使用者指南

AWS Support

API 版本 2013-04-15

AWS Support: 使用者指南

Table of Contents

AWS Support 入門

AWS Support 提供各種方案，可支援您運用各種工具與專業知識，協助您的 AWS 解決方案獲得成功並正常運作。所有支援計劃均提供全日 24 小時全年無休的客戶服務、AWS 說明文件、技術文件以及支援論壇。如需技術支援及其他資源來計畫、部署及改善您的 AWS 環境，您可以選擇適合您的 AWS 使用案例的支援計畫。

> **備註**
>
> - 若要在 AWS Management Console 中建立支援案例，請參閱「建立支援案例」。
> - 如需不同 AWS Support 計劃的詳細資訊，請參閱比較 AWS Support 計劃和 變更 AWS Support 計劃。
> - 針對您的支援案例，支援計劃會有不同的回應時間。請參閱 選擇嚴重性 和 回應時間。

主題

建立支援案例和案例管理

在 AWS Management Console 中，您可以在 AWS Support 中建立三種類型的客戶案例：

- 帳戶與帳單支援案例適用於所有 AWS 客戶。您可以取得帳單和帳戶問題的說明。
- 提升服務配額請求適用於所有 AWS 客戶。如需預設服務配額 (先前稱為限額) 的詳細資訊，請參閱《AWS 一般參考》中的 AWS服務配額。
- Technical support (技術支援) 案例，可讓您聯繫技術支援服務，協助您處理與服務相關的技術問題，在某些情況下也包含第三方應用程式。如果您擁有基本支援計劃，將無法建立技術支援案例。

> **備註**
>
> - 如需變更您的支援計劃，請參閱「變更 AWS Support 計劃」。

- 若要關閉帳戶，請參閱 AWS Billing 使用者指南中的關閉帳戶。
- 若要尋找 AWS 服務 的常見疑難排解主題，請參閱 疑難排解資源。
- 如果您是屬於 AWS Partner Network 的 AWS Partner 的客戶，並且如果您使用轉售支援，請直接聯絡您的 AWS Partner 解決任何帳單相關問題。AWS Support 無法協助處理轉售支援的非技術性問題，例如帳單和帳戶管理。如需詳細資訊，請參閱下列主題：
  - AWS 合作夥伴如何確定組織中的 AWS Support 計劃
  - AWS Partner 主導的支援

建立支援案例

您可以在 AWS Management Console 的支援中心裡建立支援案例。

備註

- 您能以您 AWS 帳戶的根使用者身分登入支援中心，或以 AWS Identity and Access Management (IAM) 使用者身分登入。如需更多詳細資訊，請參閱 管理對 AWS Support 中心的存取。
- 如果您無法登入支援中心並建立支援案例，可以改用聯絡我們頁面。您可以使用此頁面取得帳單和帳戶問題的說明。

建立支援案例

1. 登入 AWS Support Center Console。

   Tip

   在 AWS Management Console 中，您也可以選擇問號圖示 ()，然後選擇 Support Center (支援中心)。

2. 選擇 Create case (建立案例)。
3. 請選擇下列其中一個選項：
   - 帳戶和帳單

- 技術
- 如需 service quota 增加，請選擇 Looking for service limit increases? (試著提高服務限制？)，然後遵循 建立 service quota 增加 的指示。

4. 選擇 Service（服務）、Category (類別) 和 Severity (嚴重性)。

> **Tip**
>
> 您可以使用針對常見問題的建議解決方案。

5. 選擇 Next step: Additional information (下一步驟：其他資訊)
6. 在 Additional information (其他資訊) 頁面上的 Subject (主旨)，輸入與您問題相關的標題。
7. 請在 Description (描述) 欄位中，依照提示來描述您的案例，如下所示：
   - 您收到的錯誤訊息
   - 您依照哪些疑難排解步驟操作
   - 您如何存取服務：
     - AWS Management Console
     - AWS Command Line Interface (AWS CLI)
     - API 操作
8. (選用) 選擇 Attach files (附加檔案) 來將任何相關文件新增至您的案例，例如錯誤日誌或螢幕擷取畫面。您最多可以連接三個檔案。每個檔案最多可達 5 MB。
9. 選擇 Next step: Solve now or contact us (下一步驟：立即解決或聯絡我們)。
10. 在 Contact us (聯絡我們) 頁面中，選擇您偏好的語言。
11. 選擇您偏好的聯絡方式。您可以選擇以下其中一個選項：
    a. Web – 在支援中心內收到回覆。
    b. Chat (聊天) – 與支援客服人員開始線上聊天。如果您無法連線至聊天，請參閱故障診斷。
    c. Phone (電話) - 接聽來自支援客服人員的電話。如果選擇此選項，請輸入下列資訊：
       - 國家或區域
       - 電話號碼
       - （選用）擴充功能

> **備註**
>
> - 顯示的聯絡選項取決於案例類型和您的支援計畫。
> - 您可以選擇 Discard draft (捨棄草稿) 以清除您的支持案例草稿。

12. （選用）如果您訂閱商業、Enterprise On-Ramp 或企業支援計劃，才會顯示 Additional contacts (其他聯絡人) 選項。您可以輸入案例狀態發生變更時所要通知對象的電子郵件地址。如果您以 IAM 使用者身分登入，請加入您的電子郵件地址。如果您使用自己的根帳戶電子郵件地址和密碼登入，便無須附上您的電子郵件地址

> **Note**
>
> 若您擁有基本支援計畫，Additional contacts (其他聯絡人) 選項將無法使用。但是，My Account (我的帳戶) 頁面上 Alternate Contacts (替代聯絡人) 區段中所指定的 Operations (操作) 聯絡人將會收到案例通訊的副本，但僅限特定的帳戶、帳單與技術案例類型。

13. 檢閱您的案例詳細資訊，然後選擇 Submit (提交)。您的案例 ID 編號和摘要隨即出現。

描述您的問題

就您的描述盡可能提供詳細資訊。請附上相關資源以及其他有助於我們了解您問題的任何資訊。例如，若要解決效能問題，描述時應包括時間戳記和日誌。如果是功能請求或一般指導問題，描述中應包含您的環境和用途。在所有情況下，都請您遵循案例提交表單上顯示的 Description Guidance (描述指導方針)。

當您提供的資訊愈詳細，將可提高您的案例快速解決的機會。

選擇嚴重性

您可能會傾向於一律建立支援計劃允許的最高嚴重性支援案例。不過，我們建議您針對無法解決或直接影響生產應用程式的情況，為案例選擇最高的嚴重性。有關如何建置您的服務讓失去單一資源不影響您的應用程式，詳細資訊請參閱在 AWS 上建構容錯應用程式技術文件。

下表列出嚴重性層級、回應時間和範例問題。

備註

- 建立支援案例之後，您就無法變更它的嚴重性代碼。如果您的情況改變，請與您支援案例的 AWS Support 客服人員合作。
- 如需有關嚴重性層級的詳細資訊，請參閱「AWS SupportAPI 參考」。

嚴重性	嚴重性層級代碼	初次回應時間	說明及支援計劃
一般指導方針	`low`	24 小時	您有一般開發問題或想要申請功能。(*開發人員、商業、Enterprise On-Ramp 或企業支援計劃)
系統效能不佳	`normal`	12 小時	您應用程式的非關鍵性功能運作異常，或您有時間急迫的開發問題。(*開發人員、商業、Enterprise On-Ramp 或企業支援計劃)
生產系統效能不佳	`high`	4 小時	您應用程式的重要功能效能不佳或降低。(商業、Enterprise On-Ramp 或企業支援計劃)
生產系統當機	`urgent`	1 小時	您的事業受到嚴重影響。您應用程式的重要功能無法使用。(商業、Enterprise On-Ramp 或企業支援計劃)
商業關鍵系統當機	`critical`	15 分鐘	您的事業面臨危機。無法使用您應用程式的關鍵功能 (企業支援計劃)。請注意，若為 Enterprise On-Ramp 支援計劃，此為 30 分鐘。

回應時間

我們會盡一切合理的努力，在指定的時間範圍內回應您的初次請求。如需有關各項 AWS Support 方案支援範圍的資訊，請參閱 AWS Support 功能。

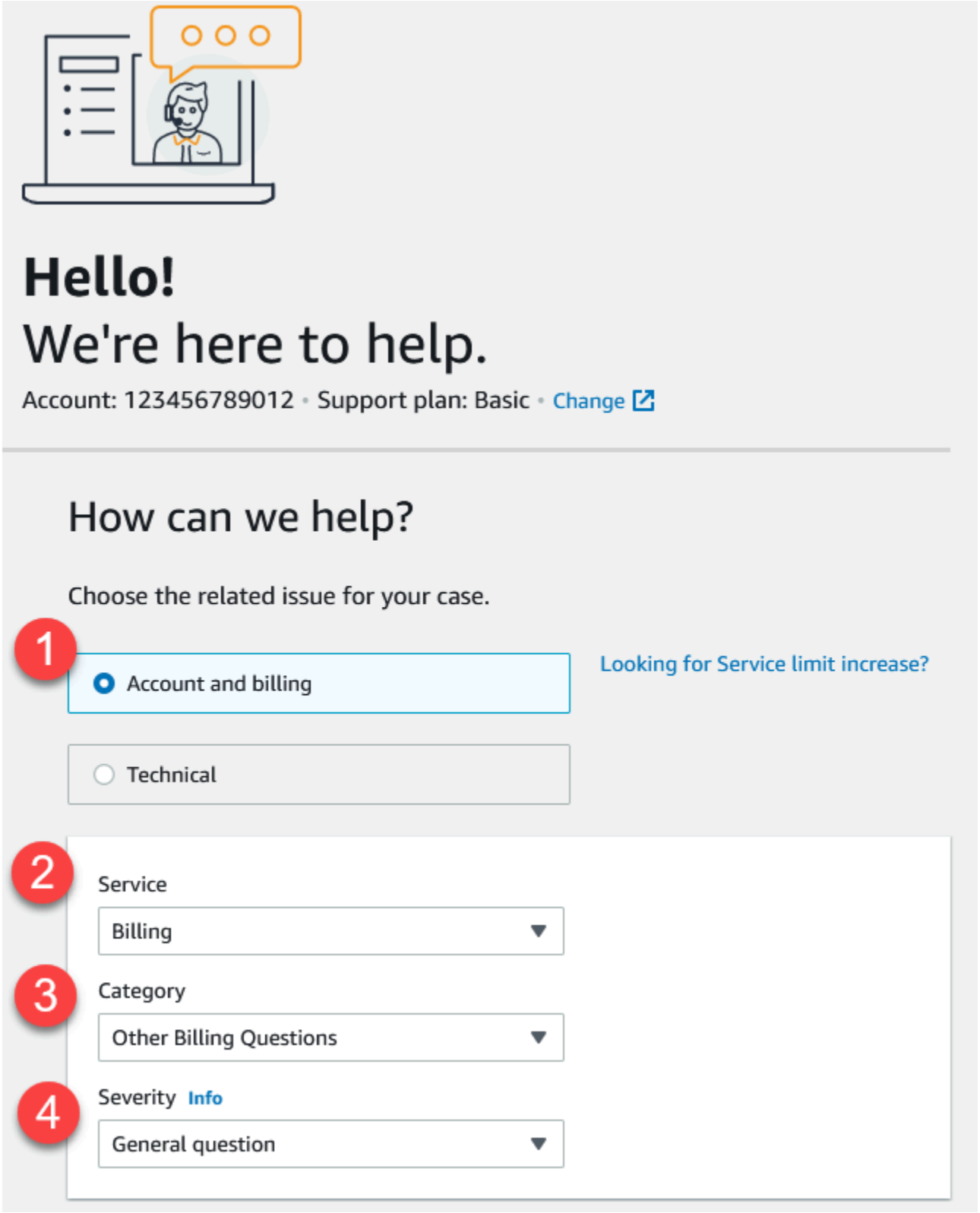
如果您擁有商業、Enterprise On-Ramp 或企業支援計劃，您可以隨時取得技術支援，全年無休。*針對開發人員支援，案例支援的回應目標以營業時間計算。營業時間一般定義為客戶國家的上午 8 點

到下午 6 點，不含假日和週末。上述時間在擁有多個時區的國家會有不同。此資訊會顯示在 AWS Management Console 中 My Account (我的帳戶) 頁面上的 Contact Information (聯絡資訊) 區段裡。

> **Note**
>
> 如果您選擇日文作為支援案例的偏好聯絡語言，系統就可能會以日文提供支援，如下所示：
>
> - 如果您需要非技術性支援案例的客戶服務，或者您有開發人員支援計畫且需要技術支援，那麼我們會在日本的營業時間 (定義為上午 09:00 至下午 06:00 日本標準時間 (GMT+9)，不含假日和週末) 內以日文提供支援。
> - 如果您擁有商業、Enterprise On-Ramp 或企業支援計劃，您可以隨時取得日文技術支援，全年無休。
>
> 如果您選擇中文作為支援案例的偏好聯絡語言，系統就可能會以中文提供支援，如下所示：
>
> - 如果您需要非技術支援案例的客戶服務，那麼我們會在上午 09:00 至下午 06:00 (GMT+8，不含假日和週末) 這段時間內以中文提供支援。
> - 如果您有開發人員支援計畫，那麼我們會在您所在國家的營業時間 (通常定義為上午 8:00 至下午 6:00，如我的帳戶中設定，不含假日和週末) 內以中文提供技術支援。這些時間在具有多個時區的國家之中，可能會有所不同。
> - 如果您擁有商業、Enterprise On-Ramp 或企業支援計畫，您可以隨時取得中文技術支援，全年無休。
>
> 如果您選擇韓文作為支援案例的偏好聯絡語言，系統就可能會以韓文提供支援，如下所示：
>
> - 如果您需要非技術支援案例的客戶服務，那麼我們會在韓國的營業時間 (定義為上午 09:00 至下午 06:00 韓國標準時間 (GMT+9)，不含假日和週末) 這段時間內以韓文提供支援。
> - 如果您有開發人員支援計畫，那麼我們會在您所在國家的營業時間 (通常定義為上午 8:00 至下午 6:00，如我的帳戶中設定，不含假日和週末) 內以韓文提供技術支援。這些時間在具有多個時區的國家之中，可能會有所不同。
> - 如果您擁有商業、Enterprise On-Ramp 或企業支援計畫，您可以隨時取得韓文技術支援，全年無休。

範例：建立帳戶和帳單支援案例

下列範例是帳單和帳戶問題的支持案例。



1. 建立案例 – 選擇要建立的案例類型。在此範例中，案例類型為帳戶和帳單。

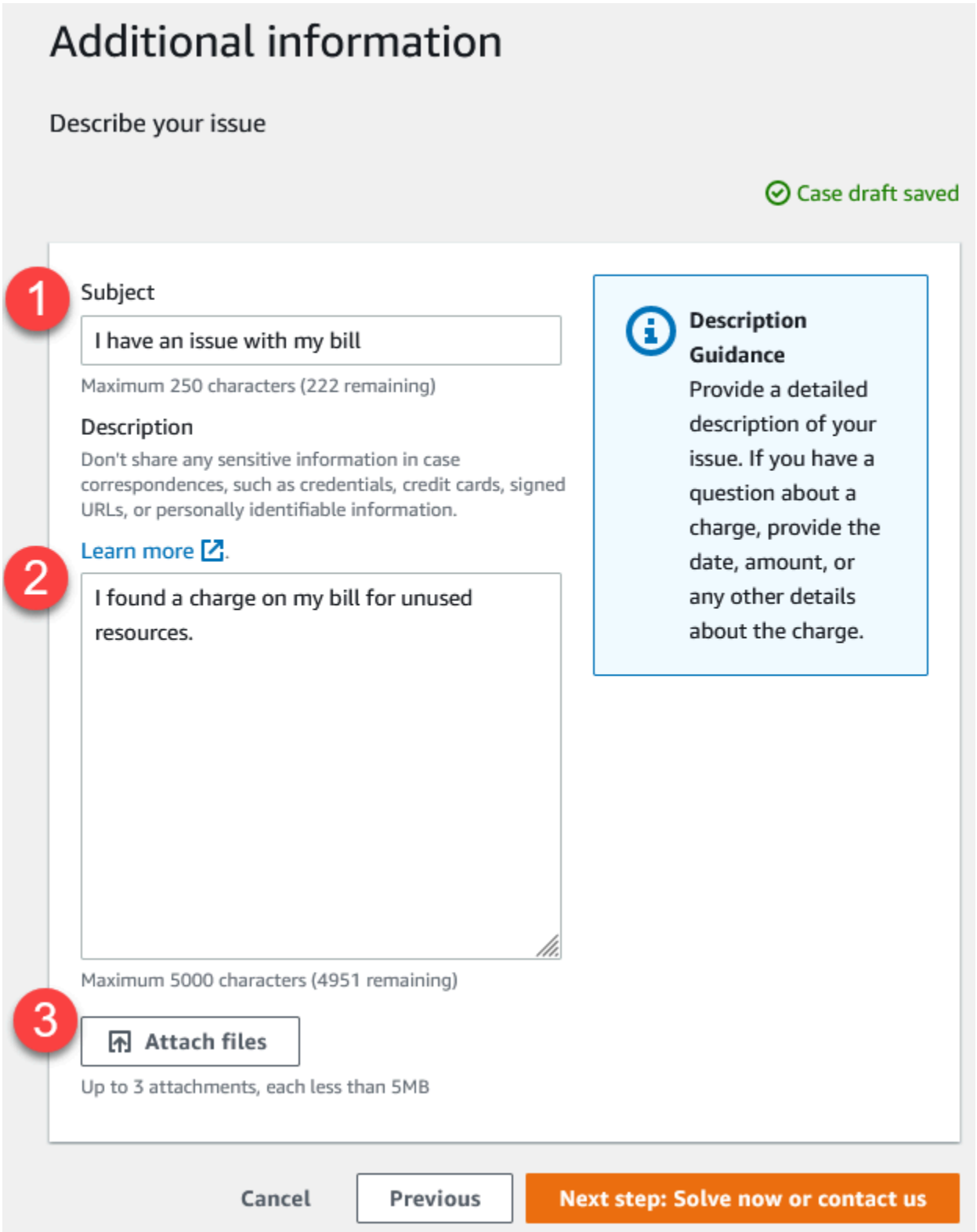
> **Note**
>
> 如果您擁有基本支援計劃，將無法建立技術支援案例。

2. Service (服務) - 如果您的問題影響多個服務，請選擇最適合的服務。
3. Category (類別) - 選擇最適合您使用案例的類別。選擇類別後，下方就會顯示可能解決問題的資訊連結。
4. Severity (嚴重性) - 付費支援計劃的客戶可選擇嚴重程度為 General guidance (一般指導) (1 天回應時間) 或 System impaired (系統效能不佳) (12 小時回應時間)。商業支援計劃客戶亦可選擇 Production system impaired (生產系統效能不佳) (4 小時回應) 或 Production system down (生產系統當機) (1 小時回 應)。擁有 Enterprise On-Ramp 或企業支援計劃的客戶可以選擇業務關鍵系統當機(企業支援為 15 分鐘回應，Enterprise On-Ramp 則為 30 分鐘回應)。

   回應時間是適用於來自 AWS Support 的第一個回應。這些回應時間不適用於後續回應。對於第三方問題，回應時間可能會比較長，這取決於專業人員的可用性。如需詳細資訊，請參閱選擇嚴重性。

> **Note**
>
> 根據您選擇的類別，系統可能會提示您輸入更多資訊。

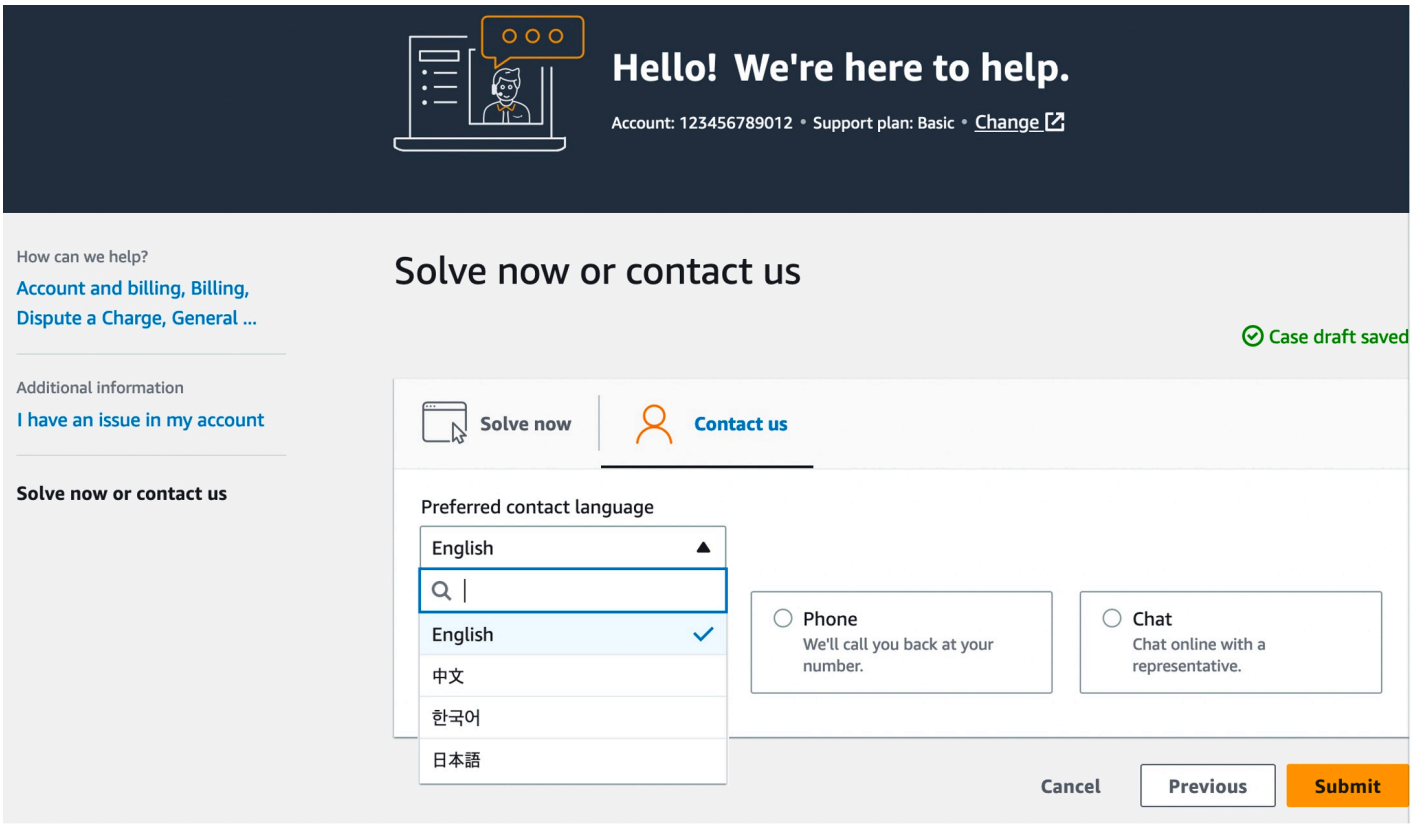
指定案例類型和分類之後，您可以指定描述和聯絡方式。



1. Subject (主旨) - 輸入簡要描述您問題的標題。

2. Description (描述)– 描述您的支援案例。這是您提供給 AWS Support 的最重要資訊。對於某些服務和類別的組合，會出現具有相關資訊的提示。使用這些連結來協助解決您的問題。如需詳細資訊，請參閱描述您的問題。
3. Attachments (附件) – 提供可以幫助客服人員更快解決您的問題的螢幕擷圖和其他檔案。您最多可以連接三個檔案。每個檔案最多可達 5 MB。

在新增案例詳細資訊之後，您可以選擇聯絡方式。



1. 偏好語言設定 - 選擇您偏好的語言。目前，您可以選擇中文、英文、日文，或韓文。支援方案會以您偏好的語言來顯示可自訂聯絡選項。
2. 選擇聯絡方式。顯示的聯絡選項取決於案例類型和您的支援計畫。
   - 如果您選擇 Web,，您可以透過支援中心讀取和回應案例進度。
   - 選擇 Chat (聊天) 或者 Phone (電話)。如果您選擇 Phone (電話)，系統會提示您輸入回撥電話號碼。
3. 填妥資訊並準備好建立案例時，選擇 Submit (提交)。

Note

如果您選擇日文作為支援案例的偏好聯絡語言，系統就可能會以日文提供支援，如下所示：

- 如果您需要非技術性支援案例的客戶服務，或者您有開發人員支援計畫且需要技術支援，那麼我們會在日本的營業時間 (定義為上午 09:00 至下午 06:00 日本標準時間 (GMT+9)，不含假日和週末) 內以日文提供支援。
- 如果您擁有商業、Enterprise On-Ramp 或企業支援計劃，您可以隨時取得日文技術支援，全年無休。

如果您選擇中文作為支援案例的偏好聯絡語言，系統就可能會以中文提供支援，如下所示：

- 如果您需要非技術支援案例的客戶服務，那麼我們會在上午 09:00 至下午 06:00 (GMT+8，不含假日和週末) 這段時間內以中文提供支援。
- 如果您有開發人員支援計畫，那麼我們會在您所在國家的營業時間 (通常定義為上午 8:00 至下午 6:00，如我的帳戶中設定，不含假日和週末) 內以中文提供技術支援。這些時間在具有多個時區的國家之中，可能會有所不同。
- 如果您擁有商業、Enterprise On-Ramp 或企業支援計畫，您可以隨時取得中文技術支援，全年無休。

如果您選擇韓文作為支援案例的偏好聯絡語言，系統就可能會以韓文提供支援，如下所示：

- 如果您需要非技術支援案例的客戶服務，那麼我們會在韓國的營業時間 (定義為上午 09:00 至下午 06:00 韓國標準時間 (GMT+9)，不含假日和週末) 這段時間內以韓文提供支援。
- 如果您有開發人員支援計畫，那麼我們會在您所在國家的營業時間 (通常定義為上午 8:00 至下午 6:00，如我的帳戶中設定，不含假日和週末) 內以韓文提供技術支援。這些時間在具有多個時區的國家之中，可能會有所不同。
- 如果您擁有商業、Enterprise On-Ramp 或企業支援計畫，您可以隨時取得韓文技術支援，全年無休。

建立 service quota 增加

若要改善服務的效能，請求增加 Service Quotas（先前稱為限額）。

> **Note**
>
> 您還可以使用 Service Quotas 服務，直接為您的服務來請求增加。目前，Service Quotas 不支援所有服務的 service quotas。如需詳細資訊，請參閱《Service Quotas 使用者指南》中的「什麼是 Service Quotas？」。

若要建立支援案例以提高 Service Quotas

1. 登入 AWS Support Center Console。

   > **Tip**
   >
   > 在 AWS Management Console 中，您也可以選擇問號圖示 ()，然後選擇 Support Center (支援中心)。

2. 選擇 Create case (建立案例)。
3. 選擇 Looking for service limit increases? (尋找增加服務限制額度？)
4. 若要請求提高，請按照提示操作。可能的選項包括下列項目：

   - 限制類型
   - 嚴重性

   > **Note**
   >
   > 根據您選擇的類別，提示可以要求提供更多資訊。

5. 對於 Requests (請求)，選擇 Region (區域)。
6. 針對 Limit (限制)，選擇服務限制類型。
7. 針對 New limit value (新的限制值)，輸入您要的值。
8. (選用) 若要請求另一個提高，請選擇 Add another request (新增其他要求)。
9. 對於 Case description (案例描述)，請描述您的支援案例。
10. 針對 Contact options (聯絡選項) 頁面，選擇您偏好的語言和聯絡方式。您可以選擇以下其中一個選項：

    - Web – 在支援中心內收到回覆。

- Chat (聊天) – 與支援客服人員開始線上聊天。如果您無法連線至聊天，請參閱故障診斷。
- Phone (電話) - 接聽來自支援客服人員的電話。如果選擇此選項，請輸入下列資訊：
  - 國家/區域
  - 電話號碼
  - （選用）擴充功能

11. 選擇 Submit (提交)。您的案例 ID 編號和摘要隨即出現。

更新、解決及重新開啟您的案例

建立支援案例後，您可以在支援中心裡監控案例狀態。新案例一開始的狀態為 Unassigned (未指派)。當支援客服人員開始處理案例，案例狀態即變更為 Work in Progress (處理中)。支援客服人員可能會向您詢問更多資訊 (Pending Customer Action (等待客戶動作))，或讓您知道此案件正在調查中 (Pending Amazon Action (等待 Amazon 動作))。

您的案例更新時，您會收到電子郵件，其中包含通訊和連至支援中心內案例的連結。使用電子郵件訊息中的連結瀏覽至支援案例。您無法透過電子郵件回覆案例通訊。

> **備註**
>
> - 您必須登入提交支援案例的 AWS 帳戶 帳戶。如果您以 AWS Identity and Access Management (IAM) 使用者身分登入，必須具有檢視支援案例所需的許可。如需更多詳細資訊，請參閱 管理對 AWS Support 中心的存取。
> - 如果您沒有在幾天內回應案例，AWS Support 會自動解決案例。
> - 處於已解決狀態超過 14 天的支援案例無法重新開啟。如果您遇到與已解決案例相關的類似問題，可以建立相關案例。如需更多詳細資訊，請參閱 建立相關案例。

主題

更新現有的支援案例

您可以更新案例，為支援客服人員提供更多資訊。例如，您可以回覆信件、開始另一個即時聊天、新增其他電子郵件收件者等等。不過，您建立案例之後就無法更新案例的嚴重等級。如需更多詳細資訊，請參閱 選擇嚴重性。

更新現有的支援案例

1. 登入 AWS Support Center Console。

   > **Tip**
   >
   > 在 AWS Management Console 中，您也可以選擇問號圖示 ()，然後選擇 Support Center (支援中心)。

2. 在 Open support cases (開啟支援案例) 下，選擇支援案例的 Subject (主旨)。
3. 選擇 Reply (回覆)。在 Correspondence (通訊) 區段中，您也可以進行下列任何變更：
   - 提供支援客服人員要求的資訊
   - 上傳檔案附件
   - 變更您偏好的聯絡方式
   - 新增電子郵件地址以接收案例更新資訊
4. 選擇 Submit (提交)。

> **Tip**
>
> 如果您關閉了聊天視窗並希望開始另一個線上聊天，您可以將 Reply (回覆) 新增到您的支援案例，選擇 Chat (聊天)，然後選擇 Submit (提交)。一個新的彈出聊天窗口便會開啟。

解決支援案例

當您對回應感到滿意或您的問題已解決，可以在支援中心中解決案例。

解決支援案例

1. 登入 AWS Support Center Console。

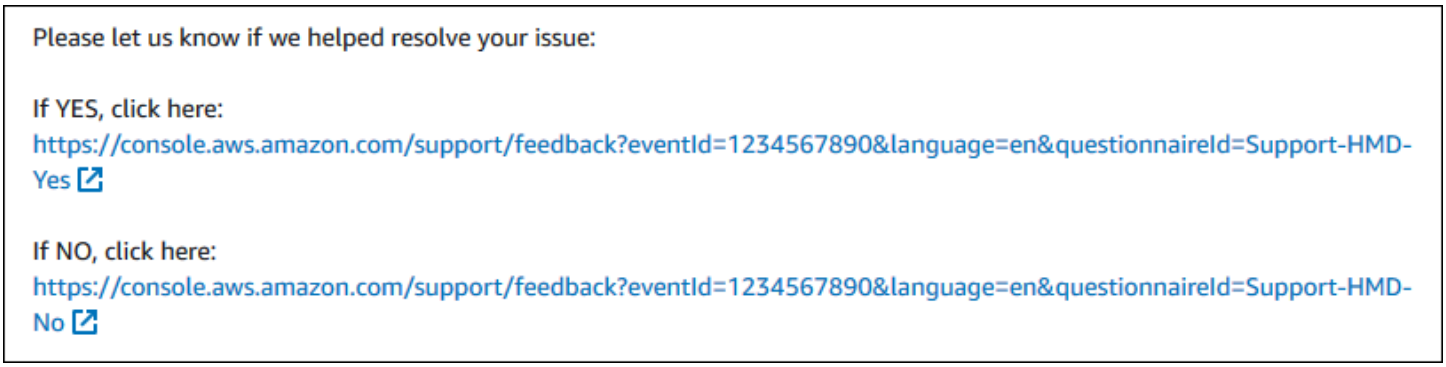
   > **Tip**
   >
   > 在 AWS Management Console 中，您也可以選擇問號圖示 ( ) ，然後選擇 Support Center (支援中心)。

2. 在 Open support cases (開啟支援案例) 下，選擇您想要解決的支援案例 Subject (主旨)。
3. (選用) 選擇 回覆 (Reply)，並在 Correspondence (通訊) 區段中，輸入您要解決案例的原因，然後選擇 Submit (提交)。例如，您可以輸入有關您如何自行解決問題的資訊，以便將來需要此資訊時提供參考。
4. 選擇 Resolve case (解決案例)。
5. 在對話方塊中，選擇 OK 即可解決這個問題。

> **Note**
>
> 如果 AWS Support 為您解決了案例，您可以使用意見回饋連結，提供關於您使用 AWS Support 經驗的更多資訊。

Example :意見回饋連結

下列螢幕擷取畫面顯示支援中心案例通訊中的意見回饋連結。



重新開啟已解決的案例

如果您再次遇到同樣的問題，可以重新開啟原始案例。提供問題再次發生的時間以及您試過的疑難排解步驟詳細資訊。加入任何相關案例編號，方便支援人員參考先前的通訊內容。

> **備註**
>
> - 您最多可以在問題解決後 14 天內重新開啟支援案例。不過，您無法重新開啟已結案超過 14 天的案例。您可以建立新案例或相關案例。如需更多詳細資訊，請參閱 建立相關案例。
> - 如果您重新開啟一個現有案例，但資訊與目前的問題不同，支援客服人員可能會要求您建立一個新案例。

重新開啟已解決的案例

1. 登入 AWS Support Center Console。

   > **Tip**
   >
   > 在 AWS Management Console 中，您也可以選擇問號圖示 ()，然後選擇 Support Center (支援中心)。

2. 選擇 View all cases (檢視所有案例)，接著選擇您想要重新開啟的支援案例的 Subject (主旨) 或 Case ID (案例 ID)。
3. 選擇 Reopen case (重新開啟案例)。
4. 在 Correspondence (通訊) 底下的 Reply (回覆) 中，輸入案例詳細資訊。
5. (選用) 選擇 Choose files (選擇檔案)，將檔案連接至您的案例。您最多可以連接 3 個檔案。
6. 針對 Contact methods (聯絡方式)，選擇以下其中一個選項：
   - Web - 透過電子郵件和支援中心接收通知。
   - Chat (聊天) - 與支援客服人員線上交談。
   - Phone (電話) - 接聽來自支援專員的電話。
7. (選用) 針對 Additional contacts (其他聯絡人)，輸入您希望接收案例通訊的其他人的電子郵件地址。
8. 檢閱您的案例詳細資訊，然後選擇 Submit (提交)。

建立相關案例

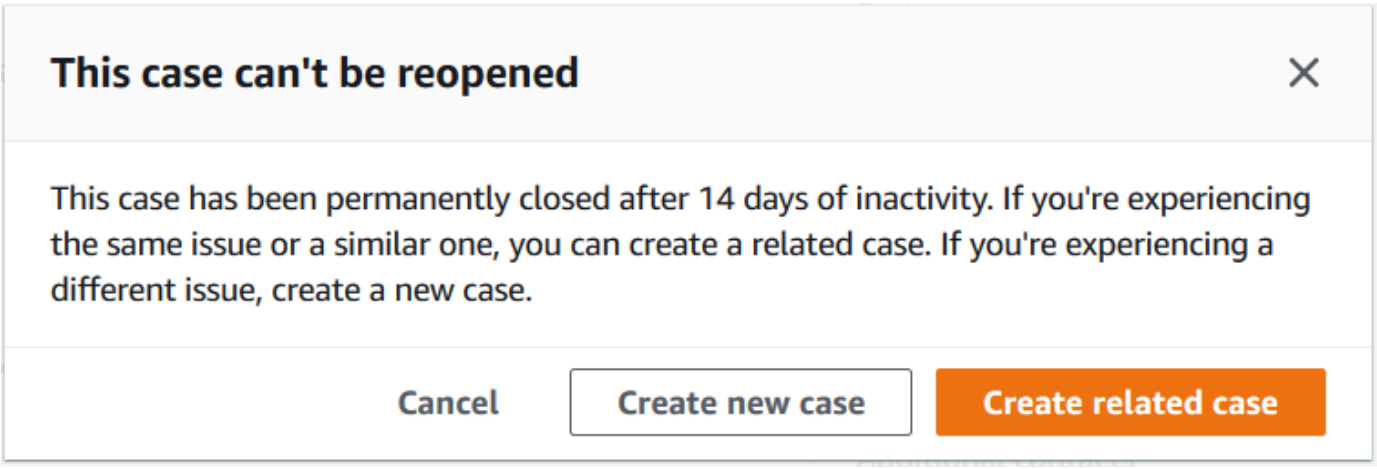
結案 14 天後，便無法重新開啟已解決的個案。如果您遇到與已解決案例相關的類似問題，可以建立相關案例。此相關案例將包含先前已解決案例的連結，方便支援客服人員檢閱先前案例的詳細資訊和通訊。如果您遇到不同問題，建議您建立新的案例。

