有者或擁有者應刪除停 Trusted Advisor 用時建立的 IAM 角色 AWS WA Tool，或停 AWS WA Tool 止收集工作負載的 Trusted Advisor 資料。

若要**`WellArchitectedRoleForTrustedAdvisor`**在 IAM 中刪除

1. 登入 AWS Management Console 並開啟 IAM 主控台，位於https://console.aws.amazon.com/iam/。
2. 在 IAM 主控台的導覽窗格中，選擇 [角色]。
3. 搜尋`WellArchitectedRoleForTrustedAdvisor-`*`WORKLOAD_OWNER_ACCOUNT_ID`*並選取角色名稱。

4. 選擇刪除。在快顯視窗中，輸入要確認刪除的角色名稱，然後再次選取 [刪除]。

如需有關從 IAM 刪除角色的詳細資訊，請參閱 IAM 使用者指南中的刪除 IAM 角色 (主控台)。

# 定義工作負載

下一步是定義工作負載。

定義工作負載

1. 請登入 AWS Management Console 並開啟 AWS Well-Architected Tool 主控台，網址為 https://console.aws.amazon.com/wellarchitected/。
2. 如果這是您第一次使用 AWS WA Tool，您會看到一個介紹服務功能的頁面。在 Define a workload (定義工作負載) 區段中，選擇 Define workload (定義工作負載)。

   或者，在左側導覽窗格中，選擇 Workloads (工作負載)，然後選擇 Define workload (定義工作負載)。

   有關如何 AWS 使用工作負載資料的詳細資訊，請選擇為什麼 AWS 需要此資料，以及如何使用這些資料？
3. 在 Name (名稱) 方塊中，輸入您的工作負載名稱。

   > **Note**
   >
   > 名稱長度必須介於 3 到 100 個字元之間。至少三個字元不能為空格。工作負載名稱不能重複。當系統檢查名稱是否為唯一時，會忽略空格和大小寫。

4. 在 Description (說明) 方塊中，輸入工作負載的說明。說明長度必須介於 3 到 250 個字元之間。
5. 在 Review owner (檢閱擁有者) 方塊中，輸入擁有工作負載檢閱程序之主要群組或個人的名稱、電子郵件地址或識別碼。
6. 在 Environment (環境) 方塊中，選擇工作負載的環境：
   - 生產 — 工作負載在生產環境中執行。
   - 生產前 — 工作負載在生產前環境中執行。
7. 在 Regions (區域) 區段中，選擇工作負載的區域：
   - AWS 區域— 選擇工作負載的執行位 AWS 區域 置，一次一個。

- 非AWS 區域 — 輸入工作負載執行位置以外 AWS 的區域名稱。您最多可以指定五個唯一區域 (以逗號分隔)。

如果適用於您的工作負載，則可同時使用兩個選項。

8. (選擇性) 在 [帳戶 ID] 方塊中，輸入與工作負載 AWS 帳戶 相關聯的 ID。您最多可以指定 100 個唯一的帳戶 ID，並以逗號分隔。

   如果 Trusted Advisor 已啟動，則會使用指定的任何帳號 ID 從中取得資料 Trusted Advisor。請參閱AWS Trusted Advisor 針對工作負載啟用，以授與 AWS WA Tool 權限，以便在 IAM 中代表您取得 Trusted Advisor 資料。

9. (選擇性) 在「應用程式」方塊中，輸入您要與此工作負載相關聯之應用程式的應用程式 ARN。AWS Service Catalog AppRegistry每個工作負載只能指定一個 ARN，而且應用程式和工作負載必須位於相同區域。

10. (選用) 在 Architectural diagram (架構圖表) 方塊中，輸入架構設計的 URL。

11. (選用) 在 Industry type (產業類型) 方塊中，選擇與工作負載相關聯的產業類型。

12. (選用) 在 Industry (產業) 方塊中，選擇最適合工作負載的產業。

13. (選擇性) 在Trusted Advisor區段中，若要開啟工作負載的 Trusted Advisor 檢查，請選取啟用 Trusted Advisor。與您的工作負載相關聯的帳戶可能需要額外的設定。請參the section called “啟動 Trusted Advisor”閱 AWS WA Tool 授與代表您取得 Trusted Advisor 資料的權限。從「資源定義」下的「工作負載中繼資料」或「全部」中選取 AppRegistry，以定義 AWS WA Tool 用於執行 Trusted Advisor 檢查的資源。

14. (選擇性) 在 Jira 區段中，若要開啟工作負載的工作負載層級 Jira 同步設定，請選取覆寫帳戶層級設定。與您的工作負載相關聯的帳戶可能需要額外的設定。請參閱 Jira 的AWS Well-Architected Tool 連接器以開始設定和設定連接器。從 [不同步工作負載]、[同步工作負載-手動] 和 [同步工作負載-自動] 中選取，然後選擇性地輸入要同步的 Jira 專案金鑰。

    > **Note**
    >
    > 如果您未覆寫帳戶層級設定，工作負載將預設為帳戶層級 Jira 同步設定。

15. (選擇性) 在「標記」區段中，新增要與工作負載關聯的任何標記。

    如需標籤的詳細資訊，請參閱標記您的 AWS WA Tool 資源。

16. 選擇下一步。

    如果必填方塊為空白或指定值無效，您必須修正此問題才能繼續。

17. (選擇性) 在「套用設定檔」步驟中，選取現有的設定檔、搜尋設定檔名稱，或選擇建立設定檔來建立設定檔，將設定檔與工作負載產生關聯。選擇下一步。
18. 選擇要套用到此工作負載的鏡頭。一個工作負載最多可以添加 20 個鏡頭。如需官方 AWS 鏡頭的說明，請參閱鏡頭。

    您可以從自訂鏡頭 (您製作或與您共用的鏡頭 AWS 帳戶)、鏡頭目錄 (所有使用者皆可使用的AWS 官方鏡頭) 或兩者中選擇鏡頭。

    > **Note**
    >
    > 如果您尚未建立自訂鏡頭或與您共用自訂鏡頭，則「自訂鏡頭」區段為空白。

    > **免責聲明**
    >
    > 通過訪問和/或 AWS 使用由其他用戶或帳戶創建的自定義鏡頭，您確認由其他用戶創建並與您共享的定制鏡頭是根據 AWS 客戶協議中定義的第三方內容。

19. 選擇 Define workload (定義工作負載)。

    如果必填方塊為空白或指定值無效，請務必在定義工作負載前修正此問題。

# 記錄工作負載

工作負載定義完畢後，您即可記錄其狀態。

記錄工作負載的狀態

1. 初次定義工作負載後，您會看到一個顯示工作負載目前詳細資訊的頁面。選擇 Start reviewing (開始檢閱) 以開始進行。

   或者，在左側導覽窗格中選擇 Workloads (工作負載)，然後選取工作負載名稱，開啟工作負載詳細資訊頁面。選擇 Continue reviewing (繼續檢閱)。

   (選擇性) 如果設定檔與您的工作負載相關聯，則左側導覽窗格會包含一份已排序優先順序的工作負載檢閱問題清單，您可以用來加速工作負載檢閱程序。
2. 現在，系統會顯示第一個問題。回答每個問題時，請注意下列事項：

   a. 請閱讀問題，並判斷問題是否適用於您的工作負載。

如需其他指引，請選擇 [資訊]，然後在說明窗格中檢視資訊。

- 如果問題不適用於工作負載，請選擇 Question does not apply to this workload (問題不適用於此工作負載)。
- 否則，請從清單中選取您目前正在執行的最佳實務。

  如果您目前沒有正在執行的最佳實務，請選擇 None of these (以上皆非)。

如需任何項目的其他指引，請選擇 [資訊]，然後在說明窗格中檢視資訊。

b. (選擇性) 如果一或多個最佳作法不適用於您的工作負載，請選擇「標示不適用於此工作負載的最佳作法」，然後選取它們。針對每個選取的最佳作法，您可以選擇性地選取原因並提供其他詳細資訊。

c. (選用) 使用 Notes (備註) 方塊記錄與問題相關的資訊。

   例如，您可以說明問題不適用的原因，或提供所選最佳實務的其他詳細資訊。

d. 選擇 Next (下一步)，繼續回答下一個問題。

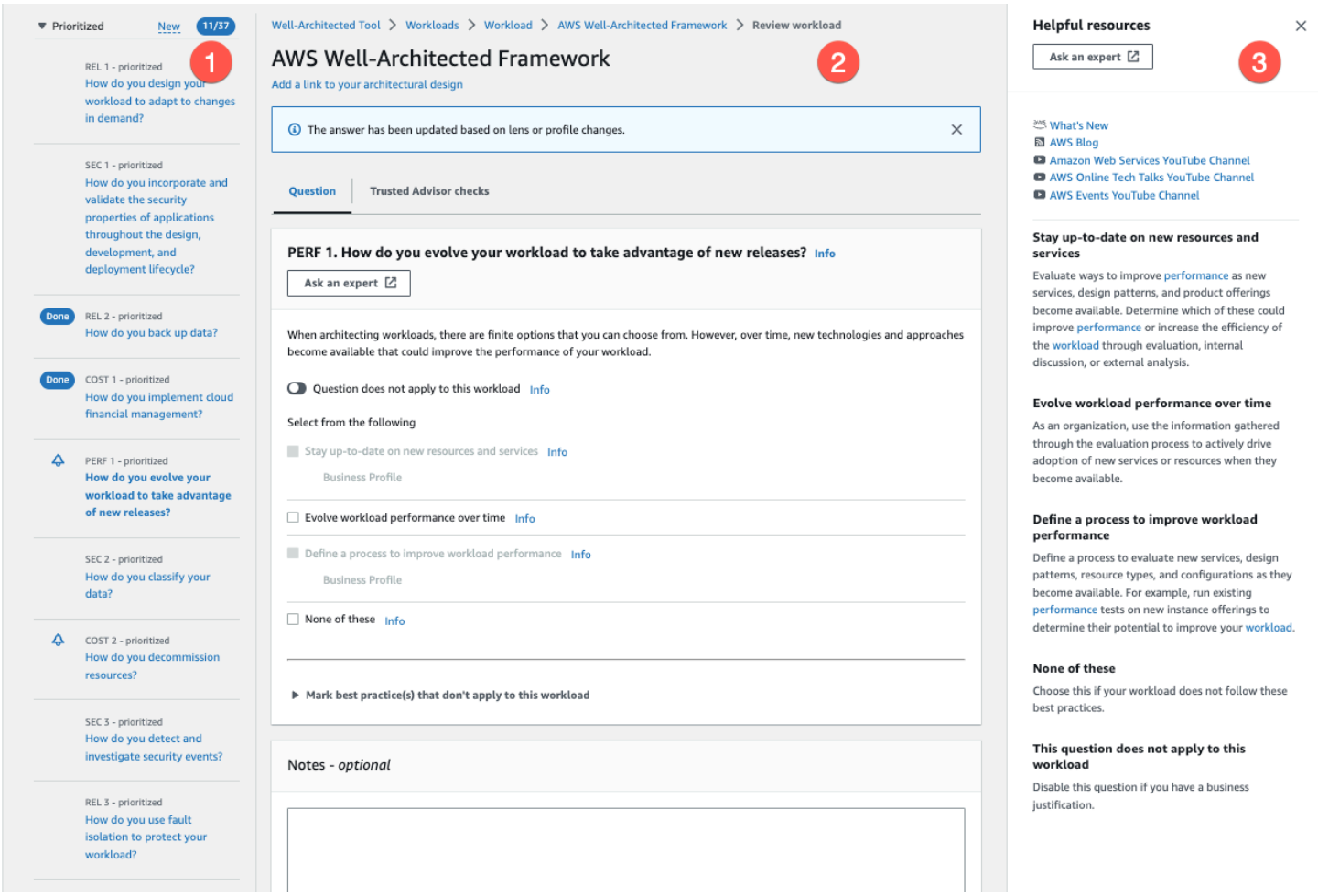
請對每個要件中的各個問題重複這些步驟。

3. 您可以隨時選擇 Save and exit (儲存並結束) 以儲存變更，並暫停記錄工作負載。

若要返回問題，請前往工作負載詳細資訊頁面，並選擇 Continue reviewing (繼續檢閱)。

# 複查工作量頁面

「複查工作負載」頁面有三個窗格。




1. 左側導覽窗格會顯示每個支柱的問題。您已回答的問題會標示為「完成」。每個要件已回答的問題數量，會顯示在要件名稱旁邊。

   您可以選擇要件名稱，然後選擇要回答的問題，即可查看其他要件的問題。

   (選擇性) 如果設定檔與您的工作負載相關聯，則 AWS WA Tool 會使用設定檔中的資訊來決定工作負載檢閱中的哪些問題具有優先順序，以及哪些問題不適用於您的業務。在左側導覽窗格中，您可以使用排定優先順序問題來協助加速工作負載檢閱程序。新增至已排序問題清單的問題旁邊會出現通知圖示。

2. 中間窗格會顯示目前的問題。選擇您正在執行的最佳實務。接著，選擇 Info (資訊) 以取得問題或最佳實務的其他資訊。選擇 [詢問專家] 以存取專門針對 Well-Architected 的 AWS Re: Post 社群。AWS AWS 回復：post 是論壇的基於主題的 question-and-answer 社區替代品。 AWS 使用 Re: post，您可以尋找答案、回答問題、加入群組、關注熱門主題，以及投票選出您最喜愛的問題和答案。

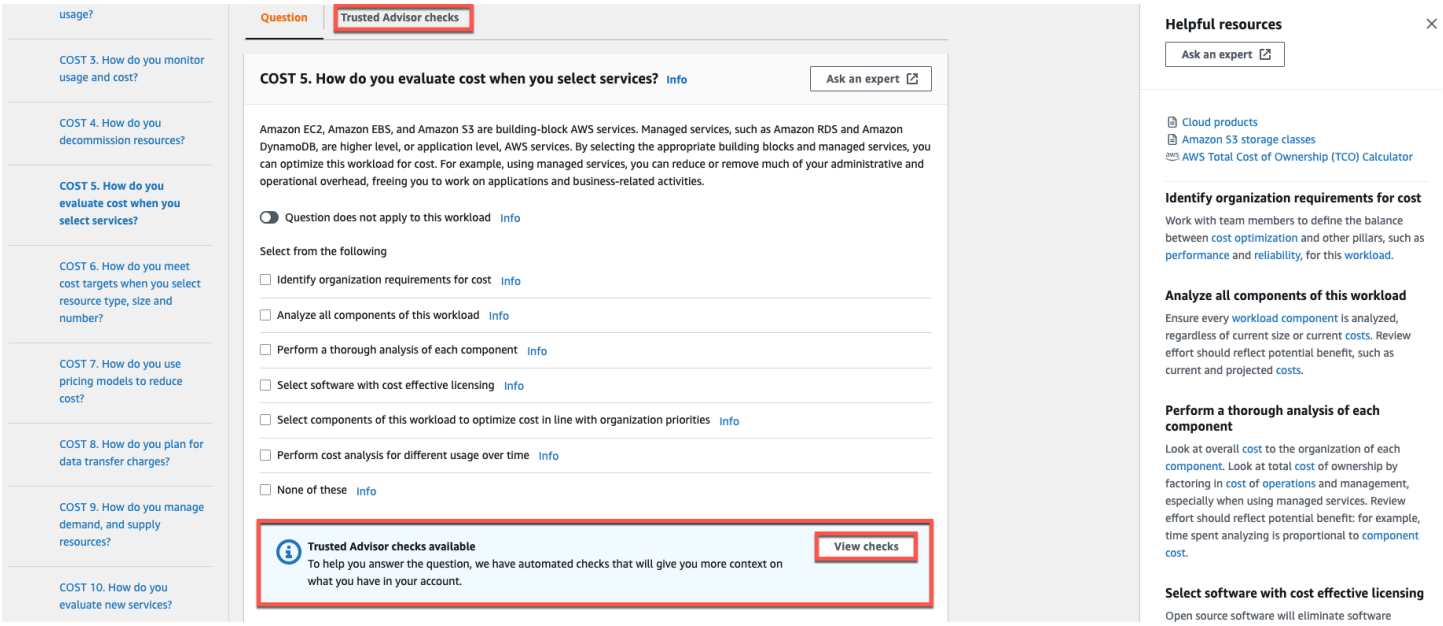
(選擇性) 若要將一或多個最佳作法標示為不適用，請選擇 [標記不適用於此工作負載的最佳作法]，然後選取它們。

使用此窗格底部的按鈕移至下一個問題、返回上一個問題，或儲存變更並退出。

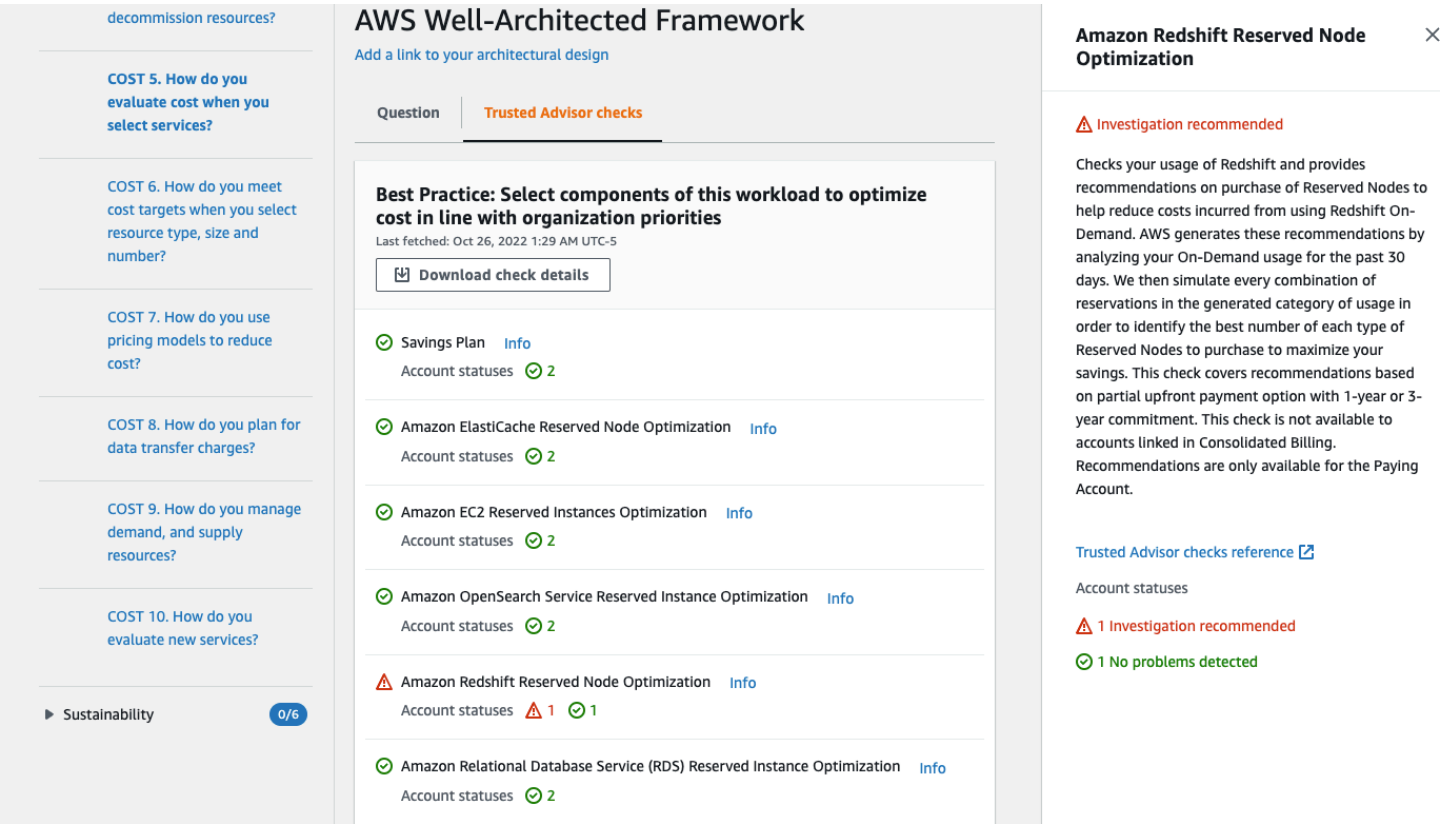
3. 右側說明窗格會顯示其他資訊和實用資源。選擇 [詢問專家] 以存取專門針對 Well-Architected 的 AWS Re: Post 社群。AWS在這個社群中，您可以提出與在上設計、建置、部署和操作工作負載相關的問題 AWS。

## Trusted Advisor 檢查

如果 Trusted Advisor 已針對您的工作負載啟動，則 [問題] 旁邊會顯示 [Trusted Advisor 檢查] 索引標籤。如果有任何可用於最佳作法的檢查，則選擇問題後會顯示有可用 Trusted Advisor 檢查的通知。選取「檢視」(View) 檢查會帶您前往Trusted Advisor 檢查標籤。




在 [Trusted Advisor 檢查] 索引標籤上，您可以檢視有關最佳作法檢查的更多詳細資訊 Trusted Advisor、檢視說明資源窗格中的 Trusted Advisor 文件連結，或 [下載檢查詳細資料]，這會提供 CSV 檔案中每個最佳作法之 Trusted Advisor 檢查和狀態的報告。




來自的檢查類別 Trusted Advisor 會顯示為彩色圖示，而每個圖示旁邊的數字則顯示該狀態的帳號數目。

- 建議採取的動作 (紅色) — Trusted Advisor 建議檢查的動作。
- 建議調查 (黃色) — Trusted Advisor 偵測檢查可能的問題。
- 未偵測到問題 (綠色) — Trusted Advisor 未偵測到支票的問題。
- 排除的項目 (灰色) - 具有已排除項目的檢查數量，例如您想要檢查忽略的資源。

若要取得有關檢查所 Trusted Advisor 提供的更多資訊，請參閱《AWS Support 使用指南》中的檢視檢查品類。

選取每個 Trusted Advisor 檢查旁邊的「資訊」(Info) 連結會顯示有關「說明資源」窗格中檢查的資訊。如需詳細資訊，請參閱《使用指南》中的AWS Support 〈AWS Trusted Advisor 檢查參考〉。

# 儲存里程碑

您隨時都可以儲存里程碑。里程碑會記錄工作負載目前的狀態。

### 儲存里程碑

1. 從工作負載詳細資訊頁面，選擇 Save milestone (儲存里程碑)。
2. 在 Milestone name (里程碑名稱) 方塊中，輸入您的里程碑名稱。

> **Note**
>
> 名稱長度必須介於 3 到 100 個字元之間。至少三個字元不能為空格。與工作負載相關聯的里程碑名稱不能重複。當系統檢查名稱是否為唯一時，會忽略空格和大小寫。

3. 選擇儲存。

儲存里程碑後，您就無法變更該里程碑中擷取的工作負載資料。

如需更多詳細資訊，請參閱 里程碑。

# 教學課程

本教學課程說明如 AWS Well-Architected Tool 何記錄和測量工作負載。本範例會逐步說明如何為零售電子商務網站定義工作負載，並加以記錄。

主題



## 步驟 1：定義工作負載

首先，您需要定義工作負載。有兩種定義工作負載的方法。在本自學課程中，我們不會從檢閱範本定義工作負載。如需有關從檢閱範本定義工作負載的詳細資訊，請參閱the section called “定義工作負載”。