建立相關案例

1. 登入 AWS Support Center Console。

   > **Tip**
   >
   > 在 AWS Management Console 中，您也可以選擇問號圖示 ( ) ，然後選擇 Support Center (支援中心)。

2. 選擇 View all cases (檢視所有案例)，接著選擇您想要重新開啟的支援案例的 Subject (主旨) 或 Case ID (案例 ID)。
3. 選擇 Reopen case (重新開啟案例)。
4. 在對話方塊中，選擇 Create related case (建立相關案例)。先前案例的資訊會自動新增至您的相關案例中。如果您遇到不同問題，請選擇 Create new case (建立新案例)。

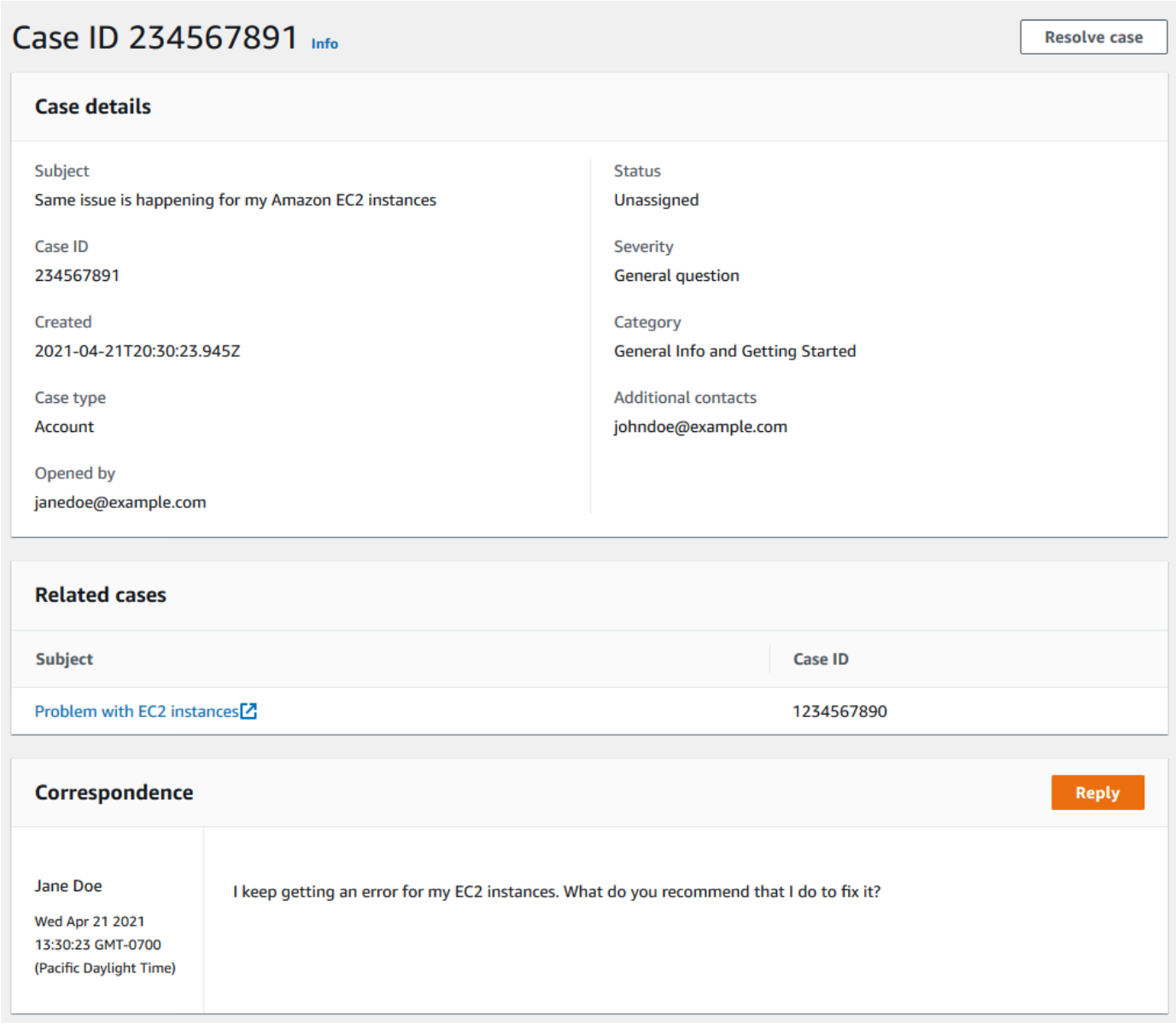


5. 請依相同步驟建立案例。請參閱 建立支援案例。

> **Note**
>
> 預設情況下，相關案例的 Type (類型)、Category (類別) 及 Severity (嚴重性) 都與先前的案例相同。您可以視需要更新案例詳細資訊。

6. 檢閱您的案例詳細資訊，然後選擇 Submit (提交)。

建立案例後，先前的案例會出現在 Related cases (相關案例) 區段中，如下列範例所示。



案例歷史記錄

建立案例後，您可以在長達 24 個月的時間內檢視案例歷史記錄資訊。

故障診斷

如果您在建立或管理支援案例上碰到問題，請參閱下列故障診斷資訊。

我想為我的案例重新開啟即時聊天

您可以回覆現有的支援案例，開啟另一個聊天視窗。如需詳細資訊，請參閱更新現有的支援案例。

我無法連線至即時聊天

如果您選擇 Chat (聊天)選項，但是您無法連線至聊天室窗，請先執行下列檢查：

- 請確定您已將瀏覽器設定為允許支援中心中的快顯視窗。

  > **Note**
  >
  > 檢閱您的瀏覽器設定。如需詳細資訊，請參閱 Chrome 說明及 Firefox 支援網站。

- 請確定您已設定網路，以便使用 AWS Support：
  - 您的網路可以存取 `*.connect.us-east-1.amazonaws.com` 端點。

    > **Note**
    >
    > 如果是 AWS GovCloud (US)，端點為 `*.connect-fips.us-east-1.amazonaws.com`。

  - 您的防火牆支援網路通訊端連線。

如果您仍然無法連線至聊天視窗，請使用電子郵件或電話聯絡選項來聯絡 AWS Support。

搭配 AWS SDK 使用 AWS Support

AWS 軟體開發套件 (SDK) 適用於許多常用的程式設計語言。每個 SDK 都提供 API、程式碼範例和說明文件，讓開發人員能夠更輕鬆地以偏好的語言建置應用程式。

SDK 文件	程式碼範例
AWS SDK for C++	AWS SDK for C++ 程式碼範例
AWS SDK for Go	AWS SDK for Go 程式碼範例
AWS SDK for Java	AWS SDK for Java 程式碼範例
AWS SDK for JavaScript	AWS SDK for JavaScript 程式碼範例
適用於 Kotlin 的 AWS SDK	適用於 Kotlin 的 AWS SDK 程式碼範例
AWS SDK for .NET	AWS SDK for .NET 程式碼範例
AWS SDK for PHP	AWS SDK for PHP 程式碼範例
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) 程式碼範例
AWS SDK for Ruby	AWS SDK for Ruby 程式碼範例
適用於 Rust 的 AWS SDK	適用於 Rust 的 AWS SDK 程式碼範例
適用於 SAP ABAP 的 AWS SDK	適用於 SAP ABAP 的 AWS SDK 程式碼範例
適用於 Swift 的 AWS SDK	適用於 Swift 的 AWS SDK 程式碼範例

可用性範例

找不到所需的內容嗎？ 請使用本頁面底部的提供意見回饋連結申請程式碼範例。

關於 AWS Support API

AWS Support API 可用於存取 AWS 支援中心的部分功能。

此 API 目前提供兩種不同的作業群組：

- 支援案例管理 作業可管理您的 AWS 支援案例，從建立案例到解決案例的整個生命週期
- 用於存取 AWS Trusted Advisor 檢查的 AWS Trusted Advisor 作業

> **Note**
>
> 您必須訂閱商業、Enterprise On-Ramp 或企業支援計劃才能使用 AWS Support API。如需詳細資訊，請參閱AWS Support。

如需有關 AWS Support 所提供的操作和資料類型的詳細資訊，請參閱《AWS Support API 參考》。

主題

- 支援案例管理
- AWS Trusted Advisor
- 端點
- AWS 軟體開發套件中的支援

支援案例管理

您可使用 API 執行下列任務：

- 開啟支援案例
- 取得有關最新支援案例的清單和詳細資訊
- 根據日期和案例識別碼 (包括已解決的案例) 篩選支援案例搜尋條件
- 將通訊和檔案附件新增到您的案例中，並新增電子郵件收件人以進行案例通訊。您最多可以連接三個檔案。每個檔案最多可達 5 MB
- 解決您的案例

AWS SupportAPI 支援 CloudTrail 記錄以進行支援案例管理作業。如需詳細資訊，請參閱使用 AWS CloudTrail 記錄 AWS Support API 呼叫。

如需有關如何管理支援案例完整生命週期的 Java 程式碼範例，請參閱使用 AWS SDK 的 AWS Support 程式碼範例。

AWS Trusted Advisor

您可使用 Trusted Advisor 作業執行下列任務：

- 取得 Trusted Advisor 檢查的名稱和識別碼
- 請求對您的 AWS 帳戶和資源執行 Trusted Advisor 檢查
- 取得 Trusted Advisor 檢查結果的摘要和詳細資訊
- 重新整理 Trusted Advisor 檢查
- 取得每個 Trusted Advisor 檢查的狀態

該 AWS Support API 支持Trusted Advisor操作 CloudTrail 日誌記錄。如需詳細資訊，請參閱CloudTrail 記錄中的 AWS Trusted Advisor 資訊。

您可以使用 Amazon CloudWatch 事件來監控檢查結果的變更Trusted Advisor。如需詳細資訊，請參閱使用 Amazon 監控AWS Trusted Advisor檢查結果 EventBridge。

如需示範如何使用 Trusted Advisor 作業的 Java 程式碼範例，請參閱「將 Trusted Advisor 做為 Web 服務使用」。

端點

AWS Support 是全球服務。這表示您使用的任何端點都會在 Support Center Console 中更新您的支援案例。

例如，如果您使用美國東部 (維吉尼亞北部) 端點建立案例，則可以使用美國西部 (奧勒岡) 或歐洲 (愛爾蘭) 或歐洲 (愛爾蘭) 端點在相同的案例中新增通信內容。

您可以對 AWS Support API 使用以下端點：

- 美國東部 (維吉尼亞北部) – https://support.us-east-1.amazonaws.com
- 美國西部 (奧勒岡) – https://support.us-west-2.amazonaws.com

- 歐洲 (愛爾蘭) – https://support.eu-west-1.amazonaws.com

> **Important**
>
> - 如果您調用CreateCase操作來創建測試支持用例，我們建議您包括一個主題行，例如測試案例，請忽略。完成測試支持案例後，請調用該ResolveCase操作以解決它。
> - 若要呼叫 AWS Support API 中的 AWS Trusted Advisor 操作，您必須使用美國東部 (維吉尼亞北部) 端點。目前，美國西部 (奧勒岡) 及歐洲 (愛爾蘭) 端點目前不支援 Trusted Advisor 操作。

如需 AWS 端點的詳細資訊，請參閱《Amazon Web Services 一般參考》中的 AWS Support 端點與配額。

AWS 軟體開發套件中的支援

AWS Command Line Interface (AWS CLI) 和 AWS 軟體開發套件 (SDK) 包含對 AWS Support API 的支援。

如需支援 AWS Support API 的語言清單，請選擇作業名稱，例如 CreateCase，然後在「另請參閱」區段中選擇您偏好的語言。

AWS Support 計劃

您可以根據您的業務需求為您的帳戶更改 AWS Support 計劃。

主題

AWS Support 計劃的特點

AWS Support 提供五種支援方案：

- 基本
- 開發人員
- 商業
- Enterprise On-Ramp
- Enterprise

免費的基本支援計劃針對帳戶和帳單相關問題，以及提高服務配額事宜提供支援。其他計劃提供了許多技術支持案例， pay-by-the-month 價格和沒有長期合同。

所有 AWS 客戶都能全年無休自動存取基本 Support 的下列功能：

- O ne-on-one 對帳戶和帳單問題的回應
- 支援論壇
- 服務運作狀態檢查
- 說明文件、技術文件及最佳實務指南

採用開發人員支援計劃的客戶可存取以下額外功能：

- 最佳實務指南
- 用戶端診斷工具
- 建置區塊架構支援：如何搭配使用 AWS 產品、功能和服務的指南
- 支持無限數量的支持案例，任何具有權限的用戶都可以打開。

此外，商業、 Enterprise On-Ramp 或企業支援計劃的客戶可存取以下功能：

- 使用案例指南 — 可以使用哪些 AWS 產品、功能和服務來最好地支援您的特定需求。
- AWS Trusted Advisor— 檢查客戶環境並識別節省金錢 AWS Support、縮小安全漏洞，以及改善系統可靠性和效能的機會之一。您可以存取所有 Trusted Advisor 檢查。
- 與 S AWS Support upport 中心和 Trusted Advisor. 您可以使用 AWS Support API 將支援案例管理和 Trusted Advisor 操作自動化。
- 第三方軟體支援 - 協助 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體作業系統和組態。此外，還可以幫助最受歡迎的第三方軟件組件的性能 AWS。第三方軟體支援不適用於採用基本或開發人員支援計劃的客戶。
- 支援無限數量的 AWS Identity and Access Management (IAM) 使用者，這些使用者可以開啟技術支援案例。

此外，Enterprise On-Ramp 或企業支援計劃的客戶可存取以下功能：

- 應用程式架構指導方針 - 搭配使用各種服務的諮詢式指導方針，以滿足您特定的使用案例、工作負載或應用程式。
- 基礎設施事件管理 - 與 AWS Support 進行短期互動以深入了解您的使用案例。分析之後，為事件提供架構和擴展方面的指導。
- 技術客戶經理 - 針對您的特定使用案例和應用程式，與技術客戶經理 (TAM) 合作。
- 案例特別處理
- 管理商業審查。

如需各支援方案功能與價格的詳細資訊，請參閱AWS Support和比較方 AWS Support 案。某些功能 (例如全日 24 小時全年無休的電話和聊天支援) 並非所有語言都提供。

變更 AWS Support 計劃

您可以使用方 AWS Support 案主控台來變更您的 AWS 帳戶. 若要變更支援方案，您必須擁有 AWS Identity and Access Management (IAM) 許可或以 root 使用者身分登入您的帳戶。如需詳細資訊，請參閱 管理對 AWS Support 計劃的存取 及 AWS 受管理的 AWS Support 計劃原則。

變更您的支援計劃

1. 請在 https://console.aws.amazon.com/support/plans/home 登入「 AWS Support 方案」主控台。

2. (選用) 在 AWS Support Plans 頁面中，比較支援計劃。如需有關定價的詳細資訊，請造訪 pricing detail (定價詳細資訊) 頁面。
3. (選用) 在 AWS Support 定價範例中，選擇查看範例，然後選擇其中一個支援計畫選項以查看估算的成本。
4. 當您選定計劃時，請為您想要的計劃選擇 Review downgrade (檢閱降級) 或者 Review upgrade (檢閱升級)。

   > **備註**
   >
   > - 如果您註冊付費支援計劃，您將負責至少一個月的 AWS Support訂閱。如需詳細資訊，請參閱 AWS Support 常見問答集。
   > - 如果您有 Enterprise On-Ramp 或企業支援計劃，請在 Change plan confirmation (變更計劃確認) 對話方塊中，聯絡 AWS Support 變更您的支援計劃。

5. 在 Change plan confirmation (變更計劃確認) 對話方塊中，您可以展開支援項目，以查看要從帳戶中新增或移除的功能。

   在 Pricing (定價) 中，您可以檢視新支援計劃的預估一次性費用。
6. 選擇 Accept and agree (接受並同意)。

相關資訊

如需有關 AWS Support 計劃的詳細資訊，請參閱AWS Support 常見問題集。您也可以在 Support Plans 主控台中選擇 Contact us (聯絡我們)。

若要關閉帳戶，請參閱 AWS Billing 使用者指南中的關閉帳戶。

AWS Trusted Advisor

Trusted Advisor 利用為數十萬名 AWS 客戶提供服務所學到的最佳實踐。 Trusted Advisor 檢查您的 AWS 環境，然後在存在機會時提出建議，以節省資金、改善系統可用性和效能，或協助縮小安全性漏洞。

如果您有基本或開發人員 Support 方案，則可以使用 Trusted Advisor 主控台存取「服務限制」類別中的所有檢查，並在「安全性」類別中進行六次檢查。

如果您擁有商業、企業級登入或企業 Support 方案，則可以使用 Trusted Advisor 主控台和 AWS Trusted Advisor API 存取所有 Trusted Advisor 檢查。您也可以使用 Amazon CloudWatch 事件來監控 Trusted Advisor 檢查的狀態。如需詳細資訊，請參閱 使用 Amazon 監控AWS Trusted Advisor檢查結果 EventBridge。

您可以 Trusted Advisor 在中存取 AWS Management Console。如需控制主控 Trusted Advisor 台存取權的詳細資訊，請參閱管理存取 AWS Trusted Advisor。

如需更多詳細資訊，請參閱 Trusted Advisor。

主題

開始使用 Trusted Advisor Recommendations

您可以使用 Trusted Advisor 主控台的 Trusted Advisor Recommendations 頁面檢閱 AWS 帳戶 的檢查結果，然後依照建議的步驟修正任何問題。例如，Trusted Advisor 可能會建議您刪除未使用的資源，以減少每月帳單金額，例如 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體。

您也可以使用 AWS Trusted Advisor API 來對 Trusted Advisor 檢查執行作業。如需詳細資訊，請參閱 AWS Trusted AdvisorAPI 參考

主題

登入 Trusted Advisor 主控台。

您可以在 Trusted Advisor 主控台中檢視檢查和每個檢查的狀態。

> **Note**
>
> 您必須擁有 AWS Identity and Access Management (IAM) 許可，才能存取 Trusted Advisor 主控台。如需詳細資訊，請參閱 管理存取 AWS Trusted Advisor。

登入 Trusted Advisor 主控台

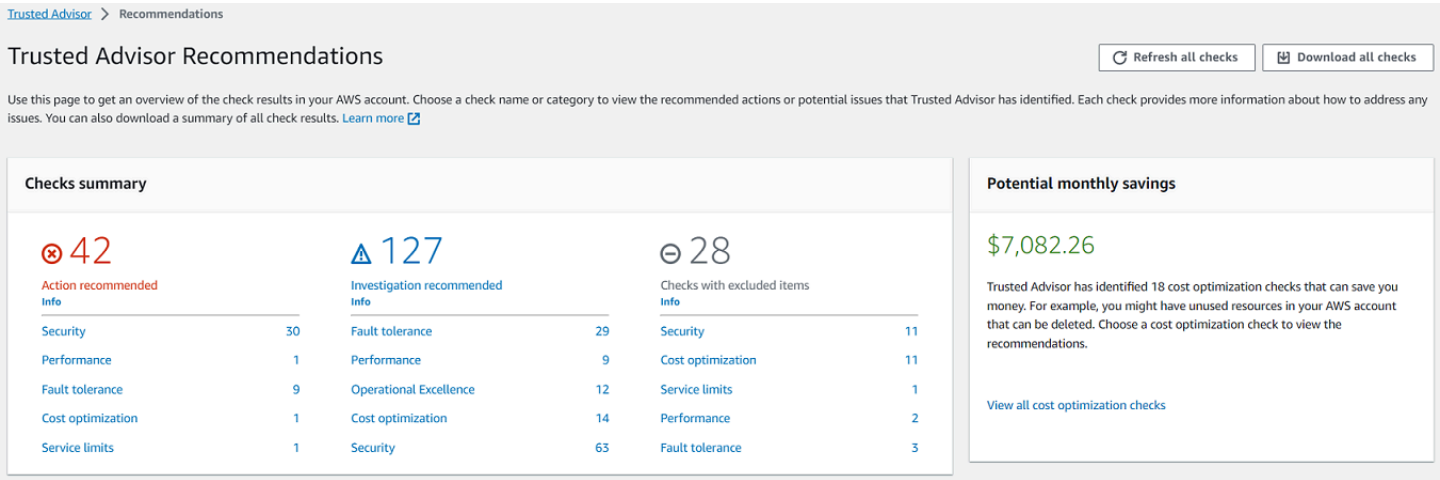
1. 登入 Trusted Advisor 主控台，網址是 https://console.aws.amazon.com/trustedadvisor/home。
2. 在 Trusted Advisor Recommendations 頁面上，檢視每種檢查類別的摘要：
   - Action recommended (建議採取動作) (紅色) - Trusted Advisor 建議為檢查執行的動作。例如，偵測 IAM 資源安全性問題的檢查可能會建議採取緊急步驟。

- Investigation recommended (建議進行調查) (黃色) - Trusted Advisor 偵測到可能的檢查問題。例如，達到資源配額的檢查可能會建議刪除未使用資源的方法。
- 含有已排除項目的檢查 (灰色) – 檢查中含已排除項目 (例如您想要檢查忽略的資源) 的檢查數量。例如，這可能是您不希望檢查評估的 Amazon EC2 執行個體。

3. 在 Trusted Advisor Recommendations 頁面上，您可以執行下列操作：
   - 若要重新整理帳戶中的所有檢查，請選擇 Refresh all checks (重新整理所有檢查)。
   - 若要建立包含所有檢查結果的 .xls 檔案，請選擇 Download all checks (下載所有檢查)。
   - 在 Checks Summary (檢查摘要) 底下，選擇 Security (安全性) 等檢查類別並檢視結果。
   - 在 Potential Monthly Savings (每月可能節省金額) 底下，可以檢視能為您的帳戶節省多少金額，以及建議的成本最佳化檢查。
   - 在 Recent changes (最近變更) 底下，您可以檢視過去 30 天內的檢查狀態變更。選擇檢查名稱，檢視該檢查的最新結果，或選擇箭頭圖示檢視下一頁。

Example ：Trusted Advisor Recommendations

下列範例顯示 AWS 帳戶 的檢查結果的摘要。



檢視檢查類別

您可以檢視下列檢查類別的檢查描述和結果：

- Cost Optimization (成本最佳化) - 可能為您省錢的建議。這些檢查會強調未使用的資源和減少帳單金額的機會。
- Performance (效能) - 可改善應用程式執行和回應速度的建議。
- Security (安全性) - 可讓 AWS 解決計劃更加安全的安全性設定建議。

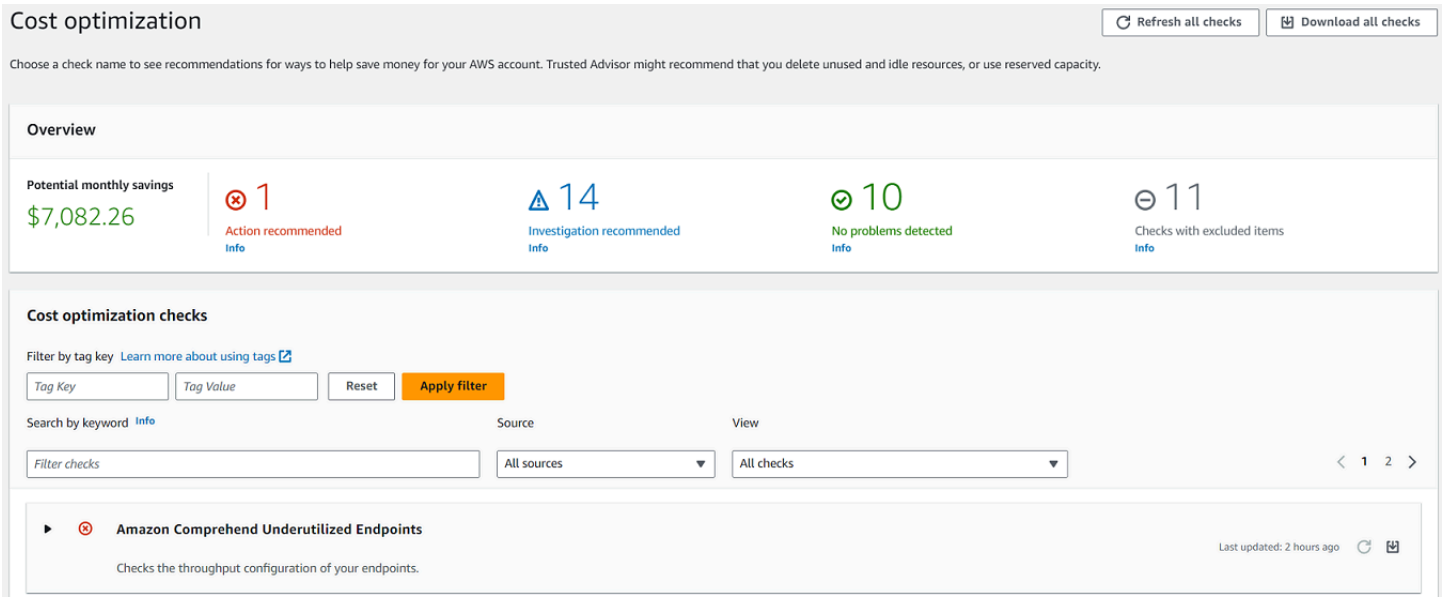
- Fault Tolerance (容錯能力) - 有助於提高 AWS 解決方案恢復力的建議。這些檢查會反白顯示備援不足與使用過度的資源。
- Service Limits (服務配額) - 檢查您帳戶的使用情況，以及您的帳戶是否接近或超過 AWS 服務和資源的限額 (也稱為配額)。
- 營運卓越 – 協助您有效且大規模營運 AWS 環境的建議。

檢視檢查類別

1. 前往 https://console.aws.amazon.com/trustedadvisor/home 登入 Trusted Advisor 主控台。
2. 在導覽窗格中選擇檢查類別。
3. 在類別頁面上，檢視每個檢查類別的摘要：
   - Action recommended (建議採取動作) (紅色) - Trusted Advisor 建議為檢查執行的動作。
   - Investigation recommended (建議進行調查) (黃色) - Trusted Advisor 偵測到可能的檢查問題。
   - No problems detected (未偵測到問題) (綠色) - Trusted Advisor 沒有偵測到檢查的問題。
   - 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。
4. 針對每項檢查，選擇重新整理圖示 () 來重新整理此檢查。
5. 選擇下載圖示 () 來建立包含此檢查結果的 .xls 檔案。

Example ：成本最佳化類別

下列範例顯示沒有任何問題的 16 項 (綠色) 檢查。



檢視特定檢查

展開檢查，檢視完整檢查說明、受影響的資源、任何建議的步驟，以及更多資訊的連結。

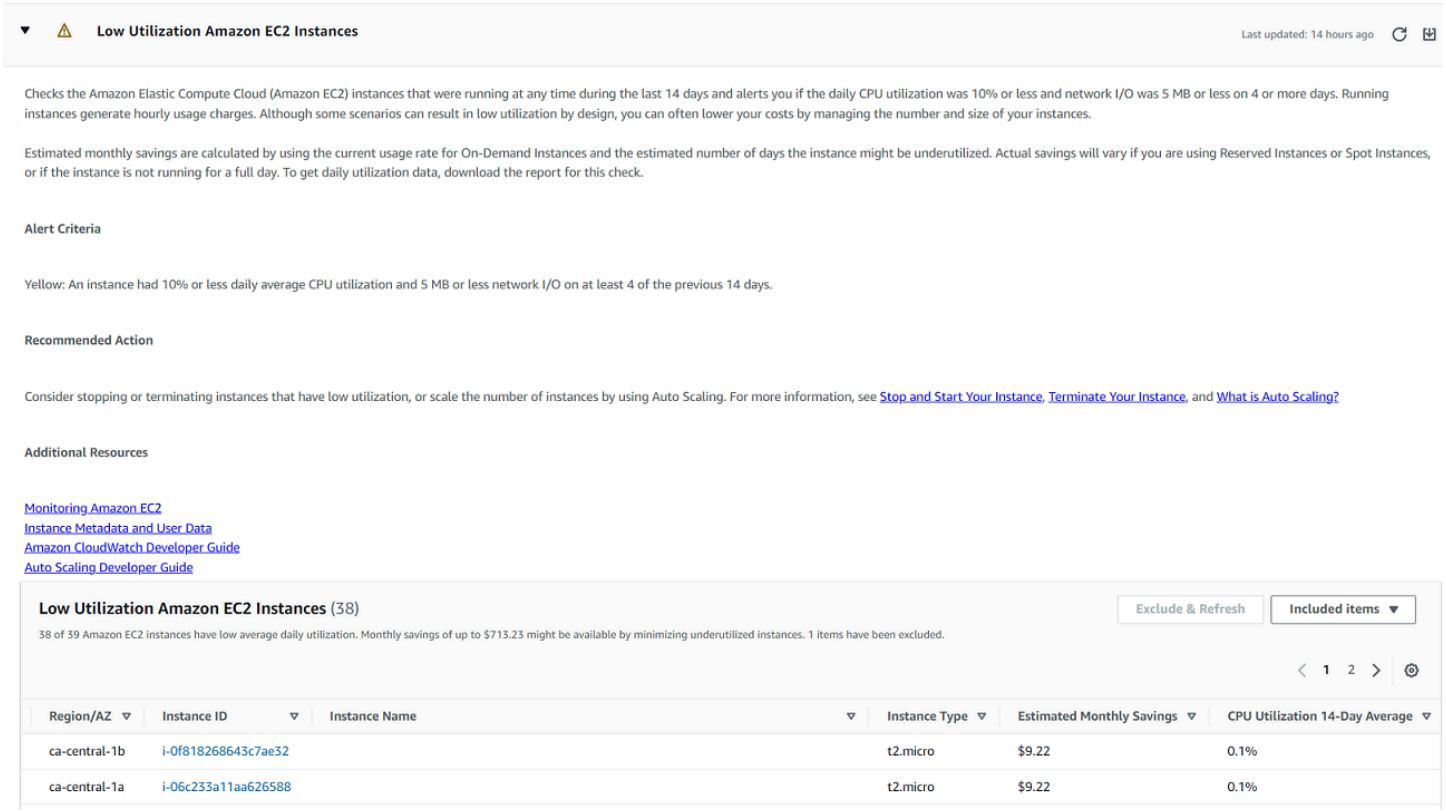
檢視特定檢查

1. 登入 Trusted Advisor 主控台，網址是 https://console.aws.amazon.com/trustedadvisor/home。
2. 在導覽窗格中選擇檢查類別。
3. 選擇檢查名稱，檢視說明及下列詳細資訊：
   - Alert Criteria (提醒條件) - 說明檢查狀態變更的臨界值。
   - Recommended Action (建議動作) - 說明此檢查的建議動作。
   - Additional Resources (其他資源) - 列出相關的 AWS 說明文件。
   - 列出您帳戶中受影響項目的表格。您可以在檢查結果中包含或排除這些項目。
4. (選用) 若要排除項目，使其不出現在檢查結果中，請執行下列動作：
   a. 選取項目並選擇 Exclude & Refresh (排除並重新整理)。
   b. 若要檢視所有排除項目，請選擇 Excluded items (排除的項目)。
5. (選用) 若要包含項目，讓檢查再次對其進行評估，請執行下列動作：
   a. 選擇 Excluded items (排除的項目)，選取項目，然後選擇 Include & Refresh (包含並重新整理)。
   b. 若要檢視所有包含的項目，請選擇 Included items 包含的項目)。

6. 選擇設定圖示
   ()。
   在 Preferences (偏好設定) 對話方塊中，您可以指定要顯示的項目數或屬性，然後選擇 Confirm (確認)。

Example ：成本最佳化檢查

下列低使用率 Amazon EC2 執行個體檢查會列出帳戶中受影響的執行個體。此檢查找出使用率低的 38 個 Amazon EC2 執行個體，並建議您停止或終止這些資源。



篩選檢查

在檢查類別頁面上，您可以指定要檢視的檢查結果。例如，您可以依偵測到帳戶中錯誤的檢查進行篩選，這樣就能先調查緊急問題。

如果您的檢查會評估帳戶中的項目，例如 AWS 資源，您可以使用標籤篩選器，只顯示具有指定標籤的項目。

篩選檢查

1. 登入 Trusted Advisor 主控台，網址是 https://console.aws.amazon.com/trustedadvisor/home。

2. 在導覽窗格或 Trusted Advisor Recommendations 頁面中，選擇檢查類別。
3. 對於 Search by keyword (依關鍵字搜尋)，請輸入檢查名稱或描述中的關鍵字來篩選結果。
4. 為 View (檢視) 清單指定要檢視的檢查：

   - All checks (所有檢查) - 列出此類別的所有檢查。
   - Action recommended (建議採取動作) - 列出建議您採取動作的檢查。這些檢查會以紅色反白。
   - Investigation recommended (建議進行調查) - 列出建議您採取可能動作的檢查。這些檢查會以黃色反白。
   - No problems detected (未偵測到問題) - 列出沒有任何問題的檢查。這些檢查會以綠色反白。
   - Checks with excluded items (含有已排除項目的檢查) - 列出您指定要從檢查結果中排除項目的檢查。
5. 如果將標籤新增至 AWS 資源，例如 Amazon EC2 執行個體或 AWS CloudTrail 追蹤記錄，您可以篩選結果，讓檢查只顯示具有指定標籤的項目。

   針對 Filter by tag (依標籤篩選)，輸入標籤索引鍵和值，然後選擇 Apply filter (套用篩選條件)。
6. 在檢查的表格中，檢查結果只會顯示具有指定索引鍵和值的項目。
7. 若要清除依標籤篩選的條件，請選擇 Reset (重設)。

相關資訊

如需有關 Trusted Advisor 標記功能的詳細資訊，請參閱下列主題：

- AWS Support 會為 Trusted Advisor 啟用標記功能
- 《AWS 一般參考》中的標記您的 AWS 資源。

重新整理檢查結果

您可以重新整理檢查以取得帳戶的最新結果。如果您有開發人員或基本支援計畫，可以登入 Trusted Advisor 主控台來重新整理檢查。如果您有商業、Enterprise On-Ramp 或企業支援計劃，Trusted Advisor 會每週自動重新整理您帳戶中的檢查。

重新整理 Trusted Advisor 檢查

1. 前往 https://console.aws.amazon.com/trustedadvisor 登入 AWS Trusted Advisor 主控台。
2. 在 Trusted Advisor Recommendations 或檢查類別頁面上，選擇 Refresh all checks (重新整理所有檢查)。

您也可以使用下列方式來重新整理特定檢查：

- 選擇個別檢查的重新整理圖示 ()。
- 使用 RefreshTrustedAdvisorCheck API 操作。

> **備註**
>
> - Trusted Advisor 每天會對某些檢查自動重新整理多次，例如 AWS Well-Architected 可靠性檢查的高風險問題。變更可能需要幾個小時才會出現在您的帳戶中。針對這些自動重新整理的檢查，您不能選擇重新整理圖示 () 來手動重新整理結果。
> - 如果為您的帳戶啟用 AWS Security Hub，則無法使用 Trusted Advisor 主控台重新整理 Security Hub 控制。如需詳細資訊，請參閱重新整理您的 Security Hub 問題清單。

下載檢查結果

您可以下載檢查結果，取得您帳戶中 Trusted Advisor 的概觀。您可以下載所有檢查或特定檢查的結果。

從 Trusted Advisor Recommendations 下載檢查結果

1. 前往 https://console.aws.amazon.com/trustedadvisor 登入 AWS Trusted Advisor 主控台。
   - 若要下載所有檢查結果，請在 Trusted Advisor Recommendations 或檢查類別頁面中，選擇 Download all checks (下載所有檢查)。
   - 若要下載特定檢查的檢查結果，請選擇檢查名稱，然後選擇下載圖示 ()。
2. 儲存或開啟 .xls 檔案。此檔案包含來自 Trusted Advisor 主控台的相同摘要資訊，例如檢查名稱、描述、狀態、受影響的資源等。

組織檢視

您可以設定組織檢視功能，為您 AWS 組織中的所有成員帳戶建立報告。如需詳細資訊，請參閱 AWS Trusted Advisor 的組織檢視。

Preferences (偏好設定)

您可以在管理Trusted Advisor 頁面上停用 Trusted Advisor。

在 Notifications (通知) 頁面上，您可以為檢查摘要設定每週電子郵件訊息。請參閱 設定通知偏好設定。

您可以在您的組織頁面上，啟用或停用 AWS Organizations 的受信任存取權。這是 AWS Trusted Advisor 的組織檢視 功能、Trusted Advisor Priority 和 Trusted Advisor Engage 的必要項目。

設定通知偏好設定

指定誰可以接收檢查結果和語言的每週 Trusted Advisor 電子郵件訊息。您每週會收到一封有關 Trusted Advisor Recommendations 檢查摘要的電子郵件通知。

Trusted Advisor Recommendations 的電子郵件通知不包含 Trusted Advisor Priority 的結果。如需詳細資訊，請參閱管理 Trusted Advisor Priority 通知。

設定通知偏好設定

1. 登入 Trusted Advisor 主控台，網址是 https://console.aws.amazon.com/trustedadvisor/home。
2. 在導覽窗格中，在 Preferences (偏好設定) 之下，選擇 Notifications (通知)。
3. 針對 Recommendations (建議)，選取要通知檢查結果的對象。您可以從 AWS Billing and Cost Management 主控台的 Account Settings (帳戶設定) 頁面新增和移除聯絡人。
4. 針對 Language (語言)，選擇電子郵件訊息的語言。
5. 選擇 Save your preferences (儲存喜好設定)。

設定組織檢視

如果您透過 AWS Organizations 設定帳戶，您可以為組織中的所有成員帳戶建立報告。如需詳細資訊，請參閱 AWS Trusted Advisor 的組織檢視。

停用 Trusted Advisor

若停用此服務，Trusted Advisor 將不會對您的帳戶執行任何檢查。嘗試存取 Trusted Advisor 主控台或使用 API 作業的任何人，都會收到存取遭拒的錯誤訊息。

停用 Trusted Advisor

1. 登入 Trusted Advisor 主控台，網址是 https://console.aws.amazon.com/trustedadvisor/home。
2. 在導覽窗格的偏好設定下，選擇管理 Trusted Advisor。
3. 在 Trusted Advisor 下，關閉 Enabled (已啟用)。此動作會為帳戶中的所有檢查停用 Trusted Advisor。
4. 然後，您可以手動刪除帳戶中的AWSServiceRoleForTrustedAdvisorTrusted Advisor。如需詳細資訊，請參閱為 Trusted Advisor刪除服務連結角色。

相關資訊

如需 Trusted Advisor 的詳細資訊，請參閱下列主題：

- 如何開始使用 Trusted Advisor？
- AWS Trusted Advisor 檢查參考

開始使用 Trusted Advisor API

AWS Trusted AdvisorAPI 參考適用於需要有關 Trusted Advisor API 操作和數據類型的詳細信息的程序員。此 API 可讓您存取帳戶或AWS組織內所有帳戶的Trusted Advisor建議。該 Trusted Advisor API 使用 HTTP 方法，該方法以 JSON 格式返回結果。

> **Note**
>
> - 您必須擁有商業、企業級支援或企業 Support 方案，才能使用 Trusted Advisor API
> - 如果您從沒有「商務」、「企業登入」或「企業 Support」方案的帳戶呼叫 AWS Trusted Advisor API，則會收到「拒絕存取」例外狀況。如需變更 Support 方案的詳細資訊，請參閱AWS支援。

您可以使用 AWS Trusted Advisor API 取得檢查清單及其說明、建議和建議資源。您也可以更新建議的生命週期。若要管理建議，請使用下列 API 作業：

- 使用ListChecks、ListRecommendationsGetRecommendation、和 ListRecommendationResourcesAPI 作業來檢視建議以及對應的帳戶和資源。
- 使用 UpdateRecommendationLifecycleAPI 作業更新由Trusted Advisor優先順序管理之建議的生命週期。
- ListOrganizationRecommendations、GetOrganizationRecommendationListOrganizationRecommendationR 和 UpdateOrganizationRecommendationLifecycleAPI 呼叫僅支援由Trusted Advisor優先順序管理的建議。這些建議也稱為優先順序建議。如果您已啟用 Trusted Advisor 優先順序，則可以從管理或委派的管理員帳戶檢視和管理您的優先順序建議。如果未啟用「優先順序」，則當您提出要求時，您會收到「拒絕存取」例外狀況。

若要取得更多資訊，請參閱 Sup AWS port 使用者指南AWS Trusted Advisor中的。

有關請求的驗證，請參閱簽名版本 4 簽名過程。

將 Trusted Advisor 做為 Web 服務使用

> **Note**
>
> Trusted Advisor在 2024 年，支援 API 將不 Support 援作業。請使用新的 AWS Trusted AdvisorAPI 以程式設計方式存取最佳實務檢查和建議

AWS Support 服務可讓您編寫與 AWS Trusted Advisor 進行互動的應用程式。此主題說明如何取得 Trusted Advisor 檢查清單、重新整理其中一個清單，以及取得詳細的檢查結果。這些任務以 Java 示範。如需其他語言支援的資訊，請參閱適用於 Amazon Web Services 的工具。

主題

- 取得可用的 Trusted Advisor 檢查清單
- 重新整理可用的 Trusted Advisor 檢查清單
- 輪詢 Trusted Advisor 檢查狀態變更
- 請求 Trusted Advisor 檢查結果
- 列印 Trusted Advisor 檢查的詳細資訊

取得可用的 Trusted Advisor 檢查清單

以下 Java 程式碼片段會建立一個 AWS Support 用戶端執行個體，您可以用它來呼叫所有 Trusted Advisor API 作業。接下來，程式碼會呼叫 DescribeTrustedAdvisorChecksAPI 作業，取得Trusted Advisor檢查清單及其對應的CheckId值。您可以使用這些資訊來建立使用者界面，讓使用者選擇他們要執行或重新整理的檢查。

```
private static AWSSupport createClient()
{
    return AWSSupportClientBuilder.defaultClient();
}
// Get the List of Available Trusted Advisor Checks
public static void getTAChecks() {
    // Possible language parameters: "en" (English), "ja" (Japanese), "fr" (French),
 "zh" (Chinese)
    DescribeTrustedAdvisorChecksRequest request = new
 DescribeTrustedAdvisorChecksRequest().withLanguage("en");
    DescribeTrustedAdvisorChecksResult result =
 createClient().describeTrustedAdvisorChecks(request);
    for (TrustedAdvisorCheckDescription description : result.getChecks()) {
        // Do something with check description.
        System.out.println(description.getId());
        System.out.println(description.getName());
    }
}
```

重新整理可用的 Trusted Advisor 檢查清單

以下 Java 程式碼片段會建立一個 AWS Support 用戶端執行個體，您可以用它來重新整理 Trusted Advisor 資料。

```
// Refresh a Trusted Advisor Check
// Note: Some checks are refreshed automatically, and they cannot be refreshed by using
 this operation.
// Specifying the check ID of a check that is automatically refreshed causes an
 InvalidParameterValue error.
public static void refreshTACheck(final String checkId) {
    RefreshTrustedAdvisorCheckRequest request = new
 RefreshTrustedAdvisorCheckRequest().withCheckId(checkId);
    RefreshTrustedAdvisorCheckResult result =
 createClient().refreshTrustedAdvisorCheck(request);
    System.out.println("CheckId: " + result.getStatus().getCheckId());
```

```
    System.out.println("Milliseconds until refreshable: " +
 result.getStatus().getMillisUntilNextRefreshable());
    System.out.println("Refresh Status: " + result.getStatus().getStatus());
}
```

輪詢 Trusted Advisor 檢查狀態變更

在您提交要求以執行Trusted Advisor檢查以產生最新狀態資料之後，您可以使用 DescribeTrustedAdvisorCheckRefreshStatusesAPI 作業來請求檢查執行的進度，以及當新資料準備好進行檢查時。

以下 Java 程式碼片段會使用與 CheckId 變數對應的值，取得以下部分請求的檢查狀態。此外，程式碼示範幾個 Trusted Advisor 服務的其他用法：

1. 您可以透過周遊包含在 DescribeTrustedAdvisorCheckRefreshStatusesResult 執行個體中的物件，以呼叫 getMillisUntilNextRefreshable。您可以使用傳回的值測試您是否希望您的程式碼進行重新整理檢查。
2. 如果 timeUntilRefreshable 等於零，您可以請求重新整理檢查。
3. 您可以使用傳回的狀態，持續輪詢狀態變更；程式碼片段會將輪詢間隔設定為建議的 10 秒。如果狀態為 enqueued 或 in_progress，迴圈將傳回並請求另一個狀態。如果呼叫傳回 successful，迴圈將會終止。
4. 最後，程式碼會傳回 DescribeTrustedAdvisorCheckResultResult 資料類型的執行個體，您可以用它來周遊檢查所產生的資訊。

附註：使用單一重新整理請求，再輪詢請求的狀態。

```
// Retrieves TA refresh statuses. Multiple checkId's can be submitted.
public static List<TrustedAdvisorCheckRefreshStatus> getTARefreshStatus(final String...
 checkIds) {
    DescribeTrustedAdvisorCheckRefreshStatusesRequest request =
            new
 DescribeTrustedAdvisorCheckRefreshStatusesRequest().withCheckIds(checkIds);
    DescribeTrustedAdvisorCheckRefreshStatusesResult result =
            createClient().describeTrustedAdvisorCheckRefreshStatuses(request);
    return result.getStatuses();
}
// Retrieves a TA check status, and checks to see if it has finished processing.
public static boolean isTACheckStatusInTerminalState(final String checkId) {
    // Since we only submitted one checkId to getTARefreshStatus, just retrieve the
 only element in the list.
```

```
    TrustedAdvisorCheckRefreshStatus status = getTARefreshStatus(checkId).get(0);
    // Valid statuses are:
    // 1. "none", the check has never been refreshed before.
    // 2. "enqueued", the check is waiting to be processed.
    // 3. "processing", the check is in the midst of being processed.
    // 4. "success", the check has succeeded and finished processing - refresh data is
 available.
    // 5. "abandoned", the check has failed to process.
    return status.getStatus().equals("abandoned") ||
 status.getStatus().equals("success");
}
// Enqueues a Trusted Advisor check refresh. Periodically polls the check refresh
 status for completion.
public static TrustedAdvisorCheckResult getFreshTACheckResult(final String checkId)
 throws InterruptedException {
    refreshTACheck(checkId);
    while(!isTACheckStatusInTerminalState(checkId)) {
        Thread.sleep(10000);
    }
    return getTACheckResult(checkId);
}
// Retrieves fresh TA check data whenever possible.
// Note: Some checks are refreshed automatically, and they cannot be refreshed by using
 this operation. This method
// is only functional for checks that can be refreshed using the
 RefreshTrustedAdvisorCheck operation.
public static void pollForTACheckResultChanges(final String checkId) throws
 InterruptedException {
    String checkResultStatus = null;
    do {
        TrustedAdvisorCheckResult result = getFreshTACheckResult(checkId);
        if (checkResultStatus != null && !checkResultStatus.equals(result.getStatus()))
 {
            break;
        }
        checkResultStatus = result.getStatus();
        // The rule refresh has completed, but due to throttling rules the checks may
 not be refreshed again
        // for a short period of time.
        // Since we only submitted one checkId to getTARefreshStatus, just retrieve the
 only element in the list.
        TrustedAdvisorCheckRefreshStatus refreshStatus =
 getTARefreshStatus(checkId).get(0);
        Thread.sleep(refreshStatus.getMillisUntilNextRefreshable());
```

```
    } while(true);
    // Signal that a TA check has changed check result status here.
}
```

請求 Trusted Advisor 檢查結果

選取所需詳細結果的檢查後，您可以使用 DescribeTrustedAdvisorCheckResultAPI 作業提交要求。

> **Tip**
>
> Trusted Advisor 檢查的名稱和描述可能會變更。建議您在程式碼中指定檢查 ID，以唯一識別某項檢查。您可以使用 DescribeTrustedAdvisorChecksAPI 作業取得檢查識別碼。

以下 Java 程式碼片段使用 (以上述程式碼片段取得的) `result` 變數參考的 `DescribeTrustedAdvisorChecksResult` 執行個體。在您提交請求執行該程式碼片段之後，其並非透過使用者界面以互動方式定義檢查，而是由每次 `result.getChecks().get(0)` 呼叫中指定索引值 0，以提交請求執行清單中的第一項檢查。接著，程式碼定義 `DescribeTrustedAdvisorCheckResultRequest` 執行個體，它會傳送到呼叫 `checkResult` 的 `DescribeTrustedAdvisorCheckResultResult` 執行個體。您可以使用此資料類型的成員結構，以檢視檢查的結果。

```
// Request a Trusted Advisor Check Result
public static TrustedAdvisorCheckResult getTACheckResult(final String checkId) {
    DescribeTrustedAdvisorCheckResultRequest request = new
 DescribeTrustedAdvisorCheckResultRequest()
            // Possible language parameters: "en" (English), "ja" (Japanese),
 "fr" (French), "zh" (Chinese)
            .withLanguage("en")
            .withCheckId(checkId);
    DescribeTrustedAdvisorCheckResultResult requestResult =
 createClient().describeTrustedAdvisorCheckResult(request);
    return requestResult.getResult();
}
```

附註：請求 Trusted Advisor 檢查結果並不會產生更新的結果資料。

列印 Trusted Advisor 檢查的詳細資訊

以下 Java 程式碼片段會逐一查看上個部分傳回的 `DescribeTrustedAdvisorCheckResultResult` 執行個體，以取得由 Trusted Advisor 檢查標記的資源清單。

```
// Print ResourceIds for flagged resources.
for (TrustedAdvisorResourceDetail flaggedResource :
    result1.getResult().getFlaggedResources())
{
    System.out.println(
        "The resource for this ResourceID has been flagged: " +
        flaggedResource.getResourceId());
}
```

AWS Trusted Advisor 的組織檢視

組織檢視可讓您檢視您 AWS Organizations 中所有帳戶的 Trusted Advisor 檢查。啟用此功能後，您可以建立報告來彙總組織中所有成員帳戶的檢查結果。此報告中包括每個帳戶的檢查結果摘要，以及有關受影響資源的資訊。例如，您可以使用報告，透過「IAM 使用」檢查來識別組織中有哪些帳戶使用 AWS Identity and Access Management(IAM)，或透過「Amazon S3 儲存貯體許可」檢查確認您是否有適用於 Amazon Simple Storage Service (Amazon S3) 的建議動作。

主題

- 先決條件
- 啟用組織檢視
- 重新整理 Trusted Advisor 檢查
- 建立組織檢視報告
- 檢視報告摘要
- 下載組織檢視報告
- 停用組織檢視
- 使用 IAM 政策允許存取組織檢視
- 使用其他 AWS 服務來檢視 Trusted Advisor 報告

先決條件

您必須符合下列要求才能啟用組織檢視：

- 此帳戶必須是 AWS 組織的成員。
- 您的組織必須啟用 Organizations 的所有功能。如需詳細資訊，請參閱 AWS Organizations 使用者指南中的啟用組織中的所有功能。
- 您組織中的管理帳戶必須有商業、Enterprise On-Ramp 或企業支援計劃。您可以在 AWS Support 中心或支援計劃頁面中找到您的支援計劃。請參閱比較 AWS Support 計劃。
- 您必須以管理帳戶 (或擔任的等效角色) 的使用者身分登入。無論您是以 IAM 使用者或 IAM 角色登入，都必須具備含有所需許可的政策。請參閱 使用 IAM 政策允許存取組織檢視。

啟用組織檢視

符合先決條件後，請依照下列步驟啟用組織檢視。啟用此功能後，會發生下列情況：

- Trusted Advisor 已在您的組織中啟用為信任的服務。如需詳細資訊，請參閱 AWS Organizations 使用者指南中的透過其他 AWS 服務啟用信任的存取權。
- `AWSServiceRoleForTrustedAdvisorReporting` 服務連結角色是為您組織中的管理帳戶建立的。這個角色包含 Trusted Advisor 代表您呼叫 Organizations 所需的許可。這個服務連結角色已鎖定，無法手動刪除。如需更多詳細資訊，請參閱 使用 Trusted Advisor的服務連結角色。

您可以從 Trusted Advisor 主控台啟用組織檢視。

啟用組織檢視

1. 以組織的管理帳戶管理員身分登入，並前往 https://console.aws.amazon.com/trustedadvisor 開啟 AWS Trusted Advisor 主控台。
2. 在導覽窗格的 Preferences (偏好設定) 中，選擇 Your organization (您的組織)。
3. 在使用 AWS Organizations 啟用受信任的存取權下，開啟已啟用。

> **Note**
>
> 為管理帳户啟用組織檢視不會為所有成員帳户提供相同的檢查。例如，如果您的成員帳户都具有基本支援，那麼這些帳户的檢查將不會與您的管理帳户相同。AWS Support 計畫確定哪些 Trusted Advisor 檢查帳户可適用於帳戶。

重新整理 Trusted Advisor 檢查

為組織建立報告之前，建議您先重新整理 Trusted Advisor 檢查的狀態。您不需重新整理 Trusted Advisor 檢查就可以下載報告，但報告中可能不含最新資訊。

如果您有商業、Enterprise On-Ramp 或企業支援計劃，Trusted Advisor 會每週自動重新整理您帳戶中的檢查。

> **Note**
>
> 如果您的組織中的帳戶具備開發人員或基本支援計劃，那些帳戶的使用者必須登入 Trusted Advisor 主控台才能重新整理檢查。您無法從組織的管理帳戶重新整理所有帳戶的檢查。

重新整理 Trusted Advisor 檢查

1. 前往 https://console.aws.amazon.com/trustedadvisor 登入 AWS Trusted Advisor 主控台。
2. 在 Trusted Advisor Recommendations 頁面，選擇 Refresh all checks (重新整理所有檢查)。這會重新整理您的帳戶中的所有檢查。

您也可以使用下列方式來重新整理特定檢查：

- 使用 RefreshTrustedAdvisorCheck API 作業。
- 選擇個別檢查的重新整理圖示 ()。

建立組織檢視報告

啟用組織檢視之後，您可以建立報告，以便檢視您組織的 Trusted Advisor 檢查結果。

最多可以建立 50 份報告。如果您建立超出此配額的報告，Trusted Advisor 會刪除最早的報告。刪除的報告無法復原。

建立組織檢視報告

1. 登入組織的管理帳戶，並前往 https://console.aws.amazon.com/trustedadvisor 開啟 AWS Trusted Advisor 主控台。
2. 在導覽窗格中，選擇 Organizational View (組織檢視)。
3. 選擇 Create report (建立報告)。
4. 根據預設，報告中包含所有 AWS 區域、檢查類別、檢查及資源狀態。在 Create report (建立報告) 頁面上，您可以使用篩選條件選項來自訂報告。例如，您可以清除 Region (區域) 的 All (全部) 選項，然後指定要包含在報告中的個別區域。

   a. 輸入報告的 Name (名稱)。
   b. 針對 Format (格式)，選擇 JSON 或 CSV。
   c. 針對 Region (區域)，指定 AWS 區域或選擇 All (全部)。
   d. 針對 Check category (檢查類別)，選擇檢查類別或選擇 All (全部)。
   e. 針對 Checks (檢查)，選擇該類別的特定檢查，或選擇 All (全部)。

   > **Note**
   >
   > Check category (檢查類別) 篩選條件會覆寫 Checks (檢查) 篩選條件。例如，如果您選擇 Security (安全性) 類別，然後選擇特定的檢查名稱，您的報告會包含該類別的所有檢查結果。若只要針對特定檢查建立報告，Check category (檢查類別) 中請保留預設的 All (全部) 值，然後選擇您的檢查名稱。

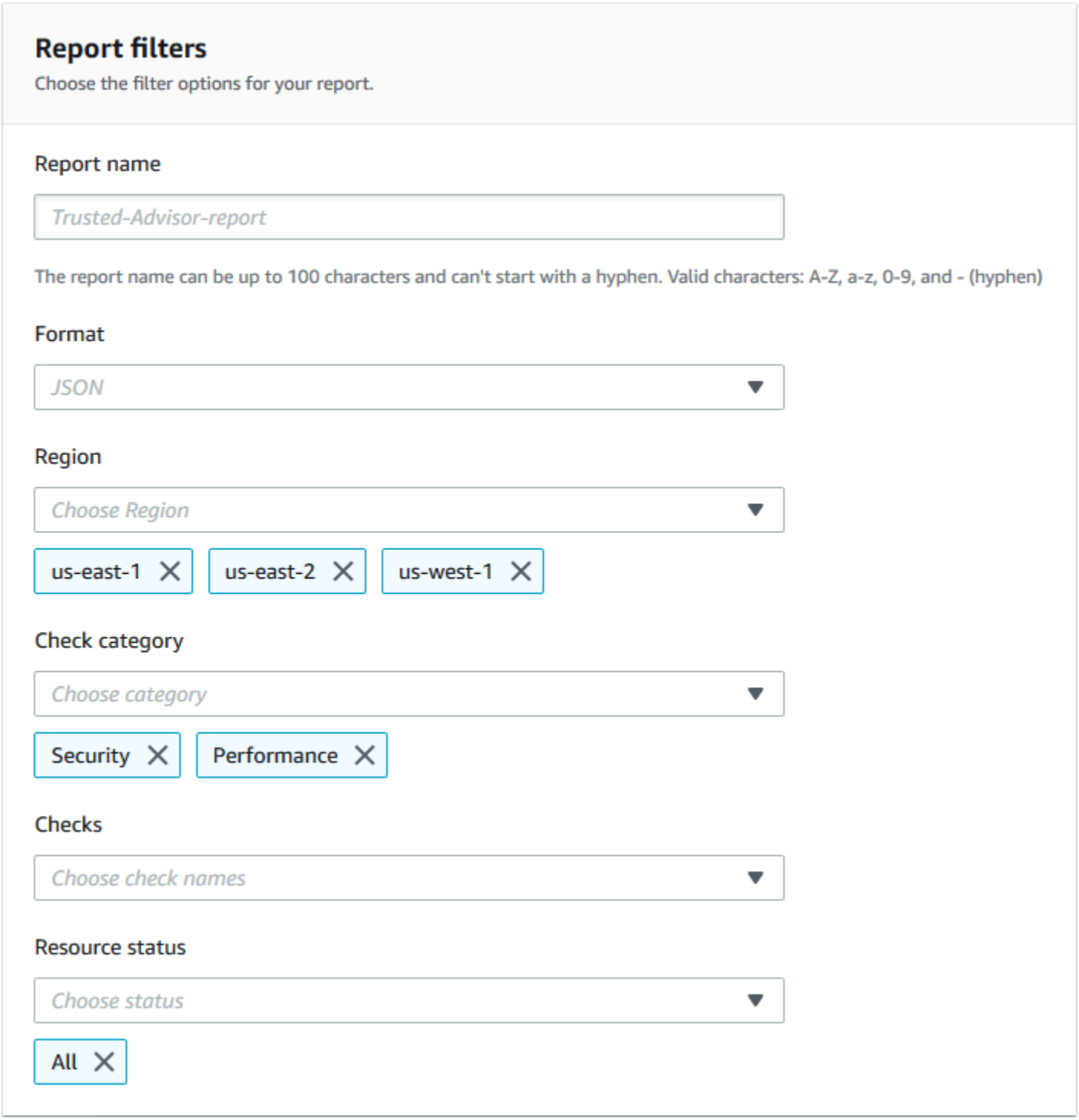
   f. 針對 Resource status (資源狀態)，選擇要篩選的狀態，例如 Warning (警告)，或選擇 All (全部)。
5. 針對 AWS Organization (AWS 組織)，選擇要包含在報告中的組織單位 (OU)。如需 OU 的詳細資訊，請參閱 AWS Organizations 使用者指南中的管理組織單位。
6. 選擇 Create report (建立報告)。

Example ：建立報告篩選條件選項

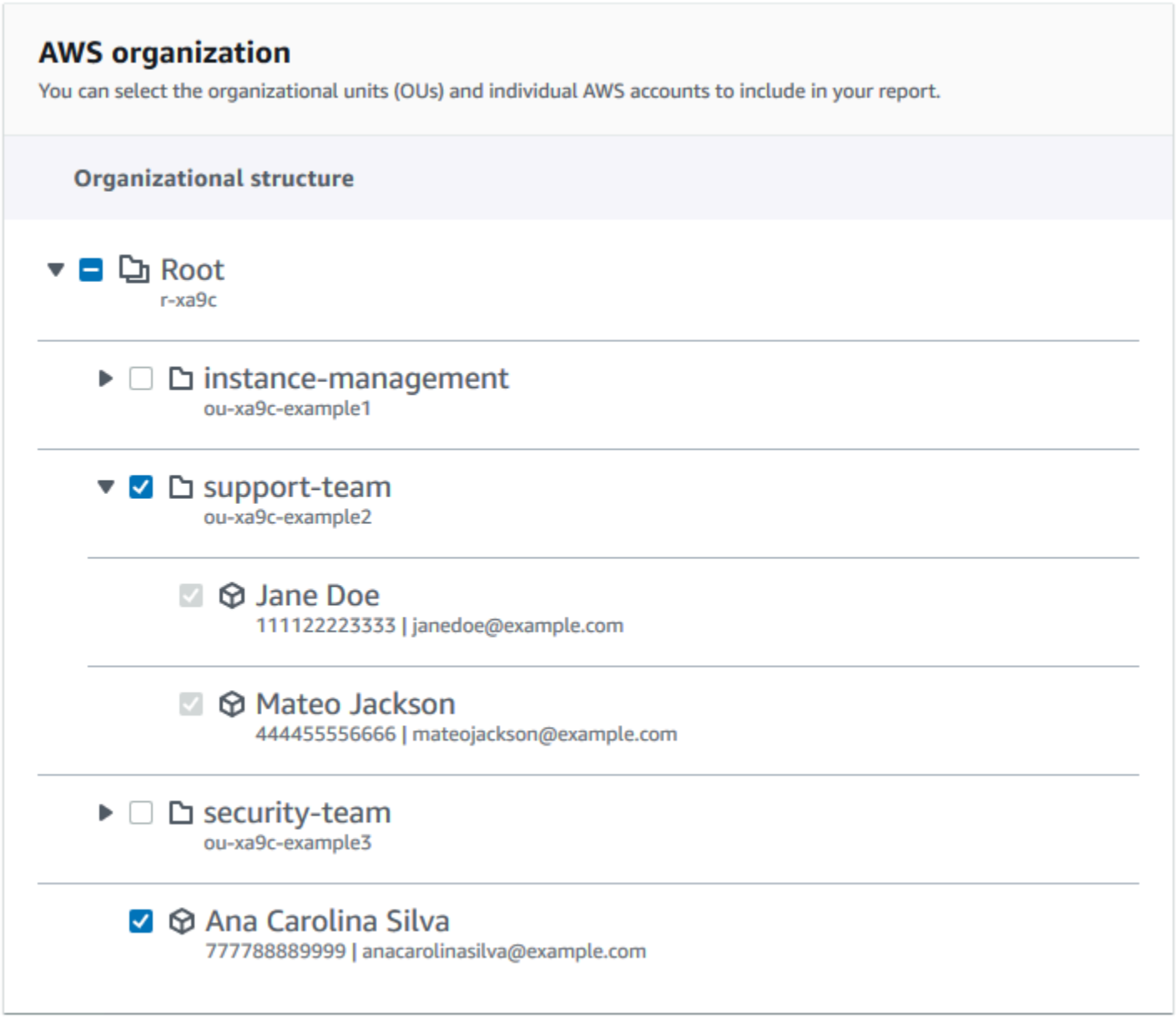
下列範例會為以下項目建立一份 JSON 報告：

- 三個 AWS 區域

- 所有 Security (安全性) 和 Performance (效能) 檢查



下列範例中，報告中包含 support-team OU 與屬於組織一部分的一個 AWS 帳戶。



備註

- 建立報告所需的時間，取決於組織中的帳戶數量和每個帳戶中的資源數量。
- 除非目前報告已執行六個小時以上，否則您無法一次建立多份報告。
- 如果頁面上未顯示報告，請重新整理頁面。

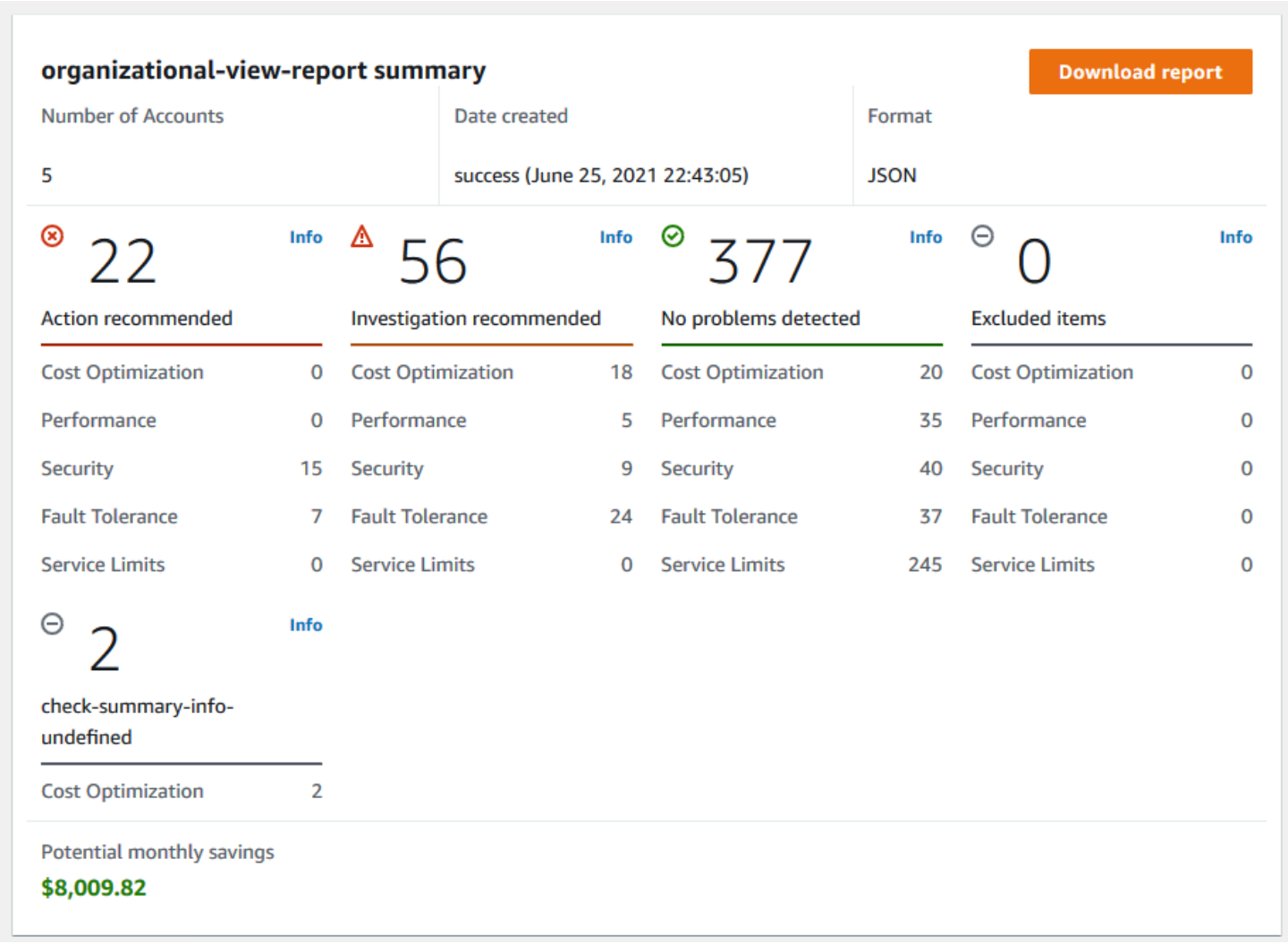
檢視報告摘要

報告準備就緒後，您可以從 Trusted Advisor 主控台檢視報告摘要。這可讓您快速檢視整個組織的檢查結果摘要。

檢視報告摘要

1. 登入組織的管理帳戶，並前往 https://console.aws.amazon.com/trustedadvisor 開啟 AWS Trusted Advisor 主控台。
2. 在導覽窗格中，選擇 Organizational View (組織檢視)。
3. 選擇報告名稱。
4. 在 Summary (摘要) 頁面上，檢視每個類別的檢查狀態。您也可以選擇 Download report (下載報告)。

Example ：組織的報告摘要



下載組織檢視報告

報告準備就緒後，可從 Trusted Advisor 主控台下載。此報告是包含三個檔案的 .zip 檔：

- `summary.json` - 包含每個檢查類別的檢查結果摘要。
- `schema.json` - 包含報告中指定檢查的結構描述。
- 資源檔案 (.json 或 .csv) - 包含組織中資源檢查狀態的詳細資訊。

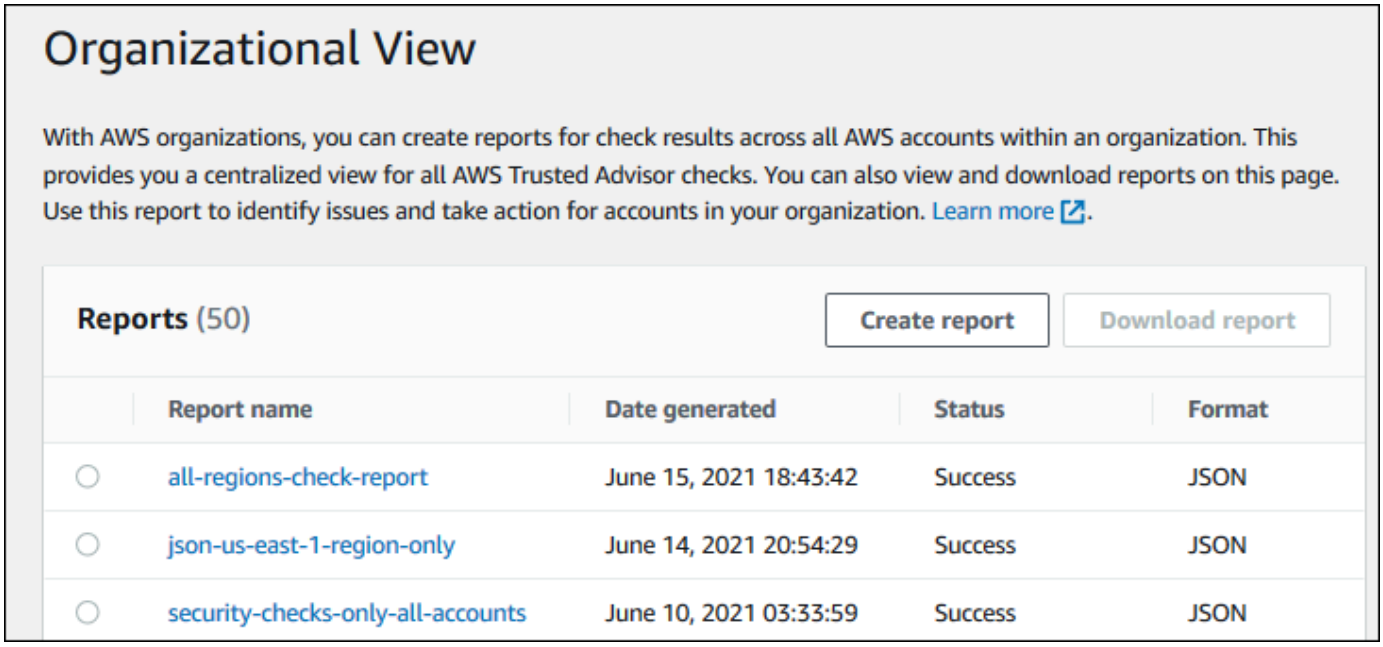
下載組織檢視報告

1. 登入組織的管理帳戶，並前往 https://console.aws.amazon.com/trustedadvisor 開啟 AWS Trusted Advisor 主控台。