定義工作負載

1. 請登入 AWS Management Console 並開啟 AWS Well-Architected Tool 主控台，網址為 https://console.aws.amazon.com/wellarchitected/。

   > **Note**
   >
   > 記錄工作負載狀態的使用者必須具有的完整存取權限 AWS WA Tool。

2. 在 Define a workload (定義工作負載) 區段中，選擇 Define workload (定義工作負載)。
3. 在 Name (名稱) 方塊中，輸入 **`Retail Website - North America`** 作為工作負載的名稱。
4. 在 Description (說明) 方塊中，輸入工作負載的說明。
5. 在 [檢閱擁有者] 方塊中，輸入負責工作負載檢閱程序的人員名稱。
6. 在 [環境] 方塊中，指出工作負載位於生產環境中。
7. 我們的工作負載在本地數據中心執行： AWS

   a. 選取AWS 區域並選擇北美洲執行工作負載的兩個區域。

   b. 同時選取非AWS 區域，然後輸入本機資料中心的名稱。
8. 「帳戶 ID」方塊是選用的。請勿將任何 AWS 帳戶 與此工作負載產生關聯。

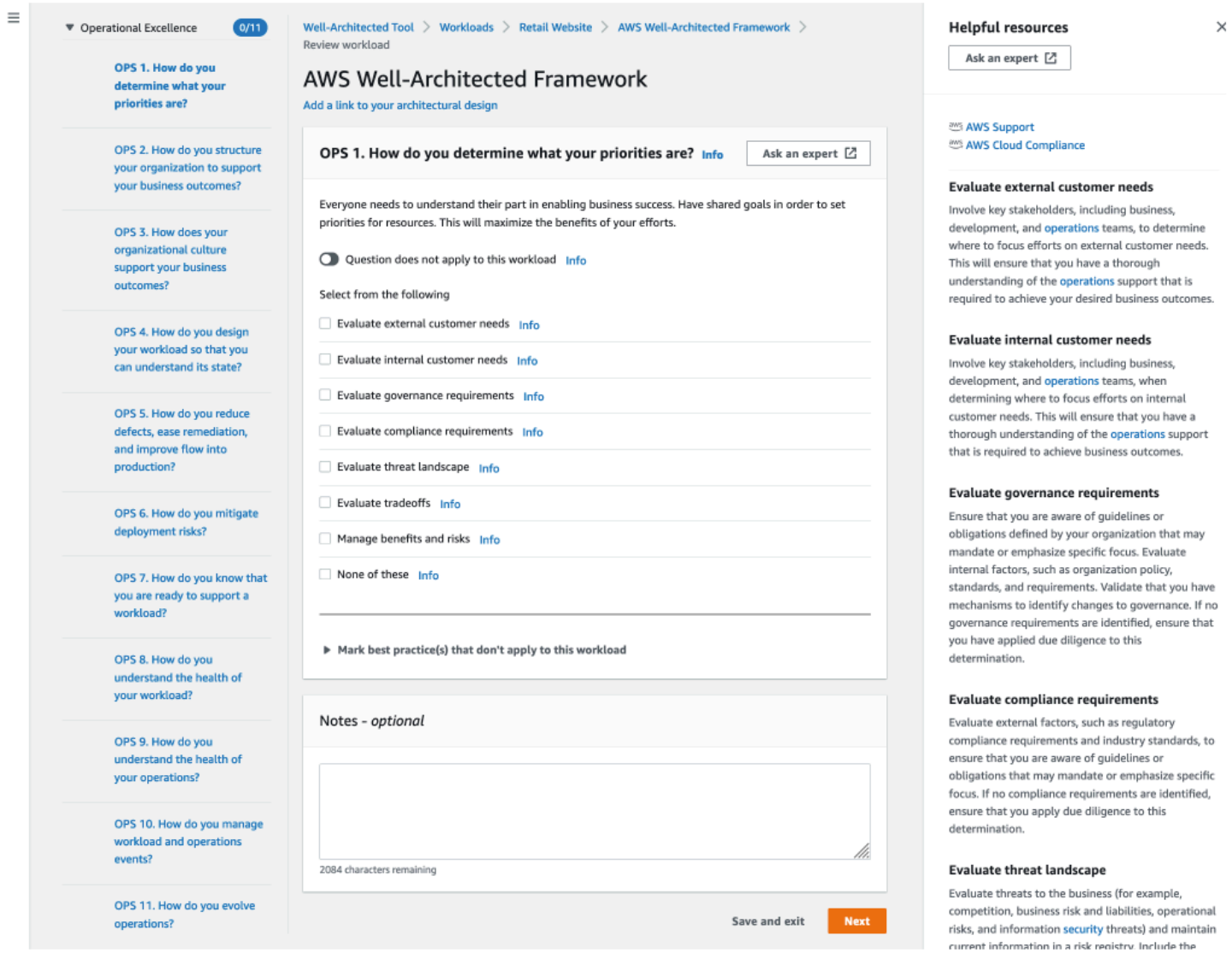
9. 「應用程式」方塊是選用的。請勿為此工作負載輸入應用程式 ARN。
10. 「建築圖」方塊是可選的。請勿將架構圖與此工作負載產生關聯。
11. Industry type (產業類型) 和 Industry (產業) 方塊為選填，且此工作負載不會指定這兩者。
12. Trusted Advisor 區段為選擇性區塊。請勿啟動 Trusted Advisor 此工作負載的 Support。
13. 「吉拉」區段是選擇性的。請勿覆寫此工作負載之 Jira 區段中的帳戶層級設定。
14. 在此範例中，請勿將任何標記套用至工作負載。選擇下一步。
15. 「套用設定檔」步驟是選擇性的。請勿針對此工作負載套用設定檔。選擇下一步。
16. 在此範例中，套用 AWS Well-Architected 的架構鏡頭，此鏡頭會自動選取。選擇 Define workload (定義工作負載)，即可儲存這些值並定義工作負載。
17. 定義工作負載後，請選擇 Start reviewing (開始檢閱) 以開始記錄工作負載的狀態。

# 步驟 2：記錄工作負載狀態

為 AWS 了記錄工作負載的狀態，您會看到所選鏡頭的問題，這些鏡頭涵蓋了良好架構的支柱：卓越的營運、安全性、可靠性、效能效率、成本最佳化和永續性。

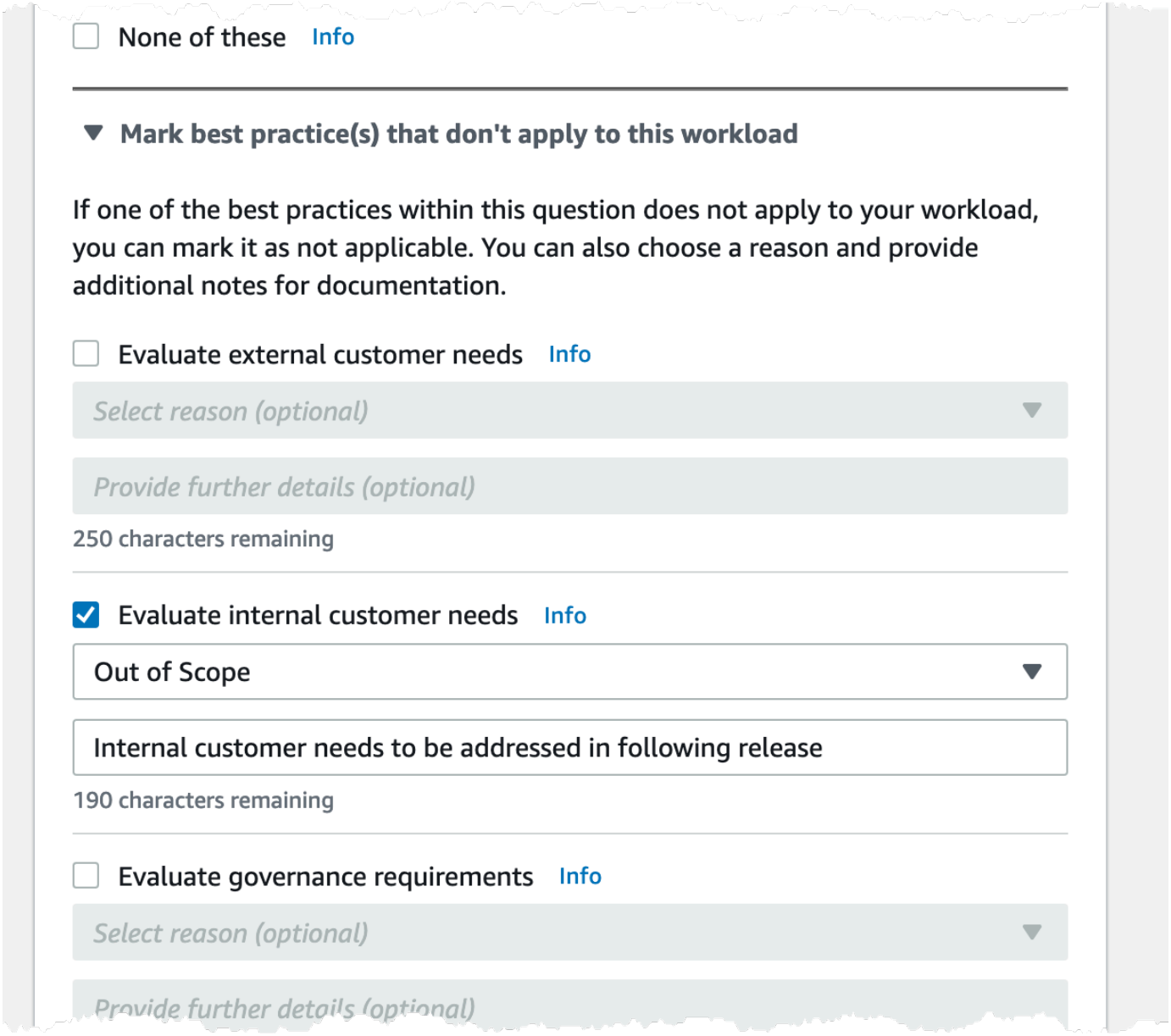
回答每個問題時，請從出現的清單中選擇您正在執行的最佳實務。如果您需要查看最佳實務的詳細資訊，請選擇 Info (資訊)，即可在右側面板中檢視其他資訊和資源。

選擇 [詢問專家] 以存取專門針對 Well-Architected 的 AWS Re: Post 社群。AWS在這個社群中，您可以提出與在上設計、建置、部署和操作工作負載相關的問題 AWS。




1. 選擇 Next (下一步)，繼續回答下一個問題。您可以使用左側面板導覽至相同要件的其他問題，或是其他要件的問題。
2. 如果您選擇 [問題不適用於此工作負載] 或 [不適用於這些工作負載]， AWS 建議您在 [附註] 方塊中加入原因。這些備註會包含在工作負載報告中，且未來變更工作負載時可能會有所幫助。

> **Note**
>
> 或者，您可以將一個或多個個別最佳作法標記為不適用。選擇 [標記不適用於此工作負載的最佳作法]，然後選取不適用的最佳做法。您可以選擇性地選取原因並提供其他明細。針對不適用的每個最佳作法重複此步驟。




> **Note**
>
> 您可以選擇 [儲存] 並結束，隨時暫停此程序。若要稍後繼續執行，請開啟 AWS WA Tool 主控台並選擇左側導覽窗格中的 [工作負載]。

3. 接著，選取工作負載名稱以開啟該工作負載的詳細資訊頁面。
4. 選擇 Continue reviewing (繼續檢閱)，然後導覽至先前停止的地方。

5. 所有問題都回答完畢後，系統會隨即顯示工作負載的概觀頁面。您可以立即查看這些詳細資訊，也可以稍後在左側導覽窗格中選擇 Workloads (工作負載)，並選取工作負載名稱來導覽至這些詳細資訊。

第一次完成工作負載狀態的記錄後，您應儲存里程碑並產生工作負載報告。

里程碑會擷取工作負載目前的狀態，讓您在根據改善計劃進行變更時，能夠衡量相關進度。

從工作負載詳細資訊頁面：

1. 在「工作負載簡介」段落中，選擇儲存里程碑按鈕。
2. 輸入**`Version 1.0 - initial review`**為「里程碑」名稱。
3. 選擇儲存。
4. 若要產生工作負載報告，請選取所需的鏡頭，然後選擇 Generate report (產生報告)，系統會隨即建立 PDF 檔案。此檔案包含工作負載的狀態、已識別的風險數量，以及建議改善項目的清單。

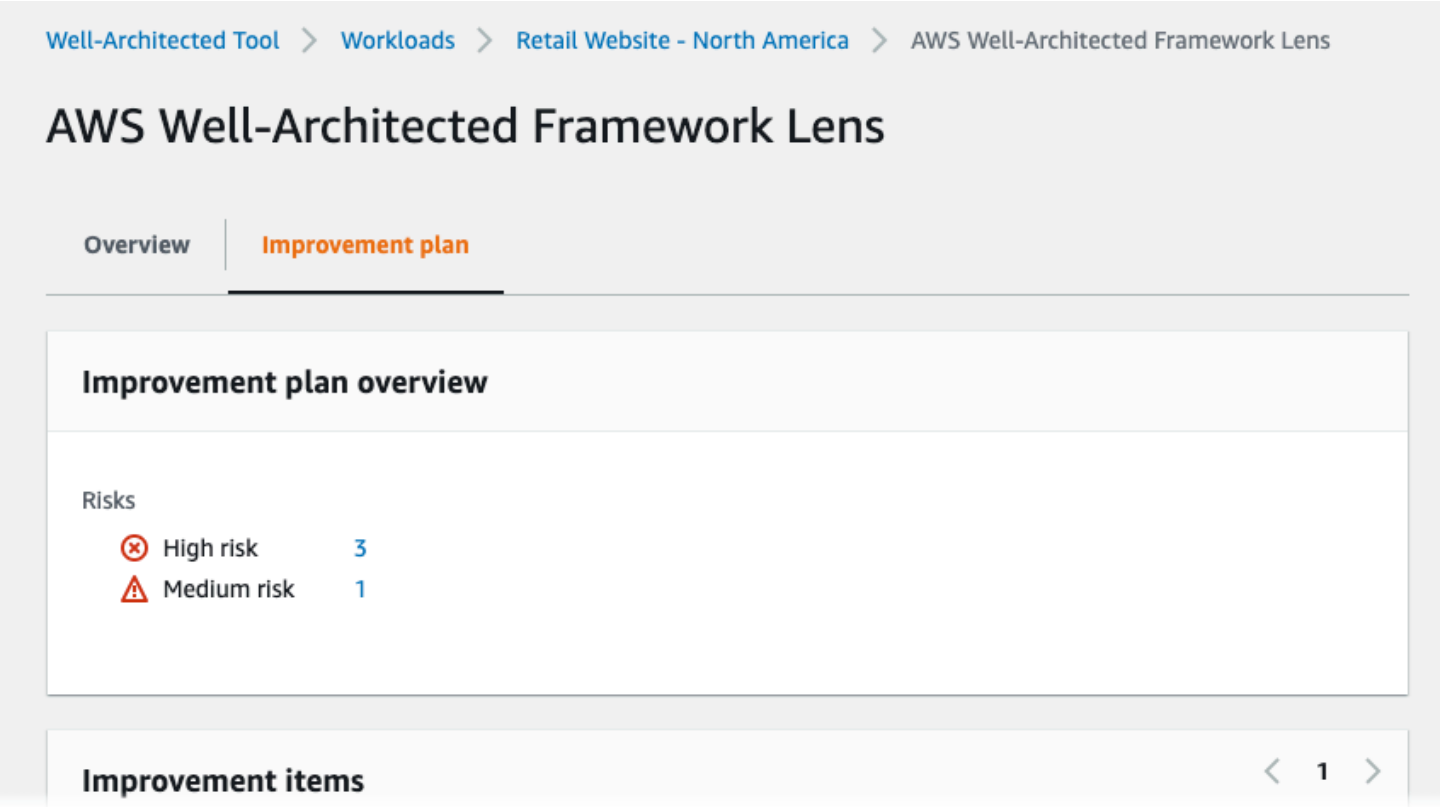
# 步驟 3：檢討改善計劃

根據選擇的最佳實踐，根據 AWS Well-Architected 的框架鏡頭來 AWS WA Tool 確定高度和中度風險的區域。

檢討改善計劃的步驟如下：

1. 從「概觀」頁面的「鏡頭」部分選擇 AWS Well-Architected 的框架。
2. 接著，選擇 Improvement plan (改善計劃)。

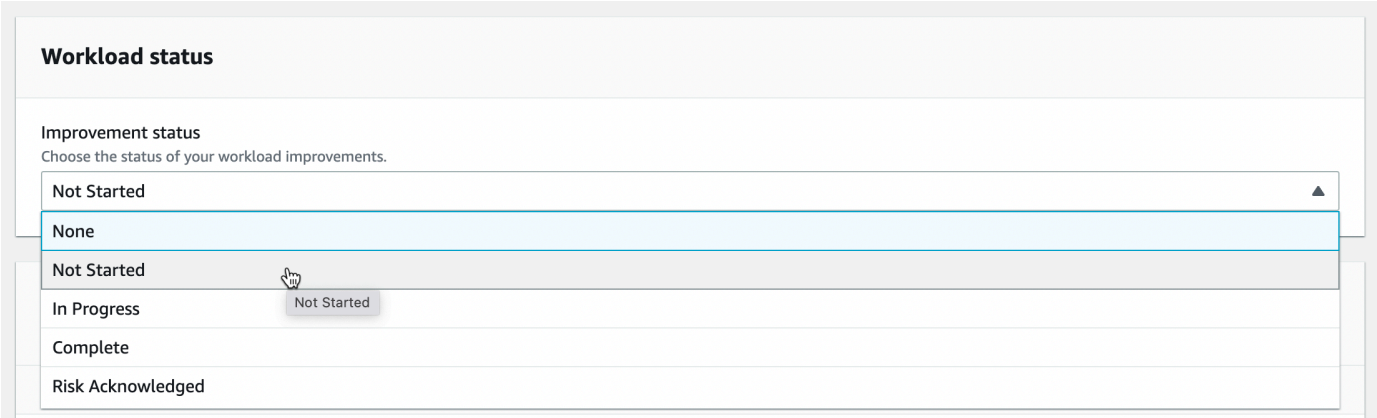
針對此特定範例工作負載， AWS Well-Architected 的架構鏡頭發現了三個高風險問題和一個中度風險問題。




更新工作負載的改進狀態，以指出工作負載的改進尚未開始。

若要變更「改善」狀態：

1. 在改善計畫中，按一下頁面頂端階層連結中的工作負載名稱 (**`Retail Website - North America`**)。
2. 點擊屬性選項卡。
3. 瀏覽至「工作負載狀態」段落，然後從下拉式清單中選取「未啟動」。



4. 按一下 [概觀] 索引標籤，然後按一下 [鏡頭] 區段中的 [AWS Well-Architected 的架構] 連結，從 [屬性] 索引標籤回到改善計畫。然後單擊頁面頂部的改進計劃選項卡。

Improvement items (改善項目) 區段會顯示系統在工作負載中找出的建議改善項目。問題會按照設定的要件優先順序來排列，且會先列出高風險問題，再列出中等風險問題。

展開 Recommended improvement items (建議改善項目)，以顯示問題的最佳實務。每個建議的改善動作會連結至詳細的專家指導，幫助您消除或至少減輕已識別的風險。

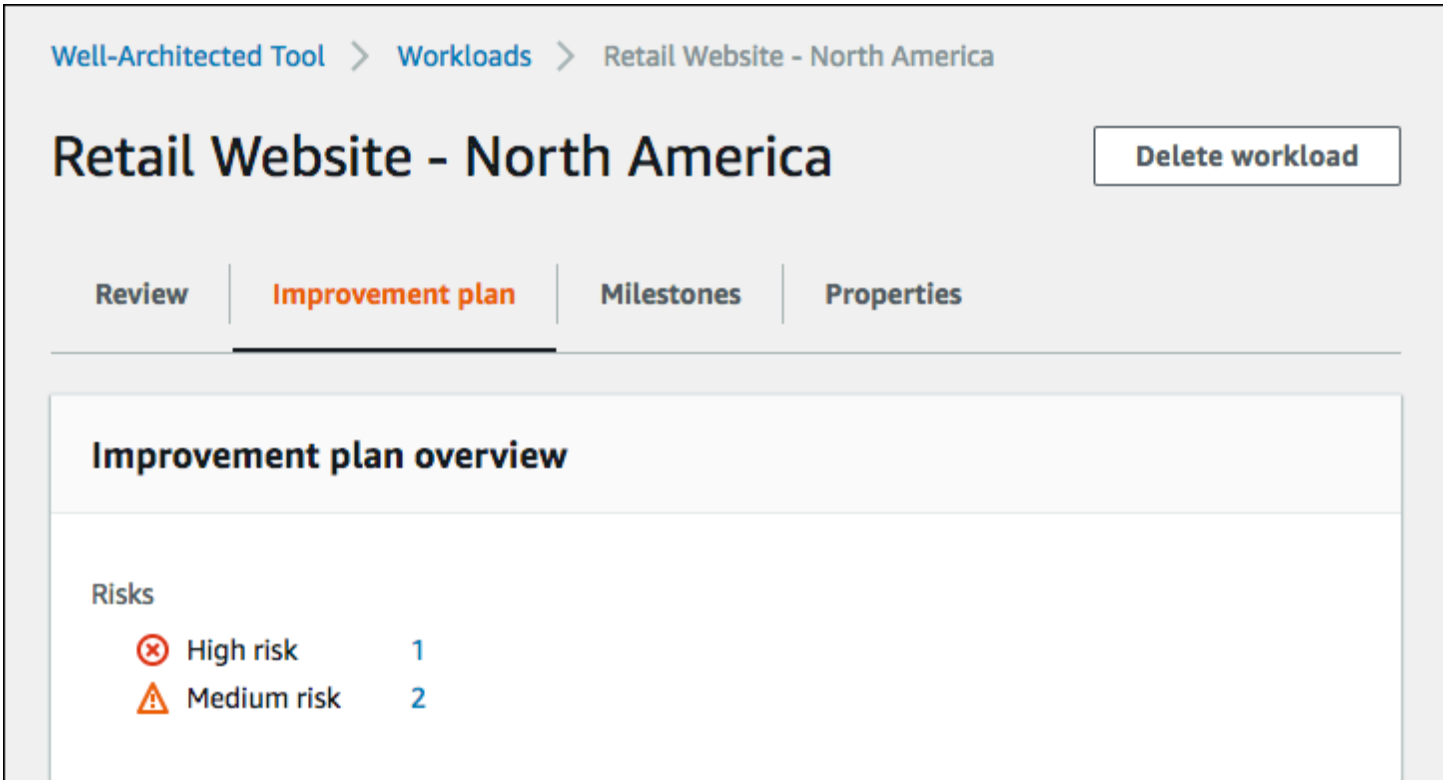
如果設定檔與工作負載相關聯，則 [改善計劃概觀] 區段中會顯示已排定優先順序的風險計數，您可以選取依設定檔排列優先順序來篩選改善項目清單。改善項目清單會顯示「優先順序」標籤。

# 步驟 4：進行改進並衡量進度

作為此改善計畫的一部分，透過在工作負載中新增 Amazon CloudWatch 和 AWS Auto Scaling 支援，已解決其中一個高風險問題。

從改進項目部分：

1. 選擇相關問題並更新選取的最佳作法以反映變更。添加註釋以記錄改進。
2. 然後選擇 [儲存並結束] 以更新工作負載的狀態。
3. 完成變更後，您可以返回 Improvement plan (改善計劃)，查看這些變更對工作負載的影響。在這個例子中，這些行動改善了風險狀況，將高風險問題的數量從三個減少到只有一個。




您可以在此時儲存里程碑，並前往 Milestones (里程碑) 來查看工作負載的改善情況。

# 工作負載

工作負載是可提供商業價值的資源和程式碼集合，例如客戶面向的應用程式或後端流程。

工作負載可能包含單一資源子集，AWS 帳戶或者是跨越多個資源的集合AWS 帳戶。小型企業可能只有少量工作負載，而大型企業可能擁有數千個工作負載。

Workloads (工作負載) 頁面位於左側導覽窗格中，其中會顯示您工作負載和與您共用之所有工作負載的相關資訊。

每個工作負載都會顯示下列資訊：

名稱

工作負載的名稱。

Owner

擁有工作負載的 AWS 帳戶 ID。

已回答問題：

已回答的問題數。

高風險

已識別的高風險問題 (HRI) 數目。

中度風險

已識別的中等風險問題 (MRI) 數目。

改善狀態

您為工作負載設定的改善狀態：

- 無
- 未開始
- 進行中
- 完成
- 已確認風險

上次更新

上次更新工作負載的日期和時間。

從清單選擇工作負載之後：

- 若要查看工作負載的詳細資訊，請選擇 View details (檢視詳細資訊)。
- 若要變更工作負載的屬性，請選擇 Edit (編輯)。
- 若要管理與其他AWS 帳戶、使用者或組織單位 (OU) 的工作負載共用，請選擇檢視詳細資料，然後選擇共用。AWS Organizations
- 若要刪除工作負載及其所有里程碑，請選擇 Delete (刪除)。只有工作負載的擁有者可刪除工作負載。

> **Warning**
>
> 刪除工作負載無法復原。系統會刪除與工作負載關聯的所有資料。

# 高風險問題 (HRI) 及中等風險問題 (MRI)

中發現的高風險問題 (HRI) AWS Well-Architected Tool 是架構和營運選擇，可能會AWS對企業造成重大負面影響。這些 HRI 可能會影響組織營運、資產和個人。中等風險問題 (MRI) 也可能對業務造成負面影響，但程度較小。這些問題是根據您在 AWS Well-Architected Tool 中的回應而定。相應的最佳做法由AWS和AWS客戶廣泛應用。這些最佳做法是 AWS Well-Architected 的框架和鏡頭所定義的指引。

> **Note**
>
> 這些只是指導方針，客戶應該評估並衡量未實施最佳實務對其業務有何影響。如果有特定技術或業務原因無法將最佳實務套用至工作負載，則風險可能會低於指定的風險。 AWS建議客戶在工作負載備註中記錄這些原因，以及它們如何影響最佳實務。針對所有已識別的 HRI 和 MRI，AWS建議客戶實作中定義的最佳實務。AWS Well-Architected Tool如果實作了最佳實務，在 AWS Well-Architected Tool 中將最佳實務標示為已符合，指出問題已解決。如果客戶選擇不實作最佳實務，則AWS建議他們記錄適用的業務層次核准，以及未實作該核准的原因。

# 定義工作負載

有兩種定義工作負載的方法。在的「工作負載」頁面上，AWS WA Tool您可以定義不使用範本的工作負載。或者，在「複查樣板」頁面上，您可以使用現有的複查樣板或建立新樣板來定義工作負載。

若要從「工作負載」頁面定義工作負載

1. 在左側導覽窗格中選取「工作負載」。
2. 選取定義工作負載下拉清單。
3. 選擇 Define workload (定義工作負載)。或者，如果您已建立檢閱範本並想要從中定義工作負載，請選擇從檢閱範本定義。
4. 依照中的指示指the section called “定義工作負載”定工作負載屬性，或 (選擇性) 套用描述檔和鏡頭。

從「複查樣板」頁面定義工作負載

1. 在左側導覽窗格中選取 [檢閱範本]。
2. 選取現有審核範本的名稱，或按照中的指示the section called “建立檢閱範本”建立新的審核範本。
3. 選擇從範本定義工作負載。
4. 依照中the section called “從範本定義工作負載”的指示從檢閱範本建立工作負載。

# 檢視工作負載

您可以查看自己擁有，以及與您共用之工作負載的詳細資訊。

檢視工作負載

1. 請登入AWS Management Console並開啟AWS Well-Architected Tool主控台，網址為 https://console.aws.amazon.com/wellarchitected/。
2. 在左側導覽窗格中，選擇 Workloads (工作負載)。
3. 選取工作負載，以下列其中一種方式檢視：
   - 選擇工作負載的名稱。
   - 選取工作負載，然後選擇 View details (檢視詳細資訊)。

系統會顯示「工作負載」詳細資訊頁面。

> **Note**
>
> 已新增必要欄位 Review owner (檢閱擁有者)，讓您輕鬆識別負責檢閱程序的主要人員或群組。

當您第一次檢視在新增此欄位之前所定義的工作負載時，系統會通知您此項變更。選擇 Edit (編輯) 以設定 Review owner (檢閱擁有者) 欄位，且無須採取進一步的動作。
選擇 Acknowledge (確認) 以延遲設定 Review owner (檢閱擁有者) 欄位。在接下來的 60 天內，會顯示一個橫幅，提醒您欄位是空白的。若要移除橫幅，請編輯您的工作負載並指定 Review owner (檢閱擁有者)。
如果您未在指定的日期內設定欄位，則會限制您對工作負載的存取。您可以繼續檢視工作負載並刪除工作負載，但是您無法編輯工作負載，除非設定 Review owner (檢閱擁有者) 欄位。當您的存取受到限制時，對工作負載的共用存取權並不會受到影響。

# 編輯工作負載

您可以編輯自己擁有的工作負載詳細資訊。

編輯工作負載

1. 請登入AWS Management Console並開啟AWS Well-Architected Tool主控台，網址為 https://console.aws.amazon.com/wellarchitected/。
2. 在左側導覽窗格中，選擇 Workloads (工作負載)。
3. 選取要編輯的工作負載，然後選擇 Edit (編輯)。
4. 對工作負載進行變更。

   如需每個欄位的說明，請參閱定義工作負載。

   > **Note**
   >
   > 更新現有工作負載時，您可以 Activate Trusted Advisor，這會自動為工作負載擁有者建立 IAM 角色。Trusted Advisor已啟動工作負載的關聯帳戶擁有者需要在 IAM 中建立角色。如需詳細資訊，請參閱 the section called “ Trusted Advisor 在 IAM 中啟用”。

5. 選擇 Save (儲存)，即可儲存您對工作負載所做的變更。

   如果必填欄位為空或指定的值無效，您必須先修正問題，才能儲存對工作負載的變更。

# 共用工作負載

您可以與其他使用者AWS 帳戶、組織和組織單位 (OU) 共用您擁有的工作負載AWS 區域。

> **Note**
>
> 您只能共用相同工作負載AWS 區域。
> 與其他人共用工作負載時AWS 帳戶，如果收件者沒
> 有`wellarchitected:UpdateShareInvitation`權限，則他們無法接受共用邀請。the section called “提供存取 AWS WA Tool”如需權限原則範例，請參閱。

與其他使用者共用AWS 帳戶工作負載

1. 請登入AWS Management Console並開啟AWS Well-Architected Tool主控台，網址為 https://console.aws.amazon.com/wellarchitected/。
2. 在左側導覽窗格中，選擇 Workloads (工作負載)。
3. 請使用下列其中一種方式選取您擁有的工作負載：
   - 選擇工作負載的名稱。
   - 選取工作負載，然後選擇 View details (檢視詳細資訊)。
4. 選擇 Shares (共用)。然後選擇 [建立並建立共用給使用者或帳戶] 以建立工作負載邀請。
5. 輸入您要與其共用工作負載之使用者的 12 位數 AWS 帳戶 ID 或 ARN。
6. 選擇您要授予的許可。

   唯讀

   提供對工作負載的唯讀存取權。

   作者群

   提供對回答與其備註的更新存取權，以及對工作負載其他部分的唯讀存取權。
7. 選擇建立，將工作負載邀請傳送給指定的AWS 帳戶或使用者。

如果未在七天內接受邀請，邀請會自動過期。

如果使用者和使用者AWS 帳戶都有工作負載邀請，則具有最高層級權限的工作負載邀請會套用至該使用者。

> **Important**
>
> 在與組織或組織單位 (OU) 共用工作負載之前，您必須啟用AWS Organizations存取權。

與您的組織或 OU 共用工作負載

1. 請登入AWS Management Console並開啟AWS Well-Architected Tool主控台，網址為 https://console.aws.amazon.com/wellarchitected/。
2. 在左側導覽窗格中，選擇 Workloads (工作負載)。
3. 請使用下列其中一種方式選取您擁有的工作負載：
   - 選擇工作負載的名稱。
   - 選取工作負載，然後選擇 View details (檢視詳細資訊)。
4. 選擇 Shares (共用)。然後選擇「建立並建立共用至 Organizations」。
5. 在 [建立工作負載共用] 頁面上，選擇要授與權限給整個組織，還是授與一或多個 OU。
6. 選擇您要授予的許可。

   唯讀

   提供對工作負載的唯讀存取權。

   作者群

   提供對回答與其備註的更新存取權，以及對工作負載其他部分的唯讀存取權。
7. 選擇建立以共用工作負載。

若要查看誰擁有工作負載的共用存取權，請從工作量詳細頁面中選擇 [共用]。

若要避免實體共用工作負載，請連接拒絕 `wellarchitected:CreateWorkloadShare` 動作的政策。

您也可以與其他使用者AWS 帳戶、您的組織和 OU 共用您擁有的自訂鏡頭AWS 區域。如需詳細資訊，請參閱共用自訂鏡頭。

## 共享考量

一個工作負載最多可以與 20 個不同的使用者AWS 帳戶和使用者共用。工作負載只能與與工作負載相同AWS 區域的帳戶和使用者共用。

若要在 2019 年 3 月 20 日之後引入的區域中共用工作負載，您和共用人都AWS 帳戶必須在中啟用該區域AWS Management Console。如需詳細資訊，請參閱AWS全球基礎架構。

您可以與帳戶中的個別使用者或兩者共用工作負載。AWS 帳戶當您與工作負載共用時AWS 帳戶，該帳戶中的所有使用者都將獲得該工作負載的存取權。如果帳戶中只有特定使用者需要存取權，請遵循授與最低權限的最佳做法，並與這些使用者個別共用工作負載。

如果帳戶中的使用者AWS 帳戶和使用者都有工作負載邀請，則具有最高層級權限的工作負載邀請將決定使用者對工作負載的權限。如果您刪除使用者的工作負載邀請，則使用者的存取權由的工作負載邀請決定AWS 帳戶。刪除這兩個工作負載邀請，以移除使用者對工作負載的存取權。

在與組織或一個或多個組織單位 (OU) 共用工作負載之前，您必須啟用AWS Organizations存取權。

如果您與組織和一個或多個 OU 共用工作負載，具有最高層級權限的工作負載邀請將決定帳戶對該工作負載的權限。

若要啟用AWS Organizations共用

1. 請登入AWS Management Console並開啟AWS Well-Architected Tool主控台，網址為 https://console.aws.amazon.com/wellarchitected/。
2. 在左側的導覽窗格中，選擇 Settings (設定)。
3. 選擇 [啟用AWS Organizations支援]。
4. 選擇儲存設定。

## 刪除共用存取

您可以刪除工作負載邀請。刪除工作負載邀請會移除對工作負載的共用存取權。

刪除工作負載的共用存取權

1. 請登入AWS Management Console並開啟AWS Well-Architected Tool主控台，網址為 https://console.aws.amazon.com/wellarchitected/。
2. 在左側導覽窗格中，選擇 Workloads (工作負載)。
3. 請以下列其中一種方法來選取工作負載：
   - 選擇工作負載的名稱。
   - 選取工作負載，然後選擇 View details (檢視詳細資訊)。
4. 選擇 Shares (共用)。
5. 選取要刪除的工作負載，並選擇 Delete (刪除)。
6. 選擇 Delete (刪除)，確認刪除。

如果使用者和使用者AWS 帳戶擁有工作負載邀請，您必須刪除兩個工作負載邀請，才能移除使用者對工作負載的權限。

## 修改共用存取

您可以修改未接受或已接受的工作負載邀請。

修改工作負載的共用存取權

1. 請登入AWS Management Console並開啟AWS Well-Architected Tool主控台，網址為 https://console.aws.amazon.com/wellarchitected/。
2. 在左側導覽窗格中，選擇 Workloads (工作負載)。
3. 請使用下列其中一種方式選取您擁有的工作負載：
   - 選擇工作負載的名稱。
   - 選取工作負載，然後選擇 View details (檢視詳細資訊)。
4. 選擇 Shares (共用)。
5. 選取要修改的工作負載，並選擇 Edit (編輯)。
6. 選擇您要授與AWS 帳戶或使用者的新權限。

   唯讀

   提供對工作負載的唯讀存取權。

   作者群

   提供對回答與其備註的更新存取權，以及對工作負載其他部分的唯讀存取權。
7. 選擇 儲存 。

如果未在七天內接受已修改工作負載邀請，邀請會自動過期。

## 接受和拒絕工作負載邀請

工作負載邀請是要求共用另一個人所擁有的工作負載AWS 帳戶。如果您接受工作負載邀請，工作負載會新增至您的 Workloads (工作負載) 和 Dashboard (儀表板) 頁面。如果您拒絕工作負載邀請，邀請會從工作負載邀請清單中移除。

您有七天的時間可決定是否要接受工作負載邀請。如果您沒有在七天內接受邀請，邀請會自動過期。

> **Note**
>
> 工作負載只能在同一工作負載內共用AWS 區域。

接受或拒絕工作負載邀請

1. 請登入AWS Management Console並開啟AWS Well-Architected Tool主控台，網址為 https://console.aws.amazon.com/wellarchitected/。
2. 在左側導覽窗格中，選擇 Workload invitations (工作負載邀請)。
3. 選取要接受或拒絕的工作負載邀請。
   - 如果要接受工作負載邀請，請選擇 Accept (接受)。

     工作負載會新增至 Workloads (工作負載) 和 Dashboard (儀表板) 頁面。
   - 如果要拒絕工作負載邀請，請選擇 Reject (拒絕)。

     工作負載邀請會從清單中移除。

若要在接受工作負載邀請後拒絕共用存取，請從工作負載的工作量詳細頁面中選擇拒絕共用。

# 刪除工作負載

不再需要工作負載時，即可將之刪除。刪除工作負載會移除與工作負載相關的所有資料，包括任何里程碑和工作負載共用邀請。只有工作負載的擁有者可刪除工作負載。

> **Warning**
>
> 刪除工作負載無法復原。系統會永久移除與工作負載關聯的所有資料。

刪除工作負載

1. 請登入AWS Management Console並開啟AWS Well-Architected Tool主控台，網址為 https://console.aws.amazon.com/wellarchitected/。
2. 在左側導覽窗格中，選擇 Workloads (工作負載)。
3. 選取您要刪除的工作負載，然後選擇 Delete (刪除)。
4. 在 Delete (刪除) 視窗中，選擇 Delete (刪除) 以確認工作負載及其里程碑的刪除。

若要避免實體刪除工作負載，請連接拒絕 `wellarchitected:DeleteWorkload` 動作的政策。

# 產生工作負載報告

您可以產生鏡頭的工作負載報告。這份報告會包含您對工作負載問題的回應、您的備註，以及目前識別的高風險和中等風險數量。如果問題有一或多個已識別風險，則該問題的改善計劃會列出需採取的動作，以減少這些風險。

如果您的工作負載具有關聯的設定檔，則設定檔概觀資訊和已排定優先順序的風險會顯示在工作負載報表上。

您可藉由該報告將工作負載詳細資訊分享給沒有權限存取 AWS Well-Architected Tool 的其他使用者。

產生工作負載報告

1. 請登入AWS Management Console並開啟AWS Well-Architected Tool主控台，網址為 https://console.aws.amazon.com/wellarchitected/。
2. 在左側導覽窗格中，選擇 Workloads (工作負載)。
3. 選取所需的工作負載，然後選擇 View details (檢視詳細資料)。
4. 選取您想要產生報告的鏡頭，然後選擇 Generate report (產生報告)。

   報告已產生，您可以下載或檢視。

# 工作量詳細

工作負載詳細資訊頁面提供您的工作負載相關資訊，包括其里程碑、改善計劃和所有工作負載共用。使用頁面頂部的索引標籤，即可導覽至不同的詳細資訊區段。

如果要刪除工作負載，請選擇 Delete workload (刪除工作負載)。只有工作負載的擁有者可刪除工作負載。

如果要移除您對共用工作負載的存取權，請選擇 Reject share (拒絕共用)。

主題

- 概觀標籤
- 里程碑標籤
- 屬性標籤
- 共用標籤

## 概觀標籤

初次檢視工作負載時，系統顯示的第一項資訊即是 Overview (概觀) 標籤。此標籤會提供工作負載的整體狀態，以及每個鏡頭的狀態。

如果您尚未完成所有問題，系統會顯示橫幅以提醒您開始或繼續記錄工作負載。

Workload overview (工作負載概觀) 區段會顯示工作負載目前的整體狀態，以及您輸入的任何 Workload notes (工作負載備註)。您可以選擇 Edit (編輯) 來更新狀態或備註。

若要擷取工作負載目前的狀態，則請選擇 Save milestone (儲存里程碑)。里程碑是固定的，且儲存後將無法變更。

若要繼續記錄工作負載的狀態，請選擇 Start reviewing (開始檢閱)，然後選取所需的鏡頭。

## 里程碑標籤

若要顯示工作負載的里程碑，請選擇 Milestones (里程碑) 索引標籤。

選取里程碑後，請選擇 Generate report (產生報告) 來建立與里程碑相關聯的工作負載報告。這份報告會包含您對工作負載問題的回應、您的備註，以及工作負載在里程碑儲存期間所擁有的高風險和中等風險數量。

處理特定里程碑時，您可以使用下列任一方式來檢視工作負載狀態的詳細資訊：

- 選擇里程碑的名稱。
- 選取里程碑，並選擇 View milestone (檢視里程碑)。

## 屬性標籤

若要顯示工作負載的屬性，請選擇 Properties (屬性) 索引標籤。這些屬性是當初定義工作負載時指定的值。選擇 Edit (編輯) 來進行變更。只有工作負載的擁有者可進行變更。

如需屬性的描述，請參閱 定義工作負載。

## 共用標籤

如果要顯示或修改您的工作負載邀請，請選擇 Shares (共用) 標籤。只有工作負載的擁有者可以看到此標籤。

針對具有工作負載共用存取權的每個使用者AWS 帳戶和使用者，會顯示下列資訊：

Principal

具有工作負載共用存取權的 AWS 帳戶 ID 或使用者 ARN。

狀態

工作負載邀請的狀態。

- 待定

  邀請正在等待接受或拒絕。如果未在七天內接受工作負載邀請，邀請會自動過期。

- 已接受

  已接受邀請。

- 已拒絕

  已拒絕邀請

- 已過期

  未在七天內接受或拒絕邀請。

許可

授與AWS 帳戶或使用者的權限。

- 唯讀

  委託人具有對工作負載的唯讀存取權。

- 作者群

  委託人可以更新回答與其備註，且對工作負載的其他部分具有唯讀存取權。

許可詳細資訊

許可的詳細說明。

若要與其他使用者AWS 帳戶或其他使用者共用工作負載AWS 區域，請選擇 [建立]。一個工作負載最多可以與 20 個不同的使用者AWS 帳戶和使用者共用。

如果要刪除工作負載邀請，請選取邀請並選擇 Delete (刪除)。

如果要修改工作負載邀請，請選取邀請並選擇 Edit (編輯)。

# 鏡頭

鏡頭可讓您根據最佳實務以一致的方式來衡量架構，並找出需要改善的區域。定義工作負載時，系統會自動套用 AWS Well-Architected 的架構鏡頭。

一個工作負載可以套用一或多個鏡頭。每個鏡頭都有自己的一組問題、最佳實務、備註和改善計劃。

有兩種鏡頭可以應用於您的工作負載：鏡頭目錄鏡頭和定制鏡頭。

- 鏡頭目錄：由創建和維護的官方鏡頭 AWS。鏡頭目錄適用於所有使用者，不需要額外安裝即可使用。
- 自訂鏡頭：非 AWS 官方內容的使用者定義鏡頭。您可以使用自己的支柱，問題，最佳實踐和改進計劃創建自定義鏡頭，並與其他人共享自定義鏡頭 AWS 帳戶。

一次可以為一個工作量添加五個鏡頭，一個工作量最多可以使用 20 個鏡頭。

如果從工作負載中移除了鏡頭，會保留與該鏡頭相關聯的資料。如果您重新將鏡頭新增到工作負載，則會還原資料。

## 將鏡頭新增至工作負載

將鏡頭新增到工作負載

1. 請登入 AWS Management Console 並開啟 AWS Well-Architected Tool 主控台，網址為 https://console.aws.amazon.com/wellarchitected/。
2. 在左側導覽窗格中，選擇 Workloads (工作負載)。
3. 選取所需的工作負載，然後選擇 View details (檢視詳細資料)。
4. 選取要新增的鏡頭，選擇 [儲存]。

   您可以從客製鏡頭、鏡頭目錄或兩者中選擇鏡頭。

一個工作負載最多可以添加 20 個鏡頭。

如需更多有關 AWS 鏡頭目錄的資訊，請瀏覽 AWS Well-Architected 的鏡頭。請注意，並非每個鏡頭白皮書都是在鏡頭目錄中作為鏡頭提供的。

**免責聲明**

通過訪問和/或 AWS 使用由其他用戶或帳戶創建的自定義鏡頭，您確認由其他用戶創建並與您共享的定制鏡頭是根據 AWS 客戶協議中定義的第三方內容。

# 從工作負載中移除鏡頭

從工作負載中移除鏡頭

1. 請登入 AWS Management Console 並開啟 AWS Well-Architected Tool 主控台，網址為 https://console.aws.amazon.com/wellarchitected/。
2. 在左側導覽窗格中，選擇 Workloads (工作負載)。
3. 選取所需的工作負載，然後選擇 View details (檢視詳細資料)。
4. 取消選取您要移除的鏡頭，然後選擇 [儲存]。