2. 在導覽窗格中，選擇 Organizational View (組織檢視)。

   Organizational View (組織檢視) 頁面會顯示可供下載的報告。

3. 選取報告，選擇 Download report (下載報告)，然後儲存檔案。您一次只能下載一份報告。



4. 解壓縮檔案。

5. 使用文字編輯器開啟 `.json` 檔案，或使用試算表應用程式開啟 `.csv` 檔案。

> **Note**
>
> 如果報告大小為 5 MB 或更大，您可能會收到多個檔案。

Example ：summary.json 檔案

`summary.json` 檔案會顯示組織中的帳戶數量，以及每個類別的檢查狀態。

Trusted Advisor 使用以下顏色代碼進辨別檢查結果：

- `Green` - Trusted Advisor 沒有偵測到檢查有問題。
- `Yellow` - Trusted Advisor 偵測到可能的檢查問題。
- `Red` - Trusted Advisor 偵測到錯誤並建議針對檢查執行動作。
- `Blue` - Trusted Advisor 無法判斷檢查的狀態。

在下列範例中，兩個檢查是 Red、一個是 Green，還有一個是 Yellow。

```
{
    "numAccounts": 3,
    "filtersApplied": {
        "accountIds": ["123456789012","111122223333","111111111111"],
        "checkIds": "All",
        "categories": [
            "security",
            "performance"
        ],
        "statuses": "All",
        "regions": [
            "us-west-1",
            "us-west-2",
            "us-east-1"
        ],
        "organizationalUnitIds": [
            "ou-xa9c-EXAMPLE1",
            "ou-xa9c-EXAMPLE2"
        ]
    },
    "categoryStatusMap": {
        "security": {
            "statusMap": {
                "ERROR": {
                    "name": "Red",
                    "count": 2
                },
                "OK": {
                    "name": "Green",
                    "count": 1
                },
                "WARN": {
                    "name": "Yellow",
                    "count": 1
                }
            },
            "name": "Security"
        }
    },
    "accountStatusMap": {
        "123456789012": {
            "security": {
```

```
                "statusMap": {
                    "ERROR": {
                        "name": "Red",
                        "count": 2
                    },
                    "OK": {
                        "name": "Green",
                        "count": 1
                    },
                    "WARN": {
                        "name": "Yellow",
                        "count": 1
                    }
                },
                "name": "Security"
            }
        }
    }
}
```

Example ：schema.json 檔案

schema.json 檔案包含報告中檢查的結構描述。下列範例包含 IAM 密碼政策 (Yw2K9puPzl) 和 IAM 金鑰輪換 (DqdJqYeRm5) 檢查的 ID 和屬性。

```
{
    "Yw2K9puPzl": [
        "Password Policy",
        "Uppercase",
        "Lowercase",
        "Number",
        "Non-alphanumeric",
        "Status",
        "Reason"
    ],
    "DqdJqYeRm5": [
        "Status",
        "IAM User",
        "Access Key",
        "Key Last Rotated",
        "Reason"
    ],
    ...
```

```
}
```

Example ：resources.csv 檔案

`resources.csv` 檔案包含組織中資源的相關資訊。此範例顯示幾個出現在報告中的資料欄，如下所示：

- 受影響帳戶的帳戶 ID
- Trusted Advisor 檢查 ID
- 資源 ID
- 報告的時間戳記
- Trusted Advisor 檢查的完整名稱
- Trusted Advisor 檢查類別
- 上層組織單位 (OU) 或根的帳戶 ID

AccountId	CheckId	ResourceId	TimeStamp	CheckName	Category
1.11122E+11	Qch7DwouX1	LnW14f1M40NMjmMLvY5(	1.58983E+12	Low Utilization Amazon EC2 Instances	Cost Optimizing
1.11122E+11	HCP4007jGY	dJrQZXw36ZdswBeo9WUl	1.58983E+12	Security Groups - Specific Ports Unrestricted	Security
1.11122E+11	HCP4007jGY	1hzakmTbWd5UmAM_a0L	1.58983E+12	Security Groups - Specific Ports Unrestricted	Security
4.44456E+11	1iG5NDGVre	dJrQZXw36ZdswBeo9WUl	1.58983E+12	Security Groups - Unrestricted Access	Security
4.44456E+11	1iG5NDGVre	1hzakmTbWd5UmAM_a0L	1.58983E+12	Security Groups - Unrestricted Access	Security
4.44456E+11	Pfx0RwqBli	vioZmlba45kf2JWIe_W0j5	1.58983E+12	Amazon S3 Bucket Permissions	Security
4.44456E+11	Pfx0RwqBli	wAvASS3YOwy6WWxIBHf	1.58983E+12	Amazon S3 Bucket Permissions	Security
1.23457E+11	Pfx0RwqBli	LIc4zRaUSiIGRSlmqaMa5V	1.58983E+12	Amazon S3 Bucket Permissions	Security
1.23457E+11	Pfx0RwqBli	gWB27TMXof2evYzMSYBg	1.58983E+12	Amazon S3 Bucket Permissions	Security
7.77789E+11	Pfx0RwqBli	M3LBsF0e15Cl9Mxppapcx	1.58983E+12	Amazon S3 Bucket Permissions	Security
7.77789E+11	Yw2K9puPzl	47DEQpj8HBSa-_TImW-5J(	1.58983E+12	IAM Password Policy	Security
7.77789E+11	H7IgTzjTYb	1xHQ5ovV8bS0H1Z-t7Kbib	1.58983E+12	Amazon EBS Snapshots	Fault Tolerance
7.77789E+11	wuy7G1zxql	10F6p6VAF0F-MuL6Dc-dl1	1.58983E+12	Amazon EC2 Availability Zone Balance	Fault Tolerance

如果資源層級存在檢查結果，則資源檔案只會包含項目。由於下列原因，您可能無法在報告中看到檢查：

- 某些檢查 (例如根帳戶上的 MFA) 沒有資源且不會顯示在報告中。沒有資源的檢查會改為顯示在 `summary.json` 檔案中。
- 有些檢查只會顯示 `Red` 或 `Yellow` 的資源。如果所有資源都是 `Green`，可能不會出現在您的報告中。
- 如果未針對需要檢查的服務啟用帳戶，則該檢查可能不會出現在報告中。例如，如果您沒有在組織中使用 Amazon Elastic Compute Cloud 預留執行個體，報告中就不會顯示 Amazon EC2 Reserved Instance Lease Expiration 檢查。

- 帳戶尚未重新整理檢查結果。具有基本或開發人員支援計劃的使用者登入 Trusted Advisor 主控台時，可能會發生此情況。如果您有商業、Enterprise On-Ramp 或企業支援計劃，使用者在註冊帳戶後最多可能需要一週的時間，才能看到檢查結果。如需更多詳細資訊，請參閱 重新整理 Trusted Advisor 檢查。
- 如果只有組織的管理帳戶啟用檢查建議，則報告不會包含組織中其他帳戶的資源。

針對資源檔案，您可以使用一般軟體 (例如 Microsoft Excel) 來開啟 .csv 檔案格式。您可以使用 .csv 檔案來對組織內所有帳戶的所有檢查進行一次性分析。如果您想要搭配應用程式使用報告，可以將報告下載為 .json 檔案。

.json 檔案格式提供比 .csv 檔案格式更多的靈活性，適用於進階使用案例，例如多個資料集的彙總和進階分析。例如，您可搭配 AWS 服務 (例如 Amazon Athena) 使用 SQL 介面，對您的報告執行查詢。您也可以使用 Amazon QuickSight 來建立儀表板並將資料視覺化。如需更多詳細資訊，請參閱 使用其他 AWS 服務來檢視 Trusted Advisor 報告。

停用組織檢視

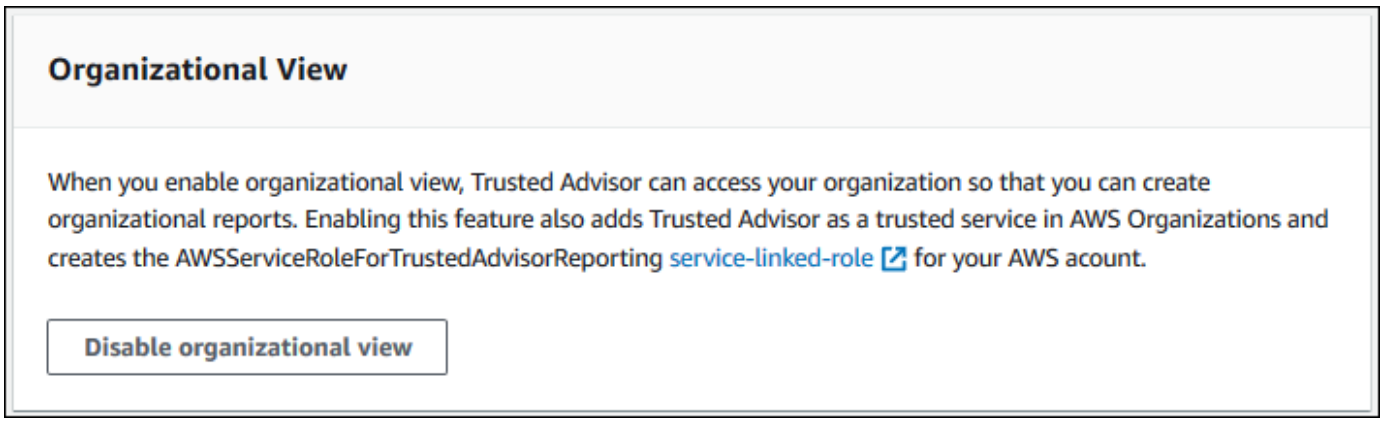
依照此程序停用組織檢視。您必須登入組織的管理帳戶，或擔任具有必要許可的角色，才能停用此功能。您無法從組織中的其他帳戶停用此功能。

停用此功能後，會發生下列情況：

- Organizations 中做為受信任服務的 Trusted Advisor 會遭移除。
- 組織管理帳戶中的 `AWSServiceRoleForTrustedAdvisorReporting` 服務連結角色會解除鎖定。這表示您可以視需要手動刪除它。
- 您無法建立、檢視或下載組織的報告。若要存取先前建立的報告，必須從 Trusted Advisor 主控台重新啟用組織檢視。請參閱 啟用組織檢視。

停用 Trusted Advisor 的組織檢視

1. 登入組織的管理帳戶，並前往 https://console.aws.amazon.com/trustedadvisor 開啟 AWS Trusted Advisor 主控台。
2. 在導覽窗格中，選擇 Preferences (偏好設定)。
3. 在 Organizational View (組織檢視) 底下，選擇 Disable organizational view (停用組織檢視)。



停用組織檢視之後，Trusted Advisor 就不會再彙總來自組織中其他 AWS 帳戶的檢查。不過 `AWSServiceRoleForTrustedAdvisorReporting` 服務連結角色會留在組織的管理帳戶上，直到您透過 IAM 主控台、IAM API 或 AWS Command Line Interface(AWS CLI) 刪除。如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

> **Note**
>
> 您可以使用其他 AWS 服務來查詢和視覺化組織檢視報告的資料。如需詳細資訊，請參閱下列資源：
>
> - AWS 管理與控管部落格中的透過 AWS Organizations 大規模檢視 AWS Trusted Advisor 的建議
> - 使用其他 AWS 服務來檢視 Trusted Advisor 報告

使用 IAM 政策允許存取組織檢視

您可以使用以下 AWS Identity and Access Management (IAM) 政策，允許帳戶中的使用者或角色在 AWS Trusted Advisor 中存取組織檢視。

Example ：組織檢視的完整存取權限

以下政策允許完整存取組織檢視功能。擁有這些許可的使用者可以執行下列動作：

- 啟用和停用組織檢視
- 建立、檢視及下載報告

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadStatement",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:DescribeOrganization",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "trustedadvisor:DescribeAccount",
                "trustedadvisor:DescribeChecks",
                "trustedadvisor:DescribeCheckSummaries",
                "trustedadvisor:DescribeAccountAccess",
                "trustedadvisor:DescribeOrganization",
                "trustedadvisor:DescribeReports",
                "trustedadvisor:DescribeServiceMetadata",
                "trustedadvisor:DescribeOrganizationAccounts",
                "trustedadvisor:ListAccountsForParent",
                "trustedadvisor:ListRoots",
                "trustedadvisor:ListOrganizationalUnitsForParent"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateReportStatement",
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:GenerateReport"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ManageOrganizationalViewStatement",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess",
                "trustedadvisor:SetOrganizationAccess"
            ],
```

```
            "Resource": "*"
        },
        {
            "Sid": "CreateServiceLinkedRoleStatement",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting"
        }
    ]
}
```

Example ：組織檢視的讀取存取權

以下政策允許唯讀存取 Trusted Advisor 的組織檢視功能。具有這些許可的使用者只能檢視和下載現有的報告。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadStatement",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:DescribeOrganization",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "trustedadvisor:DescribeAccount",
                "trustedadvisor:DescribeChecks",
                "trustedadvisor:DescribeCheckSummaries",
                "trustedadvisor:DescribeAccountAccess",
                "trustedadvisor:DescribeOrganization",
                "trustedadvisor:DescribeReports",
                "trustedadvisor:ListAccountsForParent",
                "trustedadvisor:ListRoots",
                "trustedadvisor:ListOrganizationalUnitsForParent"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

您也可以建立自己 IAM 政策。如需詳細資訊，請參閱 IAM 使用者指南中的建立 IAM 政策。

> **Note**
>
> 如果您已在帳戶中啟用 AWS CloudTrail，下列角色可能會出現在您的日誌項目中：
>
> - `AWSServiceRoleForTrustedAdvisorReporting` - Trusted Advisor 用於存取您組織中帳戶的服務連結角色。
> - `AWSServiceRoleForTrustedAdvisor` - Trusted Advisor 用於存取您組織中服務的服務連結角色。
>
> 如需服務連結角色的詳細資訊，請參閱使用 Trusted Advisor的服務連結角色。

使用其他 AWS 服務來檢視 Trusted Advisor 報告

請依照本教學課程，使用其他 AWS 服務上傳和檢視您的資料。在本主題中，您將建立 Amazon Simple Storage Service (Amazon S3) 儲存貯體來存放報告，並建立 AWS CloudFormation 範本，用來在您的帳戶中建立資源。然後，您可以使用 Amazon Athena 來對報告進行分析或執行查詢，或使用 Amazon QuickSight 在儀表板中將這些資料視覺化。

如需將報告資料視覺化的資訊和範例，請參閱 AWS 管理與控管部落格中的透過 AWS Organizations 大規模檢視 AWS Trusted Advisor 的建議。

先決條件

開始本教學課程前，您必須符合下列要求：

- 以具有管理員許可的 AWS Identity and Access Management (IAM) 使用者身分登入。
- 使用美國東部 (維吉尼亞北部) AWS 區域快速設定您的 AWS 服務和資源。
- 建立 Amazon QuickSight 帳戶。如需詳細資訊，請參閱 Amazon QuickSight 使用者指南中的開始使用 Amazon QuickSight 中的資料分析功能。

將報告上傳到 Amazon S3

下載 `resources.json` 報告後，請將檔案上傳至 Amazon S3。您必須使用美國東部 (維吉尼亞北部) 區域中的儲存貯體。

將報告上傳至 Amazon S3 儲存貯體

1. 前往 https://console.aws.amazon.com/ 登入 AWS Management Console。
2. 使用 Region selector (區域選擇器)，選擇美國東部 (維吉尼亞北部) 區域。
3. 開啟位於 https://console.aws.amazon.com/s3/ 的 Amazon S3 主控台。
4. 從儲存貯體清單中選擇一個 S3 儲存貯體，然後複製名稱。您會在接下來的程序中用到這個名稱。
5. 在 *`bucket-name (######)`* 頁面上，選擇 Create folder (建立資料夾)，輸入名稱 **`folder1`**，然後選擇 Save (儲存)。
6. 選擇 folder1。
7. 在 folder1 中，選擇 Upload (上傳)，然後選擇 `resources.json` 檔案。
8. 選擇 Next (下一步)，保留預設選項，然後選擇 Upload (上傳)。

> **Note**
>
> 如果您將新報告上傳至此儲存貯體，請重新命名 `.json` 檔案，這樣就不會覆寫現有的報告。例如，您可以為每個檔案新增時間戳記，例如 `resources-timestamp.json`、`resources-timestamp2.json`，以此類推。

使用 AWS CloudFormation 建立資源

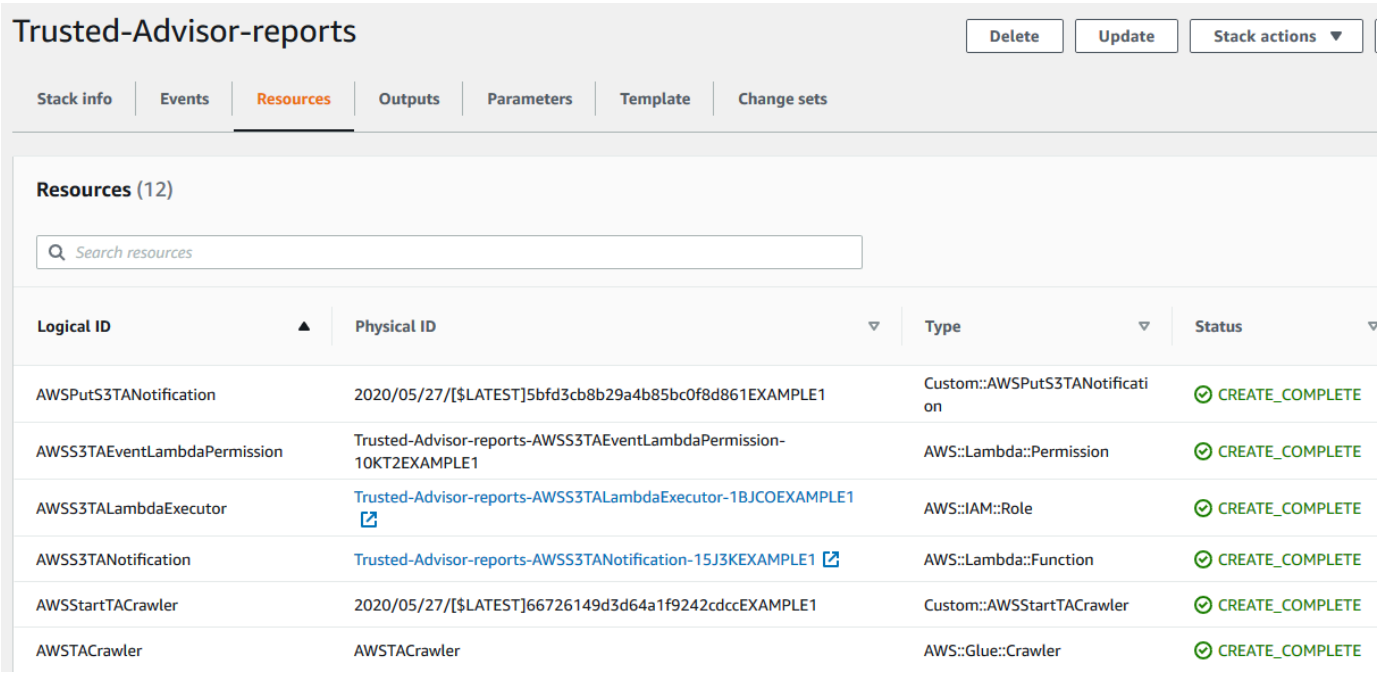
將報告上傳到 Amazon S3 後，請將下列 YAML 範本上傳到 AWS CloudFormation。這個範本會告訴 AWS CloudFormation 需為您的帳戶建立哪些資源，以便讓其他服務可以使用 S3 儲存貯體中的報告資料。範本會為 IAM、AWS Lambda 及 AWS Glue 建立資源。

使用 AWS CloudFormation 建立資源

1. 下載 trusted-advisor-reports-template.zip 檔案。
2. 解壓縮檔案。
3. 在文字編輯器中開啟範本檔案。
4. 對於 `BucketName` 和 `FolderName` 參數，將 *`your-bucket-name-here`* 和 *`folder1`* 的值取代為您帳戶中的儲存貯體名稱和資料夾名稱。

5. 儲存檔案。
6. 在以下網址開啟 AWS CloudFormation 主控台：https://console.aws.amazon.com/cloudformation。
7. 如果您尚未執行此步驟，請在 Region selector (區域選擇器) 中選擇美國東部 (維吉尼亞北部) 區域。
8. 在導覽窗格中，選擇 Stacks (堆疊)。
9. 選擇 Create stack (建立堆疊)，再選擇 With new resources (standard) (使用新資源 (標準))。
10. 在 Create stack (建立堆疊) 頁面上的 Specify Template (指定範本) 底下，選擇 Upload a template file (上傳範本檔案)、然後選擇 Choose file (選擇檔案)。
11. 選擇 YAML 檔案，然後選擇 Next (下一步)。
12. 在 Specify Details (指定詳細資訊) 頁面上，輸入堆疊名稱 (例如 **`Organizational-view-Trusted-Advisor-reports`**)，然後選擇 Next (下一步)。
13. 在 Configure stack options (設定堆疊選項) 頁面上，保留預設選項，然後選擇 Next (下一步)。
14. 在 Review (檢閱) **`Organizational-view-Trusted-Advisor-reports`** 頁面上，檢視您的選項。在頁面底部，選取 I acknowledge that AWS CloudFormation might create IAM resources (我知道 AWS CloudFormation 可能會建立 IAM 資源) 的核取方塊。
15. 選擇 Create Stack (建立堆疊)。

    建立堆疊大約需要 5 分鐘。
16. 堆疊成功建立之後，會顯示 Resources (資源) 索引標籤，如以下範例所示。



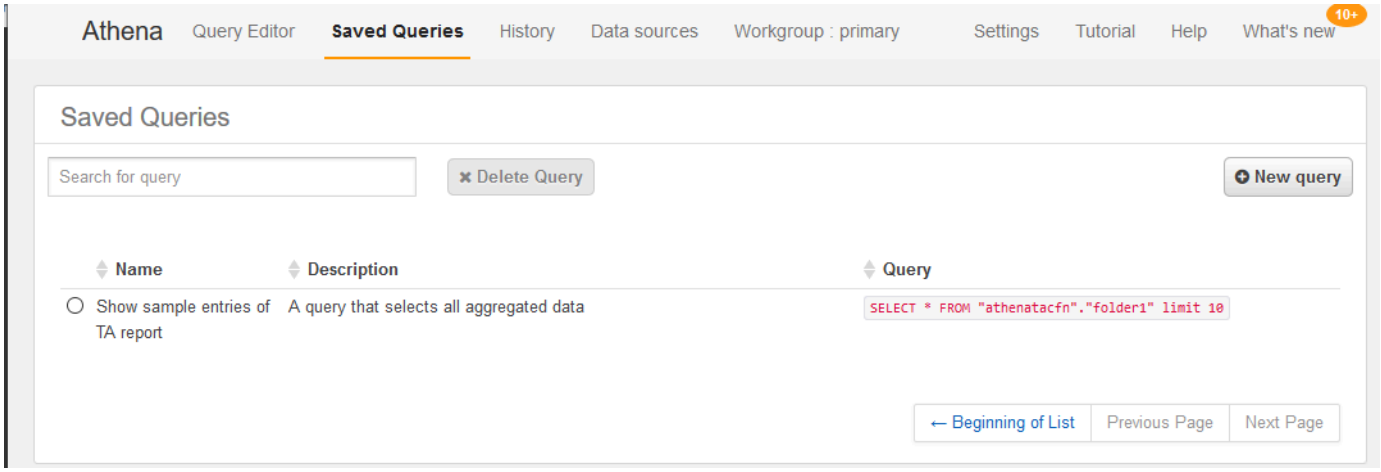
在 Amazon Athena 中查詢資料

您擁有資源之後，就可以在 Athena 中檢視資料。使用 Athena 建立查詢並分析報告的結果，例如查詢組織中帳戶的特定檢查結果。

> **備註**
>
> - 使用美國東部 (維吉尼亞北部) 區域。
> - 如果您是初次使用 Athena，您必須先指定查詢結果位置，才能對報告執行查詢。建議您為此位置指定不同的 S3 儲存貯體。如需詳細資訊，請參閱 Amazon Athena 使用者指南中的指定查詢結果位置。

在 Athena 中查詢資料

1. 前往 https://console.aws.amazon.com/athena/ 開啟 Athena 主控台。
2. 如果您尚未執行此步驟，請在 Region selector (區域選擇器) 中選擇美國東部 (維吉尼亞北部) 區域。
3. 選擇 Saved Queries (已儲存的查詢)，並在搜尋欄位中輸入 **`Show sample`**。
4. 選擇顯示的查詢，例如 Show sample entries of TA report (顯示 TA 報告的範例項目)。



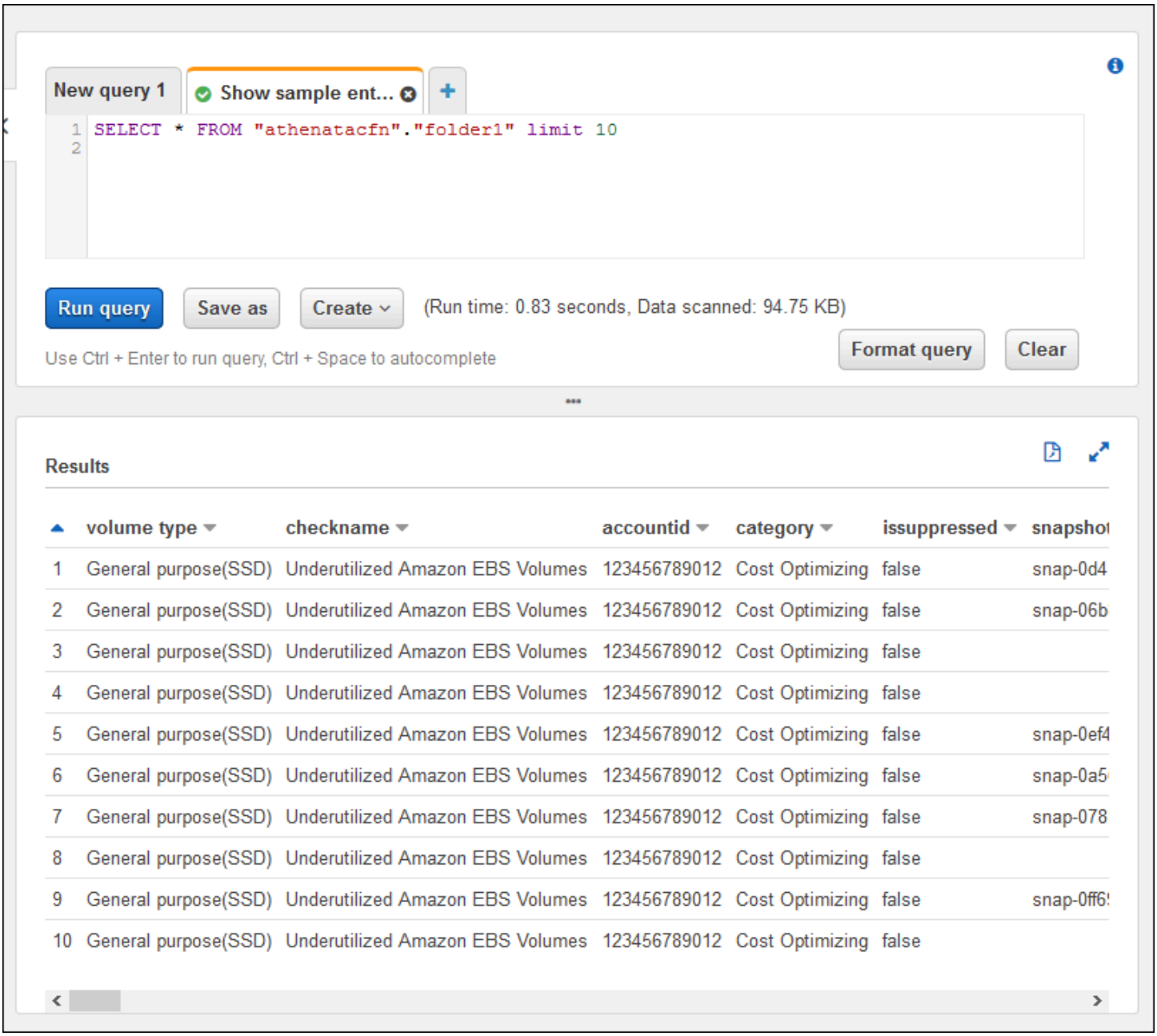
查詢看起來應該如下所示。

```
SELECT * FROM "athenatacfn"."folder1" limit 10
```

5. 選擇 Run query (執行查詢)。您的查詢結果會顯示。

Example ：Athena 查詢

下列範例顯示報告中的 10 個範例項目。



	volume type	checkname	accountid	category	issuppressed	snapshot
1	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-0d4
2	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-06b
3	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	
4	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	
5	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-0ef4
6	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-0a5
7	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-078
8	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	
9	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-0ff6
10	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	

如需詳細資訊，請參閱 Amazon Athena 使用者指南中的使用 Amazon Athena 執行 SQL 查詢。

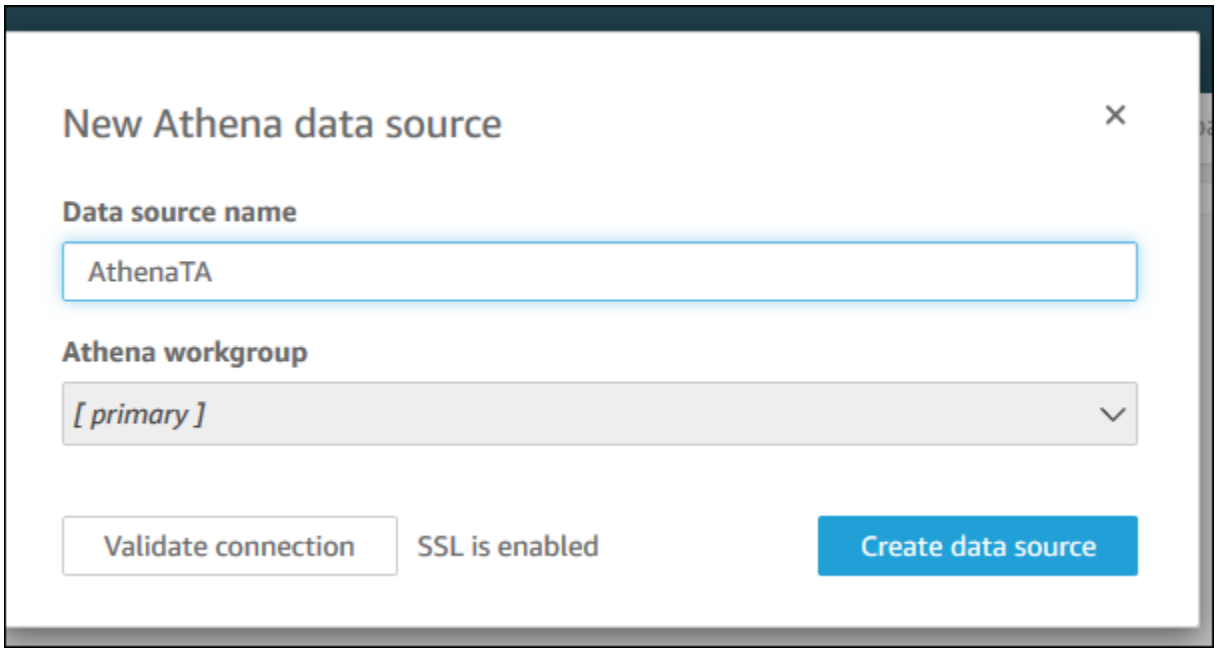
在 Amazon QuickSight 中建立儀表板

您也可以設定 Amazon QuickSight，以便在儀表板中檢視資料，並將您的報告資訊視覺化。

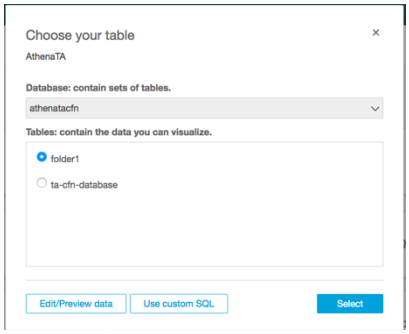
> **Note**
>
> 您必須使用美國東部 (維吉尼亞北部) 區域。

在 Amazon QuickSight 中建立儀表板

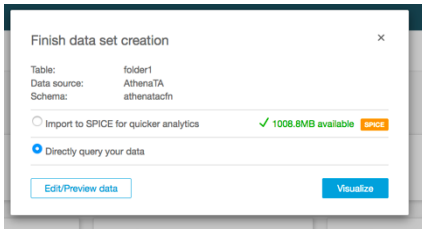
1. 導覽至 Amazon QuickSight 主控台並登入您的帳戶。
2. 選擇 New analysis (新增分析)、New dataset (新增資料集)，然後選擇 Athena。
3. 在 New Athena data source (新增 Athena 資料來源) 對話方塊中，輸入資料來源名稱 (例如 AthenaTA)，然後選擇 Create data source (建立資料來源)。



4. 在 Choose your table (選擇表格) 對話方塊中，選擇 athenatacfn 表格，選擇 folder1，然後選擇 Select (選取)。



5. 在 Finish data set creation (完成資料集建立) 對話方塊中，選擇 Directly query your data (直接查詢資料)，然後選擇 Visualize (視覺化)。



您現在可以在 Amazon QuickSight 中建立儀表板。如需詳細資訊，請參閱 Amazon QuickSight 使用者指南中的使用儀表板。

Example ：Amazon QuickSight 儀表板

下列範例儀表板顯示有關 Trusted Advisor 檢查的資訊，如下所示：

- 受影響的帳戶 ID
- 各 AWS 區域的摘要
- 檢查類別
- 檢查狀態
- 每個帳戶的報告中項目數

> **Note**
>
> 如果在建立儀表板時出現許可錯誤，請確認 Amazon QuickSight 可以使用 Athena。如需詳細資訊，請參閱 Amazon QuickSight 使用者指南中的無法連線至 Amazon Athena。

如需將報告資料視覺化的詳細資訊和範例，請參閱 AWS 管理與控管部落格中的透過 AWS Organizations 大規模檢視 AWS Trusted Advisor 的建議。

疑難排解

如果您在本教學課程中遇到問題，請參閱下列疑難排解秘訣。

我沒有在報告中看到最新的資料

建立報告時，組織檢視功能不會自動重新整理您組織中的 Trusted Advisor 檢查。若要取得最新的檢查結果，請重新整理管理帳戶和組織中每個成員帳戶的檢查。如需更多詳細資訊，請參閱 重新整理 Trusted Advisor 檢查。

我的報告中有重複的欄

如果您的報告有重複的欄，Athena 主控台可能會在表格中顯示下列錯誤。