   AWS Well-Architected 的框架鏡頭無法從工作負載中移除。

系統會保留與鏡頭相關聯的資料。如果您重新將鏡頭新增到工作負載，則會還原資料。

# 鏡頭細節

若要檢視鏡頭的詳細資料，請選擇鏡頭。

## 概觀標籤

Overview (概觀)標籤提供鏡頭的一般資訊，例如已回答的問題數目。您可以從此標籤繼續檢閱工作負載、產生報告或編輯鏡頭備註。

## 改進計劃標籤

Improvement Plan (改善計劃) 標籤提供建議動作清單，以協助您改善工作負載。您可以根據風險和要件篩選建議。

## 共用標籤

對於自訂鏡頭，[共用] 索引標籤會提供與該鏡頭共用的 IAM 主體清單。

# 訂製鏡頭

您可以使用自己的支柱，問題，最佳實踐和改進計劃創建自定義鏡頭。您可以使用與套用 AWS 提供的鏡頭相同的方式，將自訂鏡頭套用到工作負載上。您也可以與其他人分享自己製作的自訂鏡頭 AWS 帳戶，其他人擁有的自訂鏡頭也可以與您分享。

您可以在自訂鏡頭中針對特定技術量身打造問題、協助您滿足組織內的治理需求，或是擴充由 Well-Architected Framework 和鏡頭所提供的 AWS 指引。與現有鏡頭一樣，您可以透過建立里程碑來追蹤一段時間的進度，並透過產生報告來提供定期狀態。

主題



## 檢視自訂鏡頭

您可以查看自己擁有的定制鏡頭和已與您共享的定制鏡頭的詳細信息。

檢視鏡頭

1. 請登入 AWS Management Console 並開啟 AWS Well-Architected Tool 主控台，網址為 https://console.aws.amazon.com/wellarchitected/。
2. 在左側導覽窗格中，選擇 [自訂鏡頭]。

   > **Note**
   >
   > 如果您尚未建立自訂鏡頭或與您共用自訂鏡頭，則「自訂鏡頭」區段為空白。

3. 選擇您要檢視的自訂鏡頭：

- 我擁有 — 顯示您創建的自定義鏡頭。
- 與我分享 — 顯示已與您分享的自訂鏡頭。

4. 以下列其中一種方式選擇要檢視的自訂鏡頭：
   - 選擇鏡頭名稱。
   - 選取鏡頭並選擇 [檢視詳細資料]。

此時會顯示鏡頭細節頁面。

「自訂鏡頭」頁面包含下列欄位：

名稱

鏡頭的名稱。

Owner

擁有自訂鏡頭的 AWS 帳戶 ID。

Status

「已發佈」狀態表示自訂鏡頭已發佈，可套用至工作負載或與其他人共用 AWS 帳戶。

DRAFT 狀態表示自訂鏡頭已建立，但尚未發佈。必須先發佈自訂鏡頭，才能將其套用至工作負載或共用。

版本

自訂鏡頭的版本名稱。

上次更新

自訂鏡頭上次更新的日期和時間。

## 建立自訂鏡頭

建立自訂鏡頭

1. 請登入 AWS Management Console 並開啟 AWS Well-Architected Tool 主控台，網址為 https://console.aws.amazon.com/wellarchitected/。
2. 在左側導覽窗格中，選擇 [自訂鏡頭]。
3. 選擇「建立自訂鏡頭」。

4. 選擇 [下載檔案] 以下載 JSON 範本檔案。
5. 使用您最愛的文字編輯器開啟 JSON 範本檔案，並新增自訂鏡頭的資料。此資料包括您的支柱、問題、最佳做法和改善計畫連結。

   請參閱 鏡頭格式規格 以取得詳細資訊。自訂鏡頭的尺寸不得超過 500 KB。
6. 選擇 [選擇檔案] 以選取您的 JSON 檔案。
7. (選擇性) 在「標籤」區段中，新增任何您要與自訂鏡頭建立關聯的標籤。
8. 選擇「提交並預覽」以預覽自訂鏡頭，或選擇「送出」以提交自訂鏡頭而不預覽。

   如果您選擇「送出並預覽自訂鏡頭」，您可以選取「下一步」來瀏覽鏡頭預覽，或選取「結束預覽」返回「自訂鏡頭」。

如果驗證失敗，請編輯您的 JSON 檔案，然後再次嘗試建立自訂鏡頭。

AWS WA Tool 驗證您的 JSON 檔案後，您的自訂鏡頭會顯示在自訂鏡頭中。

建立自訂鏡頭後，該鏡頭處於「草稿」狀態。您必須先發佈鏡頭，才能將鏡頭套用至工作負載或與其他人共用 AWS 帳戶。

您最多可以在一個中建立 15 個自訂鏡頭 AWS 帳戶。

> **免責聲明**
>
> 請勿在您的自訂鏡頭中包含或收集終端使用者或其他可識別個人的個人識別資訊 (PII)。如果您的自訂鏡頭或與您共用並在您帳戶中使用的鏡頭確實包含或收集 PII，您必須負責：確保包含的 PII 根據適用法律進行處理，提供適當的隱私權聲明，並取得處理此類資料的必要同意。

## 預覽自訂鏡頭

預覽自訂鏡頭

1. 請登入 AWS Management Console 並開啟 AWS Well-Architected Tool 主控台，網址為 https://console.aws.amazon.com/wellarchitected/。
2. 在左側導覽窗格中，選擇 [自訂鏡頭]。
3. 只能預覽處於「草稿」(DRAFT) 狀態的鏡頭。選擇所需的 DRAFT 自訂鏡頭，然後選擇預覽體驗。

4. 選擇「下一步」以瀏覽鏡頭預覽。
5. (選擇性) 您可以在預覽中的每個問題中選取最佳做法，然後選擇根據答案更新來測試您的風險邏輯，以檢閱您的改善計畫。如果需要變更，您可以在發佈之前更新 JSON 範本中的風險規則。
6. 選擇「結束預覽」以返回自訂鏡頭。

> **Note**
>
> 您也可以在建立自訂鏡頭時選取「提交與預覽」來預覽自訂鏡頭。

## 首次發佈自訂鏡頭

發佈自訂鏡頭

1. 請登入 AWS Management Console 並開啟 AWS Well-Architected Tool 主控台，網址為 https://console.aws.amazon.com/wellarchitected/。
2. 在左側導覽窗格中，選擇 [自訂鏡頭]。
3. 選取所需的自訂鏡頭，然後選擇 [發佈鏡頭]。
4. 在「版本名稱」方塊中，輸入版本變更的唯一識別碼。此值最多可包含 32 個字元，且只能包含英數字元和句點 (「.」)。
5. 選擇「發佈自訂鏡頭」。

   自訂鏡頭發佈後，就會處於「已發佈」狀態。

自訂鏡頭現在可套用至工作負載，或與其他 AWS 帳戶 或使用者共用。

## 發佈自訂鏡頭的更新

將更新發佈到現有的自訂鏡頭

1. 請登入 AWS Management Console 並開啟 AWS Well-Architected Tool 主控台，網址為 https://console.aws.amazon.com/wellarchitected/。
2. 在左側導覽窗格中，選擇 [自訂鏡頭]。
3. 選取所需的自訂鏡頭，然後選擇 [編輯]。
4. 如果您尚未準備好更新的 JSON 檔案，請選擇 [下載檔案] 以下載目前自訂鏡頭的副本。使用您喜歡的文本編輯器編輯下載的 JSON 文件，並進行所需的更改。

5. 選擇「選擇檔案」以選取更新的 JSON 檔案，然後選擇「提交與預覽」以預覽自訂鏡頭，或選擇「送出」以提交自訂鏡頭而不預覽。

   自訂鏡頭的尺寸不得超過 500 KB。

   AWS WA Tool 驗證您的 JSON 檔案後，您的自訂鏡頭會顯示在「草稿」狀態的「自訂鏡頭」中。

6. 再次選取自訂鏡頭，然後選擇 [發佈鏡頭]。
7. 選擇 [發佈前檢視變更]，以確認對自訂鏡頭所做的變更是否正確。這包括驗證：

   - 自訂鏡頭的名稱
   - 支柱名稱
   - 新的、更新和刪除的問題

   選擇下一步。

8. 指定版本變更的類型。

   主要版本

   表示鏡頭已經進行了重大變更。用於影響自訂鏡頭意義的變更。

   套用鏡頭的任何工作負載都會收到有新版本的自訂鏡頭可供使用的通知。

   主要版本變更不會自動套用至使用鏡頭的工作負載。

   次要版本

   表示鏡頭已進行輕微變更。用於較小的變更，例如文字變更或 URL 連結的更新。

   次要版本變更會自動套用至使用自訂鏡頭的工作負載。

   選擇下一步。

9. 在「版本名稱」方塊中，輸入版本變更的唯一識別碼。此值最多可包含 32 個字元，且只能包含英數字元和句點 (「.」)。
10. 選擇「發佈自訂鏡頭」。

    自訂鏡頭發佈後，就會處於「已發佈」狀態。

更新後的自訂鏡頭現在可套用至工作負載，或與其他使用者 AWS 帳戶 或使用者共用。

如果更新是主要版本變更，套用舊版鏡頭的任何工作負載都會收到有新版本可用的通知，並提供升級選項。

次要版本更新會自動套用，恕不另行通知。

您最多可以建立 100 個自訂鏡頭版本。

## 共用自訂鏡頭

您可以與其他 AWS 帳戶、使用者和組織單位 (OU) 共用自訂鏡頭。 AWS Organizations

與其 AWS 帳戶 他使用者共用自訂鏡頭

1. 請登入 AWS Management Console 並開啟 AWS Well-Architected Tool 主控台，網址為 https://console.aws.amazon.com/wellarchitected/。
2. 在左側導覽窗格中，選擇 [自訂鏡頭]。
3. 選取要共用的自訂鏡頭，然後選擇 [檢視詳細資料]。
4. 在鏡頭細節頁面上，選擇 [共用]。然後選擇 [建立並建立共用給使用者或帳戶] 以建立鏡頭共用邀請。
5. 輸入您要與其共享自訂鏡頭的使用者的 12 位數 AWS 帳戶 ID 或 ARN。
6. 選擇「建立」，將鏡頭共用邀請傳送給指定的 AWS 帳戶 或使用者。

您最多可與 300 位 AWS 帳戶 或使用者共用自訂鏡頭。

如果未在七天內接受鏡頭分享邀請，邀請將自動過期。

> **Important**
>
> 在與組織或組織單位 (OU) 共用自訂鏡頭之前，您必須啟用 AWS Organizations 存取權。

與您的組織或 OU 共用自訂鏡頭

1. 請登入 AWS Management Console 並開啟 AWS Well-Architected Tool 主控台，網址為 https://console.aws.amazon.com/wellarchitected/。
2. 在左側導覽窗格中，選擇 [自訂鏡頭]。
3. 選擇要共用的自訂鏡頭。
4. 在鏡頭細節頁面上，選擇 [共用]。然後選擇「建立並建立共用至 Organizations」。

5. 在 [建立自訂鏡頭共用] 頁面上，選擇要授與權限給整個組織，還是授與一或多個 OU。
6. 選擇「建立」以分享自訂鏡頭。

若要查看誰擁有自訂鏡頭的共用權限，請從鏡頭細節頁面中選擇「分享」。

> **免責聲明**
>
> 透過與其他人分享您的自訂鏡頭 AWS 帳戶，即表示您確 AWS 認您的自訂鏡頭可供這些其他帳戶使用。這些其他帳戶可能會繼續存取和使用您共享的自訂鏡頭，即使您從自己的鏡頭中刪除自訂鏡頭 AWS 帳戶 或終止您的鏡頭 AWS 帳戶。

## 為自訂鏡頭新增標籤

新增標籤至自訂鏡頭

1. 請登入 AWS Management Console 並開啟 AWS Well-Architected Tool 主控台，網址為 https://console.aws.amazon.com/wellarchitected/。
2. 在左側導覽窗格中，選擇 [自訂鏡頭]。
3. 選擇您要更新的自訂鏡頭。
4. 在「標籤」區段中，選擇「管理標籤」。
5. 選取「新增標籤」，然後為您要新增的每個標籤輸入「機碼」和「值」。
6. 選取 Save (儲存)。

若要移除標記，請在您要移除的標籤旁選擇「移除」。

## 刪除自訂鏡頭

刪除自訂鏡頭

1. 請登入 AWS Management Console 並開啟 AWS Well-Architected Tool 主控台，網址為 https://console.aws.amazon.com/wellarchitected/。
2. 在左側導覽窗格中，選擇 [自訂鏡頭]。
3. 選取要刪除的自訂鏡頭，然後選擇「刪除」。
4. 選擇刪除。

套用鏡頭的現有工作負載會收到自訂鏡頭已刪除的通知，但可以繼續使用。自訂鏡頭無法再套用至新的工作負載。

**免責聲明**

透過與其他人分享您的自訂鏡頭 AWS 帳戶，即表示您確 AWS 認您的自訂鏡頭可供這些其他帳戶使用。這些其他帳戶可能會繼續存取和使用您共享的自訂鏡頭，即使您從自己的鏡頭中刪除自訂鏡頭 AWS 帳戶 或終止您的鏡頭 AWS 帳戶。

## 鏡頭格式規格

鏡頭是使用特定的 JSON 格式定義的。當您開始建立自訂鏡頭時，您可以選擇下載範本 JSON 檔案。您可以使用此文件作為自定義鏡頭的基礎，因為它定義了支柱，問題，最佳實踐和改進計劃的基本結構。

### 鏡頭部分

本節定義自訂鏡頭本身的屬性。這是它的名稱和描述。

- `schemaVersion`：要使用的自訂鏡頭結構描述版本。由範本設定，請勿變更。
- `name`：鏡頭名稱。名稱最多可包含 128 個字元。
- `description`：鏡頭的文字描述。當選取要在工作負載建立期間新增的鏡頭，或選取稍後套用至現有工作負載的鏡頭時，會顯示此文字。說明最多可有 2048 個字元。

```
   "schemaVersion": "2021-11-01",
   "name": "Company Policy ABC",
   "description": "This lens provides a set of specific questions to assess compliance
with company policy ABC-2021 as revised on 2021/09/01.",
```

### 支柱部分

本節定義了與自訂鏡頭相關的支柱。您可以將問題映射到 AWS Well-Architected 的框架的支柱，定義自己的支柱，或兩者兼而有之。

您可以在自訂鏡頭中定義多達 10 個支柱。

- id：支柱的識別碼。ID 可以介於 3 到 128 個字元之間，且僅包含英數字元和底線 (「_」) 字元。支柱中使用的 ID 必須是唯一的。

  將您的問題映射到框架的支柱時，請使用以下 ID：

  - operationalExcellence
  - security
  - reliability
  - performance
  - costOptimization
  - sustainability
- name：支柱的名稱。名稱最多可包含 128 個字元。

```
    "pillars": [
       {
           "id": "company_Privacy",
           "name": "Privacy Excellence",
           .
           .
           .
       },
       {
           "id": "company_Security",
           "name": "Security",
           .
           .
           .
       }
    ]
```

## 問題部分

本節定義與支柱相關聯的問題。

您可以在自訂鏡頭的支柱中定義多達 20 個問題。

- id：問題的識別碼。ID 可以是 3 到 128 個字元，且僅包含英數字元和底線 (「_」) 字元。問題中使用的 ID 必須是唯一的。

- `title`：問題的標題。標題最多可以有 128 個字元。
- `description`：更詳細地描述問題。說明最多可有 2048 個字元。
- `helpfulResource displayText`：選用。提供有關問題的實用資訊的文字。文字最多可以有 2048 個字元。如果已指定，`helpfulResource url`則必須指定。
- `helpfulResource url`：選用。更詳細地解釋問題的 URL 資源。網址必須以`http://`或開頭`https://`。

> **Note**
>
> 將自訂鏡頭工作負載同步至 Jira 時，問題會同時顯示問題的「id」和「標題」。吉拉門票中使用的格式是`[ QuestionID ] QuestionTitle`。

```
"questions": [
    {
        "id": "privacy01",
        "title": "How do you ensure HR conversations are private?",
        "description": "Career and benefits discussions should occur on secure channels
 only and be audited regularly for compliance.",
        "helpfulResource": {
            "displayText": "This is helpful text for the first question",
            "url": "https://example.com/poptquest01_help.html"
        },
        .
        .
        .
    },
    {
        "id": "privacy02",
        "title": "Is your team following the company privacy policy?",
        "description": "Our company requires customers to opt-in to data use and does
 not disclose customer data to third parties either individually or in aggregate.",
        "helpfulResource": {
            "displayText": "This is helpful text for the second question",
            "url": "https://example.com/poptquest02_help.html"
        },
        .
        .
        .
    }
```

```
]
```

## 選擇區段

本節定義與問題相關聯的選項。

您可以為自訂鏡頭中的問題定義多達 15 個選項。

- `id`：選擇的識別碼。ID 可以介於 3 到 128 個字元之間，且僅包含英數字元和底線 (「_」) 字元。必須為問題中的每個選項指定唯一的 ID。添加帶有後綴的選擇_no將作為問題的None of these選擇。
- `title`：選擇的標題。標題最多可以有 128 個字元。
- `helpfulResource displayText`：選用。提供有關選擇的實用資訊的文字。文字最多可以有 2048 個字元。如果已指定，則helpfulResource url必須包含在內。
- `helpfulResource url`：選用。更詳細地解釋選擇的 URL 資源。網址必須以http://或開頭https://。
- `improvementPlan displayText`：說明如何改善選擇的文字。文字最多可以有 2048 個字元。每個選擇都需要一個，None of these選擇除外。improvementPlan
- `improvementPlan url`：選用。可以幫助改進的 URL 資源。網址必須以http://或開頭https://。
- `additionalResources type`：選用。其他資源的類型。值可以是HELPFUL_RESOURCE或IMPROVEMENT_PLAN。
- `additionalResources content`：選用。指定displayText其他資源的和url值。最多可以指定五個額外的實用資源以及最多五個額外的改善計劃項目供您選擇。
  - `displayText`：選用。說明實用資源或改善計劃的文字。文字最多可以有 2048 個字元。如果已指定，則url必須包含在內。
  - `url`：選用。有用資源或改進計劃的 URL 資源。網址必須以http://或開頭https://。

> **Note**
>
> 將自訂鏡頭工作負載同步至 Jira 時，選項會顯示問題和選擇的「id」，以及選擇的「標題」。使用的格式為[ QuestionID | ChoiceID ] ChoiceTitle。

```
    "choices": [
```

```
        {
            "id": "choice_1",
            "title": "Option 1",
            "helpfulResource": {
                "displayText": "This is helpful text for the first choice",
                "url": "https://example.com/popt01_help.html"
            },
            "improvementPlan": {
                "displayText": "This is text that will be shown for improvement of
this choice.",
                "url": "https://example.com/popt01_iplan.html"
            }
        },
        {
            "id": "choice_2",
            "title": "Option 2",
            "helpfulResource": {
                "displayText": "This is helpful text for the second choice",
                "url": "https://example.com/hr_manual_CORP_1.pdf"
            },
            "improvementPlan": {
                "displayText": "This is text that will be shown for improvement of
this choice.",
                "url": "https://example.com/popt02_iplan_01.html"
            },
            "additionalResources":[
               {
                 "type": "HELPFUL_RESOURCE",
                 "content": [
                   {
                     "displayText": "This is the second set of helpful text for this
choice.",
                     "url": "https://example.com/hr_manual_country.html"
                   },
                   {
                     "displayText": "This is the third set of helpful text for this
choice.",
                     "url": "https://example.com/hr_manual_city.html"
                   }
                 ]
               },
               {
                 "type": "IMPROVEMENT_PLAN",
                 "content": [
```

```
                    {
                      "displayText": "This is additional text that will be shown for
improvement of this choice.",
                      "url": "https://example.com/popt02_iplan_02.html"
                    },
                    {
                      "displayText": "This is the third piece of improvement plan
text.",
                      "url": "https://example.com/popt02_iplan_03.html"
                    }
                    {
                      "displayText": "This is the fourth piece of improvement plan
text.",
                      "url": "https://example.com/popt02_iplan_04.html"
                    }
                  ]
                }
              ]
        },
        {
              "id": "option_no",
              "title": "None of these",
              "helpfulResource": {
                "displayText": "Choose this if your workload does not follow these best
practices.",
                "url": "https://example.com/popt02_iplan_none.html"
              }

            }
```

## 風險規則段落

本節定義選取的選擇如何決定風險層級。

您最多可以為每個問題定義三個風險規則，每個風險層級各一個風險規則。

- condition：對應至問題風險層級的選項的布林運算式，或default。

  每個問題都必須有default風險規則。
- risk：表示與條件相關聯的風險。有效值為 HIGH_RISK、MEDIUM_RISK 和 NO_RISK。

風險規則的順序很重要。第一condition個評估true設定問題風險的項目。實施風險規則的常見模式是從風險最小（通常是最細微的）規則開始，然後按照最具風險（和最不具體的）規則進行操作。

例如：

```
"riskRules": [
      {
        "condition": "choice_1 && choice_2 && choice_3",
        "risk": "NO_RISK"
      },
      {
        "condition": "((choice_1 || choice_2) && choice_3) || (!choice_1 &&
choice_3)",
        "risk": "MEDIUM_RISK"
      },
      {
        "condition": "default",
        "risk": "HIGH_RISK"
      }
]
```

如果問題有三個選項 (choice_1choice_2、和choice_3)，這些風險規則會產生下列行為：

- 如果選取所有三個選項，則沒有風險。
- 如果已選取choice_1或choice_2且choice_3已選取，則存在中等風險。
- 如果choice_1未選取但choice_3已選取，則也存在中度風險。
- 如果這些先前條件都不成立，則存在高風險。

# 鏡頭升級

隨著新服務推出、改 AWS 善雲端系統的現有最佳實務，以及加入新的最佳實務，也會隨之更新所 AWS 提供的 Well-Architected 架構鏡頭和其他鏡頭。當鏡頭推出新版本時， AWS WA Tool 會升級以反映最新的最佳實踐。任何已定義的新工作負載都會使用新版鏡頭。

當您套用至工作負載或檢閱範本的自訂鏡頭已發佈新的主要版本時，鏡頭升級也會發生。

鏡頭升級可包含以下任何組合：

- 增加新的問題或最佳實務

- 移除不再建議使用的舊問題或實務
- 更新現有問題或最佳實務
- 新增或移除支柱

系統會保留您對現有問題的答案。

> **Note**
>
> 您無法復原鏡頭升級。將工作負載升級到最新的鏡頭版本後，您將無法返回到先前版本的鏡頭。

## 選擇鏡頭升級

「通知」頁面會顯示未使用最新鏡頭版本之每個工作負載的資訊。

每個工作負載都會顯示下列資訊：

資源

工作負載或複查樣板的名稱。

資源類型

資源的類型。這可以是「工作負載」或「複查」範本。

關聯資源

鏡頭的名稱。

通知類型

升級通知的類型。

- Not current (非最新) - 工作負載使用的鏡頭版本已經不是最新的版本。請升級到最新的鏡頭版本以獲得更好的指導。
- 已取代 — 工作負載使用的鏡頭版本不再反映最佳作法。請升級到最新的鏡頭版本。
- 已刪除 — 工作負載正在使用已由其擁有者刪除的鏡頭。

使用中的版本

目前用於工作負載的鏡頭版本。

最新的可用版本

可升級的鏡頭版本；如果已刪除鏡頭，則為 None。

若要升級與工作負載相關的鏡頭，請選取工作負載並選擇 Upgrade lens version (升級鏡頭版本)。

## 升級鏡頭

鏡頭可針對工作負載進行升級，並檢閱範本。

> **Note**
>
> 您無法復原鏡頭升級。將工作負載或檢閱範本升級至最新的鏡頭版本後，您就無法返回鏡頭的先前版本。

為工作負載升級鏡頭

1. 在「通知」頁面上，選取要升級的工作負載，然後選擇升級鏡頭版本。顯示有關每個支柱中變更內容的資訊。

   > **Note**
   >
   > 您也可以從工作負載概觀索引標籤中選擇檢視可用的升級。

2. 在為工作負載升級鏡頭之前，會建立里程碑以儲存現有工作負載的狀態，以供 future 參考。在里程碑名稱欄位中輸入里程碑的唯一名稱。
3. 選取 [我瞭解並接受這些變更] 旁邊的 [確認] 方塊，然後選擇 [儲存]。

鏡頭升級後，您可以從「里程碑」標籤檢視鏡頭的先前版本。

升級檢閱範本的鏡頭

1. 若要升級檢閱範本的鏡頭，請選擇
2. 在「通知」頁面上，選取要升級的檢閱範本，然後選擇「升級鏡頭版本」。顯示有關每個支柱中變更內容的資訊。

> **Note**
>
> 您也可以從檢閱範本 [概觀] 索引標籤中選擇 [檢視可用升級]。

3. 選取 [我瞭解並接受這些變更] 旁邊的 [確認] 方塊，然後選擇 [升級並編輯範本答案] 來調整檢閱範本的最佳實務問題的答案，或 [升級] 以升級鏡頭而不調整範本答案。

## 鏡頭目錄

Lens Catalog 是一系列官方 AWS製作的鏡頭，提供 up-to-date 技術和專注於業界的最佳實踐方式。AWS WA Tool 這些鏡頭適用於所有用戶，不需要任何額外的安裝即可使用。

下表說明鏡頭目錄中目前提供的所有 AWS 官方鏡頭。

| 名稱 | 描述 |
| --- | --- |
| AWS Well-Architected 的框架 | 依預設套用至所有工作負載。收集在雲端中設計和操作可靠、安全、高效、符合成本效益且可持續發展系統的架構最佳實務。 |
| 連線行動 | 將技術集成到運輸系統中並提高整體出行體驗的最佳實踐。 |
| 容器構建 | 提供容器設計和建置程序的最佳作法。 |
| 數據分析 | 包含從實際案例研究中收集到的見解，並協助您瞭解 Well-Architected 分析工作負載的關鍵設計元素，以及改進建議。 AWS |
| DevOps | 描述各種規模的組織都可以遵循的結構化方法，以培養高速、以安全為中心的文化，能夠使用現代技術和 DevOps 最佳實務來提供可觀的商業價值。 |
| 政府 | 在上設計和提供政府服務的最佳實踐 AWS。 |
| 醫療產業 | 如何在. 中設計、部署和管理醫療保健工作負載的最佳實務和指導 AWS 雲端。 |

| 名稱 | 描述 |
| --- | --- |
| IoT | 在中管理物聯網 (IoT) 工作負載的最佳做 AWS 法 |
| 併購價值創造 | 在尋找促進公司成長的方法（例如私募股權合併和收購活動）時，提供了一系列額外的問題需要考慮。 |
| 機器學習 | 在中管理 Machine Learning 資源和工作負載的最佳做 AWS法 |
| 遷移 | 如何移轉至 AWS 雲端. |
| SaaS | 專注於設計、部署和架構您的軟體即服務 (SaaS) 工作負載。 AWS 雲端 |
| SAP | 中 SAP 工作負載的 AWS 雲端設計原則和最佳做法 |
| 無伺服器應用 | 在 AWS上建置無伺服器工作負載的最佳做法。涵蓋諸如 RESTful 微服務、行動應用程式後端、串流處理和 Web 應用程式等案例。 |

# 評論範本

您可以在中建立檢閱範本，其中包AWS WA Tool含 Well-Architected 的架構和自訂鏡頭最佳實務問題的預先填寫答案。Well-Architected 的審核範本可減少在執行 Well-Architected 審核時，手動填寫多個工作負載常見的最佳實務相同答案的需求，並協助推動跨團隊和工作負載最佳實務的一致性和標準化。

您可以建立檢閱範本來回答常見的最佳實務問題，或建立備註，這些備註可與其他 IAM 使用者或帳戶，或同一個組織或組織單位共用AWS 區域。您可以從檢閱範本定義工作負載，這有助於擴展常見的最佳做法並減少工作負載的冗餘。

## 建立檢閱範本

建立檢閱範本的步驟

1. 在左側導覽窗格中選取 [檢閱範本]。
2. 選擇 Create template (建立範本)。
3. 在 [指定範本詳細資料] 頁面上，提供檢閱範本的 [名稱] 和 [說明]。
4. (選擇性) 在「範本附註」和「標籤」區段中，新增任何您要與審核範本關聯的範本備註或標籤。所有新增的備註都會套用至使用檢閱範本的所有工作負載，而標記則專用於檢閱範本。

   如需標籤的詳細資訊，請參閱標記您的 AWS WA Tool 資源。
5. 選擇 下一步。
6. 在 [套用鏡頭] 頁面上，選取您要套用至檢閱範本的鏡頭。可以使用的鏡頭數量上限為 20 個。

   鏡頭可從客製鏡頭、鏡頭目錄或兩者中選擇。

   > **Note**
   >
   > 與您共用的鏡頭無法套用至檢閱範本。
7. 選擇 Create template (建立範本)。

若要開始回答您剛建立的檢閱範本的問題

1. 在範本概觀索引標籤的 [開始回答問題資訊] 警示中，選取 [回答問題] 下拉式清單中的鏡頭。

> **Note**
>
> 您也可以轉到「鏡頭」部分，選擇鏡頭，然後選擇「回答問題」。

2. 對於您套用至檢閱範本的每個鏡頭，請回答適用的問題，然後在完成後選擇 [儲存] 並離開。

建立檢閱範本後，您可以從中定義新的工作負載。

檢閱範本的 [概覽] 索引標籤應反映 [範本詳細資料] 區段中回答的問題總數，以及 [鏡頭] 區段中每個鏡頭回答的問題。

## 編輯檢閱範本

若要編輯檢閱範本

1. 在左側導覽窗格中選取 [檢閱範本]。
2. 選取您要編輯的檢閱範本名稱。
3. 若要更新檢閱範本的「名稱」、「說明」或「範本」附註，請在「概觀」標籤的「範本詳細資料」區段中選擇「編輯」。
   a. 對「名稱」、「描述」或「範本」備註進行變更。
   b. 選擇「儲存範本」以根據您的變更更新檢閱範本。
4. 若要更新要套用至檢閱範本的鏡頭，請在「概覽」標籤的「鏡頭」區段中，選擇「編輯套用的鏡頭」。
   a. 選取或取消選取您要新增或移除的鏡頭核取方塊。

      您可以從自訂鏡頭、鏡頭目錄或兩者中選擇或取消選擇鏡頭。
   b. 選擇「儲存範本」以儲存變更。
5. 若要更新鏡頭上最佳實務問題的答案，請在「概觀」標籤的「鏡頭」區段中選取鏡頭名稱。
   a. 在「鏡頭概覽」區段中，選擇「回答問題」。

      > **Note**
      >
      > 或者，您可以在左側導覽窗格的 [檢閱範本] 下拉式清單中選取鏡頭名稱，以前往 [鏡頭概述] 區段。

   b. 選取或取消選取您要變更的最佳作法答案旁邊的核取方塊。

c. 選擇 [儲存並結束] 以儲存變更。

## 共用檢閱範本

審核範本可與使用者或帳戶共用，也可以與整個組織或組織單位共用審核範本。

若要共用檢閱範本

1. 在左側導覽窗格中選取 [檢閱範本]。
2. 選取您要共用的審核範本名稱。
3. 選擇 [共用] 索引標籤。
4. 若要共用至使用者或帳戶，請選擇 [建立]，然後選取 [與 IAM 使用者或帳戶共用]。在「傳送邀請」方塊中，指定使用者或帳戶 ID，然後選擇「建立」。
5. 若要共用至組織或組織單位，請選擇 [建立]，然後選取 [與組 Organizations 共用]。若要共用至整個組織，請選取 [授與權限給整個組織]。若要與組織單位共用，請選取 [授與個別組織單位的權限]，在方塊中指定組織單位，然後選擇 [建立]。

> **Important**
>
> 與組織或組織單位 (OU) 共用設定檔之前，您必須先啟用AWS Organizations存取權。

## 從範本定義工作負載

您可以從您建立的檢閱範本或已與您共用的檢閱範本定義工作負載。您無法從已刪除的檢閱範本中定義新的工作負載，如果檢閱範本包含鏡頭的過期版本，則必須先升級檢閱範本，然後才能從該範本定義新的工作負載。如需有關如何升級檢閱範本的資訊，請參閱the section called “升級鏡頭”。

> **Note**
>
> 若要從檢閱範本定義工作負載，您必須具有 IAM 許可才能建立工作負載啟用：`wellarchitected:CreateWorkload`，以及下列檢閱範本權限：`wellarchitected:GetReviewTemplatewellarchitected:GetReviewTemplateAnswerw`和`wellarchitected:GetReviewTemplateLensReview`。如需 IAM 許可的詳細資訊，請參閱 AWSIdentity and Access Management 使用者指南。

若要從檢閱樣板定義工作負載

1. 在左側導覽窗格中選取 [檢閱範本]。
2. 選取您要從中定義工作負載的複查樣板名稱。
3. 選擇從範本定義工作負載。

> **Note**
>
> 您也可以從「工作負載」頁面的「定義工作負載」下拉式清單選擇「從檢閱範本定義

4. 在 [選取檢閱範本] 步驟中，選取檢閱範本卡片，然後選擇 [下一步]。
5. 在「指定特性」 步驟中，填寫工作負載屬性的必要欄位，然後選擇下一步。如需詳細資訊，請參閱the section called “定義工作負載”。
6. (選擇性) 在「套用設定檔」步驟中，選取現有的設定檔、搜尋設定檔名稱或選擇建立設定檔來建立設定檔，將設定檔與工作負載產生關聯。選擇 下一步。

   Well-Architected 的設定檔和審閱範本可以同時使用。在檢閱範本中預先填入的問題仍會在工作負載中得到解答，而問題會根據您的設定檔排定優先順序。
7. (選擇性) 在「套用鏡頭」步驟中，您可以選擇套用尚未套用至檢閱範本的自訂鏡頭或鏡頭目錄中的其他鏡頭。
8. 選擇 Define workload (定義工作負載)。

# 刪除檢閱範本

若要刪除檢閱範本

1. 在左側導覽窗格中選取 [檢閱範本]。
2. 在 [檢閱範本] 區段中，選擇您要刪除的檢閱範本，然後在 [動作] 下拉式清單中選取 [刪除]。

> **Note**
>
> 您也可以選取範本的名稱，然後從「檢閱範本概述」標籤中選擇「刪除」。

3. 在「刪除檢閱樣板」對話方塊中，於欄位中輸入要確認刪除的檢閱樣板名稱。
4. 選擇 刪除。

您無法從已刪除的檢閱樣板建立新工作負載。如果您已與其他 IAM 使用者、帳戶或組織共用已刪除的檢閱範本，則他們將無法從該範本建立工作負載。

# 描述檔

您可以建立設定檔來提供您的業務內容，並在執行「架構良好」審核時識別您想要達成的目標。 AWS Well-Architected Tool使用從您的設定檔收集到的資訊，協助您專注於在工作負載檢閱期間與您的業務相關的問題排列優先順序清單。將設定檔附加至您的工作負載也可協助您瞭解哪些風險優先順序，以便根據您的改善計畫來解決。

您可以從「設定檔」頁面建立設定檔並將其與新工作負載建立關聯，或者將設定檔新增至現有的工作負載。

## 建立 設定檔

建立設定檔

1. 在左側導覽窗格中選取 [設定檔]。
2. 選擇 Create profile (建立設定檔)。
3. 在「設定檔屬性」區段中，為您的設定檔提供「名稱」和「說明」。
4. 若要在工作負載檢閱和改善計畫中針對您的業務優先順序排定的資訊，請在「設定檔問題」區段中選取與您業務最相關的答案。
5. (選擇性) 在「標籤」區段中，新增任何您要與描述檔建立關聯的標籤。

   如需標籤的詳細資訊，請參閱標記您的 AWS WA Tool 資源。
6. 選擇 儲存 。成功建立設定檔時，會出現成功訊息。

建立設定檔時，會顯示設定檔概觀。概述顯示與配置文件相關的數據，包括名稱，描述，ARN，創建和更新日期以及配置文件問題的答案。在個人檔案總覽頁面中，您可以編輯、刪除或分享您的個人檔案。

## 編輯設定檔

編輯設定檔

1. 在左側導覽窗格中選取「設定檔」，或從工作負載的「設定檔」區段中選擇「檢視設定檔」。
2. 選取您要更新的設定檔名稱。
3. 在「設定檔概觀」頁面選擇 「編輯」。

4. 對個人資料問題進行任何必要的更新。
5. 選擇 儲存 。

# 分享個人檔案

設定檔可以與使用者或帳戶共用，也可以與整個組織或組織單位共用設定檔。

若要共用設定檔

1. 在左側導覽窗格中選取 [設定檔]。
2. 選取您要共用的設定檔名稱。
3. 選擇 [共用] 索引標籤。
4. 若要共用至使用者或帳戶，請選擇 [建立]，然後選取 [建立共用給 IAM 使用者或帳戶]。在「傳送邀請」方塊中，指定使用者或帳戶 ID，然後選擇「建立」。
5. 若要共用至組織或組織單位，請選擇 [建立]，然後選取 [建立共用給組織]。若要共用至整個組織，請選取 [授與權限給整個組織]。若要與組織單位共用，請選取 [授與個別組織單位的權限]，在方塊中指定組織單位，然後選擇 [建立]。

> **Important**
>
> 與組織或組織單位 (OU) 共用設定檔之前，您必須先啟用AWS Organizations存取權。

# 將設定檔新增至工作負載

您可以將設定檔新增至現有的工作負載，或在定義工作負載時，加速工作負載檢閱程序。 AWS WA Tool使用從您的設定檔收集到的資訊，在工作負載檢閱中與您的業務相關的問題排定優先順序。

如需在定義工作負載時新增設定檔的詳細資訊，請參閱the section called “定義工作負載”。

將設定檔新增至現有工作負載

1. 在左側導覽窗格中選取「工作負載」，然後選取要與設定檔建立關聯的工作負載名稱。

> **Note**
>
> 一個工作負載只能關聯一個設定檔。

2. 在「設定檔」區段中，選擇「新增設定檔」
3. 從可用設定檔清單中選取要套用至工作負載的設定檔，或選擇「建立設定檔」。如需詳細資訊，請參閱the section called “建立 設定檔”。
4. 選擇 Save (儲存)。

工作負載概觀會根據關聯設定檔中的資訊，顯示已回答的優先順序問題和已排定優先順序的風險計數。選擇繼續檢閱以解決工作負載檢閱中排定優先順序的問題。如需詳細資訊，請參閱the section called “記錄工作負載”。

「設定檔」段落會顯示與工作負載關聯之設定檔的名稱、說明、ARN、版本和上次更新日期。

## 從工作負載移除設定檔

從工作負載中移除設定檔會將工作負載還原為設定檔關聯之前的版本，而且工作負載檢閱問題和風險不再具有優先順序。

若要從工作負載中移除設定檔

1. 在工作負載的「設定檔」區段中，選擇「移除」。
2. 若要確認移除，請在文字輸入欄位中輸入描述檔的名稱。
3. 選擇 Remove (移除)。

顯示已成功從工作負載移除設定檔的通知。移除設定檔會將工作負載還原為設定檔關聯之前的版本，而且工作負載檢閱問題和風險不再具有優先順序。

## 從中刪除設定檔 AWS WA Tool

如果您已建立設定檔，您可以從中的可用設定檔清單中刪除該設定檔AWS WA Tool。

從「設定檔」頁面刪除設定檔並不會從任何關聯的工作負載中移除該設定檔。您可以在刪除之前繼續使用已共用且與工作負載相關聯的設定檔，但是，沒有新的工作負載可以與已刪除的設定檔相關聯。 the section called “設定檔通知”使用刪除的設定檔傳送給工作負載擁有者。

**免責聲明**

透過與其他人分享您的個人檔案AWS 帳戶，即表示您確認AWS會將您的個人資料提供給這些其他帳戶。這些其他帳戶可能會繼續存取和使用您的共用設定檔，即使您從自己的設定檔刪除AWS 帳戶或終止您的設定檔AWS 帳戶。

若要從設定檔清單中移除設定檔

1. 在左側導覽窗格中選取 [設定檔]。
2. 選取您要移除的設定檔名稱。
3. 選擇 刪除 。
4. 若要確認移除，請在文字輸入欄位中輸入設定檔名稱。
5. 選擇 刪除 。

如果要將設定檔保留在「設定檔」清單中，但要將其從工作負載中移除，請參閱the section called “從工作負載移除設定檔”。

# AWS Well-Architected Tool 連接器用於吉拉

您可以使用 Jira AWS Well-Architected Tool 連接器將您的 Jira 帳戶 AWS Well-Architected Tool 與工作負載中的改進項目同步到 Jira 專案，以協助您建立實作改進的封閉迴圈機制。

連接器同時提供自動和手動同步。如需詳細資訊，請參閱設定連接器。

連接器可在帳戶層級和工作負載層級進行設定，並可選擇覆寫每個工作負載的帳戶層級設定。在工作負載層級上，您也可以選擇將工作負載排除在完全同步之外。

您可以選擇將改善項目同步至預設 WA Jira 專案，或指定要同步到的現有專案金鑰。在工作負載層級，您可以視需要將每個工作負載同步至唯一的 Jira 專案。

> **Note**
>
> 連接器僅支援 Jira 中的 scrum 和看板專案。

當改善項目同步到 Jira 時，它們的組織方式如下：

- 專案：WA (或您指定的現有專案)
- 史詩：工作負載
- 任務：問題
- 子任務：最佳實踐
- 標籤:支柱

在「設定」頁面中設定 Jira 帳戶同步後，您可以設定 Jira 連接器並將改善項目同步到您的 J ira 帳戶。

## 設定連接器

安裝連接器

> **Note**
>
> 以下所有步驟都在您的 Jira 帳戶中執行，而不是在您 AWS 帳戶的。

1. 登入您的 Jira 帳戶。
2. 在頂端導覽列中，選擇「應用程式」，然後選取「探索更多 App」。
3. 在「探索 Jira 的應用程式和整合」頁面中，輸入 AWS Well-Architected。然後，選擇 Jira 的AWS Well-Architected Tool 連接器。
4. 在應用程式頁面中，選擇取得應用程式。
5. 在「新增至 Jira」窗格中，選擇「立即取得」。
6. 安裝應用程式後，若要完成設定，請選擇 [設定]。
7. 在「AWS Well-Architected Tool 組態」頁面中，選擇「Connect 新的」 AWS 帳戶。
8. 輸入您的 AccessKeyID 和密鑰。選用性：輸入您的工作階段權杖。然後，選擇「Connect」。

> **Note**
>
> 確保您的帳戶具有權限`wellarchitected:ConfigureIntegration`。需要此權限才能添加 AWS 帳戶 到 Jira。
> 多個 AWS 帳戶 可以連接到 AWS WA Tool。

> **Note**
>
> 作為安全性最佳實務，強烈建議您使用短期 IAM 登入資料。如需為您建立 AccessKeyID 和私密金鑰的詳細資訊 AWS 帳戶，請參閱管理存取金鑰 (主控台)，如需使用短期認證的詳細資訊，請參閱要求臨時登入資料。

9. 針對「區域」，選取 AWS 區域 您要連線的。然後，選擇「Connect」。

### 吉拉項目設置

使用自訂專案時，請確定您的專案設定中有下列問題類型：

- Scrum：史詩，故事，子任務
- 看板：史詩，任務，子任務

如需管理問題類型的詳細資訊，請參閱自助 Support | 新增、編輯和刪除問題類型。

檢查中連接器狀態的步驟 AWS Well-Architected Tool

1. 登錄到您的 AWS 帳戶 並導航到 AWS Well-Architected Tool。
2. 在左側導覽窗格中選取 [設定]。
3. 在 Jira 帳戶同步部分的 Jira 應用程序連接狀態下，檢查已配置狀態。

連接器現在已設定並準備好進行設定。若要在帳戶和工作負載層級設定 Jira 同步設定，請參閱設定連接器。

# 設定 連接器

使用 Jira 的 AWS Well-Architected Tool 連接器，您可以在帳戶層級、工作負載層級或兩者設定 Jira 同步。您可以設定與帳戶層級設定無關的工作負載層級 Jira 設定，或覆寫特定工作負載上的帳戶層級設定，以指定工作負載的同步行為。您也可以在定義工作負載時設定 Jira 設定。

連接器提供兩種同步方法：自動和手動同步。在這兩種同步方法中，在中所做的更改 AWS WA Tool 都會反映在您的 Jira 項目中，並且在 Jira 中所做的更改會同步回到。 AWS WA Tool

> **Important**
>
> 使用自動同步，即表示您同意 AWS WA Tool 修改工作負載以回應 Jira 中的變更。
> 如果您有不想同步到 Jira 的敏感資訊，請勿將此資訊輸入工作負載的「備註」欄位中。

- 自動同步：每次更新問題時，連接器都會自動更新您的 Jira 專案和工作負載，包括選取或取消選取最佳做法以及完成問題。
- 手動同步:當您想要在 Jira 和 Jira 之間同步改進項目時，必須在工作負載儀表板中選擇「與 Jira 同步」。 AWS WA Tool您也可以選擇要同步的特定支柱和問題。如需詳細資訊，請參閱同步工作負載。

在帳戶層級設定連接器

1. 在左側導覽窗格中選取 [設定]。
2. 在「Jira 帳戶同步」窗格中，選擇「編輯」。
3. 針對同步類型，選取下列其中一項：

   a. 若要在進行變更時自動同步工作負載，請選取「自動」。

b. 若要手動選擇同步工作負載的時間，請選取手動。

4. 依預設，連接器會建立 WA Jira 專案。要指定您自己的 Jira 項目密鑰，請執行以下操作：

   a. 選取「取代預設的 Jira 專案金鑰」。

   b. 輸入您的 Jira 專案金鑰。

   > **Note**
   >
   > 除非您在工作負載層級變更專案，否則所有工作負載都會使用指定的 Jira 專案金鑰。

5. 選擇儲存設定。

在工作負載層級設定連接器

1. 在左側導覽窗格中選取「工作負載」，然後選取要設定的工作負載名稱。
2. 選擇 Properties (屬性)。
3. 在「Jira」窗格中，選擇「編輯」。
4. 若要設定工作負載的 Jira 設定，請選取覆寫帳戶層級設定。

   > **Note**
   >
   > 必須選取覆寫帳戶層級設定，才能套用特定於工作負載的設定。

5. 針對同步覆寫，選取下列其中一項：

   a. 若要從 Jira 同步中排除工作負載，請選取不同步工作負載。

   b. 若要手動選擇同步工作負載的時間，請選取同步工作負載-手動。

   c. 要自動同步工作負載變更，請選取同步工作負載-自動。

6. (選擇性) 對於 Jira 專案金鑰，請輸入要將工作負載同步至的專案金鑰。此專案金鑰可以與您的帳戶層級專案金鑰不同。

   如果您未指定專案金鑰，連接器會建立 WA Jira 專案。

7. 選擇儲存。

如需有關執行手動同步的詳細資訊，請參閱同步工作負載。

# 同步工作負載

對於自動同步，當您更新工作負載時 (例如，當您完成問題或選取新的最佳做法時)，連接器會自動同步改善項目。

在手動同步和自動同步中，在 Jira 中所做的任何更改（例如完成問題或最佳實踐）都會同步回到 AWS Well-Architected Tool。

手動同步工作負載

1. 準備好將工作負載同步到 Jira 時，請在左側導覽窗格中選取「工作負載」。然後，選取要同步的工作負載。
2. 在工作負載概觀中，選擇「與 Jira 同步」。
3. 選擇您要同步的鏡頭。
4. 對於要同步到 Jira 的問題，請選擇要同步到 Jira 項目的問題或整個支柱。
    - 若要移除任何問題，請選取問題標題旁邊的 X 圖示。
5. 選擇「同步」。

# 解除安裝連接器

若要完全解除安裝 Jira 的 AWS Well-Architected Tool 連接器，請執行下列工作：

- 在覆寫帳戶層級同步設定的任何工作負載中關閉 Jira 同步
- 在帳戶級別關閉 Jira 同步
- 取消鏈接你 AWS 帳戶 在吉拉
- 從您的 Jira 帳戶解除安裝連接器

在帳戶層級關閉連接器

> **Note**
>
> 下列步驟會在您的 AWS 帳戶.