```
HIVE_INVALID_METADATA: Hive metadata for table folder1 is invalid: Table
descriptor contains duplicate columns
```

例如，如果您在報告中新增已存在的欄，當您嘗試在 Athena 主控台中檢視報告資料時可能會造成問題。您可以按照下列步驟修正此問題。

尋找重複的欄

您可以使用 AWS Glue 主控台來檢視結構描述，並快速識別報告中是否有重複的欄。

尋找重複的欄

1. 開啟位於 https://console.aws.amazon.com/glue/ 的 AWS Glue 主控台。
2. 如果您尚未執行此步驟，請在 Region selector (區域選擇器) 中選擇美國東部 (維吉尼亞北部) 區域。
3. 在導覽窗格中，選擇 Tables (資料表)。

4. 選擇資料夾名稱 (例如 ***folder1***)，然後在 Schema (結構描述) 底下查看 Column name (欄名稱) 的值。

   如果有欄重複，您必須將新報告上傳到 Amazon S3 儲存貯體。請參閱 上傳新的報告 一節。

上傳新的報告

找到重複的欄後，建議您以新報告取代現有的報告。這可確保在本教學課程中建立的資源使用您組織的最新報告資料。

上傳新的報告

1. 如果您尚未重新整理，請先重新整理您組織中帳戶的 Trusted Advisor 檢查。請參閱 重新整理 Trusted Advisor 檢查。
2. 在 Trusted Advisor 主控台中建立並下載另一個 JSON 報告。請參閱 建立組織檢視報告。在本教學課程中您必須使用 JSON 檔案。
3. 登入 AWS Management Console，並開啟位於 https://console.aws.amazon.com/s3/ 的 Amazon S3 主控台。
4. 選擇您的 Amazon S3 儲存貯體，然後選擇 *folder1* 資料夾。
5. 選取上一個 *resources*`.json` 報告並選擇 Delete (刪除)。
6. 在 Delete objects (刪除物件) 頁面中的 Permanently delete objects? (永久刪除物件？) 中，輸入 **`permanently delete`**，然後選擇 Delete objects (刪除物件)。
7. 在您的 S3 儲存貯體中，選擇 Upload (上傳)，然後指定新報告。這個動作會自動更新您的 Athena 表格和 AWS Glue 爬蟲程式資源 (包含最新的報告資料)。重新整理資源可能需要幾分鐘的時間。
8. 在 Athena 主控台中輸入新的查詢。請參閱 在 Amazon Athena 中查詢資料。

> **Note**
>
> 如果您對於本教學課程仍有問題，您可以前往 AWS Support Center 建立技術支援案例。

檢視由 AWS Config 提供技術的 AWS Trusted Advisor 檢查

AWS Config是 一項服務，可持續評估、稽核及估算您所需設定的資源組態。AWS Config 提供預先定義的受管規則、可自訂的法規遵循檢查，AWS Config 會使用這些來評估您的 AWS 資源是否符合常用最佳實務。

AWS Config 主控台會逐步引導您設定和啟用受管規則。您也可以使用 AWS Command Line Interface (AWS CLI) 或 AWS Config API 來傳遞 JSON 程式碼，以定義受管規則的組態。您可以自訂受管規則的行為，以符合您的需求。您可以自訂規則的參數，以定義資源必須具備哪些屬性才能符合規則。若要進一步瞭解啟用 AWS Config，請參閱《AWS Config 開發人員指南》。

AWS Config 受管規則為跨所有類別的一組 Trusted Advisor 檢查提供技術。當您啟用特定受管理規則時，系統會自動啟用對應的 Trusted Advisor 檢查。若要查看哪些 Trusted Advisor 檢查是由特定 AWS Config 受管理規則提供技術，請參閱 AWS Trusted Advisor 檢查參考。

AWS Config 提供技術的檢查適用於具有 AWS Business Support、AWS Enterprise On-Ramp 和 AWS Enterprise Support 計畫的客戶。如果您啟用 AWS Config 且擁有下列其中一個 AWS Support 計畫，則您會自動看見由對應部署的 AWS Config 受管規則提供技術的建議。

> **Note**
>
> 這些檢查的結果會根據對 AWS Config 受管規則所作的由變更所觸發的更新而自動重新整理。不允許重新整理請求。目前，您無法從這些檢查中排除資源。

疑難排解

如果您在這項整合上遇到問題，請參閱以下故障診斷資訊。

內容

- 我剛剛啟用了 AWS Config 的記錄與受管規則，但卻看不見對應的 Trusted Advisor 檢查。
- 我部署了兩次相同的 AWS Config 受管規則，我會在 Trusted Advisor 中看到什麼結果？
- 我關閉了 AWS Config 在 AWS 區域中的記錄功能。我在 Trusted Advisor 中會看見什麼？

我剛剛啟用了 AWS Config 的記錄與受管規則，但卻看不見對應的 Trusted Advisor 檢查。

AWS Config 規則產生評估結果後，您會以近乎即時的速度看見 Trusted Advisor 中的結果。如果您對本功能有任何問題，請在 AWS Support 中心建立技術支援案例。

我部署了兩次相同的 AWS Config 受管規則，我會在 Trusted Advisor 中看到什麼結果？

您會在每個安裝的受管規則的 Trusted Advisor 檢查結果中看到不同的項目。

我關閉了 AWS Config 在 AWS 區域中的記錄功能。我在 Trusted Advisor 中會看見什麼？

如果您關閉 AWS 區域中 AWS Config 的資源記錄，則 Trusted Advisor 不會再接收該區域中對應受管規則和檢查的資料。根據記錄器保留政策，現有的受管規則結果會一直保留在 AWS Config 和 Trusted Advisor 中，直到 AWS Config 過期為止。如果您刪除受管規則，則系統通常會以近乎即時的速度刪除 Trusted Advisor 檢查資料。

檢視 AWS Security Hub 中的 AWS Trusted Advisor 控制項

在為您的 AWS 帳戶 啟用 AWS Security Hub 後，您可以在 Trusted Advisor 主控台檢視您的安全控制項和其問題清單。您可以使用 Security Hub 控制項來識別帳戶中的安全漏洞，方法與您可以使用 Trusted Advisor 檢查的方法一樣。您可以查看檢查的狀態、受影響的資源列表，然後按照 Security Hub 的建議來解決您的安全問題。您可以使用此功能在一個方便的位置找到 Trusted Advisor 和 Security Hub 中的安全建議。

> **備註**
>
> - 在 Trusted Advisor 中，您可以檢視 AWS 基礎安全最佳實務安全標準中的控制項，具有類別：復原 > 彈性的控制項除外。如需支援的控制項清單，請參閱《AWS Security Hub 使用者指南》中的 AWS 基礎安全最佳實務控制項。
>
>   如需有關 Security Hub 類別的詳細資訊，請參閱控制項類別。
> - 目前，當 Security Hub 將新的控制項新增到AWS基礎安全最佳實務安全標準時，可能要在兩週至四週之後，您才能在 Trusted Advisor 上檢視內容。此時間框架為盡最大努力的結果，且不能保證。

主題

先決條件

您必須符合下列要求，才能啟用與 Trusted Advisor 的 Security Hub 整合：

- 您必須訂閱此功能的商業、Enterprise On-Ramp 或企業支援計劃。您可以在 AWS Support 中心或支援計劃頁面中找到您的支援計劃。如需詳細資訊，請參閱比較 AWS Support 計劃。
- 您必須為要用於 Security Hub 控制項的 AWS 區域 啟用 AWS Config 中的資源記錄。如需詳細資訊，請參閱啟用並設定 AWS Config。
- 您必須啟用 Security Hub 並選擇 AWS 基礎安全最佳實務 v1.0.0 安全標準。如果您尚未執行，請參閱《AWS Security Hub 使用者指南》中的設定 AWS Security Hub。

> **Note**
>
> 如果您已完成這些先決條件，您可以跳至 檢視 Security Hub 問題清單。

關於 AWS Organizations 帳戶

如果您已經完成了管理帳戶的先決條件，則系統會為組織中的所有成員帳戶自動啟用此整合。個人會員帳戶無需聯絡 AWS Support 來啟用此功能。但是，如果組織中的成員希望在 Trusted Advisor 查看問題清單，他們的帳戶必須啟用 Security Hub。

如果您要停用特定成員帳戶的這項整合，請參閱 停用 AWS Organizations 帳戶的這項功能。

檢視 Security Hub 問題清單

為您的帳戶啟用 Security Hub 後，您的 Security Hub 的問題清單最多可能需要 24 個小時才會顯示在 Trusted Advisor 主控台的安全性頁面。

檢視 Trusted Advisor 中的 Security Hub 問題清單

1. 導覽至 Trusted Advisor 主控台，然後選擇 Security (安全) 類別。
2. 在 Search by keyword (依關鍵字搜尋) 欄位中，請在欄位中輸入控制項的名稱或描述。

> **Tip**
>
> 針對 Source (來源)，您可以選擇 AWS Security Hub 來篩選 Security Hub 控制項。

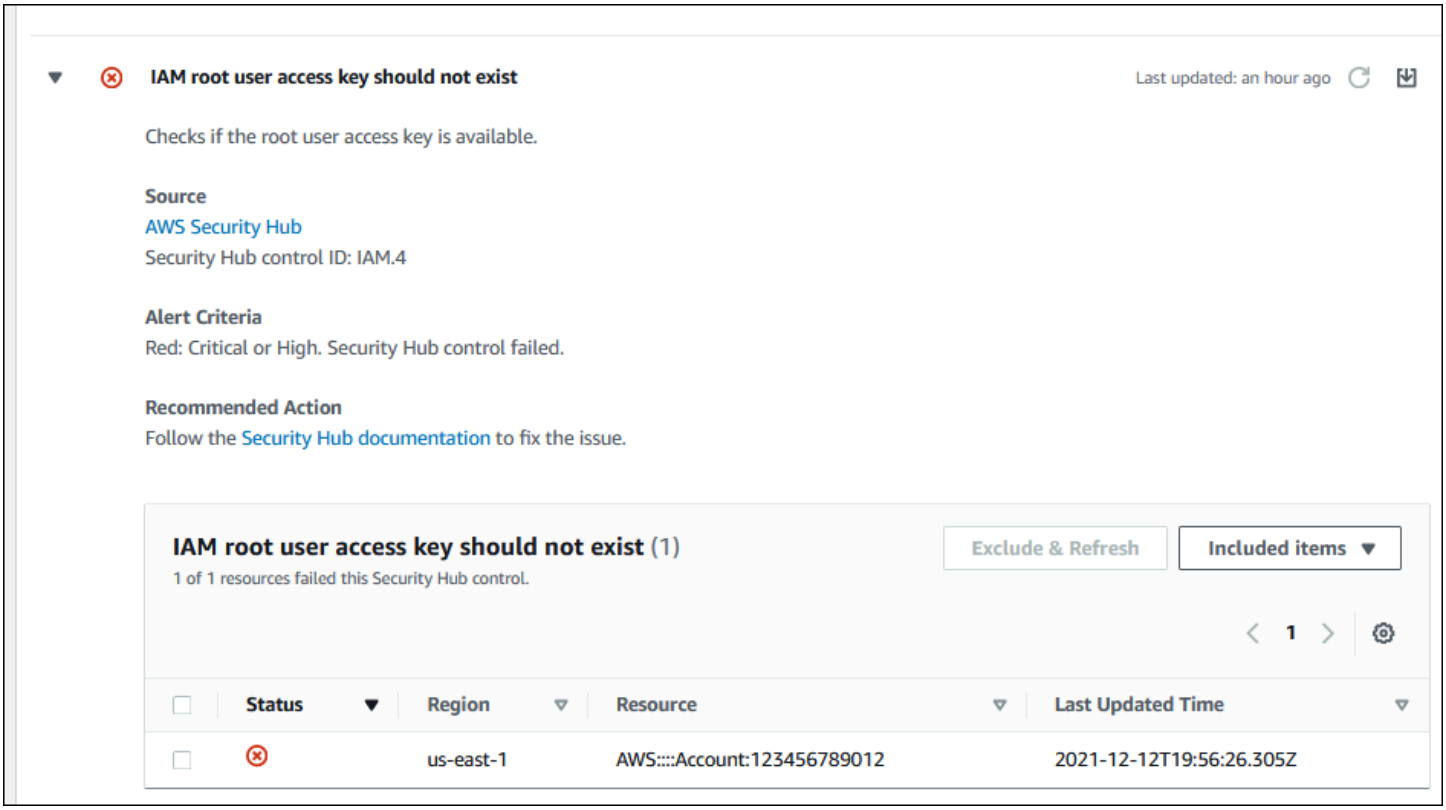
3. 選擇 Security Hub 控制項名稱來檢視下列資訊：

   - 描述 – 描述此控制項如何檢查您的帳戶是否存在安全漏洞。
   - Source (來源) – 檢查是否來自 AWS Trusted Advisor 或 AWS Security Hub 。針對 Security Hub 控制項，您可以找到控制項 ID。
   - Alert Criteria (提醒條件) – 控制項的狀態。例如，如果 Security Hub 偵測到重要問題，則狀態可能是紅色：嚴重或高。
   - Recommended Action (建議的動作) – 使用 Security Hub 文件連結尋找解決此問題的建議步驟。
   - Security Hub resources (Security Hub 資源) – 您可以在您的帳戶中查找 Security Hub 檢測到問題的資源。

> **備註**
>
> - 您必須使用 Security Hub 從問題清單中排除資源。目前，您無法使用 Trusted Advisor 主控台從 Security Hub 控制項中排除項目。如需詳細資訊，請參閱設定問題清單的工作流程狀態。
> - 組織檢視功能支援與 Security Hub 的這項整合。您可以在整個組織中查看 Security Hub 控制項的問題清單，然後建立並下載報告。如需詳細資訊，請參閱 AWS Trusted Advisor 的組織檢視。

Example 範例：IAM 使用者存取金鑰的 Security Hub 控制項不應存在

以下是 Trusted Advisor 主控台 Security Hub 控制項的範例問題清單。



重新整理您的 Security Hub 問題清單

啟用安全標準後，Security Hub 最多可能需要兩個小時才會有資源的問題清單。該筆資料要在 Trusted Advisor 主控台出現，可能要花費長達 24 小時。如果您最近啟用了 AWS 基礎安全最佳實務 v1.0.0 安全標準，請稍後再次檢查 Trusted Advisor 主控台。

> **Note**
>
> - 每個 Security Hub 控制項的重新整理排程為定期或變更觸發。目前，您無法使用 Trusted Advisor 主控台或 AWS Support API 來重新整理您的 Security Hub 控制項。如需詳細資訊，請參閱執行安全檢查的排程。
> - 如果您想要從問題清單中排除資源，必須使用 Security Hub。目前，您無法使用 Trusted Advisor 主控台從 Security Hub 控制項中排除項目。如需詳細資訊，請參閱設定問題清單的工作流程狀態。

從 Trusted Advisor 停用 Security Hub

如果您不希望 Security Hub 資訊顯示在 Trusted Advisor 主控台中，請遵循此程序。此程序僅停用與 Trusted Advisor 的 Security Hub 整合。它不會影響與 Security Hub 的配置。您可以繼續使用 Security Hub 主控台檢視您的安全控制項、資源和建議。

停用 Security Hub 整合

1. 請聯絡 AWS Support 並請求停用與 Trusted Advisor 的 Security Hub 整合。

   AWS Support 停用此功能後，Security Hub 不再將資料傳送至 Trusted Advisor。您的 Security Hub 資料會從 Trusted Advisor 中移除。
2. 如果您要再次啟用此整合，請聯絡 AWS Support。

停用 AWS Organizations 帳戶的這項功能

如果您已經完成了管理帳戶的先前程序，則 Security Hub 整合將自動從組織中的所有成員帳戶中移除。組織的個別成員帳戶無需分別聯絡 AWS Support。

如果您是組織的成員帳戶，您可以聯絡 AWS Support，僅從您的帳戶中刪除此功能。

疑難排解

如果您在這項整合上遇到問題，請參閱以下故障診斷資訊。

內容

- 我沒有在 Trusted Advisor 主控台中看到 Security Hub 問題清單
- 我正確設定了 Security Hub 和 AWS Config，但是我的問題清單仍然缺失
- 我想要停用特定的 Security Hub 控制項
- 我想尋找已排除的 Security Hub 資源
- 我想啟用或停用屬於 AWS 組織的成員帳戶的這項功能。
- 我看到多個 AWS 區域 用於 Security Hub 檢查的相同受影響資源
- 我在一個區域關閉了 Security Hub 或 AWS Config
- 我的控制項封存在 Security Hub 中，但我仍然可以在 Trusted Advisor 中看到問題清單。
- 我仍然無法檢視我的 Security Hub 問題清單

我沒有在 Trusted Advisor 主控台中看到 Security Hub 問題清單

驗證您是否已完成下列步驟：

- 您具備商業、Enterprise On-Ramp 或企業支援計劃。
- 您已在與 Security Hub 相同的區域內啟用了 AWS Config 中的資源記錄。
- 您啟用了 Security Hub 並選擇了 AWS 基礎安全最佳實務 v1.0.0 安全標準。
- 來自 Security Hub 的新控制項已於兩週至四週內在 Trusted Advisor 中新增為檢查。參閱注意事項。

如需詳細資訊，請參閱 先決條件。

我正確設定了 Security Hub 和 AWS Config，但是我的問題清單仍然缺失

Security Hub 最多可能需要兩個小時才會有資源的問題清單。該筆資料要在 Trusted Advisor 主控台出現，可能要花費長達 24 小時。請稍後再次檢查 Trusted Advisor 主控台。

> **備註**
>
> - 只有您在 AWS 基礎安全最佳實務安全標準中的控制項問題清單才會出現在 Trusted Advisor，具有類別：復原 > 彈性的控制項除外。
> - 如果 Security Hub 出現服務問題或 Security Hub 無法使用，則最多可能需要 24 小時才會在 Trusted Advisor 中顯示。請稍後再次檢查 Trusted Advisor 主控台。

我想要停用特定的 Security Hub 控制項

Security Hub 會自動將您的資料傳送至 Trusted Advisor。如果停用 Security Hub 控制項或不再具有該控制項的資源，則您的問題清單將不會在 Trusted Advisor 中顯示。

您可以登入至 Security Hub 主控台，並驗證您的控制項是否已啟用或停用。

如果您停用 Security Hub 控制項，或停用所有 AWS 基礎安全最佳實務安全標準的控制項，在接下來的五天內將封存您的問題清單。這個五天的封存期限僅為近似值，會盡力而為，但不一定保證實現。您的問題清單封存後，就會從 Trusted Advisor 中移除。

如需詳細資訊，請參閱下列主題：

- 停用和啟用個別控制項
- 停用或啟用安全標準

我想尋找已排除的 Security Hub 資源

在 Trusted Advisor 主控台中，您可以選擇 Security Hub 控制項名稱，然後選擇 Excluded items (已排除的項目) 選項。此選項會在 Security Hub 中顯示禁止的所有資源。

如果資源的工作流程狀態設定為 SUPPRESSED，那麼該資源是 Trusted Advisor 中的已排除項目。您無法從 Trusted Advisor 主控台中禁止 Security Hub 資源。若要執行此作業，請使用 Security Hub 主控台。如需詳細資訊，請參閱設定問題清單的工作流程狀態。

我想啟用或停用屬於 AWS 組織的成員帳戶的這項功能。

根據預設，成員帳戶從 AWS Organizations 管理帳戶繼承該功能。如果管理帳戶已啟用該功能，則組織中的所有帳戶也將具有該功能。如果您有成員帳戶，並想要為您的帳戶進行特定的變更，您必須聯絡 AWS Support。

我看到多個 AWS 區域 用於 Security Hub 檢查的相同受影響資源

一些 AWS 服務 為全域性質，並非特定於某個區域，例如：IAM 和 Amazon CloudFront。依預設，Amazon S3 儲存貯體等全域資源會顯示在美國東部 (維吉尼亞北部) 區域。

對於評估全域服務資源的 Security Hub 檢查，您可能會看到受影響資源的多個項目。例如，如果 `Hardware MFA should be enabled for the root user` 檢查識別到您的帳戶尚未啟用此功能，您會在相同資源的資料表中看到多個區域。

您可以設定 Security Hub 和 AWS Config，以便相同資源不會顯示多個區域。如需詳細資訊，請參閱您可能想要停用的 AWS 基本最佳實務控制。

我在一個區域關閉了 Security Hub 或 AWS Config

如果您使用 AWS Config 停止資源記錄，或在 AWS 區域 中停用 Security Hub，則 Trusted Advisor 不再接收該區域中任何控制項的資料。Trusted Advisor 會在 7-9 天內移除您的 Security Hub 問題清單。此時間框架為盡最大努力的結果，且不能保證。如需詳細資訊，請參閱停用 Security Hub。

若要停用您帳戶的這項功能，請參閱從 Trusted Advisor 停用 Security Hub。

我的控制項封存在 Security Hub 中，但我仍然可以在 Trusted Advisor 中看到問題清單。

問題的狀態從 `RecordState` 變更為 `ARCHIVED` 後，Trusted Advisor 會從您的帳戶中刪除該 Security Hub 控制項問題。在刪除問題清單之前，您最多可能會在 7-9 天內在 Trusted Advisor 中仍然看到問題清單。此時間框架為盡最大努力的結果，且不能保證。

我仍然無法檢視我的 Security Hub 問題清單

如果您對於本功能仍有問題，您可以前往 AWS Support 中心建立技術支援案例。

對於 AWS Compute Optimizer 檢查，選擇使用 Trusted Advisor

運算最佳化工具是一項可分析 AWS 資源組態和使用率指標的服務。此服務會報告您的資源是否正確設定，能夠實現效率和可靠性。此服務還會建議您可以實施提高工作負載效能的改善項目。若使用 Compute Optimizer，您會在 Trusted Advisor 檢查中看到同樣的建議。

您可以選擇僅用於 AWS 帳戶 或選擇屬於 AWS Organizations 組織一部分的所有成員帳戶。如需詳細資訊，請參閱《AWS Compute Optimizer 使用者指南》中的「入門」。

一旦選擇使用 Compute Optimizer 後，下列檢查會從您的 Lambda 函數和 Amazon EBS 磁碟區接收資料。最多可能需要 12 小時才會產生問題清單和最佳化建議。最多可能需要 48 小時才能針對下列檢查在 Trusted Advisor 中查看結果：

成本最佳化

- Amazon EBS 過度佈建的磁碟區
- AWS Lambda 過度佈建的函數 (對於記憶體大小)

效能

- Amazon EBS 佈建不足的磁碟區
- AWS Lambda 佈建不足的函數 (對於記憶體大小)

> **備註**
>
> - 這些檢查的結果會每天自動重新整理數次。不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從這些檢查中排除資源。
> - Trusted Advisor 已經有使用不足的 Amazon EBS 磁碟區和過度使用的 Amazon EBS 磁帶磁碟區檢查。
>
>   一旦選擇使用 Compute Optimizer，建議您改為使用全新 Amazon EBS 過度佈建的磁碟區和 Amazon EBS 佈建不足的磁碟區檢查。

相關資訊

如需詳細資訊，請參閱下列主題：

- 在《AWS Compute Optimizer 使用者指南》中，檢視 Amazon EBS 磁碟區建議
- 在《AWS Compute Optimizer 使用者指南》中，檢視 Lambda 函數建議
- 在《AWS Lambda 開發人員指南》中，設定 Lambda 函數記憶體
- 在《適用於 Linux 執行個體的 Amazon EC2 使用者指南》中，請求修改您的 Amazon EBS 磁碟區

開始使用 AWS Trusted Advisor 優先權

Trusted Advisor Priority 可幫助您保護和優化 AWS 帳戶，以便遵循 AWS 最佳實務。使用 Trusted Advisor Priority，您的 AWS 帳戶 團隊可以主動監控您的帳戶並在發現機會時建立優先的建議。

例如，您的客戶團隊可以識別您的 AWS 帳戶根使用者是否缺少多重要素驗證 (MFA)。您的客戶團隊可以建立建議，讓您可以立即對檢查採取行動，例如 `MFA on Root Account`。建議在 Trusted Advisor 主控台的 Trusted Advisor Priority 頁面中顯示為作用中的優先建議。接著您可以按照建議解決問題。

Trusted Advisor Priority 建議會來自以下兩個來源：

- AWS 服務 – 服務，例如Trusted Advisor、AWS Security Hub，和 AWS Well-Architected，可自動建立建議。您的客戶團隊會與您分享這些建議，讓這些建議可以出現在 Trusted Advisor Priority 中。
- 您的客戶團隊 – 您的客戶團隊可以建立手動建議。

Trusted Advisor 優先權可以幫助您專注於最重要的建議。您和您的客戶團隊可以監控建議生命週期，從您的客戶團隊分享建議，到您確認、解決或關閉建議。您可以使用 Trusted Advisor Priority 查找您組織中所有成員帳戶的建議。

主題

- 必要條件
- 啟用 Trusted Advisor 優先權
- 檢視優先建議
- 確認建議
- 關閉建議
- 解決建議
- 重新開啟建議

- 下載建議詳細資訊
- 註冊委派的管理員
- 取消註冊委派的管理員
- 管理 Trusted Advisor Priority 通知
- 停用 Trusted Advisor 優先權

必要條件

您必須符合下列要求才能使用 Trusted Advisor Priority：

- 您必須擁有 Enterprise Support 計畫。
- 您的帳戶必須是 AWS Organizations 中啟用了所有功能的組織的一部分。如需詳細資訊，請參閱 AWS Organizations 使用者指南中的啟用組織中的所有功能。
- 您的組織必須具有已啟用受信任的 Trusted Advisor 存取權。若要啟用受信任的存取權，請以管理帳戶登入。在 Trusted Advisor 主控台中開啟您的組織頁面。
- 您必須登入 AWS 帳戶，才能檢視適用於您帳戶的 Trusted Advisor Priority 建議。
- 您必須登入組織的管理帳戶或委派的管理員帳戶，才能檢視整個組織的彙總建議。如需如何註冊委派管理員帳戶的指示，請參閱 註冊委派的管理員。
- 您必須擁有 AWS Identity and Access Management (IAM) 許可，才能存取 Trusted Advisor Priority。如需有關如何控制 Trusted Advisor Priority 存取權的詳細資訊，請參閱 管理存取 AWS Trusted Advisor 和 AWS 受管理的政策 AWS Trusted Advisor。

啟用 Trusted Advisor 優先權

請洽詢您的客戶團隊來為您啟用此功能。您必須擁有企業支援計劃，並且是組織的管理帳戶擁有者。如果主控台中的 Trusted Advisor Priority 頁面顯示您需要 AWS Organizations 的受信任存取權，那麼請選擇啟用 AWS Organizations 的受信任存取權。如需詳細資訊，請參閱 必要條件 一節。

檢視優先建議

帳戶團隊為您啟用 Trusted Advisor Priority 之後，您就能檢視針對您的 AWS 團隊所提供的最新建議。

若要檢視優先建議

1. 登入 Trusted Advisor 主控台，網址是 https://console.aws.amazon.com/trustedadvisor/home。
2. 在 Trusted Advisor Priority 頁面上，您可以檢視下列項目：

如果您使用的是 AWS Organizations 管理或委派管理員帳戶，則請切換至我的帳戶分頁。

- 需要採取行動 - 等待回應或進行中的建議數量。
- Overview (概觀) - 下列資訊：
  - 過去 90 天內被關閉的建議
  - 過去 90 天內已解決的建議
  - 超過 30 天內沒有更新的建議
  - 解決建議的平均時間

3. 在作用中分頁上，作用中的優先建議會顯示您的客戶團隊為您優先處理的建議。已關閉標籤會顯示已解決或已關閉的建議。

   - 若要篩選結果，請使用下列選項：

     - Recommendation (建議) – 輸入關鍵字，按名稱搜尋。這可以是檢查名稱，或者是客戶團隊建立的自訂名稱。
     - 狀態 – 建議是處於等待回應、進行中、已關閉或已解決。
     - Source (來源) – 優先建議的來源。建議可能來自 AWS 服務、您的 AWS 帳戶 團隊或者計劃的服務事件。
     - Category (類別) – 建議的類別，例如安全性或成本優化。
     - Age (時間) – 您的客戶團隊與您分享建議的時間。

4. 選擇建議以瞭解其詳細資訊、受影響的資源和建議行動。然後，您可以確認或關閉建議。

若要檢視 AWS 組織中所有帳戶之間的優先建議

管理帳戶和 Trusted Advisor Priority 委派管理員皆可檢視整個組織的彙總建議。

> **Note**
>
> 成員帳戶無法存取彙總建議。

1. 登入 Trusted Advisor 主控台，網址是 https://console.aws.amazon.com/trustedadvisor/home。
2. 在 Trusted Advisor Priority 頁面上，確定您位於我的組織分頁上。
3. 若要檢視一個帳戶的建議，請在從您的組織選取帳戶下拉式清單中選取帳戶。或者，您也可以檢視所有帳戶的建議。

在我的組織分頁上，您可以檢視下列項目：

- 需要採取行動：組織間等待回應或進行中的建議數量。
- 概觀：顯示下列項目：

  - 過去 90 天內關閉的建議。

  - 過去 90 天內解決的建議。

  - 超過 30 天內沒有更新的建議。

  - 解決建議所需的平均時間。

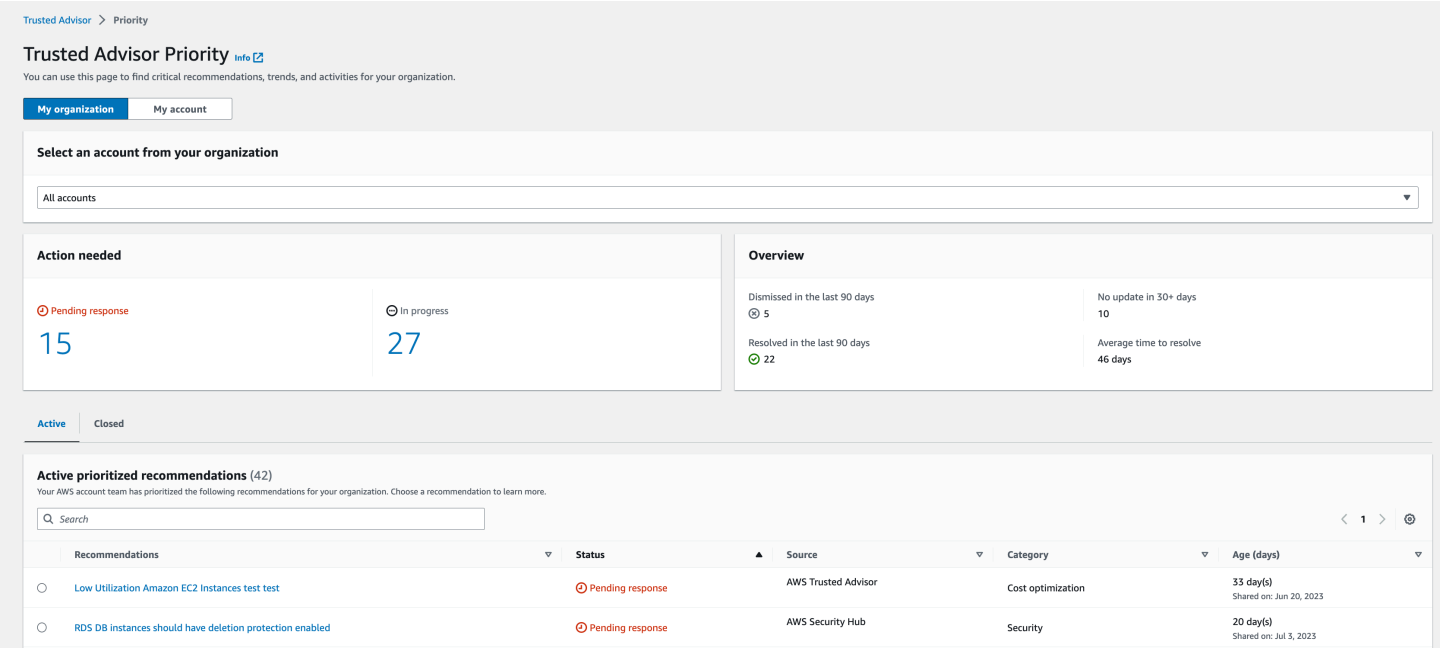
4. 在作用中分頁下，作用中的優先建議區段會顯示您的客戶團隊為您優先處理的建議。已關閉標籤會顯示已解決或已關閉的建議。

   若要篩選結果，請使用下列選項：

   - Recommendation (建議) – 輸入關鍵字，按名稱搜尋。這可以是檢查名稱，或者是客戶團隊建立的自訂名稱。
   - 狀態 – 建議是處於等待回應、進行中、已關閉或已解決。
   - Source (來源) – 優先建議的來源。建議可能來自 AWS 服務、您的 AWS 帳戶 團隊或者計劃的服務事件。
   - Category (類別) – 建議的類別，例如安全性或成本優化。