1. 在左側導覽窗格中選取 [設定]。

2. 在「Jira 帳戶同步」部分中，選擇 「編輯」。
3. 清除開啟 Jira 帳戶同步選項。
4. 選擇儲存設定。

若要取消連結 AWS 帳戶

> **Note**
> 以下所有步驟都在您的 Jira 帳戶中執行，而不是在您 AWS 帳戶的。

1. 登入您的 Jira 帳戶。
2. 在頂端導覽列中，選擇「App」，然後選取「管理您的應用程式」。
3. 選擇 Jira AWS Well-Architected Tool 連接器旁邊的下拉箭頭，然後選擇配置。
4. 在 [ AWS Well-Architected Tool 組態] 窗格中，若要取消連結 AWS 帳戶，請在 [動作] 下選擇 [X]。

解除安裝連接器

> **Note**
> 以下所有步驟都在您的 Jira 帳戶中執行，而不是在您 AWS 帳戶的。
> 建議您在解除安裝連接器之前，先確認連接器組態中所有連線 AWS 帳戶 都已解除連結。

1. 登入您的 Jira 帳戶。
2. 在頂端導覽列中，選擇「App」，然後選取「管理您的應用程式」。
3. 選擇 Jira AWS Well-Architected Tool 連接器旁邊的下拉箭頭。
4. 選擇卸載，然後選擇卸載應用程序。

# 里程碑

里程碑會記錄特定時間點的工作負載狀態。

在您初次完成與工作負載相關聯的所有問題後，請儲存里程碑。當您根據改善計劃中的項目來變更工作負載時，可以儲存額外的里程碑來衡量相關進度。

最佳實務是在每次改善工作負載時儲存里程碑。

## 保存裏程碑

里程碑會記錄工作負載目前的狀態。工作負載的擁有者可以隨時儲存里程碑。

儲存里程碑

1. 從工作負載詳細資訊頁面，選擇 Save milestone (儲存里程碑)。
2. 在 Milestone name (里程碑名稱) 方塊中，輸入您的里程碑名稱。

   > **Note**
   >
   > 名稱長度必須介於 3 到 100 個字元之間。至少三個字元不能為空格。與工作負載相關聯的里程碑名稱不能重複。當系統檢查名稱是否為唯一時，會忽略空格和大小寫。

3. 選擇 Save (儲存) 以儲存里程碑。

儲存里程碑後，您就無法變更已記錄的工作負載資料。當您刪除工作負載時，其相關里程碑也會遭到刪除。

## 查看裏程碑

您可以透過下列方式來檢視工作負載的里程碑：

- 在工作負載詳細資訊頁面上，選擇 Milestones (里程碑)，然後選擇要檢視的里程碑。
- 在 Dashboard (儀表板) 頁面上選擇工作負載，並在 Milestones (里程碑) 區段中選擇要檢視的里程碑。

# 產生裏程碑報告

您可以產生里程碑報告。這份報告會包含您對工作負載問題的回應、您的備註，以及儲存里程碑時出現的任何高風險和中等風險項目。

您可藉由該報告將里程碑詳細資訊分享給沒有權限存取 AWS Well-Architected Tool 的其他使用者。

產生里程碑報告

1. 以下列其中一種方法來選擇里程碑。
   - 在工作負載詳細資訊頁面上，選擇 Milestones (里程碑)，接著選擇該里程碑。
   - 在 Dashboard (儀表板) 頁面上，選擇要回報里程碑的工作負載。在 Milestones (里程碑) 區段中，選擇該里程碑。
2. 選擇 Generate report (產生報告) 來產生報告。

   PDF 檔案已產生，而且您可以下載或檢視。

# 分享邀請

共用邀請是要求共用另一個AWS帳戶所擁有的工作負載、自訂鏡頭或審核範本。工作負載或鏡頭可以與個人使用者或兩者AWS 帳戶中的所有使用者共用。

- 如果您接受工作負載邀請，工作負載會新增至您的「工作負載」和「儀表板」頁面。
- 如果您接受自訂鏡頭邀請卡，鏡頭就會新增至您的自訂鏡頭頁面。
- 如果您接受設定檔邀請，設定檔就會新增至您的「設定檔」頁面。
- 如果您接受審核範本邀請，該範本就會新增至您的「審核範本」頁面。

如果您拒絕邀請，邀請便會從清單中移除。

> **Note**
>
> 工作負載、自訂鏡頭、設定檔和審核範本只能在同一個範本中共用AWS 區域。

具有共用存取權的工作負載或自訂鏡頭控制的擁有者。

左側導覽列中的「共用邀請」頁面提供有關待處理的工作負載和自訂鏡頭邀請的資訊。

每個工作負載邀請都會顯示下列資訊：

名稱

要共用的工作負載、自訂鏡頭或檢閱範本的名稱。

資源類型

邀請的類型：工作負載、自訂鏡頭、設定檔或檢閱範本。

Owner

擁有工作負載的 AWS 帳戶 ID。

許可

您獲授予的工作負載許可。

- 唯讀

  提供工作負載、自訂鏡頭、設定檔或檢閱範本的唯讀存取權。

- 作者群

  提供對回答與其備註的更新存取權，以及對工作負載其他部分的唯讀存取權。此權限僅適用於工作負載。

許可詳細資訊

許可的詳細說明。

# 接受分享邀請

接受分享邀請

1. 選取要接受的共用邀請。
2. 選擇 Accept (接受)。

對於工作負載邀請，工作負載會新增至「工作負載」和「儀表板」頁面 對於自訂鏡頭邀請卡，自訂鏡頭會新增至自訂鏡頭頁面。對於設定檔邀請，設定檔會新增至「設定檔」頁面。對於審核範本邀請，範本會新增至「審核範本」頁面。

你有七天的時間接受邀請。如果您沒有在七天內接受邀請，邀請會自動過期。

如果使用者及其AWS 帳戶雙方都已接受工作負載邀請，則該使用者的工作負載邀請將決定使用者的權限。

# 拒絕共享邀請

拒絕共享邀請

1. 選取要拒絕的工作負載或自訂鏡頭邀請。
2. 選擇 Reject (拒絕)。

邀請即會從清單中移除。

# 通知

[通知] 頁面會顯示工作負載的版本差異，並檢閱具有相關聯鏡頭和描述檔的範本。您可以從「通知」頁面升級到工作負載的鏡頭或設定檔的最新版本。

## 鏡頭通知

當有新版鏡頭可用時，「工作負載」或「審核範本」頁面頂端會出現橫幅，通知您。如果您使用過時的鏡頭檢視特定工作負載或檢閱範本，您也會看到橫幅，指出有新鏡頭版本可供使用。

選擇 [檢視可用的升級] 以取得工作負載清單，或檢閱可升級的範本。

the section called “升級鏡頭”如需升級工作負載或檢閱範本鏡頭的指示，請參閱。

當共用鏡頭的擁有者刪除該鏡頭時，如果您的工作負載與刪除的鏡頭相關聯，您將會收到通知，告知您仍然可以在現有的工作負載中使用該鏡頭，但無法將其新增至新的工作負載。

## 設定檔通知

設定檔通知有兩種類型：

- 設定檔升級
- 設定檔刪除

編輯與工作負載關聯的設定檔後 (如需詳細資訊，請參閱the section called “編輯設定檔”)，設定檔通知中會顯示設定檔有新版本的通知。

當共用設定檔的擁有者刪除該設定檔時，如果您的工作負載與已刪除的設定檔相關聯，您將會收到通知，告知您仍然可以在現有工作負載中使用該設定檔，但無法將其新增至新的工作負載。

升級設定檔版本

1. 在左側導覽窗格中，選取 [通知]。
2. 從「設定檔通知」頁籤上的清單中選取工作負載的名稱，或使用搜尋列按工作負載名稱進行搜尋。
3. 選擇升級配置文件版本。
4. 在「確認」區段中，選取「我理解並接受這些變更」的確認方塊。
5. (選擇性) 如果選擇儲存里程碑，請選取儲存里程碑方塊並提供里程碑名稱。

6. 選取 Save (儲存)。

升級設定檔後，最新的版本號碼和更新日期會顯示在工作負載的「設定檔」區段中。

如需詳細資訊，請參閱「描述檔」。

# Dashboard (儀表板)

「儀表板」可從左側導覽列取得，讓您存取工作負載及其相關的中度和高風險問題。您也可以將已分享給您的再分享出去。「儀表板」由四個部分組成。

- 摘要 — 顯示所有工作負載的工作負載總數、具有中高風險的工作負載數，以及所有工作負載中高風險問題的總數。
- 每個支柱 Well-Architected 的架構問題 — 以圖形方式呈現您所有工作負載的高中風險問題。
- 每個工作負載 Well-Architected 的架構問題 — 依支柱顯示每個工作負載的中高風險問題。
- 改善計劃項目的 Well-Architected 的架構問題 — 顯示所有工作負載的改進計劃項目。

## 總結

本節顯示 Well-Architected 的框架鏡頭和所有其他鏡頭的工作負載總數，以及存在高度和中度風險問題的工作負載數量。顯示所有工作負載中的高風險問題總數，無論是由您的工作負載擁有或與您AWS 帳戶共用的工作負載。

選擇 [包含與我共用的工作負載]，可讓摘要統計資料、合併報表和其他儀表板區段反映您的工作負載和已與您共用的工作負載。

選擇「產生報告」，將合併報表建立為 PDF 檔案。

報告名稱的格式為：`wellarchitected_consolidatedreport_`*`account-ID`*`.pdf`。

## 每個支柱的 Well-Architected

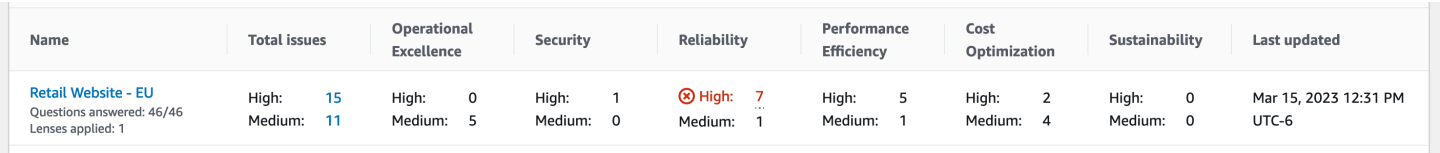
每個支柱區段中 Well-Architected 的架構問題會以圖形方式顯示所有工作負載的支柱中高風險問題數目。

使用圖標板的其餘部分可從一個詳細資料層級移至下一個詳細資料層級。

> **Note**
>
> 本節僅包含 Well-Architected 的框架鏡頭中的問題。

# 每個工作負載 Well-Architected

每個工作負載的 Well-Architected 的架構問題區段會顯示每個工作負載的資訊。




每個工作負載都會顯示下列資訊：

名稱

工作負載的名稱。還顯示了回答的問題數量以及應用於工作量的鏡頭數量。

選擇工作負載名稱以瀏覽工作負載詳細資料頁面，並檢視里程碑、改善計畫和共用。

問題總數

Well-Architected 的架構鏡頭針對工作負載識別出的問題總數。

選擇高或中風險問題的數目，以檢視這些問題的建議改善計畫。

卓越營運

在卓越營運支柱的工作負載中識別出的高風險問題 (HRI) 和中度風險問題 (MRI) 的數量。

安全性

針對安全性支柱識別的 HRI 和 MRI 的數目。

可靠性

針對可靠性支柱識別的 HRI 和 MRI 的數量。

效能效率

針對「效能效率」支柱所識別的 HRI 和 MRI 數目。

成本最佳化

針對「成本最佳化」支柱識別的 HRI 和 MRI 數目。

可持續

為可持續發展支柱確定的 HRI 和 MRI 的數目。

上次更新

上次更新工作負載的日期和時間。

對於每個工作負載，突出顯示具有最多高風險問題（HRI）數量的支柱。

> **Note**
>
> 本節僅包含 Well-Architected 的框架鏡頭中的問題。

## Well-Architected Well-l-l-Architected

依改善計劃項目排列的 Well-Architected 的架構問題區段會顯示您所有工作負載的改善計劃項目。您可以根據支柱和嚴重性過濾項目。

將列出與您共享的每個改進計劃項目的再分享出去。

改進項目

改進計劃項目的名稱。

選擇名稱，以顯示與改善計劃項目相關聯的最佳作法。

支柱

與改善項目相關聯的支柱。

Risk

指出相關問題是高風險還是中等風險。

適用工作量

套用此改善計畫的工作負載數目。

選取改善計劃項目以查看適用的工作負載。

> **Note**
>
> 本節僅包含 Well-Architected 的架構鏡頭中的改善計劃項目。

# 中的安全性 AWS Well-Architected Tool

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

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

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

本文件可協助您瞭解如何在使用時套用共同責任模型 AWS WA Tool。下列主題說明如何設定 AWS WA Tool 以符合安全性與合規性目標。您也會學到如何使用其他可協助您監控和保護 AWS WA Tool 資源的 AWS 服務。

主題

- 資料保護 AWS Well-Architected Tool
- 的身分識別與存取管理 AWS Well-Architected Tool
- 事件回應 AWS Well-Architected Tool
- 符合性驗證 AWS Well-Architected Tool
- 韌性 AWS Well-Architected Tool
- 基礎結構安全 AWS Well-Architected Tool
- 中的配置和漏洞分析 AWS Well-Architected Tool
- 預防跨服務混淆代理人

## 資料保護 AWS Well-Architected Tool

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

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

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源進行通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用設定 API 和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案以及其中的所有默認安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2 概觀。

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

## 靜態加密

儲存的所有資料都會在靜態時加密。 AWS WA Tool

## 傳輸中加密

傳送至和傳出的所有資料都會 AWS WA Tool 在傳輸過程中加密。

## 如何 AWS 使用您的資料

AWS Well-Architected 的團隊會從中收集彙總資料， AWS Well-Architected Tool 以便為客戶提供並改善 AWS WA Tool 服務。個別客戶資料可能會與 AWS 帳戶 團隊共用，以支援我們客戶改善工作負載和架構的努力。 AWS Well-Architected 的團隊只能存取每個問題的工作負載屬性和選取的選項。 AWS 不會共用 AWS WA Tool 外部的任何資料 AWS。

AWS Well-Architected 的團隊可存取的工作負載屬性包括：

- 工作負載名稱
- 檢閱擁有者

- 環境
- 區域
- 帳戶 ID
- 產業類型

AWS Well-Architected 的團隊無法存取：

- 工作負載說明
- 架構設計
- 您輸入的任何備註

# 的身分識別與存取管理 AWS Well-Architected Tool

AWS Identity and Access Management (IAM) 可協助管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM 管理員控制哪些人可以通過身份驗證 (登入) 和授權 (具有權限) 來使用 AWS WA Tool 資源。IAM 是您可以使用的 AWS 服務 ，無需額外付費。

主題



## 物件

您使用 AWS Identity and Access Management (IAM) 的方式會有所不同，具體取決於您在進行的工作 AWS WA Tool。

服務使用者 — 如果您使用 AWS WA Tool 服務執行工作，則管理員會為您提供所需的認證和權限。當您使用更多 AWS WA Tool 功能來完成工作時，您可能需要其他權限。了解存取的管理方式可協助您

向管理員請求正確的許可。若您無法存取 AWS WA Tool中的某項功能，請參閱 疑難排解 AWS Well-Architected Tool 身分和存取。

服務管理員 — 如果您負責公司的 AWS WA Tool 資源，您可能擁有完整的存取權 AWS WA Tool。決定您的服務使用者應該存取哪些 AWS WA Tool 功能和資源是您的工作。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步瞭解貴公司如何搭配使用 IAM AWS WA Tool，請參閱如何與 IAM AWS Well-Architected Tool 搭配使用。

IAM 管理員：如果您是 IAM 管理員，建議您掌握如何撰寫政策以管理 AWS WA Tool存取權的詳細資訊。若要檢視可在 IAM 中使用的 AWS WA Tool 基於身分的政策範例，請參閱。AWS Well-Architected Tool 以識別為基礎的原則範例

## 使用身分驗證

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

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

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

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

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

### AWS 帳戶 根使用者

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

## 聯合身分

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

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

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

## IAM 使用者和群組

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

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

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

## IAM 角色

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

使用暫時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱 IAM 使用者指南中的為第三方身分提供者建立角色。如果您使用 IAM Identity Center，

則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。

- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權：您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的主體) 存取您帳戶的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。若要了解跨帳戶存取角色和以資源為基礎的政策之間的差異，請參閱 IAM 使用者指南中的 IAM 中的跨帳戶資源存取。
- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉寄存取工作階段 (FAS) — 當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。
  - 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務服務。
  - 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon EC2 上執行的應用程式 — 您可以使用 IAM 角色來管理在 EC2 執行個體上執行的應用程式以及發出 AWS CLI 或 AWS API 請求的臨時登入資料。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並提供給其所有應用程式，請建立連接至執行個體的執行個體設定檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得暫時憑證。如需詳細資訊，請參閱 IAM 使用者指南中的利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式。

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

## 使用政策管理存取權

您可以透 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS ，當與身分識別或資源相關聯時，會定義其權限。 AWS 當主參與者 (使用者、root 使用者或角色

工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以 JSON 文件的形式儲存在中。如需 JSON 政策文件結構和內容的詳細資訊，請參閱 IAM 使用者指南中的 JSON 政策概觀。

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

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

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

### 身分型政策

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

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶. 受管政策包括 AWS 受管政策和客戶管理的策略。如需了解如何在受管政策及內嵌政策間選擇，請參閱 IAM 使用者指南中的在受管政策和內嵌政策間選擇。

### 資源型政策

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

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

### 存取控制清單 (ACL)

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

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

### 其他政策類型

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

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

### 多種政策類型

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

## 如何與 IAM AWS Well-Architected Tool 搭配使用

在您使用 IAM 管理存取權限之前 AWS WA Tool，請先了解哪些 IAM 功能可搭配使用 AWS WA Tool。

您可以搭配使用的 IAM 功能 AWS Well-Architected Tool

| IAM 功能 | AWS WA Tool 支持 |
| --- | --- |
| 身分型政策 | 是 |
| 資源型政策 | 否 |

| IAM 功能 | AWS WA Tool 支持 |
| --- | --- |
| 政策動作 | 是 |
| 政策資源 | 是 |
| 政策條件索引鍵 (服務特定) | 是 |
| ACL | 否 |
| ABAC (政策中的標籤) | 是 |
| 臨時憑證 | 是 |
| 主體許可 | 是 |
| 服務角色 | 否 |
| 服務連結角色 | 否 |

若要深入瞭解如何以 AWS WA Tool 及其他 AWS 服務如何使用大多數 IAM 功能，請參閱 IAM 使用者指南中的搭配 IAM 使用的AWS 服務。

## AWS WA Tool 身分型政策

| | |
| --- | --- |
| 支援政策動作 | 是 |

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

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

政策會使用動作來授予執行相關聯動作的許可。

## 以資源為基礎的政策 AWS WA Tool

| | |
|---|---|
| 支援以資源基礎的政策 | 否 |

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

如需啟用跨帳戶存取權，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，作為資源型政策的主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主體和資源位於不同時 AWS 帳戶，受信任帳戶中的 IAM 管理員也必須授與主體實體 (使用者或角色) 權限，才能存取資源。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱 IAM 使用者指南中的 IAM 中的跨帳戶資源存取。

## 的政策動作 AWS WA Tool

| | |
|---|---|
| 支援政策動作 | 是 |

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

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

政策會使用動作來授予執行相關聯動作的許可。

中的策略動作在動作之前 AWS WA Tool 使用下列前置詞：`wellarchitected:`例如，若要允許實體定義工作負載，管理員必須連接允許 `wellarchitected:CreateWorkload` 動作的政策。同樣地，若要避免實體刪除工作負載，管理員可以連接拒絕 `wellarchitected:DeleteWorkload` 動作的政策。政策陳述式必須包含 `Action` 或 `NotAction` 元素。 AWS WA Tool 會定義一組自己的動作，來描述您可以使用此服務執行的任務。

若要查看 AWS WA Tool 動作清單，請參閱服務授權參考 AWS Well-Architected Tool中的定義動作。

## 政策資源

| | |
|---|---|
| 支援政策資源 | 是 |

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

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

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

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

若要查看 AWS WA Tool 資源類型及其 ARN 的清單，請參閱服務授權參考 AWS Well-Architected Tool中所定義的資源。若要了解您可以使用哪些動作指定每個資源的 ARN，請參閱 AWS Well-Architected Tool定義的動作。

AWS WA Tool 工作負載資源具有以下 ARN：

```
arn:${Partition}:wellarchitected:${Region}:${Account}:workload/${ResourceId}
```

如需 ARN 格式的詳細資訊，請參閱 Amazon 資源名稱 (ARN) 和 AWS 服務命名空間。

您可以在 Workload properties (工作負載屬性) 頁面上找到工作負載的 ARN。例如，若要指定特定的工作負載：

```
"Resource": "arn:aws:wellarchitected:us-
west-2:123456789012:workload/11112222333344445555666677778888"
```

若要指定屬於特定帳戶的所有工作負載，請使用萬用字元 (*)：

```
"Resource": "arn:aws:wellarchitected:us-west-2:123456789012:workload/*"
```