   - Age (時間) – 您的客戶團隊與您分享建議的時間。
5. 選擇建議以瞭解其他詳細資訊、受影響的帳戶與資源，以及建議行動。然後，您可以確認或關閉建議。

Example ：Trusted Advisor 優先權建議

下列範例會顯示正在等待回應的 15 個建議，以及在需要採取行動區段下進行中的 27 個建議。下圖顯示作用中的優先建議標籤中正在等待回應的兩個建議。



確認建議

在作用中標籤下，您可以進一步了解建議，然後決定是否要確認建議。

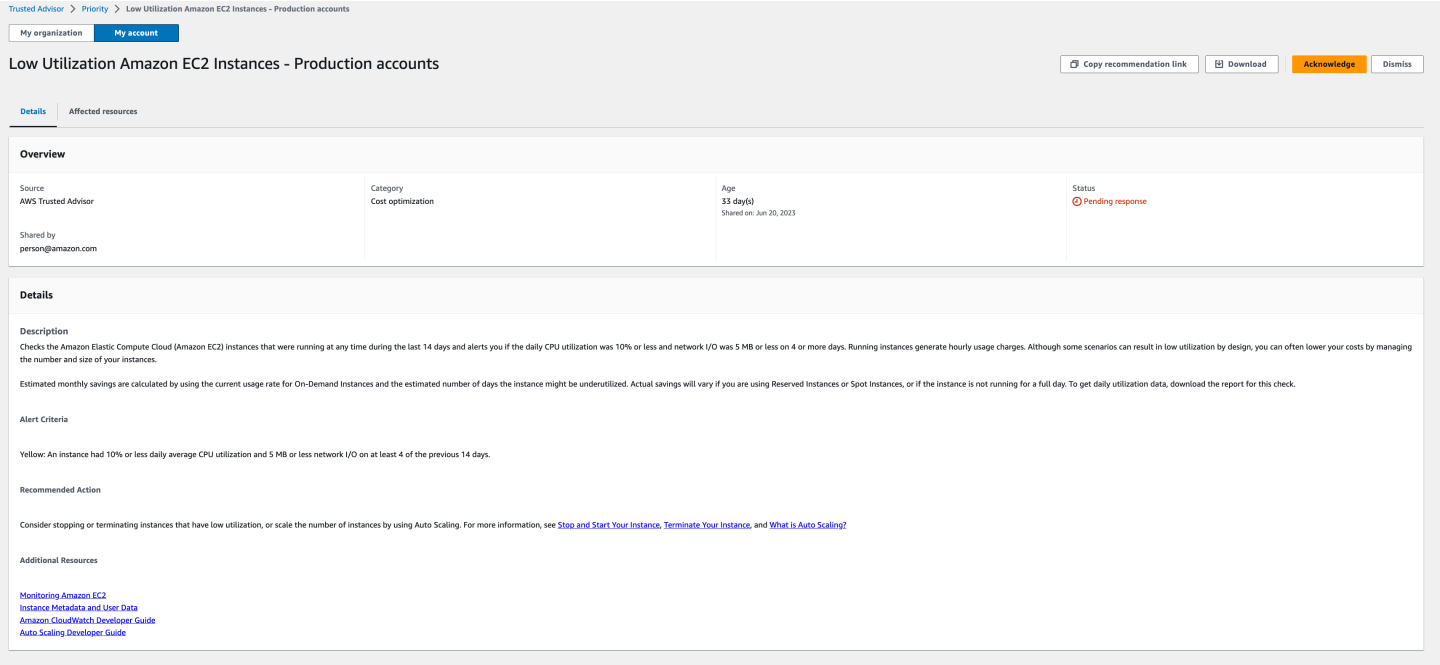
若要確認建議

1. 登入 Trusted Advisor 主控台，網址是 https://console.aws.amazon.com/trustedadvisor/home。
2. 如果您使用的是 AWS Organizations 管理或委派管理員帳戶，則請切換至我的帳戶分頁。
3. 在 Trusted Advisor Priority 頁面的 Active (作用中) 索引標籤中，選擇建議名稱。
4. 在詳細資訊區段中，您可以檢閱解決建議的建議行動。
5. 在受影響的資源區段中，您可以檢閱受影響的資源並依狀態來篩選。
6. 選擇確認。
7. 在確認建議對話方塊中，選擇確認。

   建議狀態會變更為 In progress (進行中)。正在進行中或等待回應的建議會顯示在 Trusted Advisor Priority 頁面的 Active (作用中) 索引標籤中。
8. 遵循建議的行動來解決建議。如需詳細資訊，請參閱解決建議。

Example ：來自 Trusted Advisor 優先權的手動建議

以下影像顯示正在等待回應的低利用率 EC2 執行個體建議。



若要確認 AWS 組織中所有帳戶的建議

管理帳戶或 Trusted Advisor 委派管理員可以確認所有受影響帳戶的建議。

> **Note**
>
> 成員帳戶無法存取彙總建議。

1. 登入 Trusted Advisor 主控台，網址是 https://console.aws.amazon.com/trustedadvisor/home。
2. 在 Trusted Advisor Priority 頁面上，確定您位於我的組織分頁上。
3. 在作用中分頁中，選取建議名稱。
4. 選擇確認。
5. 在確認建議對話方塊中，選擇確認。

   建議狀態會變更為 In progress (進行中)。
6. 遵循建議的行動來解決建議。如需詳細資訊，請參閱解決建議。
7. 若要檢視建議詳細資訊，請選擇建議名稱。

   您可以在詳細資訊區段中檢閱下列有關建議的資訊：

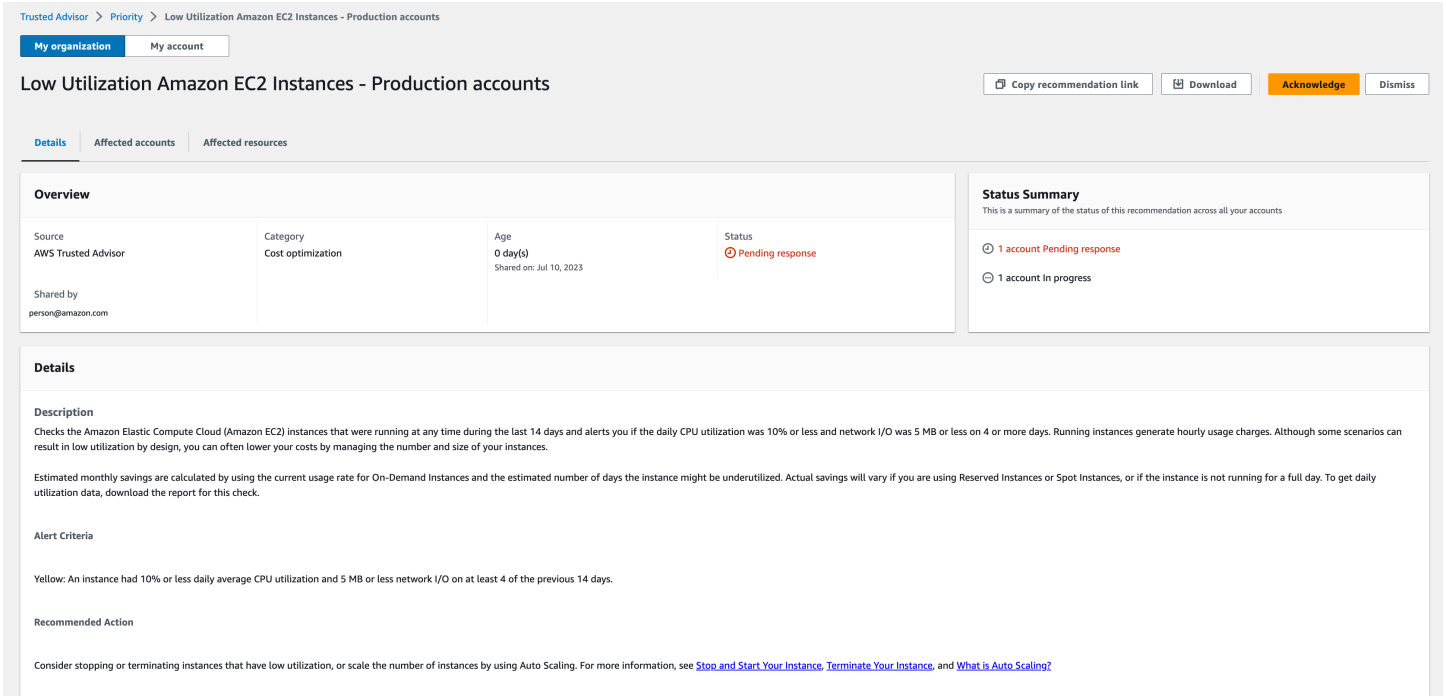
   - 建議概觀以及涵蓋要完成之建議動作的詳細資訊區段。

狀態摘要，顯示所有受影響帳戶的建議。

- 在受影響的帳戶區段中，您可以檢閱所有帳戶中受影響的資源。您可以按照帳號和狀態來篩選。
- 在受影響的資源區段中，您可以檢閱所有帳戶中受影響的資源。您可以按照帳號和狀態來篩選。

Example ：來自 Trusted Advisor 優先權的手動建議

以下影像顯示正在等待回應的低利用率 Amazon EC2 執行個體建議。一個受影響的帳戶已確認該建議。另一個帳號正在等待回應，建議狀態為待定回應。



關閉建議

您也可以關閉建議。這意味著您確認建議，但無法解決該建議。如果建議與您的帳戶無關，您可以關閉該建議。例如，如果您計劃刪除一個 AWS 帳戶 的測試，則不需要遵循該建議的行動。

若要關閉建議

1. 登入 Trusted Advisor 主控台，網址是 https://console.aws.amazon.com/trustedadvisor/home。
2. 如果您使用的是 AWS Organizations 管理或委派管理員帳戶，則請切換至我的帳戶分頁。
3. 在 Trusted Advisor Priority 頁面的 Active (作用中) 索引標籤中，選擇建議名稱。
4. 在建議詳細資訊頁面上，檢閱有關受影響資源的資訊。
5. 如果此建議不適用於您的帳戶，請選擇關閉。

6. 在關閉建議對話方塊中，選取您無法解決該建議的原因。
7. (選用) 輸入詳述您關閉建議之原因的備註。如果您選擇其他，則必須在備註區段中輸入說明。
8. 選擇關閉。建議狀態會變更為已關閉並顯示在 Trusted Advisor Priority 頁面的已關閉標籤中。

若要關閉 AWS 組織中所有帳戶的建議

管理帳戶或 Trusted Advisor Priority 的委派管理員可以關閉其所有帳戶的建議。

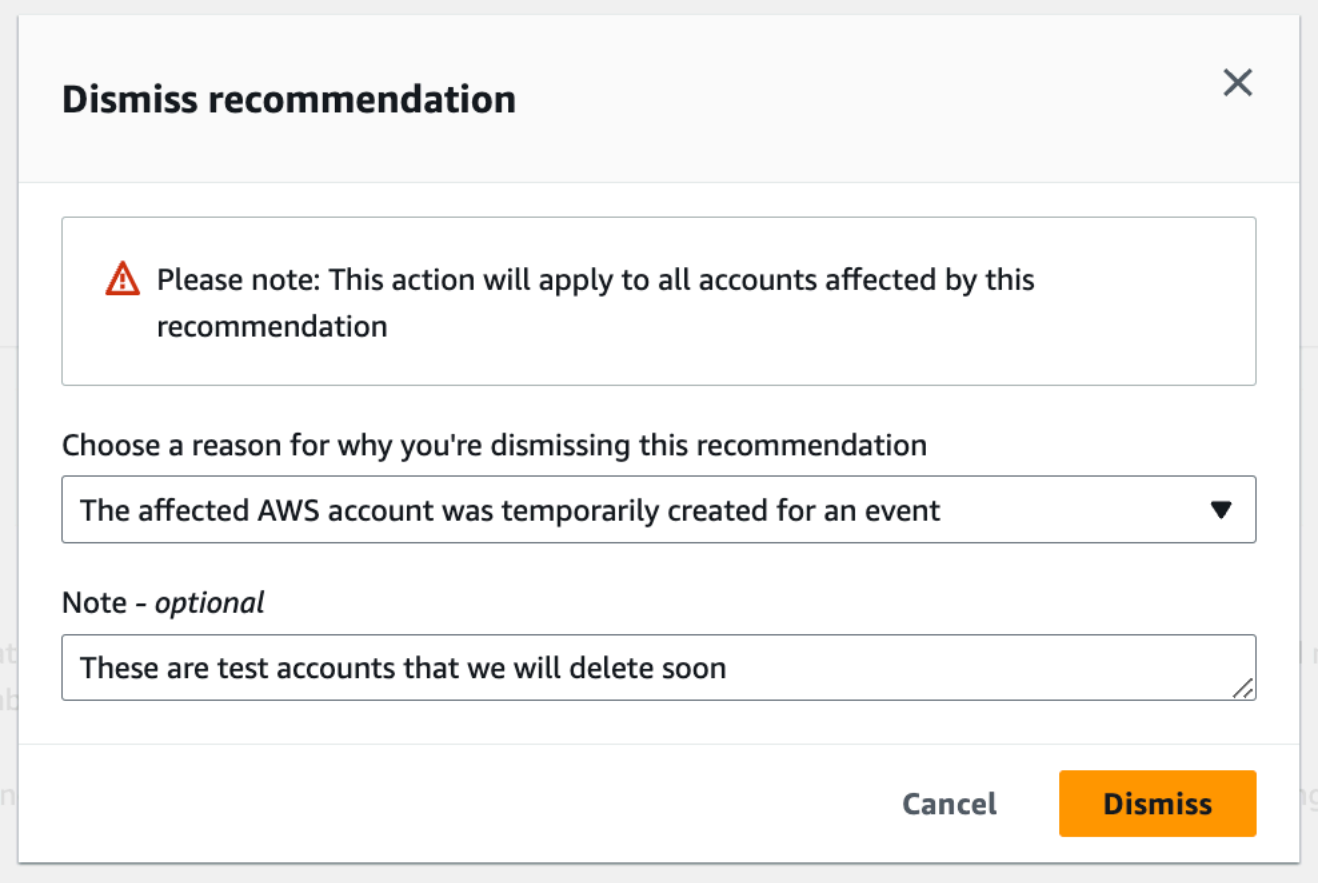
1. 登入 Trusted Advisor 主控台，網址是 https://console.aws.amazon.com/trustedadvisor/home。
2. 在 Trusted Advisor Priority 頁面上，確定您位於我的組織分頁上。
3. 在作用中分頁中，選取建議名稱。
4. 如果此建議不適用於您的帳戶，那麼請選擇關閉。
5. 在關閉建議對話方塊中，選取您無法解決該建議的原因。
6. (選用) 輸入詳述您關閉建議之原因的備註。如果您選擇其他，那麼就必須在備註區段中輸入說明。
7. 選擇關閉。建議狀態會變更為已關閉。建議會在 Trusted Advisor Priority 頁面上的已結案分頁中顯示。

> **Note**
>
> 您可以選擇建議名稱，然後選擇檢視備註以尋找關閉的原因。如果您的客戶團隊為您關閉了建議，其電子郵件地址會顯示在備註旁邊。

Trusted Advisor Priority 也會通知您的客戶團隊您關閉了該建議。

Example ：關閉 Trusted Advisor Priority 的建議

以下範例顯示如何關閉建議。



解決建議

您在確認建議並完成建議的行動後，即可解決該建議。

> **Tip**
>
> 解決建議後，您便無法重新開啟該建議。如果您想稍後重新檢視該建議，請參閱關閉建議。

若要解決建議

1. 登入 Trusted Advisor 主控台，網址是 https://console.aws.amazon.com/trustedadvisor/home。
2. 在 Trusted Advisor Priority 頁面上，確定您位於我的組織分頁上。
3. 在 Trusted Advisor Priority 頁面中，選擇建議，然後選擇 Resolve (解決)。
4. 在解決建議對話方塊中，選擇解決。已解決的建議會顯示在 Trusted Advisor Priority 頁面的 Closed (已關閉) 索引標籤下。Trusted AdvisorPriority 會通知您的客戶團隊您已解決該建議。

若要解決 AWS 組織中所有帳戶的建議

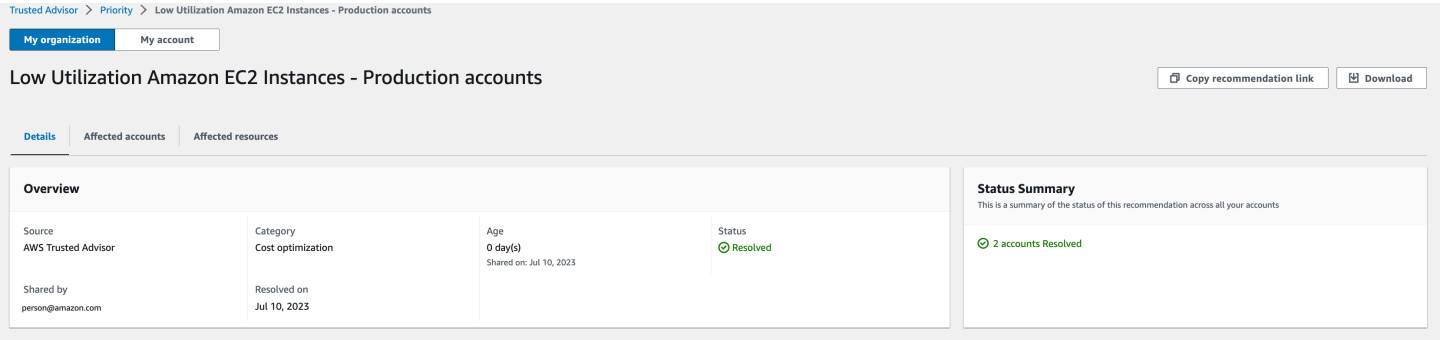
管理帳戶或 Trusted Advisor Priority 委派管理員可以解決其所有帳戶的建議。

> **Note**
>
> 成員帳戶無法存取彙總建議。

1. 登入 Trusted Advisor 主控台，網址是 https://console.aws.amazon.com/trustedadvisor/home。
2. 如果您使用的是 AWS Organizations 管理或委派管理員帳戶，請切換至我的帳戶分頁。
3. 在作用中分頁中，選取建議名稱。
4. 如果建議不適用於您的帳戶，請選擇解決。
5. 在解決建議對話方塊中，選擇解決。已解決的建議會顯示在 Trusted Advisor Priority 頁面的 Closed (已關閉) 索引標籤下。Trusted AdvisorPriority 會通知您的客戶團隊您已解決該建議。

Example ：來自 Trusted Advisor 優先權的手動建議

以下範例顯示已解決的低利用率 Amazon EC2 執行個體建議。



重新開啟建議

關閉建議後，您或您的客戶團隊可以重新開啟該建議。

若要重新開啟建議

1. 登入 Trusted Advisor 主控台，網址是 https://console.aws.amazon.com/trustedadvisor/home。
2. 如果您使用的是 AWS Organizations 管理或委派管理員帳戶，則請切換至我的帳戶分頁。
3. 在 Trusted Advisor Priority 頁面中，選擇 Closed (已關閉) 標籤。
4. 在已關閉的建議中，選取已關閉的建議，然後選擇重新開啟。

5. 在重新開啟建議對話方塊中，說明重新開啟建議的原因。
6. 選擇 Reopen (重新開啟)。建議狀態會變更為 In progress (進行中) 並出現在 Active (作用中) 標籤中。

> **Tip**
>
> 您可以選擇建議名稱，然後選擇檢視備註以尋找重新開啟的原因。如果您的客戶團隊為您重新開啟建議，其名稱會顯示在備註旁。

7. 按照建議詳細資訊中的步驟。

若要重新開啟 AWS 組織中所有帳戶的建議

管理帳戶或 Trusted Advisor Priority 委派管理員可以重新開啟其所有帳戶的建議。

> **Note**
>
> 成員帳戶無法存取彙總建議。

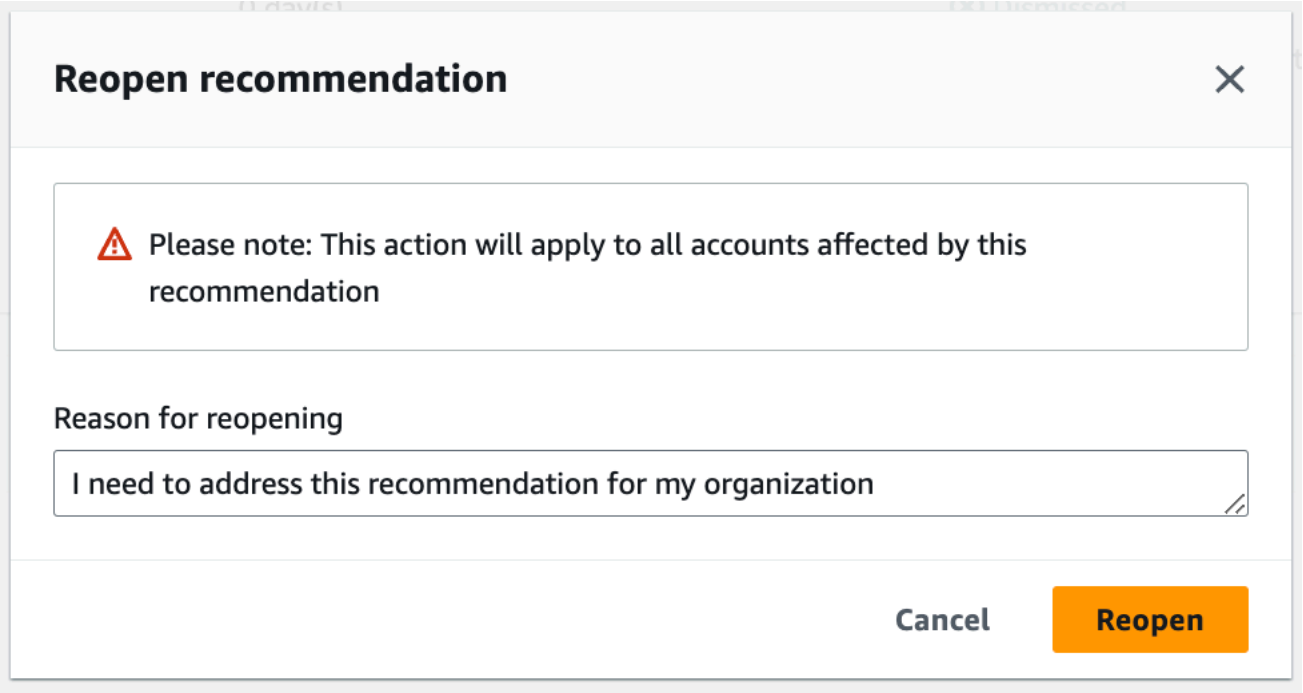
1. 登入 Trusted Advisor 主控台，網址是 https://console.aws.amazon.com/trustedadvisor/home。
2. 在 Trusted Advisor Priority 頁面上，確定您位於我的組織分頁上。
3. 在已關閉的建議中，選取已關閉的建議，然後選擇重新開啟。
4. 在重新開啟建議對話方塊中，說明重新開啟建議的原因。
5. 選擇 Reopen (重新開啟)。建議狀態會變更為 In progress (進行中) 並出現在 Active (作用中) 標籤中。

> **Tip**
>
> 您可以選擇建議名稱，然後選擇檢視備註以尋找重新開啟的原因。如果您的客戶團隊為您重新開啟建議，其名稱會顯示在備註旁。

6. 按照建議詳細資訊中的步驟。

Example ：從 Trusted Advisor Priority 中重新開啟建議

以下範例顯示您要重新開啟的建議。



下載建議詳細資訊

您還可以從 Trusted Advisor 優先權中下載優先建議的結果。

> **Note**
>
> 目前,一次只能下載一個建議。

若要下載建議

1. 登入 Trusted Advisor 主控台，網址是 https://console.aws.amazon.com/trustedadvisor/home。
2. 在 Trusted Advisor Priority 頁面中，選取建議，然後選擇 Download (下載)。
3. 開啟檔案以檢視建議的詳細資訊。

註冊委派的管理員

您可以將屬於組織的成員帳戶新增為委派管理員。委派管理員帳戶可以在 Trusted Advisor Priority 中檢閱、確認、解決、關閉和重新開啟建議。

註冊帳戶後，您必須對委派管理員授予所需的 AWS Identity and Access Management 許可，以便存取 Trusted Advisor Priority。如需詳細資訊，請參閱 管理存取 AWS Trusted Advisor 及 AWS 受管理的政策 AWS Trusted Advisor。

您可以註冊最多五個成員帳戶。只有管理帳戶可以為組織新增委派管理員。您必須登入組織的管理帳戶，才能註冊或取消註冊委派管理員。

若要註冊委派管理員

1. 以管理帳戶登入 Trusted Advisor 主控台，網址是 https://console.aws.amazon.com/trustedadvisor/home。
2. 在導覽窗格的 Preferences (偏好設定) 中，選擇 Your organization (您的組織)。
3. 在 Delegated administrator (委派的管理員) 下，選擇 Register new account (註冊新帳戶)。
4. 在對話方塊中，輸入成員帳戶 ID，然後選擇 Register (註冊)。
5. (選用) 若要取消註冊帳戶，請選取帳戶並選擇 Deregister (取消註冊)。在對話方塊中，再次選擇 Deregister (取消註冊)。

取消註冊委派的管理員

當您取消註冊成員帳戶時，該帳戶將不再擁有與管理帳戶相同的 Trusted Advisor Priority 存取權。不再是委派管理員的帳戶將不會收到來自 Trusted Advisor Priority 的電子郵件通知。

若要取消註冊委派管理員

1. 以管理帳戶登入 Trusted Advisor 主控台，網址是 https://console.aws.amazon.com/trustedadvisor/home。
2. 在導覽窗格的 Preferences (偏好設定) 中，選擇 Your organization (您的組織)。
3. 在委派管理員下，選取帳戶，然後選擇取消註冊。
4. 在對話方塊中，選擇 Deregister (取消註冊)。

管理 Trusted Advisor Priority 通知

Trusted Advisor Priority 透過電子郵件傳送通知。此電子郵件通知包含您的客戶團隊為您優先處理的建議摘要。您可以指定從 Trusted Advisor Priority 接收更新的頻率。

如果您將成員帳戶註冊為委託管理員，他們也可以設定其帳戶以接收 Trusted Advisor Priority 電子郵件通知。

Trusted Advisor Priority 電子郵件通知不包含個別帳戶的檢查結果，並且獨立於每週的 Trusted Advisor Recommendations 通知。如需詳細資訊，請參閱設定通知偏好設定。

> **Note**
>
> 只有管理帳戶或委派管理員可以設定 Trusted Advisor Priority 電子郵件通知。

管理您的 Trusted Advisor Priority 通知

1. 以管理或委派管理員帳戶登入 Trusted Advisor 主控台，網址是 https://console.aws.amazon.com/trustedadvisor/home。
2. 在導覽窗格中，在 Preferences (偏好設定) 之下，選擇 Notifications (通知)。
3. 在 Priority 下，您可以選取下列選項。
   a. Daily (每日) - 每天收到電子郵件通知。
   b. Weekly (每週) - 每週收到一次電子郵件通知。
   c. 選擇要接收的通知：
      - 優先建議摘要
      - 解決日期
4. 對於收件人，選取要接收電子郵件通知的其他聯絡人。您可以從 AWS Billing and Cost Management 主控台的 Account Settings (帳戶設定) 頁面新增和移除聯絡人。
5. 對於 Language (語言)，選擇電子郵件通知的語言。
6. 選擇 Save your preferences (儲存喜好設定)。

> **Note**
>
> Trusted Advisor Priority 從 noreply@notifications.trustedadvisor.us-west-2.amazonaws.com 地址傳送電子郵件通知。您可能需要確認您的電子郵件用戶端不會將這些電子郵件識別為垃圾郵件。

停用 Trusted Advisor 優先權

請聯絡您的客戶團隊，請他們為您停用此功能。停用此功能後，您的 Trusted Advisor 主控台中將不再顯示優先建議。

如果停用 Trusted Advisor Priority，然後再次啟用它，您仍然可以檢視在您停用 Trusted Advisor Priority 之前客戶團隊傳送的建議。

開始使用 AWS Trusted Advisor Engage (預覽版)

> **Note**
>
> AWS Trusted Advisor Engage 目前為預覽版本，並可能有所變更。您可以在此處查看預覽版本的服務條款： https://aws.amazon.com/service-terms/。

您可以使用 AWS Trusted Advisor Engage 來讓您輕鬆查看、請求和追蹤所有積極業務開發，藉此充分運用您的 AWS Support 計畫，並與您的 AWS 帳戶 團隊溝通有關正在進行的業務開發。

例如，您可以前往 AWS Trusted Advisor 主控台中的 Engage 頁面，向 AWS 帳戶 團隊請求「管理商業審查」。然後，系統會指派 AWS 專家至您的請求，並繼續完成整個業務開發。

主題

必要條件

您必須採取必要的行動，滿足下列要求才能使用 Trusted Advisor Engage：

- 您必須擁有 Enterprise On-Ramp Support 計畫。
- 您的帳戶必須是 AWS Organizations 中啟用了所有功能的組織的一部分。如需詳細資訊，請參閱 AWS Organizations 使用者指南中的啟用組織中的所有功能。
- 您的組織必須具有已啟用受信任的 Trusted Advisor 存取權。以管理帳戶身分登入，然後前往 Trusted Advisor 主控台中的您的組織頁面，即可啟用受信任的存取權。
- 您必須擁有 AWS Identity and Access Management (IAM) 許可，才能存取 Trusted Advisor Engage。如需有關如何控制 Trusted Advisor Engage 存取權的詳細資訊，請參閱 管理存取 AWS Trusted Advisor。

> **Note**
>
> AWS Organization 內的任何帳戶皆可建立業務開發請求。如果業務開發擁有的帳戶移至其他 AWS Organization，則該業務開發僅可由該帳戶存取。若要限制控制權，請參閱 適用於 AWS Trusted Advisor的服務控制政策範例。

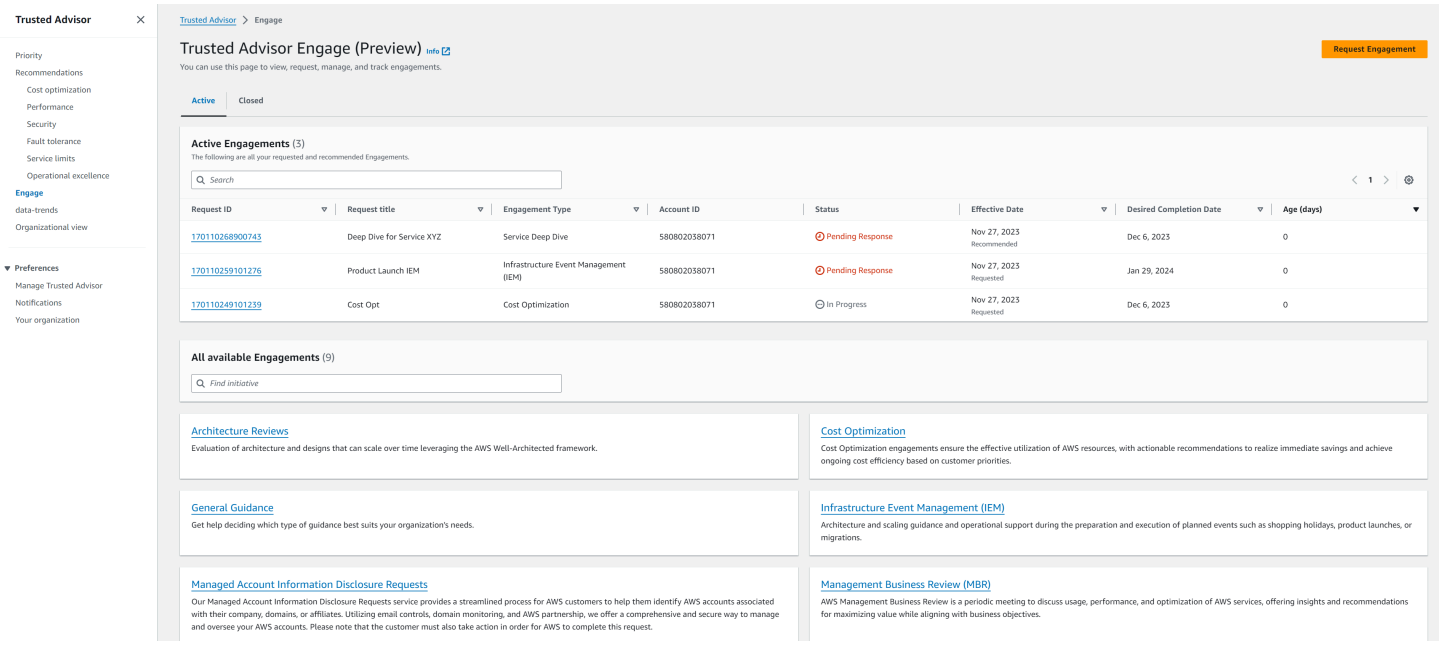
檢視業務開發儀表板

取得存取權後，您可以在 Trusted Advisor 主控台內存取 Trusted Advisor Engage 頁面來檢視儀表板，您可以在其中與您的 AWS 帳戶 團隊管理參與。

若要管理您的業務開發：

1. 登入 Trusted Advisor 主控台，網址是 https://console.aws.amazon.com/trustedadvisor/home。
2. 在 Trusted Advisor Engage 頁面上，您可以檢視：
   - 請求業務開發按鈕
   - 作用中參與表格
   - 已結案業務開發表格
   - 所有可用的參與型錄

Example ：參與儀表板



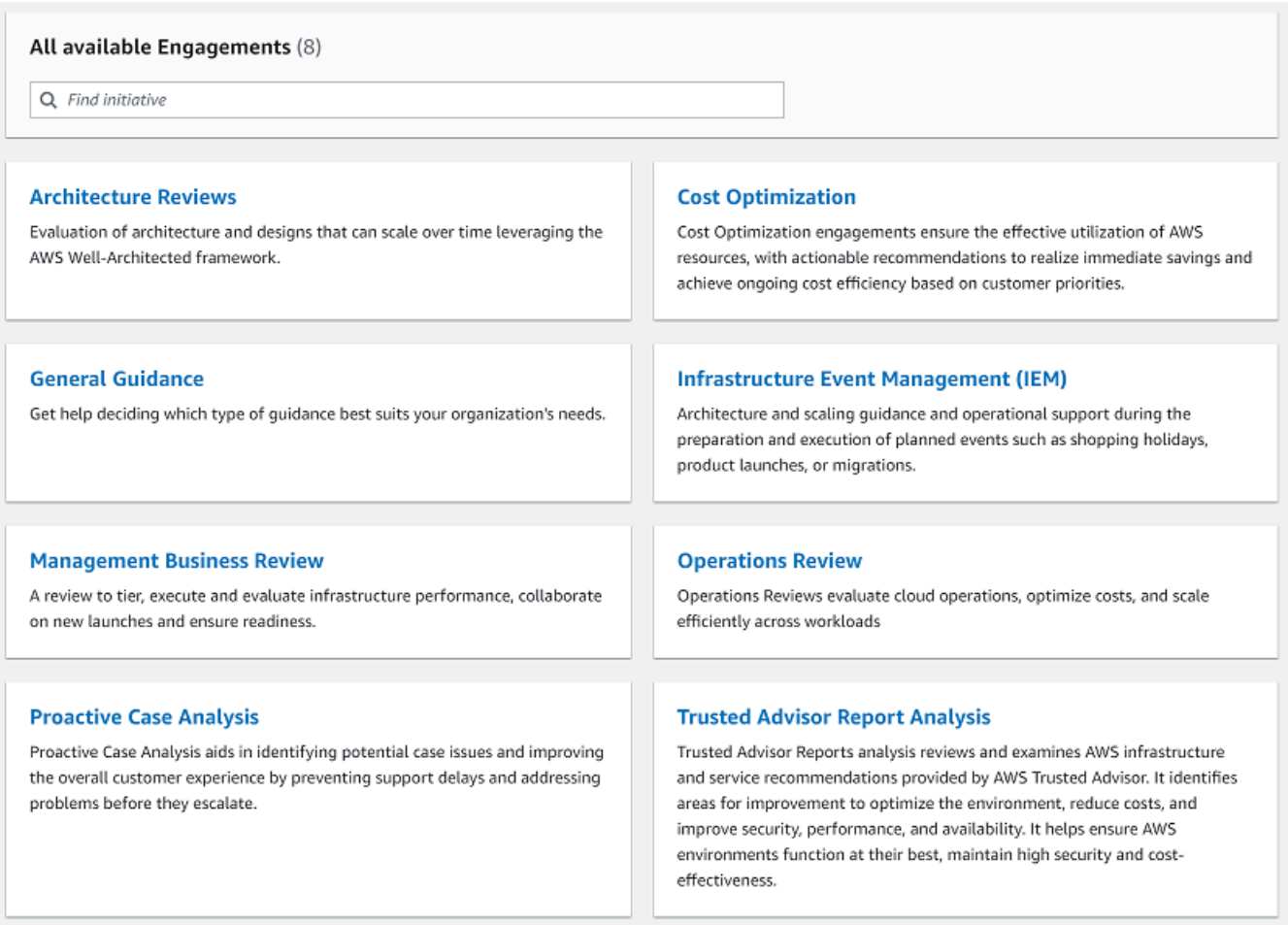
檢視業務開發類型的型錄

您可以檢視業務開發類型的型錄，找出可向您的 AWS 帳戶 團隊請求的最新業務開發類型。

若要檢視業務開發類型的型錄：

1. 登入 Trusted Advisor 主控台，網址是 https://console.aws.amazon.com/trustedadvisor/home。
2. 在 Trusted Advisor Engage 頁面上，您可以找到業務開發類型的型錄。

Example ：參與類型型錄



請求業務開發

您可以根據 AWS Support Plan 中包含的業務開發類型來向您的 AWS 帳戶 團隊請求業務開發。

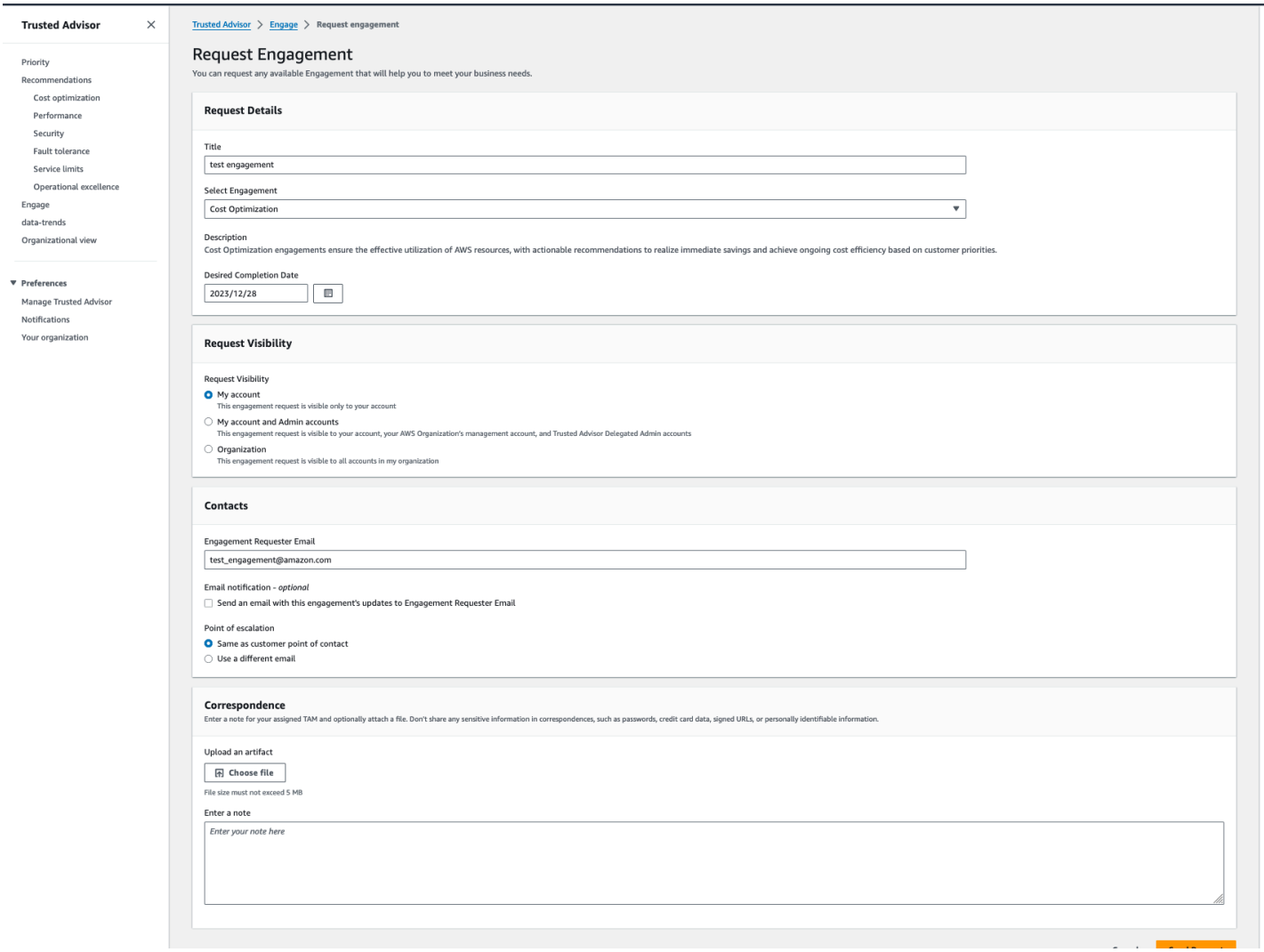
若要請求業務開發：

1. 登入 Trusted Advisor 主控台，網址是 https://console.aws.amazon.com/trustedadvisor/home。
2. 在 Trusted Advisor Engage 頁面上，選擇請求業務開發。
3. 填寫以下欄位：
   - 標題
   - 選取業務開發：您要請求的業務開發之類型。
   - 預計完成日期：業務開發的預計完成日期。每個「業務開發類型」皆有不同的前置時間，前置時間是以最小預計完成日期計算。

- 請求可見性：
  - 我的帳戶：唯有您的帳戶才能看到此業務開發請求。
  - 我的帳戶和管理員帳戶：您的帳戶以及 AWS Organization 的管理帳戶和所有委派管理員帳戶均可看到此業務開發請求。
  - 組織：您的 AWS Organization 中的所有帳戶均可看見此業務開發請求。
- 參與請求者電子郵件：AWS將用作此參與主要聯絡人的電子郵件地址。
- 電子郵件通知設定：選擇「參與請求者電子郵件」是否會收到有關參與的電子郵件通知。
- 提升點：AWS 會在此業務開發需要提升時使用的電子郵件地址。
- 通訊：備註與選擇性檔案附件，供您提供有關此業務開發的詳細資訊。

4. 選擇傳送請求。

Example ：請求業務開發



編輯業務開發

您可以編輯業務開發請求的詳細資訊。

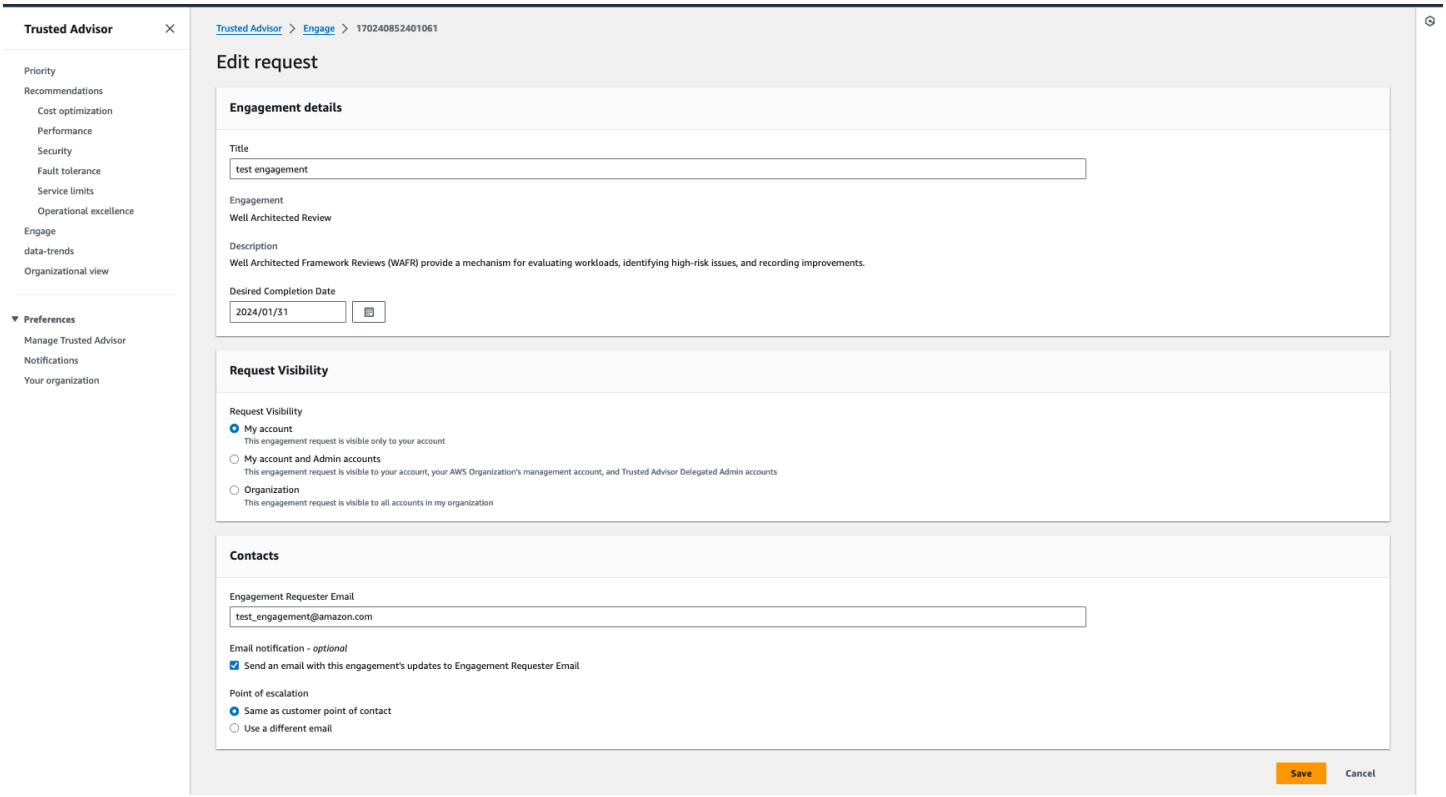
若要編輯業務開發：

1. 登入 Trusted Advisor 主控台，網址是 https://console.aws.amazon.com/trustedadvisor/home。
2. 在 Trusted Advisor Engage 頁面上，選取現有的業務開發。
3. 選擇 Edit (編輯)。
4. 您可以編輯下列項目：
   - 標題

- 預計完成日期：業務開發的預計完成日期。每個「業務開發類型」皆有不同的前置時間，前置時間是以最小預計完成日期計算。
- 請求可見性：
  - 我的帳戶：唯有您的帳戶才能看到此業務開發請求。
  - 我的帳戶和管理員帳戶：您的帳戶以及 AWS Organization 的管理帳戶和所有委派管理員帳戶均可看到此業務開發請求。
  - 組織：您的 AWS Organization 中的所有帳戶均可看見此業務開發請求。
- 參與請求者電子郵件：AWS將用作此參與主要聯絡人的電子郵件地址。
- 電子郵件通知設定：選擇「參與請求者電子郵件」是否會收到有關參與的電子郵件通知。
- 提升點：AWS 會在此業務開發需要提升時使用的電子郵件地址。

5. 選擇儲存。

Example ：編輯參與



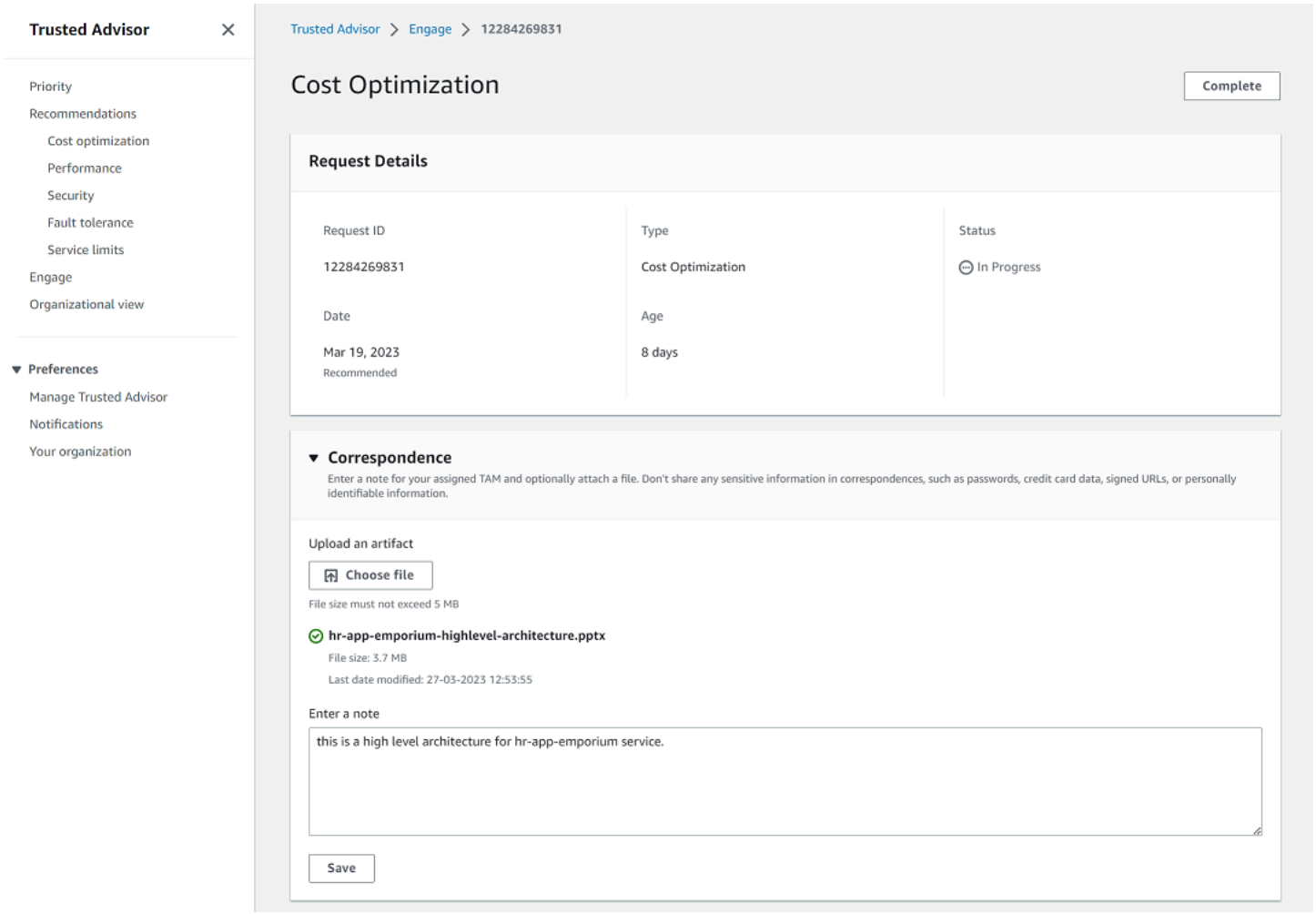
提交附件和備註

您可以透過傳送備註與檔案附件的方式與您的 AWS 帳戶 團隊就個別業務開發進行溝通，藉此支援業務開發請求。您可以在每次通訊中包含單一附件與備註，您只能將檔案附加至具有與請求業務開發相同的 AWS 帳戶 之業務開發，且您無法在傳送通訊之後刪除附件或備註。

若要附加檔案或將備註新增至作用中業務開發請求：

1. 登入 Trusted Advisor 主控台，網址是 https://console.aws.amazon.com/trustedadvisor/home。
2. 在 Trusted Advisor Engage 頁面上，選擇您要附加檔案或新增備註的作用中業務開發之 ID。
3. 選擇通訊以展開表單。
4. 為指派的 TAM 輸入備註，另可選擇是否要附加檔案。不要在通訊中分享任何敏感資訊，例如密碼、信用卡資料、簽署的 URL，或可識別個人身分的資訊。
5. 選擇儲存。

Example ：新增備註並將檔案附加至參與



變更業務開發狀態

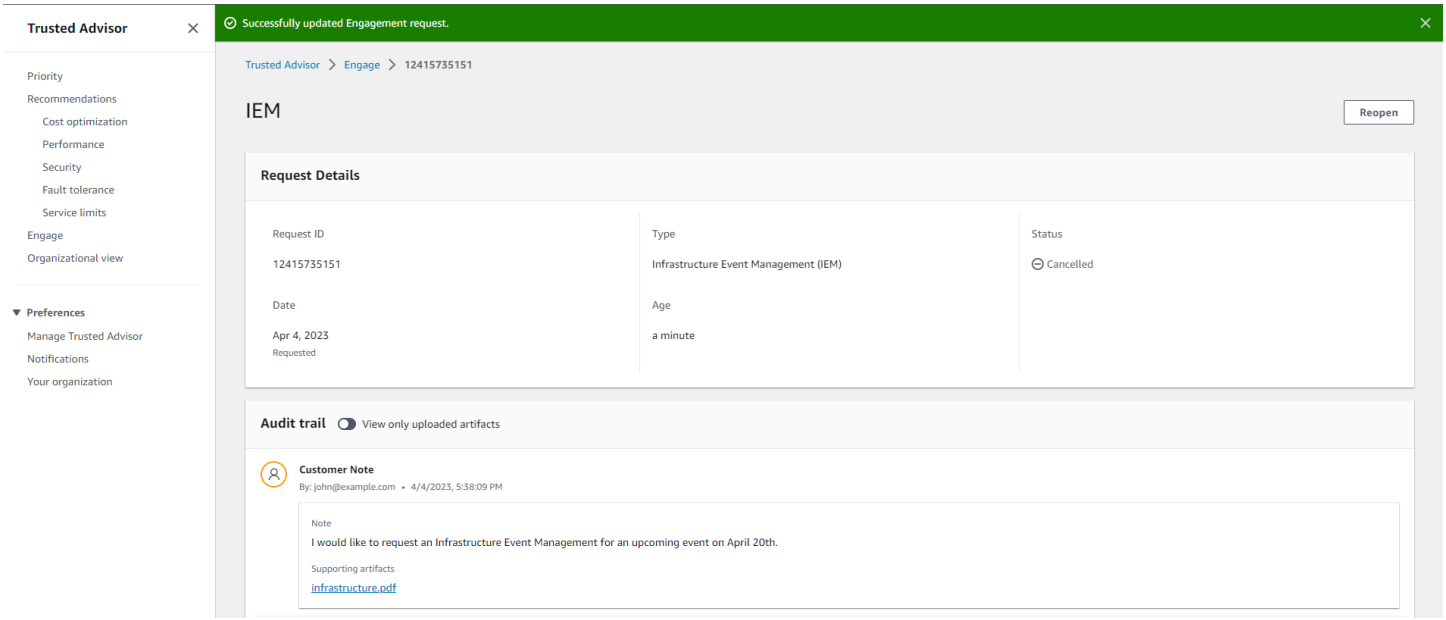
您可以變更該業務開發狀態以取消待定回應的業務開發、完成進行中的業務開發，以及重新開啟標示為已取消或已結案的業務開發。

若要變更業務開發的狀態：

1. 登入 Trusted Advisor 主控台，網址是 https://console.aws.amazon.com/trustedadvisor/home。
2. 在 Trusted Advisor Engage 頁面上，選擇您要變更狀態的作用中業務開發之 ID。
3. 在業務開發詳細資訊頁面上，您可以將狀態變更為已取消或已完成。
   - 當業務開發狀態為待定回應時，您可以選取取消。
   - 當業務開發狀態為進行中時，您可以選取完成。

- 您可以為已結案的業務開發選取重新開啟。已取消的業務開發會移至待定回應，而完成的業務開發會移至進行中。

Example ：變更參與狀態



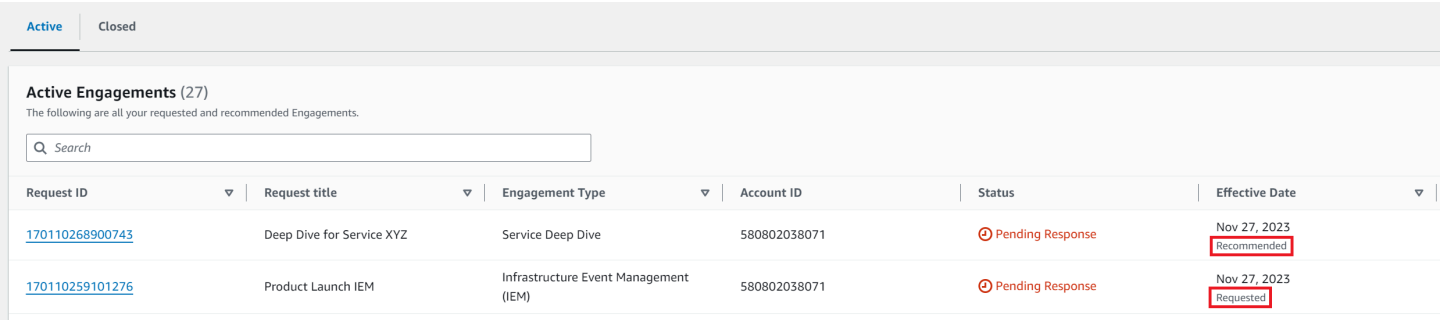
區分建議和請求的業務開發

您可以識別業務開發的來源，藉此瞭解業務開發是由您所請求還是由您的 AWS 帳戶 團隊所建議。

若要檢視作用中業務開發的不同來源：

1. 登入 Trusted Advisor 主控台，網址是 https://console.aws.amazon.com/trustedadvisor/home。
2. 在「Trusted Advisor參與」頁面上，檢視「生效日期」欄，以區分「建議」與「請求的參與」：
   - 建議：由您的 AWS 帳戶 團隊所建立的業務開發請求。
   - 請求：由使用者建立的業務開發請求。

Example ：區分建議和請求的業務開發



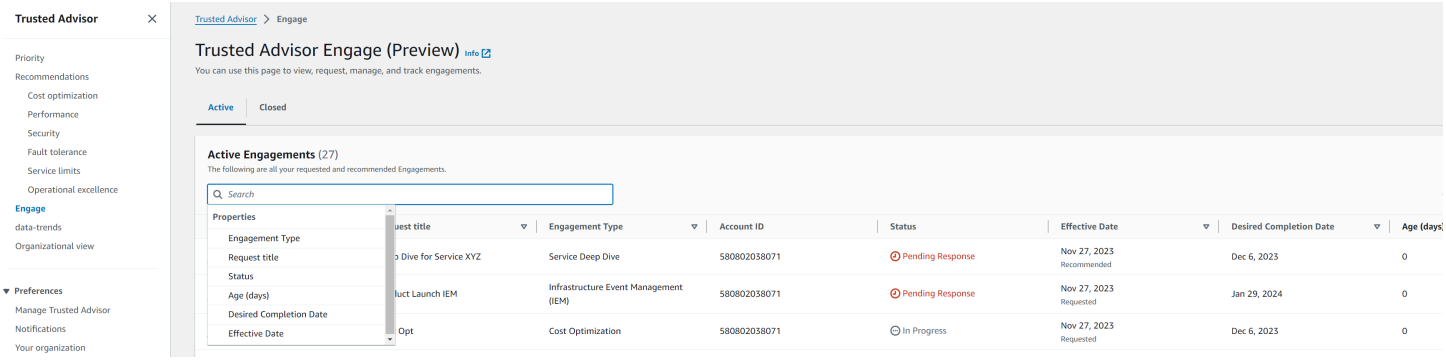
搜尋業務開發

您可以使用篩選條件來搜尋目前作用中和已結案的業務開發。

若要搜尋業務開發：

1. 登入 Trusted Advisor 主控台，網址是 https://console.aws.amazon.com/trustedadvisor/home。
2. 在 Trusted Advisor Engage 頁面上，您可以選取下列篩選條件：
   - 效齡 (天)
   - 業務開發類型
   - 請求標題
   - 狀態
   - 期望完成日期
   - 生效日期

Example ：搜尋參與



AWS Trusted Advisor 檢查參考

您可以檢視下列參考中的所有 Trusted Advisor 檢查名稱、描述和 ID。您也可登入 Trusted Advisor 主控台，檢視有關檢查、建議的動作及狀態的詳細資訊。

如果您有商業、Enterprise On-Ramp 或企業支援計劃，也可以使用 AWS Trusted Advisor API 和 AWS Command Line Interface (AWS CLI) 存取所有檢查。如需詳細資訊，請參閱下列主題：

- 開始使用 Trusted Advisor API
- AWS Trusted Advisor API 參考

> **Note**
>
> 如果您有基本支援或開發人員支援計劃，可以使用 Trusted Advisor 主控台存取 服務限制 類別中的所有檢查，以及安全性類別中的下列檢查：
>
> - Amazon EBS 公有快照
> - Amazon RDS 公有快照
> - Amazon S3 儲存貯體許可
> - IAM 使用情形
> - 根帳戶的 MFA
> - 安全群組— 不受限制的特定連接埠

檢查類別

- 成本最佳化
- 效能
- 安全
- 容錯能力
- 服務限制
- 營運卓越

成本最佳化

您可以針對成本最佳化類別使用下列檢查。

檢查名稱

- AWS 帳戶不是 AWS Organizations 的一部分
- Amazon Comprehend 使用率不足的端點
- Amazon EBS 過度佈建的磁碟區
- Microsoft SQL 伺服器的 Amazon EC2 執行個體合併
- Microsoft SQL 伺服器過度佈建的 Amazon EC2 執行個體
- Amazon EC2 執行個體已停止
- Amazon EC2 Reserved Instance Lease Expiration
- Amazon EC2 預留執行個體最佳化
- 未設定生命週期政策的 Amazon ECR 儲存庫
- Amazon ElastiCache 保留節點優化
- Amazon OpenSearch 服務預留實例優化
- Amazon RDS 閒置資料庫執行個體
- Amazon Redshift 預留節點最佳化
- Amazon Relational Database Service (RDS) 預留執行個體最佳化
- Amazon Route 53 延遲資源記錄集
- 已設定 Amazon S3 儲存貯體生命週期政策
- Amazon S3 不完整的多部分上傳中止組態
- 已啟用版本功能的 Amazon S3 儲存貯體 (未設定生命週期政策)
- 具有過多逾時的 AWS Lambda 函數
- 具有高錯誤率的 AWS Lambda 函數
- AWS Lambda 過度佈建的函數 (對於記憶體大小)
- AWS Well-Architected 成本最佳化的高風險問題
- 閒置負載平衡器
- Amazon EC2 執行個體低使用率
- Savings Plan
- 無關聯彈性 IP 地址
- 利用率過低的 Amazon EBS 磁碟區
- 利用率過低的 Amazon Redshift 叢集

AWS 帳戶不是 AWS Organizations 的一部分

描述

檢查 AWS 帳戶是否屬於適當管理帳戶下 AWS Organizations 的一部分。

AWS Organizations 是一種帳戶管理服務，用於將多個 AWS 帳戶整合到一個集中管理的組織中。這可讓您集中結構帳戶以進行帳單合併，並在工作負載於 AWS 擴展時實作擁有權與安全政策。

您可以使用AWS Config規則的MasterAccountId參數指定管理帳戶 ID。

如需詳細資訊，請參閱什麼是 AWS Organizations？

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz127
```

來源

```
AWS Config Managed Rule: account-part-of-organizations
```

警示條件

黃色：此 AWS 帳戶不是 AWS Organizations 的一部分。

建議的動作

將此 AWS 帳戶新增為 AWS Organizations 的一部分。

如需詳細資訊，請參閱教學課程：建立和設定組織。

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則

- 輸入參數
- 上次更新時間

Amazon Comprehend 使用率不足的端點

描述

檢查端點的輸送量組態。此檢查會在端點未主動用於即時推論請求時提醒您。系統會將超過連續 15 天未使用的端點視為未充分利用。所有端點都會根據設定的輸送量以及端點處於作用中的時間長度計費。

> **Note**
>
> 此檢查為每天自動重新整理一次。目前，您無法從此檢查中排除資源。

檢查 ID

`Cm24dfsM12`

警示條件

黃色：端點處於作用中狀態，但在過去 15 天其未用於即時推論請求。

建議的動作

如果過去 15 天未使用過該端點，建議您使用 Application Auto Scaling 定義資源的擴展政策。

如果端點已有定義的擴展政策，而且端點在過去 30 天內未使用，請考慮刪除該端點並使用非同步推論。如需詳細資訊，請參閱 Deleting an endpoint with Amazon Comprehend (使用 Amazon Comprehend 刪除端點)。

報告欄位

- Status
- 區域
- 端點 ARN
- 已佈建的推論單元
- AutoScaling 狀態
- 原因

- 上次更新時間

Amazon EBS 過度佈建的磁碟區

描述

檢查回顧期間在任何時間執行的 Amazon Elastic Block Store (Amazon EBS) 磁碟區。此檢查會提醒您注意工作負載 EBS 磁碟區過度佈建的情形。當您擁有過度佈建的磁碟區時，您需要為未使用的資源付費。雖然某些案例的本質可能會導致最佳化降低，但通常可以透過變更 EBS 磁碟區的組態來降低成本。預估每月節省成本是根據 EBS 磁碟區的目前使用率計算得出。如果磁碟區一整個月都沒有出現，實際節省的成本將有所不同。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`COr6dfpM03`

警示條件

黃色：回顧期間過度佈建的 EBS 磁碟區。若要判斷磁碟區是否過度佈建，我們會考慮所有預設 CloudWatch 指標 (包括 IOPS 和輸送量)。用於識別過度佈建的 EBS 磁碟區的演算法是依據 AWS 最佳實務。找出新的模式時，該演算法會更新。

建議的動作

請考慮縮減低使用率磁碟區的大小。

如需詳細資訊，請參閱 對於 AWS Compute Optimizer 檢查，選擇使用 Trusted Advisor。

報告欄位

- Status
- 區域
- 磁碟區 ID
- 磁碟區類型

- 磁碟區大小 (GB)
- 磁碟區基準 IOPS
- 磁碟區高載 IOPS
- 磁碟區高載輸送量
- 建議的磁碟區類型
- 建議的磁碟區大小 (GB)
- 建議的磁碟區基準 IOPS
- 建議的磁碟區高載 IOPS
- 建議的磁碟區基準輸送量
- 建議的磁碟區高載輸送量
- 回顧期間 (天)
- 成本節省機會 (%)
- 預估每月節省成本
- 預估每月節省成本貨幣
- 上次更新時間

Microsoft SQL 伺服器的 Amazon EC2 執行個體合併

描述

檢查過去 24 小時內執行 SQL 伺服器的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體。如果您的執行個體少於 SQL 伺服器授權的最小數量，這項檢查會提醒您。依據《Microsoft SQL Server 授權指南》，即使一個執行個體只有 1 個或 2 個 vCPU，您仍需支付 4 個 vCPUs 授權。您可以合併較小的 SQL 伺服器執行個體，以協助降低成本。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
Qsdfp3A4L2
```

警示條件

黃色：使用 SQL Server 的執行個體擁有的 vCPU 是少於 4 個。

建議的動作

請考慮將較小的 SQL Server 工作負載整合到至少具有 4 個 vCPU 的執行個體中。

其他資源

- 將 Microsoft SQL Server 遷移至 AWS
- AWS 上的 Microsoft 授權
- Microsoft SQL Server 授權指南

報告欄位

- Status
- 區域
- 執行個體 ID
- 執行個體類型
- vCPU
- vCPU 數量下限
- SQL Server 版本
- 上次更新時間

Microsoft SQL 伺服器過度佈建的 Amazon EC2 執行個體

描述

檢查過去 24 小時內執行 SQL 伺服器的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體。SQL 伺服器資料庫對每個執行個體都有運算容量限制。具有 SQL 伺服器標準版的執行個體最多可以使用 48 個 vCPUs。具有 SQL 伺服器 Web 版的執行個體最多可以使用 32 個 vCPUs。此檢查會在執行個體超過此 vCPU 限制時發出提醒。

如果您的執行個體過度佈建，則您會支付全額價格卻無法感受到效能提升。您可以管理執行個體的數量和大小，以協助降低成本。

預估每月節省成本是根據相同的執行個體系列搭配 SQL Server 執行個體可以使用的 vCPUs 數量上限以及隨需定價計算得出。如果您使用預留執行個體 (RI) 或是如果執行個體一整天都沒有執行，則實際節省的成本將有所不同。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`Qsdfp3A4L1`

警示條件

- 紅色：使用 SQL Server Standard 版的執行個體擁有的 vCPU 數量超過 48 個。
- 紅色：使用 SQL Server Web 版的執行個體擁有的 vCPU 數量超過 32 個。

建議的動作

如果是 SQL Server Standard 版，請考慮變更為使用具有 48 個 vCPU 的相同執行個體系列中的執行個體。如果是 SQL Server Web 版，請考慮變更為使用具有 32 個 vCPU 的相同執行個體系列中的執行個體。如果需要大量記憶體，請考慮變更為使用記憶體最佳化 R5 執行個體。如需詳細資訊，請參閱 Best Practices for Deploying Microsoft SQL Server on Amazon EC2 (《Amazon EC2 上部署 Microsoft SQL Server 的最佳實務》。

其他資源

- 將 Microsoft SQL Server 遷移至 AWS
- 您可以使用 Launch Wizard 來簡化您在 EC2 上的 SQL Server 部署。

報告欄位

- Status
- 區域
- 執行個體 ID
- 執行個體類型
- vCPU
- SQL Server 版本
- vCPU 數量上限
- 建議的執行個體類型
- 預估每月節省成本
- 上次更新時間

Amazon EC2 執行個體已停止

描述

檢查是否有已停止超過 30 天的 Amazon EC2 執行個體。

您可以在參數中指定允許的天AllowedDaysAWS Config數值。

如需詳細資訊，請參閱當我所有的執行個體終止時，為何會向我收取 Amazon EC2 的費用？

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz150
```

來源

```
AWS Config Managed Rule: ec2-stopped-instance
```

警示條件

- 黃色：有 Amazon EC2 執行個體已停止超過允許的天數。

建議的動作

檢閱已停止 30 天以上的 Amazon EC2 執行個體。為避免產生不必要的成本，請終止任何不再需要的執行個體。

如需詳細資訊，請參閱終止您的執行個體。

其他資源

- Amazon EC2 隨需定價

報告欄位

- Status
- 區域
- 資源

- AWS Config 規則
- 輸入參數
- 上次更新時間

Amazon EC2 Reserved Instance Lease Expiration

描述

排定在未來 30 天內過期，或已在過去 30 天內過期的 Amazon EC2 預留執行個體檢查。

預留執行個體不會自動續約。您可以繼續使用保留所涵蓋的 Amazon EC2 執行個體而無須中斷，但需支付依隨需費率計費的費用。新的預留執行個體可以具有與過期參數相同的參數，也可以購買具有不同參數的預留執行個體。

預估每月節省成本是在使用相同執行個體類型的情況下，使用隨需和預留執行個體費率間的差異。

檢查 ID

`1e93e4c0b5`

警示條件

- 黃色：預留執行個體的租賃將在 30 天後到期。
- 黃色：預留執行個體的租賃已在 30 天前到期。

建議的動作

請考慮購買新的預留執行個體來取代即將到期的預留執行個體。如需詳細資訊，請參閱如何購買預留執行個體和購買預留執行個體。

其他資源

- 預留執行個體
- 執行個體類型

報告欄位

- Status
- 區域
- 執行個體類型
- 平台
- 執行個體計數

- 目前每月成本
- 預估每月節省成本
- 到期日期
- 預留執行個體 ID
- 原因

Amazon EC2 預留執行個體最佳化

描述

使用 AWS 的重點之一是平衡您的預留執行個體 (RI) 用量和隨需執行個體用量。此檢查提供建議，說明哪些 RI 有助於降低使用隨需執行個體所產生的成本。

我們會分析過去 30 天內的隨需用量，用於建立這些建議。接著我們將用量分類為符合資格的保留類別。我們會在產生的用量類別中模擬每個保留組合，藉此識別每種 RI 類別的建議購買數量。這個模擬和最佳化過程讓我們能最大限度地節省您的成本。此檢查涵蓋以標準預留執行個體為基礎的建議，並提供部分預付款選項。

此檢查不適用於合併帳單的連結帳戶。此檢查的建議僅適用於付款帳戶。

檢查 ID

`cX3c2R1chu`

警示條件

黃色：最佳化部分預付預留執行個體的使用有助於降低成本。

建議的動作

請參閱 Cost Explorer 頁面以取得更詳細的自訂建議。此外，請參閱購買指南了解如何購買預留執行個體以及可用的選項。

其他資源

- 您可以在此處找到有關預留執行個體及其如何為您節省成本的資訊。
- 如需有關此建議的詳細資訊，請參閱《Trusted Advisor 常見問題》中的預留執行個體最佳化檢查問題。

報告欄位

- 區域

- 執行個體類型
- 平台
- 建議購買的預留執行個體數量
- 預期的預留執行個體平均使用率
- 依建議操作後預估可節省的成本 (每月)
- 預付預留執行個體成本
- 預估預留執行個體成本 (每月)
- 依建議購買預留執行個體後的預估隨需成本 (每月)
- 預估實現收支平衡的時間 (月)
- 回顧期間 (天)
- 期限 (年)

未設定生命週期政策的 Amazon ECR 儲存庫

描述

檢查私有 Amazon ECR 儲存庫是否至少設定了一個生命週期政策。生命週期政策可讓您定義一組規則，以自動清理舊的或未使用的容器映像。這可讓您控制映像的生命週期管理、讓 Amazon ECR 儲存庫更有條理，並有助於降低整體儲存成本。

如需詳細資訊，請參閱生命週期政策。

檢查 ID

```
c18d2gz128
```

來源

```
AWS Config Managed Rule: ecr-private-lifecycle-policy-configured
```

警示條件

黃色：Amazon ECR 私有儲存庫沒有任何已設定的生命週期政策。

建議的動作

請考慮為您的私有 Amazon ECR 儲存庫建立至少一個生命週期政策。

如需詳細資訊，請參閱建立生命週期政策。

其他資源

- 生命週期政策。
- 建立生命週期政策。
- 生命週期政策範例。

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

Amazon ElastiCache 保留節點優化

描述

檢查您的使用情況， ElastiCache 並提供有關購買預留節點的建議。提供這些建議是為了降低使用 ElastiCache 隨需產生的成本。我們會分析過去 30 天內的隨需用量，用於建立這些建議。

我們會使用此分析來模擬所產生用量類別中的每個保留組合。如此一來我們能建議每種預留節點類別的購買數量，讓您能最大程度節省成本。此檢查涵蓋的建議是依據搭配 1 年或 3 年綁約的部分預付款選項。

此檢查不適用於合併帳單的連結帳戶。此檢查的建議僅適用於付款帳戶。

檢查 ID

`h3L1otH3re`

警示條件

黃色：最佳化 ElastiCache 預留節點的購買有助於降低成本。

建議的動作

如需更詳細的建議、自訂選項 (例如、回顧期、付款選項等) 以及購買 ElastiCache 預留節點，請參閱 Cost Explorer 頁面。

其他資源

- 您可以在這裡找到有關 ElastiCache 預留節點以及如何為您節省資金的資訊。

- 如需有關此建議的詳細資訊，請參閱《Trusted Advisor 常見問題》中的預留執行個體最佳化檢查問題。
- 如需有關欄位的詳細資訊，請參閱 Cost Explorer 文件

報告欄位

- 區域
- 系列
- 節點類型
- 產品描述
- 建議購買的預留節點數量
- 預期的預留節點平均使用率
- 依建議操作後預估可節省的成本 (每月)
- 預付預留節點成本
- 預估預留節點成本 (每月)
- 依建議購買預留節點後的預估隨需成本 (每月)
- 預估實現收支平衡的時間 (月)
- 回顧期間 (天)
- 期限 (年)

Amazon OpenSearch 服務預留實例優化

描述

檢查 Amazon OpenSearch 服務的使用情況，並提供購買預留執行個體的建議。提供這些建議是為了降低使用 OpenSearch 隨需產生的成本。我們會分析過去 30 天內的隨需用量，用於建立這些建議。

我們會使用此分析來模擬所產生用量類別中的每個保留組合。如此一來我們能建議每種預留執行個體類別的購買數量，讓您能最大程度節省成本。此檢查涵蓋的建議是依據搭配 1 年或 3 年綁約的部分預付款選項。

此檢查不適用於合併帳單的連結帳戶。此檢查的建議僅適用於付款帳戶。

檢查 ID

```
7ujm6yhn5t
```

警示條件

黃色：優化購買 Amazon OpenSearch 服務預留執行個體可協助降低成本。

建議的動作

如需更詳細的建議、自訂選項 (例如回顧期、付款選項等)，以及購買 Amazon Ser OpenSearch vice 預留執行個體，請參閱 Cost Explorer 頁面。

其他資源

- 您可以在這裡找到有關 Amazon OpenSearch 服務預留執行個體的資訊，以及它們如何為您節省成本。
- 如需有關此建議的詳細資訊，請參閱《Trusted Advisor 常見問題》中的預留執行個體最佳化檢查問題。
- 如需有關欄位的詳細資訊，請參閱 Cost Explorer 文件

報告欄位

- 區域
- 執行個體類別
- 執行個體大小
- 建議購買的預留執行個體數量
- 預期的預留執行個體平均使用率
- 依建議操作後預估可節省的成本 (每月)
- 預付預留執行個體成本
- 預估預留執行個體成本 (每月)
- 依建議購買預留執行個體後的預估隨需成本 (每月)
- 預估實現收支平衡的時間 (月)
- 回顧期間 (天)
- 期限 (年)