某些 AWS WA Tool 動作 (例如用於建立和列出工作負載的動作) 無法在特定資源上執行。在這些情況下，您必須使用萬用字元 (*)。

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

若要查看 AWS WA Tool 資源類型及其 ARN 的清單，請參閱服務授權參考資料 AWS Well-Architected Tool中的定義資源。若要了解您可以使用哪些動作指定每個資源的 ARN，請參閱 AWS Well-Architected Tool定義的動作。

## 的政策條件索引鍵 AWS WA Tool

| | |
|---|---|
| 支援服務特定政策條件金鑰 | 是 |

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

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

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

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

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

AWS WA Tool 提供一個服務特定條件索引鍵 (wellarchitected:JiraProjectKey)，並支援使用某些全域條件金鑰。若要查看所有 AWS 全域條件索引鍵，請參閱服務授權參考中的AWS 全域條件內容索引鍵。

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

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

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

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

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

## ACL 在 AWS WA Tool

| | |
|---|---|
| 支援 ACL | 否 |

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

## 以 AWS WA Tool 標籤為基礎的授權

| | |
|---|---|
| 支援 ABAC (政策中的標籤) | 是 |

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

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的條件元素中，提供標籤資訊。

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

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

## 使用臨時登入資料 AWS WA Tool

| | |
|---|---|
| 支援臨時憑證 | 是 |

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

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

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

## 的跨服務主體權限 AWS WA Tool

| | |
|---|---|
| 支援轉寄存取工作階段 (FAS) | 是 |

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

## AWS WA Tool的服務角色

| | |
|---|---|
| 支援服務角色 | 否 |

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

### 服務連結角色 AWS WA Tool

| | |
|---|---|
| 支援服務連結角色。 | 否 |

服務連結角色是一種連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需建立或管理服務連結角色的詳細資訊，請參閱可搭配 IAM 運作的AWS 服務。在表格中尋找服務，其中包含服務連結角色欄中的 Yes。選擇是連結，以檢視該服務的服務連結角色文件。

## AWS Well-Architected Tool 以識別為基礎的原則範例

根據預設，使用者和角色不具備建立或修改 AWS WA Tool 資源的權限。他們也無法使用 AWS Management Console AWS CLI、或 AWS API 執行工作。IAM 管理員必須建立 IAM 政策，授予使用者和角色在指定資源上執行特定 API 操作的所需許可。管理員接著必須將這些政策連接至需要這些許可的使用者或群組。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱 IAM 使用者指南中的在 JSON 索引標籤上建立政策。

主題

- 政策最佳實務
- 使用 AWS WA Tool 主控台
- 允許使用者檢視他們自己的許可
- 授與工作負載的完整存取
- 授與工作負載的唯讀存取
- 存取單一工作負
- 針對 Jira 的 AWS Well-Architected Tool 連接器使用服務特定條件金鑰

### 政策最佳實務

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

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始將權限授與使用者和工作負載，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們可用在您的 AWS 帳戶. 建議您透過定義特定

於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。

- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需詳細資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。
- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 API 存取。

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

## 使用 AWS WA Tool 主控台

若要存取 AWS Well-Architected Tool 主控台，您必須擁有最少一組權限。這些權限必須允許您列出和檢視有關 AWS 帳戶. AWS WA Tool 如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

若要確保這些實體仍可使用 AWS WA Tool 主控台，請同時將下列 AWS 受管理的原則附加至實體：

```
WellArchitectedConsoleReadOnlyAccess
```

若要允許建立、變更和刪除工作負載，請將下列 AWS 受管政策連接到實體：

```
WellArchitectedConsoleFullAccess
```

如需詳細資訊，請參閱《IAM 使用者指南》中的新增許可到使用者。

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

## 允許使用者檢視他們自己的許可

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

## 授與工作負載的完整存取

在此範例中，您想要授與使用者 AWS 帳戶 完整存取您工作負載的權限。「完整」存取權可讓使用者在中執行所有動作 AWS WA Tool。需要具備此存取權限，才能定義工作負載、刪除工作負載、檢視工作負載和更新工作負載。

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

## 授與工作負載的唯讀存取

在此範例中，您想要授與使用者對工作負載的 AWS 帳戶 唯讀存取權限。唯讀存取權限僅允許使用者在 AWS WA Tool中檢視工作負載。

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

## 存取單一工作負

在此範例中，您想要授與使用者對us-west-2區域中其中一個工作負載的 AWS 帳戶 唯讀存取權。999999999999555555555555666666667777888899999 是您的帳戶 ID。

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

```
     "Effect" : "Allow",
     "Action" : [
          "wellarchitected:Get*",
          "wellarchitected:List*"
     ],
     "Resource": "arn:aws:wellarchitected:us-
west-2:777788889999:workload/99999999999955555555555666666666"
     }
   ]
}
```

## 針對 Jira 的 AWS Well-Architected Tool 連接器使用服務特定條件金鑰

此範例示範如何使用服務特定條件金鑰`wellarchitected:JiraProjectKey`來控制哪些 Jira 專案可以連結至您帳戶中的工作負載。

以下說明條件索引鍵的相關用法：

- **`CreateWorkload`:**套用`wellarchitected:JiraProjectKey`至時`CreateWorkload`，您可以定義哪些自訂 Jira 專案可以連結至使用者建立的任何工作負載。例如，如果使用者嘗試使用專案 ABC 建立新的工作負載，但該策略僅指定專案 PQR，則會拒絕該動作。
- **`UpdateWorkload`:**套用`wellarchitected:JiraProjectKey`至時`UpdateWorkload`，您可以定義哪些自訂 Jira 專案可以連結至此特定工作負載或任何工作負載。例如，如果使用者嘗試使用專案 ABC 更新現有工作負載，但原則指定了專案 PQR，則會拒絕該動作。此外，如果使用者的工作負載已連結至專案 PQR，並嘗試更新要連結至專案 ABC 的工作負載，則會拒絕該動作。
- **`UpdateGlobalSettings`:**當您套用`wellarchitected:JiraProjectKey`至時`UpdateGlobalSettings`，您可以定義可以將哪些自訂 Jira 專案連結 AWS 帳戶至. 帳戶層級設定可保護您帳戶中不會覆寫帳戶層級 Jira 設定的工作負載。例如，如果使用者具有存取權`UpdateGlobalSettings`，則無法將您帳戶中的工作負載連結至策略中未指定的任何專案。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": [
    "wellarchitected:UpdateGlobalSettings",
    "wellarchitected:CreateWorkload"
   ],
```

```
    "Resource": "*",
    "Condition": {
     "StringEqualsIfExists": {
      "wellarchitected:JiraProjectKey": ["ABC, PQR"]
     }
    }
   },
   {
    "Sid": "VisualEditor1",
    "Effect": "Allow",
    "Action": [
     "wellarchitected:UpdateWorkload"
    ],
    "Resource": "WORKLOAD_ARN",
    "Condition": {
     "StringEqualsIfExists": {
      "wellarchitected:JiraProjectKey": ["ABC, PQR"]
     }
    }
   }
  ]
}
```

# AWS 受管理的政策 AWS Well-Architected Tool

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

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

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

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

## AWS 受管理的策略：WellArchitectedConsoleFullAccess

您可將 `WellArchitectedConsoleFullAccess` 政策連接到 IAM 身分。

此政策授予的完整存取權限 AWS Well-Architected Tool。

**許可詳細資訊**

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

## AWS 受管理的策略：WellArchitectedConsoleReadOnlyAccess

您可將 `WellArchitectedConsoleReadOnlyAccess` 政策連接到 IAM 身分。

此原則會授與的唯讀存取權 AWS Well-Architected Tool。

**許可詳細資訊**

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

## AWS 受管理的策略：AWSWellArchitectedOrganizationsServiceRolePolicy

您可將 `AWSWellArchitectedOrganizationsServiceRolePolicy` 政策連接到 IAM 身分。

此原則會授與中 AWS Organizations 支援與 Organizations AWS Well-Architected Tool 整合所需的管理權限。這些權限允許組織管理帳號啟用資源共用 AWS WA Tool。

許可詳細資訊

此政策包含以下許可。

- organizations:ListAWSServiceAccessForOrganization-允許主參與者檢查是否已啟用 AWS 服務存取。 AWS WA Tool
- organizations:DescribeAccount— 允許主參與者擷取組織中帳號的相關資訊。
- organizations:DescribeOrganization— 允許主參與者擷取有關組織組態的資訊。
- organizations:ListAccounts— 允許主參與者擷取屬於組織的帳戶清單。
- organizations:ListAccountsForParent— 允許主參與者從組織中的指定根節點擷取屬於組織的帳號清單。
- organizations:ListChildren— 允許主參與者從組織中的指定根節點擷取屬於組織的帳戶和組織單位清單。
- organizations:ListParents— 允許主參與者擷取組織內 OU 或帳戶所指定的直接父項清單。
- organizations:ListRoots-允許主參與者擷取組織內所有根節點的清單。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListChildren",
                "organizations:ListParents",
                "organizations:ListRoots"
            ],
            "Resource": "*"
        }
    ]
}
```

## AWS 受管理的策略： AWSWellArchitectedDiscoveryServiceRolePolicy

您可將 AWSWellArchitectedDiscoveryServiceRolePolicy 政策連接到 IAM 身分。

此原則允許存 AWS Well-Architected Tool 取與資源相關的 AWS 服務和資 AWS WA Tool 源。

許可詳細資訊

此政策包含以下許可。

- trustedadvisor:DescribeChecks— 列出可用的 Trusted Advisor 檢查。
- trustedadvisor:DescribeCheckItems— 獲取 Trusted Advisor 檢查數據，包括由標記的狀態和資源。 Trusted Advisor
- servicecatalog:GetApplication— 獲取 AppRegistry 應用程序的詳細信息.
- servicecatalog:ListAssociatedResources列出與應用程式相關聯的 AppRegistry 資源。
- cloudformation:DescribeStacks取得 AWS CloudFormation 堆疊的詳細資訊。
- cloudformation:ListStackResources列出與 AWS CloudFormation 堆疊相關聯的資源。
- resource-groups:ListGroupResources列出來自的 ResourceGroup資源。
- tag:GetResources— 需要 ListGroupResources.
- servicecatalog:CreateAttributeGroup— 視需要建立服務管理的屬性群組。
- servicecatalog:AssociateAttributeGroup— 將服務管理的屬性群組與 AppRegistry 應用程式產生關聯。
- servicecatalog:UpdateAttributeGroup— 更新服務管理的屬性群組。
- servicecatalog:DisassociateAttributeGroup取消服務管理屬性群組與應用程式的關聯。 AppRegistry
- servicecatalog:DeleteAttributeGroup— 必要時刪除服務管理的屬性群組。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "trustedadvisor:DescribeChecks",
    "trustedadvisor:DescribeCheckItems"
   ],
   "Resource": [
```

```
    "*"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "cloudformation:DescribeStacks",
    "cloudformation:ListStackResources",
    "resource-groups:ListGroupResources",
    "tag:GetResources"
   ],
   "Resource": [
    "*"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "servicecatalog:ListAssociatedResources",
    "servicecatalog:GetApplication",
    "servicecatalog:CreateAttributeGroup"
   ],
   "Resource": [
    "*"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "servicecatalog:AssociateAttributeGroup",
    "servicecatalog:DisassociateAttributeGroup"
   ],
   "Resource": [
    "arn:*:servicecatalog:*:*:/applications/*",
    "arn:*:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "servicecatalog:UpdateAttributeGroup",
    "servicecatalog:DeleteAttributeGroup"
   ],
   "Resource": [
```

```
    "arn:*:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
   ]
  }
 ]
}
```

## AWS WA ToolAWS 受管理策略的更新

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

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| AWS WA Tool 已變更的受管理 | 已新增 `"wellarchitected:Export*"` 到 `WellArchitectedConsoleReadOnlyAccess` 。 | 2023 年 6 月 22 日 |
| AWS WA Tool 新增的服務角色原則 | 已新增`AWSWellArchitectedDiscoveryServiceRolePolicy` 以 AWS Well-Architected Tool 允許存取與資源相關的 AWS 服務和 AWS WA Tool 資源。 | 2023 年 5 月 3 日 |
| AWS WA Tool 添加的權限 | 已新增要授予的新動作，`ListAWSServiceAccessForOrganization` 以 AWS WA Tool 允許檢查是否已啟用 AWS 服務存取權 AWS WA Tool。 | 2022 年 7 月 22 日 |
| AWS WA Tool 開始追蹤變更 | AWS WA Tool 開始追蹤其 AWS 受管理策略的變更。 | 2022 年 7 月 22 日 |

# 疑難排解 AWS Well-Architected Tool 身分和存取

使用下列資訊可協助您診斷和修正使用和 IAM 時可能會遇到的 AWS WA Tool 常見問題。

主題

- 我沒有執行動作的授權 AWS WA Tool

### 我沒有執行動作的授權 AWS WA Tool

如果 AWS Management Console 告訴您您沒有執行動作的授權，則您必須聯絡您的管理員以尋求協助。您的管理員是為您提供簽署憑證的人員。

當 *mateojackson* 使用者嘗試使用主控台執行DeleteWorkload動作但沒有權限時，就會發生下列範例錯誤。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to
 perform: wellarchitected:DeleteWorkload on resource: 11112222333344445555666677778888
```

在此範例中，要求管理員更新您的政策，以允許您使用 wellarchitected:DeleteWorkload 動作存取 11112222333344445555666677778888 資源。

## 事件回應 AWS Well-Architected Tool

的事件回應 AWS Well-Architected Tool 是一項 AWS 責任。 AWS 有一個正式的，記錄的政策和程序來管理事件響應。

AWS 具有廣泛影響的作業問題會張貼在 AWS Service Health Dashboard 上。

系統也會透過 AWS Health Dashboard，將操作問題張貼至個別帳戶。若要取得有關如何使用的資訊 AWS Health Dashboard，請參閱《使AWS Health 用指南》。

## 符合性驗證 AWS Well-Architected Tool

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用時的合規責任取決 AWS 服務 於您資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。

- 在 Amazon Web Services 上架構 HIPAA 安全性與合規性 — 本白皮書說明公司如何使用建立符合 HIPAA 資格的應 AWS 用程式。

> **Note**
>
> 並非所有人 AWS 服務 都符合 HIPAA 資格。如需詳細資訊，請參閱 HIPAA 資格服務參照。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)) 中，保 AWS 服務 護指引並對應至安全控制的最佳實務。
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。
- Amazon GuardDuty — 透過監控環境中的 AWS 帳戶可疑和惡意活動，藉此 AWS 服務 偵測您的工作負載、容器和資料的潛在威脅。 GuardDuty 可協助您滿足特定合規性架構所要求的入侵偵測需求，例如 PCI DSS 等各種合規性需求。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化管理風險以及遵守法規和業界標準的方式。

## 韌性 AWS Well-Architected Tool

AWS 全球基礎架構是圍繞 AWS 區域 和可用區域建立的。 AWS 區域 提供多個實體分離和隔離的可用區域，這些區域透過低延遲、高輸送量和高度備援的網路連線。透過可用區域，您所設計與操作的應用程式和資料庫，就能夠在可用區域之間自動容錯移轉，而不會發生中斷。可用區域的可用性、容錯能力和擴充能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域 和可用區域的詳細資訊，請參閱AWS 全域基礎結構。

## 基礎結構安全 AWS Well-Architected Tool

作為託管服務， AWS Well-Architected Tool 受到 AWS 全球網絡安全的保護。有關 AWS 安全服務以及如何 AWS 保護基礎結構的詳細資訊，請參閱AWS 雲端安全 若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全性支柱架構良 AWS 好的架構中的基礎結構保護。

您可以使用 AWS 已發佈的 API 呼叫透 AWS WA Tool 過網路進行存取。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與 IAM 主體相關聯的私密存取金鑰來簽署。或者，您可以透過 AWS Security Token Service (AWS STS) 來產生暫時安全憑證來簽署請求。

# 中的配置和漏洞分析 AWS Well-Architected Tool

配置和 IT 控制是與您（我們的客戶） AWS 之間的共同責任。如需詳細資訊，請參閱 AWS 共用的責任模型。

# 預防跨服務混淆代理人

混淆代理人問題屬於安全性議題，其中沒有執行動作許可的實體可以強制具有更多許可的實體執行該動作。在中 AWS，跨服務模擬可能會導致混淆的副問題。在某個服務 (呼叫服務) 呼叫另一個服務 (被呼叫服務) 時，可能會發生跨服務模擬。可以操縱呼叫服務來使用其許可，以其不應有存取許可的方式對其他客戶的資源採取動作。為了預防這種情況， AWS 提供的工具可協助您保護所有服務的資料，而這些服務主體已獲得您帳戶中資源的存取權。

建議您在資源策略中使用aws:SourceArn和aws:SourceAccount全域條件前後關聯索引鍵，以限制將其他服務 AWS Well-Architected Tool 提供給資源的權限。如果您想要僅允許一個資源與跨服務存取相關聯，則請使用 aws:SourceArn。如果您想要允許該帳戶中的任何資源與跨服務使用相關聯，請使用 aws:SourceAccount。

防範混淆代理人問題的最有效方法是使用 aws:SourceArn 全域條件內容索引鍵，以及資源的完整 ARN。如果不知道資源的完整 ARN，或者如果您指定了多個資源，請使用 aws:SourceArn 全域內容條件索引鍵搭配萬用字元 (*) 來表示 ARN 的未知部分。例如 arn:aws:wellarchitected:*:*123456789012*:*。

如果 aws:SourceArn 值不包含帳戶 ID (例如 Amazon S3 儲存貯體 ARN)，您必須使用這兩個全域條件內容索引鍵來限制許可。

的值aws:SourceArn必須是工作負載或鏡頭。

下列範例顯示如何在中使用aws:SourceArn和aws:SourceAccount全域條件前後關聯鍵字 AWS WA Tool 來避免混淆的副問題。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "wellarchitected.amazonaws.com"
    },
    "Action": "wellarchitected:ActionName",
    "Resource": [
      "arn:aws:wellarchitected:::ResourceName/*"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:wellarchitected:*:123456789012:*"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

# 分享您的AWS WA Tool資源

若要共用您擁有的資源，請執行下列動作：

- 在其中啟用資源共用 AWS Organizations (選用)
- 共用工作負載
- 分享自訂鏡頭
- 分享個人檔案
- 共用檢閱範本

> **備註**
>
> - 共用資源使其可供建立資源之外的主參與者AWS 帳戶使用。共用不會變更建立該資源的帳號中套用至資源的任何權限。
> - AWS WA Tool是一項區域服務。與您共用的主參與者只能存取建立資源共用的AWS 區域資源共用。
> - 若要在 2019 年 3 月 20 日之後推出的區域中共用資源，您和共用人都AWS 帳戶必須在中啟用該地區AWS Management Console。如需詳細資訊，請參閱AWS全球基礎架構。

## 在其中啟用資源共用 AWS Organizations

當您的帳戶由管理時AWS Organizations，您可以利用它更輕鬆地共享資源。無論是否有「Organizations」，使用者都可以與個別帳戶共用。不過，如果您的帳戶位於組織中，則您可以與個別帳戶共用，或與組織或 OU 中的所有帳戶共用，而不必列舉每個帳戶。

若要共用組織內的資源，您必須先使用AWS WA Tool主控台或 AWS Command Line Interface (AWS CLI) 啟用與共用AWS Organizations。當您共用組織中的資源時，AWS WA Tool不會傳送邀請給主體。組織中的主參與者無需交換邀請即可存取共用資源。

當您在組織內啟用資源共用時，AWS WA Tool會建立名為`AWSServiceRoleForWellArchitected`的服務連結角色。此角色只能由AWS WA Tool服務擔任，並使用AWS受管理的原則AWS WA Tool授與擷取其所屬組織相關資訊的權限`AWSWellArchitectedOrganizationsServiceRolePolicy`。

如果您不再需要與整個組織或 OU 共用資源，您可以停用資源共用。

請求

- 您只能在組織的管理帳戶中以主參與者身分登入時執行這些步驟。
- 組織必須啟用所有功能。如需詳細資訊，請參閱使AWS Organizations用者指南中的啟用組織中的所有功能。

> **Important**
>
> 您必須使用AWS WA Tool主機開啟共用功能。AWS Organizations此可確保建立了 `AWSServiceRoleForWellArchitected` 服務連結角色。如果您使用AWS Organizations主控台或 enable-aws-service-accessAWS CLI命令啟用AWS Organizations受信任的存取權，則不會建立`AWSServiceRoleForWellArchitected`服務連結角色，而且您無法共用組織內的資源。

若要在組織內啟用資源共用

1. 請登入AWS Management Console並開啟AWS Well-Architected Tool主控台，網址為 https://console.aws.amazon.com/wellarchitected/。

   您必須以組織管理帳戶中的主參與者身分登入。
2. 在左側的導覽窗格中，選擇 Settings (設定)。
3. 選擇啟用AWS Organizations支援。
4. 選擇儲存設定。

若要停用組織內的資源共用

1. 請登入AWS Management Console並開啟AWS Well-Architected Tool主控台，網址為 https://console.aws.amazon.com/wellarchitected/。

   您必須以組織管理帳戶中的主參與者身分登入。
2. 在左側的導覽窗格中，選擇 Settings (設定)。
3. 取消選取「啟動AWS Organizations支援」。
4. 選擇儲存設定。

# 標記您的 AWS WA Tool 資源

為協助您管理 AWS WA Tool 資源，您可以用標籤形式將您自己的中繼資料指派給每個資源。本主題說明標籤並示範如何建立它們。

目錄



## 標籤基本概念

標籤是您指派給 AWS 資源的標籤。每個標籤皆包含由您定義的一個金鑰與一個選用值。

標籤可讓您分類 AWS 資源，例如依用途、擁有者或環境。當您有許多相同類型的資源時，您可以依據先前指派的標籤，快速識別特定的資源。例如，您可以為 AWS WA Tool 服務定義一組標籤，協助您追蹤每個服務的擁有者和堆疊層級。建議您為每個資源類型設計一組一致的標籤金鑰。

標籤不會自動指派給您的資源。新增標籤後，您可以隨時編輯標籤索引鍵和值，或從資源移除標籤。如果您刪除資源，也會刪除任何該資源的標籤。

標籤對 AWS WA Tool 來說不具有任何語意意義，並會嚴格解譯為字元字串。您可以將標籤的值設為空白字串，但您無法將標籤的值設為 Null。若您將與現有標籤具有相同鍵的標籤新增到該資源，則新值會覆寫舊值。

您可以使用 AWS Management Console、AWS CLI 和 AWS WA Tool API 來使用標籤。

如果您使用 AWS Identity and Access Management (IAM)，您可以控制哪些使用者AWS 帳戶有權建立、編輯或刪除標籤。

## 標記您的  資源

您可以標記新資源或現有AWS WA Tool資源。

如果您使用AWS WA Tool主控台，則可以在建立新資源時將標籤套用至新資源，或隨時套用至現有資源。對於現有的工作負載，您可以透過內容索引標籤套用標記 對於現有的自定義鏡頭，配置文件和評論模板，您可以通過概述標籤應用標籤。

如果您使用的是 AWS WA Tool API、AWS CLI 或 AWS 開發套件，您可以在相關 API 動作上使用 `tags` 參數，將標籤套用到新資源，或使用 `TagResource` API 動作，將標籤套用到現有的資源。如需詳細資訊，請參閱TagResource。

有些資源建立動作可讓您在建立資源時指定資源的標籤。如果無法在資源建立時套用標籤，則資源建立程序會失敗。這可確保您要在建立時標記的資源是以指定的標籤建立，不然就根本不會建立。如果您在建立時標記資源，則不需要在建立資源之後執行自訂標記指令碼。

下表說明可標記的 AWS WA Tool 資源，以及可在建立時標記的資源。

AWS WA Tool 資源的標記支援

| 資源 | 支援標籤 | 支援標籤傳播 | 支援在建立時標記 (AWS WA Tool API、AWS CLI、AWS 開發套件) |
|---|---|---|---|
| AWS WA Tool工作量 | 是 | 否 | 是 |
| AWS WA Tool訂製鏡片 | 是 | 否 | 是 |
| AWS WA Tool設定檔 | 是 | 否 | 是 |
| AWS WA Tool檢閱範本 | 是 | 否 | 是 |

# 標籤限制

以下基本限制適用於標籤：

- 每一資源最多標籤數 – 50
- 對於每一個資源，每個標籤金鑰必須是唯一的，且每個標籤金鑰只能有一個值。
- 索引鍵長度上限 - 128 個 UTF-8 Unicode 字元

- 值的長度上限 - 256 個 UTF-8 Unicode 字元
- 如果您的標記結構描述用於多個 AWS 服務和資源，請記得，其他服務可能限制允許的字元。通常允許的字元包括：可用 UTF-8 表示的英文字母、數字和空格，還有以下字元：+ - = . _ : / @。
- 標籤鍵與值皆區分大小寫。
- 請勿使用 `aws:`、`AWS:` 或其任何大小寫組合做為索引鍵或值的字首，因為這已預留給 AWS 使用。您不可編輯或刪除具此字首的標籤金鑰或值。具有此前置字元的標籤不會計入您的 tags-per-resource 限制。

# 透過主控台使用標籤

使用主AWS WA Tool控台，您可以管理與新資源或現有資源相關聯的標籤。

## 在建立個別資源時新增標籤

您可以在建立AWS WA Tool資源時將標籤新增至資源。

## 在個別資源上新增和刪除標籤

AWS WA Tool可讓您直接從工作負載的 [屬性] 索引標籤中新增或刪除與資源相關聯的標籤，以及從自訂鏡頭、設定檔和檢閱範本的概觀索引標籤中新增或刪除。

若要在工作負載上新增或刪除標記

1. 請登入AWS Management Console並開啟AWS Well-Architected Tool主控台，網址為 https://console.aws.amazon.com/wellarchitected/。
2. 在導覽列中，選擇要使用的「區域」。
3. 在導覽窗格中，選擇「工作負載」。
4. 選取要修改的工作負載，然後選擇特性。
5. 在 Tags (標籤) 區段中，選擇 Manage tags (管理標籤)。
6. 視需要新增或刪除標籤。
   - 若要新增標籤，請選擇「新增標籤」，然後填寫「關鍵字」和「值」欄位。
   - 若要刪除標籤，請選擇 Remove (移除)。
7. 針對您要新增、修改或刪除的每個標籤重複此程序。選擇 Save (儲存) 儲存變更。

在自訂鏡頭上新增或刪除標籤

1. 請登入AWS Management Console並開啟AWS Well-Architected Tool主控台，網址為 https://console.aws.amazon.com/wellarchitected/。
2. 在導覽列中，選擇要使用的「區域」。
3. 在導覽窗格中，選擇 [自訂鏡頭]。
4. 選取要修改的自訂鏡頭名稱。
5. 在「概觀」標籤的「標籤」區段中，選擇「管理標籤」。
6. 視需要新增或刪除標籤。
   - 若要新增標籤，請選擇「新增標籤」，然後填寫「關鍵字」和「值」欄位。
   - 若要刪除標籤，請選擇 Remove (移除)。
7. 針對您要新增、修改或刪除的每個標籤重複此程序。選擇 Save (儲存) 儲存變更。

在設定檔上新增或刪除標籤

1. 請登入AWS Management Console並開啟AWS Well-Architected Tool主控台，網址為 https://console.aws.amazon.com/wellarchitected/。
2. 在導覽列中，選擇要使用的「區域」。
3. 在導覽窗格中，選擇 [設定檔]。
4. 選取要修改的設定檔名稱。
5. 在「概觀」標籤的「標籤」區段中，選擇「管理標籤」。
6. 視需要新增或刪除標籤。
   - 若要新增標籤，請選擇「新增標籤」，然後填寫「關鍵字」和「值」欄位。
   - 若要刪除標籤，請選擇 Remove (移除)。
7. 針對您要新增、修改或刪除的每個標籤重複此程序。選擇 Save (儲存) 儲存變更。

若要在檢閱範本上新增或刪除標籤

1. 請登入AWS Management Console並開啟AWS Well-Architected Tool主控台，網址為 https://console.aws.amazon.com/wellarchitected/。
2. 在導覽列中，選擇要使用的「區域」。
3. 在導覽窗格中，選擇 [檢閱範本]。

4. 選取要修改的檢閱範本名稱。
5. 在「概觀」標籤的「標籤」區段中，選擇「管理標籤」。
6. 視需要新增或刪除標籤。
   - 若要新增標籤，請選擇「新增標籤」，然後填寫「關鍵字」和「值」欄位。
   - 若要刪除標籤，請選擇 Remove (移除)。
7. 針對您要新增、修改或刪除的每個標籤重複此程序。選擇 Save (儲存) 儲存變更。

# 使用 API 處理標籤

使用下列 AWS WA Tool API 作業來新增、更新、列出和刪除資源的標籤。

AWS WA Tool 資源的標記支援

| 任務 | API 動作 |
| --- | --- |
| 新增或覆寫一或多個標籤。 | TagResource |
| 刪除一或多個標籤。 | UntagResource |
| 列出資源的標籤。 | ListTagsForResource |

有些資源建立動作可讓您在建立資源時指定標籤。下列動作支援在建立時新增標籤。

| 任務 | API 動作 |
| --- | --- |
| 建立工作負載 | CreateWorkload |
| 匯入新鏡頭 | ImportLens |
| 建立 設定檔 | CreateProfile |
| 建立檢閱範本 | CreateReviewTemplate |

# 使用 AWS CloudTrail 記錄 AWS WA Tool API 呼叫

AWS Well-Architected Tool與整合AWS CloudTrail，這項服務可提供由使用者、角色或中AWS服務所採取之動作的記錄AWS WA Tool。 CloudTrail 將的所有 API 呼叫擷取AWS WA Tool為事件。擷取的呼叫包括從 AWS WA Tool 主控台進行的呼叫，以及針對 AWS WA Tool API 操作的程式碼呼叫。如果您建立追蹤，就可以將 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括的事件AWS WA Tool。即使您未設定線索，依然可以透過 CloudTrail 主控台中的 Event history (事件歷史記錄) 檢視最新事件。您可以使用收集的資訊來 CloudTrail判斷提交給和的請求AWS WA Tool、提出請求的 IP 地址、提出請求的對象、提出請求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱使AWS CloudTrail用者指南。

## AWS WA Tool中的資訊 CloudTrail

CloudTrail 當您建立帳AWS 帳戶時，系統即會在中啟用。當中發生活動時AWS WA Tool，系統便會將該活動記錄至 CloudTrail 事件歷史記錄，並將其他AWS服務事件記錄到事件中。您可以檢視、搜尋和下載 AWS 帳戶 的最新事件。如需詳細資訊，請參閱使用 CloudTrail 事件歷史記錄檢視事件。

如需您 AWS 帳戶 帳戶中正在進行事件的記錄 (包含 AWS WA Tool 的事件)，請建立追蹤。線索能 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 Amazon S3 儲存貯體。此外，您還能設的其他AWS服務，以進一步分析和處理 CloudTrail 日誌中收集的事件資料。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務與整合
- 設的 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 日誌檔案，以及從多個帳接收 CloudTrail 日誌檔案

所有AWS WA Tool動作均由記錄， CloudTrail 並記錄在定義的動作中AWS Well-Architected Tool。例如，呼叫`CreateWorkload`、`DeleteWorkload`、和`CreateWorkloadShare`動作會在 CloudTrail 記錄檔中產生項目。

每一筆事件或日誌項目都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 該請求是否使用使用者或根使用者登入資料提出。

- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 該請求是否由另一項 AWS 服務提出。

如需詳細資訊，請參閱 CloudTrail 使用者身分元素。

# 了解 AWS WA Tool 日誌檔案項目

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

以下範例顯示的是展示`CreateWorkload`動作的 CloudTrail 日誌項目。

```
   {
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:dev-dsk-xiulan-2a-1111111c.us-
west-2.amazon.com",
        "arn": "arn:aws:sts::444455556666:assumed-role/well-architected-api-svc-integ-
test-read-write/dev-dsk-xiulan-2a-1111111c.us-west-2.amazon.com",
        "accountId": "444455556666",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::444455556666:role/well-architected-api-svc-integ-
test-read-write",
                "accountId": "444455556666",
                "userName": "well-architected-api-svc-integ-test-read-write"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-10-14T03:41:39Z"
            }
        }
    },
```

```
    "eventTime": "2020-10-14T04:43:13Z",
    "eventSource": "wellarchitected.amazonaws.com",
    "eventName": "CreateWorkload",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.178",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.848
 Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.262-b10
 java/1.8.0_262 vendor/Oracle_Corporation",
    "requestParameters": {
           "ClientRequestToken": "08af866a-0238-4070-89c2-b689ca8339f7",
           "Description": "***",
           "AwsRegions": [
               "us-west-2"
           ],
           "ReviewOwner": "***",
           "Environment": "PRODUCTION",
           "Name": "***",
           "Lenses": [
               "wellarchitected",
               "serverless"
           ]
    },
    "responseElements": {
         "Arn": "arn:aws:wellarchitected:us-
west-2:444455556666:workload/8cdcdf7add10b181fdd3f686dacffdac",
         "Id": "8cdcdf7add10b181fdd3f686dacffdac"
    },
    "requestID": "22bad4e3-aa51-4ff1-b480-712ee07cedbd",
    "eventID": "50849dfd-36ed-418e-a901-49f6ac7087e8",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "444455556666"
}
```

# EventBridge

AWS Well-Architected Tool傳送事件到 Amazon EventBridge 當對 Well-Architected 的資源採取操作時。您可以使用 EventBridge 和這些事件來撰寫規則，以便在資源變更時採取動作，例如通知您。如需詳細資訊，請參閱什麼是 Amazon EventBridge？

> **Note**
>
> 活動是盡力交付。

以下操作會導致 EventBridge 事件：

- 工作負載相關
  - 創建或刪除工作負載
  - 創建裏程碑
  - 更新工作負載的屬性
  - 共享或解除共用工作負載
  - 更新共享邀請的狀態
  - 新增或移除標籤
  - 更新回答
  - 更新審閱註釋
  - 從工作負載中添加或移除鏡頭
- 鏡頭相關
  - 導入或導出自定義鏡頭
  - 發佈自訂鏡頭
  - 刪除自訂鏡頭
  - 共享或解除共用自訂鏡頭
  - 更新共享邀請的狀態
  - 從工作負載中添加或移除鏡頭

# 的範例事件AWS WA Tool

本節包含來自 AWS Well-Architected Tool 的範例事件。

### 更新工作負載中的答案


```
{
  "version":"0",
  "id":"00de336a-83cc-b80b-f0e6-f44c88a96050",
  "detail-type":"AWS API Call via CloudTrail",
  "source":"aws.wellarchitected",
  "account":"123456789012",
  "time":"2022-02-17T08:01:25Z",
  "region":"us-west-2",
  "resources":[],
  "detail":{
     "eventVersion":"1.08",
     "userIdentity":{
        "type":"AssumedRole",
        "principalId":"AROA4JUSXMN5ZR6S7LZNP:sample-user",
        "arn":"arn:aws:sts::123456789012:assumed-role/Admin/example-user",
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "sessionContext":{
           "sessionIssuer":{
              "type":"Role",
              "principalId":"AROA4JUSXMN5ZR6S7LZNP",
              "arn":"arn:aws:iam::123456789012:role/Admin",
              "accountId":"123456789012",
              "userName":"Admin"
           },
           "webIdFederationData":{},
           "attributes":{
              "creationDate":"2022-02-17T07:21:54Z",
              "mfaAuthenticated":"false"
           }
        }
     },
     "eventTime":"2022-02-17T08:01:25Z",
     "eventSource":"wellarchitected.amazonaws.com",
     "eventName":"UpdateAnswer",
     "awsRegion":"us-west-2",
```

```
      "sourceIPAddress":"10.246.162.39",
      "userAgent":"aws-internal/3 aws-sdk-java/1.12.127
 Linux/5.4.156-94.273.amzn2int.x86_64 OpenJDK_64-Bit_Server_VM/25.312-b07
 java/1.8.0_312 vendor/Oracle_Corporation cfg/retry-mode/standard",
      "requestParameters":{
         "Status":"Acknowledged",
         "SelectedChoices":"***",
         "ChoiceUpdates":"***",
         "QuestionId":"priorities",
         "WorkloadId":"ee73fda518f9bd4aa804c6252e4e37b0",
         "IsApplicable":true,
         "LensAlias":"wellarchitected",
         "Reason":"NONE",
         "Notes":"***"
      },
      "responseElements":{
         "Answer":"***",
         "LensAlias":"wellarchitected",
         "WorkloadId":"ee73fda518f9bd4aa804c6252e4e37b0"
      },
      "requestID":"7bae1153-26a8-4dc0-9307-68b17b107619",
      "eventID":"8339c258-4ddd-48aa-ab21-3f82ce9d79cd",
      "readOnly":false,
      "eventType":"AwsApiCall",
      "managementEvent":true,
      "recipientAccountId":"123456789012",
      "eventCategory":"Management"
   }
}
```

### 發佈自訂鏡頭

```
{
   "version":"0",
   "id":"4054a34b-60a9-53c1-3146-c1a384dba41b",
   "detail-type":"AWS API Call via CloudTrail",
   "source":"aws.wellarchitected",
   "account":"123456789012",
   "time":"2022-02-17T08:58:34Z",
   "region":"us-west-2",
   "resources":[],
```

```
   "detail":{
      "eventVersion":"1.08",
      "userIdentity":{
         "type":"AssumedRole",
         "principalId":"AROA4JUSXMN5ZR6S7LZNP:example-user",
         "arn":"arn:aws:sts::123456789012:assumed-role/Admin/example-user",
         "accountId":"123456789012",
         "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
         "sessionContext":{
            "sessionIssuer":{
               "type":"Role",
               "principalId":"AROA4JUSXMN5ZR6S7LZNP",
               "arn":"arn:aws:iam::123456789012:role/Admin",
               "accountId":"123456789012",
               "userName":"Admin"
            },
            "webIdFederationData":{},
            "attributes":{
               "creationDate":"2022-02-17T07:21:54Z",
               "mfaAuthenticated":"false"
            }
         }
      },
      "eventTime":"2022-02-17T08:58:34Z",
      "eventSource":"wellarchitected.amazonaws.com",
      "eventName":"CreateLensVersion",
      "awsRegion":"us-west-2",
      "sourceIPAddress":"10.246.162.39",
      "userAgent":"aws-internal/3 aws-sdk-java/1.12.127
 Linux/5.4.156-94.273.amzn2int.x86_64 OpenJDK_64-Bit_Server_VM/25.312-b07
 java/1.8.0_312 vendor/Oracle_Corporation cfg/retry-mode/standard",
      "requestParameters":{
         "IsMajorVersion":true,
         "LensVersion":"***",
         "ClientRequestToken":"03f46163-e95c-4455-8479-266373aa09c7",
         "LensAlias":"***"
      },
      "responseElements":{
         "LensArn":"arn:aws:wellarchitected:us-
west-2:123456789012:lens/6261deecb9def44f9aecc938ca25d94e",
         "LensVersion":"***"
      },
      "requestID":"167b7051-980d-42ee-9967-0b4b3163e948",
      "eventID":"c7ef2b47-419d-45b7-8982-fbade9b558c7",
```

```
      "readOnly":false,
      "eventType":"AwsApiCall",
      "managementEvent":true,
      "recipientAccountId":"123456789012",
      "eventCategory":"Management"
   }
}
```

# 文件歷史記錄

下表說明此版本 AWS Well-Architected Tool的文件。

- API 版本：最新
- 最新文件更新：2024 年 4 月 16 日

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| 吉拉 | 此版本新增了 Jira 的 AWS Well-Architected Tool 連接器。 | 2024年4月16日 |
| 全新鏡頭 | 此版本為鏡頭目錄增加了新鏡頭。 | 2024年3月26日 |
| 已更新的功能 | 此版本將鏡頭目錄功能新增至 AWS WA Tool。 | 2023 年 11 月 26 日 |
| 已更新的功能 | 此版本會將「檢閱範本」功能新增至 AWS WA Tool。 | 2023 年 10 月 3 日 |
| WellArchitectedConsoleReadOnlyAccess 管理策略已更新 | 已新增 `"wellarchitected:ExportLens"` 到 `WellArchitectedConsoleReadOnlyAccess` 。 | 2023 年 6 月 22 日 |
| 已更新的功能 | 此版本將設定檔功能新增至 AWS WA Tool。 | 2023 年 6 月 13 日 |
| 已更新的功能 | 此版本可增強 AWS Trusted Advisor 與 AWS Service Catalog AppRegistry 整合，並將其新增`AWS WellArchitectedDiscoveryServiceRolePolicy` 至受 AWS 管理的策略。 | 2023 年 5 月 3 日 |

| | | |
|---|---|---|
| 內容更新 | 儀表板頁面已更新，以包含詳細的風險和改進計劃資訊。還新增了建立合併工作負載報告的功能。 | 2023 年 3 月 30 日 |
| 內容更新 | 已更正WellArchitected ConsoleReadOnlyAccess策略的名稱。 | 2023 年 1 月 19 日 |
| 已更新的 IAM 指引， AWS WA Tool | 更新了指南以符合 IAM 最佳實務。如需詳細資訊，請參閱 IAM 中的安全最佳實務。 | 2023 年 1 月 4 日 |
| 已更新的功能 | 此版本將從工具中移除 FTR 鏡頭。 | 2022 年 12 月 14 日 |
| 已更新的功能 | 此版本增加了 AWS Trusted Advisor 和 AWS Service Catalog AppRegistry 整合。 | 2022 年 11 月 7 日 |
| 內容更新 | 已更正的自訂鏡頭 JSON 範例中的問題`choices`。 | 2022 年 9 月 29 日 |
| 內容更新 | 自訂鏡頭 JSON 規格的`choices`區段已更新。 | 2022 年 8 月 2 日 |
| 已更新的功能 | 此版本為其 AWS 受管理的策略添加了跟踪更改，並添加了一個新的操作以將`ListAWSServiceAccessForOrganization` 權限授予`AWSWellArchitectedOrganizationsServiceRolePolicy` . | 2022 年 7 月 22 日 |
| 已新增組織共用 | 此版本增加了與組織和組織單位 (OU) 共用工作負載和自訂鏡頭的功能。 | 2022 年 6 月 30 日 |

| | | |
|---|---|---|
| 已更新的功能 | 此版本增加了為自訂鏡頭中的選擇指定其他資源的功能，在發佈前預覽自訂鏡頭，以及為自訂鏡頭新增標籤。 | 2022 年 6 月 21 日 |
| 已更新的功能 | 此版本增加了在 Re: POST 上存取 AWS Well-Architected 社群的 AWS 功能。 | 2022 年 5 月 31 日 |
| 已更新的功能 | 此版本為「教學課程」增加了可持續發展支柱和小更新。 | 2022 年 3 月 31 日 |
| EventBridge 支持添加 | AWS WA Tool 現在當對 Well-Architected 的資源進行變更 EventBridge 時，會將事件傳送至 Amazon。 | 2022 年 3 月 3 日 |
| 添加了定制鏡頭 | 添加了添加自定義鏡頭的功能。 | 2021 年 11 月 29 日 |
| 已更新的功能 | 個別最佳做法現在可以標示為不適用。 | 2021 年 7 月 14 日 |
| 可用的資源標記 | 此版本新增了為工作負載新增標籤的功能。 | 2021 年 3 月 3 日 |
| API 現已可用 | 此版本新增了 AWS WA Tool API。 AWS CloudTrail 日誌記錄信息添加。 | 2020 年 12 月 16 日 |
| 已更新的功能 | 此版本將 FTR 和 SaaS 鏡頭添加到該工具中。 | 2020 年 12 月 3 日 |
| 資料保護已更新 | 資料保護資訊已更新。 | 2020 年 11 月 5 日 |
| 內容更新 | 澄清，升級工作負載以使用新鏡頭後，您無法返回到以前的版本。 | 2020 年 7 月 8 日 |

| | | |
|---|---|---|
| 內容更新 | 澄清 AWS 區域 了在 2019 年 3 月 20 日之後推出的分享。 | 2020 年 6 月 24 日 |
| 已更新的功能 | 工作負載共用邀請遭拒時，會立即移除工作負載共用的存取權。當接受共用時，就會授予共用存取權。 | 2020 年 6 月 17 日 |
| 內容更新 | 新增高風險問題 (HRI) 和中等風險問題 (MRI) 的定義。 | 2020 年 6 月 12 日 |
| 內容更新 | 有關如何添加數據 AWS 使用的部分。 | 2020 年 5 月 21 日 |
| 已更新的功能 | 此版本在工作負載中新增了檢閱擁有者。 | 2020 年 4 月 1 日 |
| 已更新的功能 | 此版本會新增架構圖表連結至工作負載。 | 2020 年 3 月 10 日 |
| 內容更新 | 澄清工作負載共 AWS 區域用是特定的。 | 2020 年 1 月 10 日 |
| 已更新的功能 | 這個版本新增了工作負載共用。 | 2020 年 1 月 9 日 |
| 內容更新 | 安全性部分已更新最新的指導。 | 2019 年 12 月 6 日 |
| 已更新的功能 | 此版本可在定義工作負載時選用產業欄位。 | 2019 年 8 月 19 日 |
| 已更新的功能 | 此版本新增改良計劃項目到工作負載報告。 | 2019 年 7 月 29 日 |
| 已更新的功能 | 發行版本會將 DeleteWorkload 動作新增至原則。 | 2019 年 7 月 18 日 |
| 內容更新 | 本指南內容已更新次要修正。 | 2019 年 6 月 19 日 |

| | | |
|---|---|---|
| 內容更新 | 本指南內容已更新次要修正。 | 2019 年 5 月 30 日 |
| 已更新的功能 | 此版本支援升級用於工作負載檢閱的架構版本。 | 2019 年 5 月 1 日 |
| 已更新的功能 | 此版本新增了在定義工作負載 AWS 區域 時指定非指定的功能。 | 2019 年 2 月 14 日 |
| AWS Well-Architected Tool 一般可用性 | 此版本推出 AWS Well-Architected Tool。 | 2018 年 11 月 29 日 |

# AWS 詞彙表

如需最新的 AWS 術語，請參閱《AWS 詞彙表 參考》中的 AWS 詞彙表。