Amazon RDS 閒置資料庫執行個體

描述

針對任何疑似閒置的資料庫 (DB) 執行個體，檢查 Amazon Relational Database Service (Amazon RDS) 的組態。

如果資料庫執行個體長時間沒有連線，您可以刪除執行個體以降低成本。如果執行個體在過去 7 天內沒有連線，系統便會將資料庫執行個體視為閒置。如果執行個體上的資料需要持久性儲存，您可以使用成本較低的選項，例如拍攝和保留資料庫快照。手動建立的資料庫快照會保留到您刪除為止。

檢查 ID

`Ti39halfu8`

警示條件

黃色：作用中資料庫執行個體在過去 7 天內未有連線。

建議的動作

請考慮建立閒置資料庫執行個體的快照，然後停止或刪除該資料庫執行個體。停止資料庫執行個體可免除其部分成本，但不會免除儲存成本。已停止的執行個體會在設定的保留期間內保留所有自動備份。與刪除執行個體並僅保留最終快照相比，停止資料庫執行個體通常會產生額外費用。請參閱暫時停止 Amazon RDS 執行個體和刪除具有最終快照的資料庫執行個體。

其他資源

備份與恢復

報告欄位

- 區域
- 資料庫執行個體名稱
- Multi-AZ
- 執行個體類型
- 已佈建的儲存空間 (GB)
- 自上次連線以來的天數
- 預估每月節省成本 (隨需)

Amazon Redshift 預留節點最佳化

描述

檢查您的 Amazon Redshift 使用情況，並提供預留節點購買建議，協助降低使用隨需 Amazon Redshift 產生的成本。

我們會分析過去 30 天內的隨需用量，用於產生這些建議。我們會使用此分析來模擬所產生用量類別中的每個保留組合。如此一來我們能找出每種預留節點類別的最佳數量，讓您能最大程度節省成本。此檢查涵蓋的建議是依據搭配 1 年或 3 年綁約的部分預付款選項。

此檢查不適用於合併帳單的連結帳戶。此檢查的建議僅適用於付款帳戶。

檢查 ID

`1qw23er45t`

警示條件

黃色：最佳化 Amazon Redshift 預留節點的購買有助於降低成本。

建議的動作

請參閱 Cost Explorer 頁面以取得更詳細的建議、自訂選項 (例如，回顧期間、支付選項等) 以及 Amazon Redshift 預留節點購買的相關資訊。

其他資源

- 您可以在此處找到有關 Amazon Redshift 預留節點及其如何為您節省成本的資訊。
- 如需有關此建議的詳細資訊，請參閱《Trusted Advisor 常見問題》中的預留執行個體最佳化檢查問題。
- 如需有關欄位的詳細資訊，請參閱 Cost Explorer 文件

報告欄位

- 區域
- 系列
- 節點類型
- 建議購買的預留節點數量
- 預期的預留節點平均使用率
- 依建議操作後預估可節省的成本 (每月)
- UpFront 預留節點的成本
- 預估預留節點成本 (每月)
- 依建議購買預留節點後的預估隨需成本 (每月)
- 預估實現收支平衡的時間 (月)
- 回顧期間 (天)
- 期限 (年)

Amazon Relational Database Service (RDS) 預留執行個體最佳化

描述

檢查您的 RDS 使用情況，並提供預留執行個體購買建議，協助降低使用隨需 RDS 產生的成本。

我們會分析過去 30 天內的隨需用量，用於產生這些建議。我們會使用此分析來模擬所產生用量類別中的每個保留組合。如此一來我們能找出每種預留執行個體類別的最佳數量，讓您能最大程度節省成本。此檢查涵蓋的建議是依據搭配 1 年或 3 年綁約的部分預付款選項。

此檢查不適用於合併帳單的連結帳戶。此檢查的建議僅適用於付款帳戶。

檢查 ID

`1qazXsw23e`

警示條件

黃色：最佳化 Amazon RDS 預留執行個體的購買有助於降低成本。

建議的動作

請參閱 Cost Explorer 頁面以取得更詳細的建議、自訂選項 (例如，回顧期間、支付選項等) 以及 Amazon RDS 預留節點購買的相關資訊。

其他資源

- 您可以在此處找到有關 Amazon RDS 預留執行個體及其如何為您節省成本的資訊。
- 如需有關此建議的詳細資訊，請參閱《Trusted Advisor 常見問題》中的預留執行個體最佳化檢查問題。
- 如需有關欄位的詳細資訊，請參閱 Cost Explorer 文件

報告欄位

- 區域
- 系列
- 執行個體類型
- 授權模式
- 資料庫版本
- 資料庫引擎
- 部署選項
- 建議購買的預留執行個體數量
- 預期的預留執行個體平均使用率

- 依建議操作後預估可節省的成本 (每月)
- 預付預留執行個體成本
- 預估預留執行個體成本 (每月)
- 依建議購買預留執行個體後的預估隨需成本 (每月)
- 預估實現收支平衡的時間 (月)
- 回顧期間 (天)
- 期限 (年)

Amazon Route 53 延遲資源記錄集

描述

檢查是否有設定效率低下的 Amazon Route 53 延遲記錄集。

若要允許 Amazon Route 53 將查詢路由到 AWS 區域，您應為不同區域中的特定網域名稱 (例如 example.com) 建立延遲資源記錄集。如果您只為網域名稱建立一個延遲資源記錄集，則所有查詢都會路由到一個區域，而且您需為以延遲為基礎的路由額外付費，而不會獲得好處。

AWS 服務建立的託管區域不會出現在您的檢查結果中。

檢查 ID

`51fC20e7I2`

警示條件

黃色：特定網域名稱僅設定有一個延遲資源記錄集。

建議的動作

如果您在多個區域擁有資源，請務必為每個區域定義一個延遲資源記錄集。請參閱以延遲為基礎的路由。

如果您只在一個 AWS 區域 擁有資源，請考慮在多個 AWS 區域 中建立資源，並為每個區域定義延遲資源記錄集；請參閱以延遲為基礎的路由。

如果您不想使用多個 AWS 區域，應該使用簡單的資源記錄集。請參閱使用資源記錄集。

其他資源

- 《Amazon Route 53 開發人員指南》
- Amazon Route 53 定價

報告欄位

- 託管區域名稱
- 託管區域 ID
- 資源記錄集名稱
- 資源記錄集類型

已設定 Amazon S3 儲存貯體生命週期政策

描述

檢查 Amazon S3 儲存貯體是否設定了生命週期政策。Amazon S3 生命週期政策可確保儲存貯體內的 Amazon S3 物件在其整個生命週期內以具成本效益的方式儲存。對於滿足資料保留和儲存的法規要求而言，這一點非常重要。政策組態是一組定義由 Amazon S3 服務套用至物件群組之動作的規則。生命週期政策可讓您自動將物件轉換為成本較低的儲存類別，或隨著這些物件效齡增加而予以刪除。例如，您可以在建立物件後 30 天內將物件轉換至 Amazon S3 Standard-IA 儲存體，或在 1 年後轉換至 Amazon S3 Glacier。

您也可以定義物件到期時間，讓 Amazon S3 在一段時間後代表您刪除物件。

您可以使用 AWS Config 規則中的參數來調整檢查組態

如需詳細資訊，請參閱管理儲存生命週期。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz100
```

來源

```
AWS Config Managed Rule: s3-lifecycle-policy-check
```

警示條件

黃色：Amazon S3 儲存貯體沒有已設定的生命週期政策。

建議的動作

確保您在 Amazon S3 儲存貯體中設定了生命週期政策。

如果您的組織未準備保留政策，請考慮使用 Amazon S3 Intelligent-Tiering 來最佳化成本。

如需如何定義 Amazon S3 生命週期政策的相關資訊，請參閱在儲存貯體上設定生命週期組態。

如需 Amazon S3 Intelligent-Tiering 的相關資訊，請參閱 Amazon S3 Intelligent-Tiering 儲存類別

其他資源

設定儲存貯體的生命週期組態

S3 生命週期組態範例

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數

Amazon S3 不完整的多部分上傳中止組態

描述

檢查每個 Amazon S3 儲存貯體是否設定了生命週期規則，以中止 7 天後仍不完整的多部分上傳。建議使用生命週期規則中止這些不完整的上傳並刪除相關的儲存空間。

> **Note**
>
> 此檢查的結果會每天自動重新整理一次或多次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c1cj39rr6v
```

警示條件

黃色：生命週期組態值區不包含生命週期規則，可中止 7 天後仍未完成的所有分段上傳。

建議的動作

檢閱值區的生命週期組態，而不需要清除所有不完整分段上傳的生命週期規則。24 小時後未完成的上傳不太可能完成。按一下此處以遵循指示建立生命週期規則。建議您將此選項套用至值區中的所有物件。如果您需要將其他生命週期動作套用至值區中選取的物件，則可以使用不同篩選器建立多個規則。如需詳細資訊，請查看儲存鏡頭儀表板或呼叫 ListMultipartUpload API。

其他資源

建立生命週期組態

探索和刪除不完整的分段上傳以降低 Amazon S3 成本

使用分段上傳來上載和複製物件

生命週期組態元

描述生命週期動作的元素

中止多部分上傳的生命週期組態

報告欄位

- Status
- 區域
- 儲存貯體名稱
- 儲存貯體 ARN
- 刪除不完整 MPU 的生命週期規則
- 啟動後的天數
- 上次更新時間

已啟用版本功能的 Amazon S3 儲存貯體 (未設定生命週期政策)

描述

檢查已啟用版本功能的 Amazon S3 儲存貯體是否設定了生命週期政策。

如需詳細資訊，請參閱管理儲存生命週期。

您可以使用 AWS Config 規則中的 bucketNames 參數來指定要檢查的儲存貯體名稱。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

c18d2gz171

來源

AWS Config Managed Rule: s3-version-lifecycle-policy-check

警示條件

黃色：已啟用版本功能的 Amazon S3 儲存貯體沒有已設定的生命週期政策。

建議的動作

為 Amazon S3 儲存貯體設定生命週期政策以管理您的物件，使其在整個生命週期之中能以更符合成本效益的方式儲存。

如需詳細資訊，請參閱在儲存貯體上設定生命週期組態。

其他資源

管理儲存生命週期

設定儲存貯體的生命週期組態

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數

- 上次更新時間

具有過多逾時的 AWS Lambda 函數

描述

檢查是否有 Lambda 函數具有高逾時率而可能導致高成本。

Lambda 費用是根據您函數的執行時間和請求數量計費。函數逾時導致的錯誤可能會引發重試。重試函數會產生額外的請求和執行時間費用。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`L4dfs2Q3C3`

警示條件

黃色：過去 7 天內，有任何一天由於逾時導致超過 10% 的叫用以錯誤結束的函數。

建議的動作

檢查函數記錄和 X-Ray 追蹤，找出函數高持續時間的貢獻來源。在相關部分 (例如 API 呼叫或資料庫連線之前或之後) 在程式碼中實作記錄。根據預設，AWS SDK 用戶端逾時可能會超過設定的函數持續時間。調整 API 和 SDK 連線用戶端，以便在函數逾時內重試或失敗。如果預期的持續時間長於設定的逾時，您可以增加函數的逾時設定時長。如需詳細資訊，請參閱監控與疑難排解 Lambda 應用程式。

其他資源

- 監控與疑難排解 Lambda 應用程式
- Lambda 函數重試逾時 SDK
- 將 AWS Lambda 與 AWS X-Ray 搭配使用
- 訪問 Amazon CloudWatch 日誌 AWS Lambda
- AWS Lambda 的錯誤處理器範例應用程式

報告欄位

- Status
- 區域
- 函數 ARN
- 每日逾時率上限
- 達到每日逾時率上限的日期
- 平均每日逾時率
- 函數逾時設定 (毫秒)
- 每日損失的運算成本
- 平均每日叫用次數
- 當日叫用次數
- 當日逾時率
- 上次更新時間

具有高錯誤率的 AWS Lambda 函數

描述

檢查是否有 Lambda 函數具有高錯誤率而可能導致成本較高。

Lambda 費用是根據您函數的請求數量和彙總執行時間計費。函數錯誤可能會導致重試，而產生額外費用。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`L4dfs2Q3C2`

警示條件

黃色：過去 7 天內，有任何一天有超過 10% 的叫用以錯誤結束的函數。

建議的動作

請考慮遵循下列指南，以減少錯誤。函數錯誤包含函式程式碼所傳回的錯誤，以及函式執行階段所傳回的錯誤。

為了協助您疑難排解 Lambda 錯誤，Lambda 與 Amazon CloudWatch 和AWS X-Ray. 您可以組合使用日誌、指標、警示及 X-Ray 追蹤，快速偵測及識別您的函數程式碼、API 或其他支援您應用程式的資源中的問題。如需詳細資訊，請參閱監控與疑難排解 Lambda 應用程式。

如需有關使用特定執行階段處理錯誤的詳細資訊，請參閱 AWS Lambda 中錯誤處理和自動重試。

如需其他疑難排解，請參閱針對 Lambda 中的問題進行疑難排解。

您還可以從 AWS Lambda 合作夥伴所提供的監控和觀察工具生態系統中進行選擇。如需詳細資訊，請參閱 AWS Lambda 合作夥伴。

其他資源

- AWS Lambda 中錯誤處理和自動重試
- 監控與疑難排解 Lambda 應用程式
- Lambda 函數重試逾時 SDK
- 針對 Lambda 中的問題進行疑難排解
- API 叫用錯誤
- AWS Lambda 的錯誤處理器範例應用程式

報告欄位

- Status
- 區域
- 函數 ARN
- 每日錯誤率上限
- 達到最大錯誤率的日期
- 平均每日錯誤率
- 每日損失的運算成本
- 平均每日叫用次數
- 當日叫用次數

  當日錯誤率

- 上次更新時間

AWS Lambda 過度佈建的函數 (對於記憶體大小)

描述

檢查回顧期間已呼叫至少一次的 AWS Lambda 函數。此檢查會提醒您任何 Lambda 函數在記憶體大小過度佈建的情形。如果您的 Lambda 函數在記憶體大小過度佈建，則需要為未使用的資源付費。雖然某些案例的本質可能會導致使用率低，但通常可以透過變更 Lambda 函數的記憶體組態來降低成本。預估每月節省成本是根據 Lambda 函數的目前使用率計算得出。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`C0r6dfpM05`

警示條件

黃色：在回顧期間記憶體大小過度佈建的 Lambda 函數。若要判斷 Lambda 函數是否過度佈建，我們會考慮該函數的所有預設 CloudWatch 指標。用於識別記憶體大小過度佈建的 Lambda 函數的演算法是依據 AWS 最佳實務。找出新的模式時，該演算法會更新。

建議的動作

請考慮縮減 Lambda 函數的記憶體大小。

如需詳細資訊，請參閱 對於 AWS Compute Optimizer 檢查，選擇使用 Trusted Advisor。

報告欄位

- Status
- 區域
- 函數名稱
- 函數版本
- 記憶體大小 (MB)
- 建議的記憶體大小 (MB)

- 回顧期間 (天)
- 成本節省機會 (%)
- 預估每月節省成本
- 預估每月節省成本貨幣
- 上次更新時間

AWS Well-Architected 成本最佳化的高風險問題

描述

檢查成本最佳化支柱中，工作負載是否有高風險問題 (HRI)。這項檢查是以您的 AWS-Well Architected 檢閱為基礎。您的檢查結果取決於您是否使用 AWS Well-Architected 完成工作負載評估。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`Wxdfp4B1L1`

警示條件

- 紅色：在 AWS Well-Architected 的成本最佳化支柱中發現至少一個待處理的高風險問題。
- 綠色：綠色：在 AWS Well-Architected 的成本最佳化支柱中未發現任何待處理的高風險問題。

建議的動作

AWS Well-Architected 在工作負載評估期間偵測到高風險問題。解決這些問題，可能有機會降低風險和節省成本。登入 AWS Well-Architected 工具，檢閱答案並採取行動，解決待處理的問題。

報告欄位

- Status
- 區域
- 工作負載 ARN
- 工作負載名稱

- 檢閱者姓名
- 工作負載類型
- 工作負載開始日期
- 工作負載上次修改日期
- 成本最佳化方面已識別的高風險問題數量
- 成本最佳化方面已解決的高風險問題數量
- 成本最佳化方面已回答的問題數量
- 成本最佳化支柱中的問題總數
- 上次更新時間

閒置負載平衡器

描述

檢查 Elastic Load Balancing 組態是否有閒置的負載平衡器。

任何已設定的負載平衡器都會累積費用。如果負載平衡器沒有相關聯的後端執行個體，或者網路流量受到嚴重限制，便無法有效使用負載平衡器。這項檢查目前只會檢查 ELB 服務中的 Classic Load Balancer 類型。不包括其他 ELB 類型 (Application Load Balancer、Network Load Balancer)。

檢查 ID

`hjLMh88uM8`

警示條件

- 黃色：負載平衡器沒有作用中的後端執行個體。
- 黃色：負載平衡器沒有運作良好的後端執行個體。
- 黃色：在過去 7 天內，負載平衡器每天的請求數量少於 100 個。

建議的動作

如果您的負載平衡器沒有作用中的後端執行個體，請考慮註冊執行個體或刪除您的負載平衡器。請參閱向 Load Balancer 註冊 Amazon EC2 執行個體或刪除負載平衡器。

如果您的負載平衡器沒有運作良好的後端執行個體，請參閱疑難排解 Elastic Load Balancing：運作狀態檢查組態。

如果您的負載平衡器請求數量較低，請考慮刪除負載平衡器。請參閱刪除負載平衡器。

其他資源

- 管理負載平衡器
- 疑難排解彈性負載平衡

報告欄位

- 區域
- 負載平衡器名稱
- 原因
- 預估每月節省成本

Amazon EC2 執行個體低使用率

描述

檢查過去 14 天內在任何時間執行的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體。如果每日 CPU 使用率為 10% 或以下，且網路輸入/輸出為 5 MB 或以下至少 4 天，此檢查就會發出提醒。

執行中的執行個體會產生以小時計的使用費。雖然某些案例的本質可能會導致使用率低，但通常可以透過管理執行個體的數量和大小來降低成本。

預估每月節省成本是根據隨需執行個體的目前使用率以及執行個體可能利用率過低的預估天數計算得出。如果您使用預留執行個體或 Spot 執行個體，或是當執行個體一整天都沒有執行，實際節省的成本將有所不同。若要取得每日使用率資料，請下載此檢查的報告。

檢查 ID

```
Qch7DwouX1
```

警示條件

黃色：在過去 14 天中,有執行個體至少 4 天每日平均 CPU 使用率為 10% 或更低，網路 I/O 量為 5 MB 或更少。

建議的動作

請考慮停止或終止使用率低的執行個體，或使用 Auto Scaling 來調整執行個體數量。如需詳細資訊，請參閱停止和啟動執行個體、終止您的執行個體，以及 Auto Scaling 是什麼？

其他資源

- 監控 Amazon EC2

- 執行個體中繼資料與使用者資料
- Amazon CloudWatch 用戶指南
- 《Auto Scaling 開發者指南》

報告欄位

- 區域/可用區域
- 執行個體 ID
- 執行個體名稱
- 執行個體類型
- 預估每月節省成本
- 14 天 CPU 平均使用率
- 14 天平均網路 I/O 量
- 使用率低的天數

Savings Plan

描述

檢查過去 30 天內 Amazon EC2、Fargate 和 Lambda 的使用情況，並提供 Savings Plan 購買建議。這些建議可讓您以每小時美元計價的一致用量綁約一年或三年，來換取折扣的費率。

這些資料的來源是 AWS Cost Explorer，可取得更詳細的建議資訊。您也可以透過 Cost Explorer 購買 Savings Plan。這些建議應視為您的 RI 建議的替代方案。建議您只針對一組建議採取行動。同時對兩組採取行動可能會導致綁約內容超過負荷。

此檢查不適用於合併帳單的連結帳戶。此檢查的建議僅適用於付款帳戶。

檢查 ID

`vZ2c2W1srf`

警示條件

黃色：最佳化 Savings Plans 的購買有助於降低成本。

建議的動作

請參閱 Cost Explorer 頁面以取得更詳細的自訂建議，以及 Savings Plans 購買的相關資訊。

其他資源

- Savings Plan User Guide (《Savings Plans 使用者指南》)
- Savings Plans 常見問題集

報告欄位

- Savings Plans 類型
- 付款選項
- 預付成本
- 每小時承諾購買量
- 預估平均使用率
- 預估每月節省成本
- 預估節省百分比
- 期限 (年)
- 回顧期間 (天)

無關聯彈性 IP 地址

描述

檢查與執行中 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體無關聯的彈性 IP 地址 (EIP)。

EIP 是針對動態雲端運算設計的靜態 IP 地址。與傳統靜態 IP 地址不同，EIP 會透過將公有 IP 地址重新映射至帳戶中的另一個執行個體，藉此遮罩執行個體或可用區域的故障。針對與執行中的執行個體無關聯的 EIP，會收取名目費用。

檢查 ID

Z4AUBRNSmz

警示條件

黃色：已分配的彈性 IP 地址 (EIP) 未與執行中的 Amazon EC2 執行個體建立關聯。

建議的動作

將 EIP 與執行中的作用中執行個體建立關聯，或釋出沒有關聯的 EIP。如需詳細資訊，請參閱建立彈性 IP 地址與其他執行中的執行個體的關聯和釋出彈性 IP 地址。

其他資源

彈性 IP 地址

報告欄位

- 區域
- IP Address (IP 地址)

利用率過低的 Amazon EBS 磁碟區

描述

檢查 Amazon Elastic Block Store (Amazon EBS) 磁碟區組態，並在磁碟區利用率似乎過低時發出警告。

磁碟區建立時會開始計費。如果磁碟區在一段時間內維持未連接狀態或寫入活動非常少 (不包括開機磁碟區)，表示該磁碟區利用率過低。建議您移除利用率過低的磁碟區以降低成本。

檢查 ID

DAvU99Dc4C

警示條件

黃色：在過去 7 天內，磁碟區未連接或磁碟區每天的 IOPS 數量少於 1 個。

建議的動作

請考慮建立快照並刪除磁碟區以降低成本。如需詳細資訊，請參閱建立 Amazon EBS 快照和刪除 Amazon EBS 磁碟區。

其他資源

- Amazon Elastic Block Store (Amazon EBS)
- 監控您的磁碟區狀態

報告欄位

- 區域
- 磁碟區 ID
- 磁碟區名稱
- 磁碟區類型
- 磁碟區大小

- 每月儲存成本
- 快照 ID
- 快照名稱
- 快照存在時間

> **Note**
>
> 如果您選擇使用 AWS Compute Optimizer 專用帳戶，建議您改用 Amazon EBS 過度佈建的磁碟區。如需詳細資訊，請參閱 對於 AWS Compute Optimizer 檢查，選擇使用 Trusted Advisor。

利用率過低的 Amazon Redshift 叢集

描述

檢查您的 Amazon Redshift 組態是否有似乎利用率過低的叢集。

如果 Amazon Redshift 叢集長時間沒有連線，或者使用的 CPU 量很低，您可以使用成本較低的選項，例如縮小叢集或關閉叢集並拍攝最終快照。即使刪除叢集，最終快照仍會保留。

檢查 ID

`G31sQ1E9U`

警示條件

- 黃色：在過去 7 天內，執行中的叢集沒有連線。
- 黃色：在過去 7 天內，執行中的叢集 99% 的時間叢集平均 CPU 使用率低於 5%。

建議的動作

請考慮關閉叢集並建立最終快照，或縮減叢集的大小。請參閱 Shutting Down and Deleting Clusters (關閉及刪除叢集) 和 Resizing a Cluster (調整叢集大小)。

其他資源

Amazon CloudWatch 用戶指南

報告欄位

- Status

- 區域
- 叢集
- 執行個體類型
- 原因
- 預估每月節省成本

效能

透過檢查服務配額 (先前稱為限額) 來改善服務的效能，如此一來您便可利用佈建的輸送量、監控利用率過高的執行個體，以及偵測任何未使用的資源。

您可以針對效能類別使用下列檢查。

檢查名稱

- 針對讀取工作負載佈建不足的 Amazon Aurora 資料庫
- 未啟用 Amazon DynamoDB Auto Scaling
- 未啟用 Amazon EBS 最佳化
- Amazon EBS 佈建 IOPS (SSD) 磁碟區連接組態
- Amazon EBS 佈建不足的磁碟區
- Amazon EC2 Auto Scaling 群組並未與啟動範本關聯
- Amazon EC2 對 EBS 輸送量最佳化
- EC2 虛擬化類型為半虛擬化
- Amazon ECS 記憶體硬性限制
- Amazon EFS 輸送量模式最佳化
- Amazon RDS 自動真空參數已關閉
- Amazon RDS 資料庫叢集僅支援最多 64 TiB 磁碟區
- 叢集中具有異質執行個體類別的 Amazon RDS 資料庫執行個體
- 叢集中具有異質執行個體大小的 Amazon RDS 資料庫執行個體
- Amazon RDS 數據庫內存參數與默認值不同
- Amazon RDS 啟用索引訪問參數已關閉
- Amazon RDS 啟用索引掃描參數已關閉

- Amazon RDS 一般記錄參數已打開
- Amazon RDS 使用小於最佳值的 InnoDB 更改緩衝參數
- Amazon RDS 開啟文件參數低
- Amazon RDS 統計持久參數已關閉
- 針對系統容量佈建不足的 Amazon RDS 執行個體
- Amazon RDS 磁碟區正在使用
- Amazon RDS 參數組不使用大型頁面
- Amazon RDS 查詢緩存參數已打開
- 需要更新 Amazon RDS 資源執行個體類別
- 需要更新 Amazon RDS 資源主要版本
- Amazon RDS 資源使用已包含授權的終止支援引擎版本
- Amazon Route 53 別名資源記錄集
- AWS Lambda 佈建不足的函數 (對於記憶體大小)
- 沒有設定並行限制的 AWS Lambda 函數
- AWS Well-Architected 效能的高風險問題
- CloudFront 替代網域名稱
- CloudFront 內容傳遞最佳化
- CloudFront 標頭轉送和快取命中率
- Amazon EC2 執行個體高使用率
- 大量 EC2 安全群組規則套用至執行個體
- EC2 安全群組中有大量規則
- 利用率過高的 Amazon EBS 磁帶磁碟區

針對讀取工作負載佈建不足的 Amazon Aurora 資料庫

描述

檢查 Amazon Aurora 資料庫叢集是否具有支援讀取工作負載的資源。

檢查 ID

```
c1qf5bt038
```

警示條件

黃色：

增加的資料庫讀取：資料庫負載很高，而且資料庫讀取的資料列數量超過寫入或更新資料列。

建議的動作

建議您調整查詢以減少資料庫負載，或將讀取器資料庫執行個體新增至資料庫叢集，其執行個體類別和大小與叢集中的寫入器資料庫執行個體相同。目前的組態至少有一個資料庫執行個體，且資料庫負載持續高，主要是由於讀取作業所造成。將另一個資料庫執行個體新增至叢集，並將讀取工作負載導向至資料庫叢集唯讀端點，以散佈這些作業。

其他資源

Aurora 資料庫叢集具有一個用於唯讀連線的讀取器端點。此端點使用負載平衡來管理對資料庫叢集中資料庫負載最大貢獻的查詢。讀取器端點會將這些陳述式導向 Aurora 僅供讀取複本，並減少主要執行個體的負載。讀取器端點也會調整容量，以便使用叢集中的 Aurora 僅供讀取複本數量來處理並行 SELECT 查詢。

如需詳細資訊，請參閱將 Aurora 複本新增至資料庫叢集和管理 Aurora 資料庫叢集的效能和擴展。

報告欄位

- Status
- 區域
- 資源
- 增加資料庫讀取 (計數)
- 上次偵測週期
- 上次更新時間

未啟用 Amazon DynamoDB Auto Scaling

描述

檢查您的 Amazon DynamoDB 資料表和全域次要索引是否已啟用自動擴展或隨需功能。

Amazon DynamoDB Auto Scaling 功能會使用 Application Auto Scaling 服務代您動態調整佈建的輸送容量，藉此回應實際流量模式。這可讓資料表或全域次要索引增加其佈建的讀取與寫入容量，

不需調節就以處理突然增加的流量。當工作負載降低時，Application Auto Scaling 可降低輸送量，讓您無須為未使用的佈建容量付費。

您可以使用 AWS Config 規則中的參數來調整檢查組態。

如需詳細資訊，請參閱使用 DynamoDB Auto Scaling 自動管理輸送容量。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

c18d2gz136

來源

AWS Config受管規則： dynamodb-autoscaling-enabled

警示條件

黃色：您的 DynamoDB 資料表和/或全域次要索引未啟用自動擴展。

建議的動作

除非您已經有機制可根據工作負載需求來自動擴展 DynamoDB 資料表和/或全域次要索引的佈建輸送量，否則請考慮為 Amazon DynamoDB 資料表啟用自動擴展功能。

如需詳細資訊，請參閱使用 AWS 管理主控台與 DynamoDB Auto Scaling。

其他資源

使用 DynamoDB Auto Scaling 功能自動管理輸送容量

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則

- 輸入參數
- 上次更新時間

未啟用 Amazon EBS 最佳化

描述

檢查 Amazon EC2 執行個體是否已啟用 Amazon EBS 最佳化。

Amazon EBS 最佳化執行個體使用最佳化組態堆疊，並為 Amazon EBS I/O 提供額外專用容量。此最佳化透過減少 Amazon EBS I/O 與執行個體的其他流量之間的爭用情況，為您的 Amazon EBS 磁碟區提供最佳效能。

如需詳細資訊，請參閱 Amazon EBS 最佳化執行個體。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`c18d2gz142`

來源

AWS Config受管規則： ebs-optimized-instance

警示條件

黃色：Amazon EBS 最佳化未於支援的 Amazon EC2 執行個體上啟用。

建議的動作

在支援的執行個體上開啟 Amazon EBS 最佳化。

如需詳細資訊，請參閱啟動時啟用 EBS 最佳化。

其他資源

Amazon EBS 最佳化執行個體

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

Amazon EBS 佈建 IOPS (SSD) 磁碟區連接組態

描述

檢查是否有連接到可針對 Amazon EBS 最佳化的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體之佈建 IOPS (SSD) 磁碟區尚未針對 EBS 最佳化。

Amazon Elastic Block Store (Amazon EBS) 中的佈建 IOPS (SSD) 磁碟區，設計為只有在連接到針對 EBS 最佳化的執行個體時才能提供預期的效能。

檢查 ID

`PPkZrjsH2q`

警示條件

黃色：可以進行 EBS 最佳化的 Amazon EC2 執行個體具有連接的佈建 IOPS (SSD) 磁碟區，但是該執行個體並沒有進行 EBS 最佳化。

建議的動作

建立 EBS 最佳化的新執行個體、分離磁碟區，然後將磁碟區重新連接至新執行個體。如需詳細資訊，請參閱 Amazon EBS 最佳化執行個體及將 Amazon EBS 磁碟區連接到執行個體。

其他資源

- Amazon EBS 磁碟區類型
- Amazon EBS 磁碟區效能

報告欄位

- Status
- 區域/可用區域

- 磁碟區 ID
- 磁碟區名稱
- 磁碟區連接
- 執行個體 ID
- 執行個體類型
- EBS 優化

Amazon EBS 佈建不足的磁碟區

描述

檢查回顧期間在任何時間執行的 Amazon Elastic Block Store (Amazon EBS) 磁碟區。此檢查會提醒您注意工作負載 EBS 磁碟區佈建不足的情形。穩定的高使用率可能表示最佳化、穩定的效能，但也可能表示應用程式的資源不足。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`C0r6dfpM04`

警示條件

黃色：回顧期間佈建不足的 EBS 磁碟區。若要判斷磁碟區是否佈建不足，我們會考慮所有預設 CloudWatch 指標 (包括 IOPS 和輸送量)。用於識別佈建不足的 EBS 磁碟區的演算法是依據 AWS 最佳實務。找出新的模式時，該演算法會更新。

建議的動作

考慮提升高使用率磁碟區的大小。

如需詳細資訊，請參閱 對於 AWS Compute Optimizer 檢查，選擇使用 Trusted Advisor。

報告欄位

- Status

- 區域
- 磁碟區 ID
- 磁碟區類型
- 磁碟區大小 (GB)
- 磁碟區基準 IOPS
- 磁碟區高載 IOPS
- 磁碟區高載輸送量
- 建議的磁碟區類型
- 建議的磁碟區大小 (GB)
- 建議的磁碟區基準 IOPS
- 建議的磁碟區高載 IOPS
- 建議的磁碟區基準輸送量
- 建議的磁碟區高載輸送量
- 回顧期間 (天)
- 效能風險
- 上次更新時間

Amazon EC2 Auto Scaling 群組並未與啟動範本關聯

描述

檢查 Amazon EC2 Auto Scaling 群組是否從 Amazon EC2 啟動範本建立。

使用啟動範本來建立您的 Amazon EC2 Auto Scaling 群組，以確保存取最新的 Auto Scaling 群組功能和改進項目。例如，版本控制和多個執行個體類型。

如需詳細資訊，請參閱啟動範本。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

c18d2gz102

來源

AWS Config受管規則： autoscaling-launch-template

警示條件

黃色：Amazon EC2 Auto Scaling 群組並未與有效的啟動範本關聯。

建議的動作

使用 Amazon EC2 啟動範本來建立 Amazon EC2 Auto Scaling 群組。

如需詳細資訊，請參閱建立 Auto Scaling 群組的啟動範本。

其他資源

- 啟動範本
- 建立啟動範本

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

Amazon EC2 對 EBS 輸送量最佳化

描述

檢查是否有 Amazon EBS 磁碟區的效能可能受到所連接 Amazon EC2 執行個體的最大輸送量容量影響。

若要最佳化效能，應確保 Amazon EC2 執行個體的最大輸送量大於連接 EBS 磁碟區的彙總輸送量上限。此檢查會計算每個針對 EBS 最佳化的執行個體前一天每五分鐘期間的 EBS 磁碟區總輸送量 (以國際標準時間 (UTC) 為基礎)，並在超過一半期間的用量超過 EC2 執行個體最大輸送量的 95% 時發出提醒。

檢查 ID

Bh2xRR2FGH

警示條件

黃色：在前一天 (UTC)，連接至 EC2 執行個體的 EBS 磁碟區彙總輸送量 (MB/s)，在 50% 以上的時間內超過執行個體與 EBS 磁碟區之間發佈輸送量的 95%。

建議的動作

比較 Amazon EBS 磁碟區的最大輸送量 (請參閱 Amazon EBS 磁碟區類型) 與磁碟區所連接 Amazon EC2 執行個體的最大輸送量。請參閱支援 EBS 最佳化的執行個體類型。

請考慮將磁碟區連接到支援對 Amazon EBS 更高輸送量的執行個體，以獲得最佳效能。

其他資源

- Amazon EBS 磁碟區類型
- Amazon EBS 最佳化的執行個體
- 監控您的磁碟區狀態
- 將 Amazon EBS 磁碟區連接至執行個體
- 將 Amazon EBS 磁碟區與執行個體分離
- 刪除 Amazon EBS 磁碟區

報告欄位

- Status
- 區域
- 執行個體 ID
- 執行個體類型
- 時間接近最大值

EC2 虛擬化類型為半虛擬化

描述

檢查 Amazon EC2 執行個體的虛擬化類型是否為半虛擬化。

最佳實務是盡可能使用硬體虛擬機器 (HVM) 執行個體而非半虛擬執行個體。這是因為 HVM 虛擬化中的增強以及 HVM AMI 之 PV 驅動程式的可用性，消除了 PV 和 HVM 訪客之間以往存在的效能差

距。請務必注意，目前這一代的執行個體類型不支援 PV AMI。因此，選擇 HVM 執行個體類型可提供最佳效能以及與現代硬體的相容性。

如需詳細資訊，請參閱 Linux AMI 虛擬化類型。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

c18d2gz148

來源

AWS Config受管規則：ec2-paravirtual-instance-check

警示條件

黃色：Amazon EC2 執行個體的虛擬化類型為半虛擬化。

建議的動作

為您的 Amazon EC2 執行個體使用 HVM 虛擬化，並使用相容的執行個體類型。

如需有關選擇適當虛擬化類型的資訊，請參閱變更執行個體類型的相容性。

其他資源

變更執行個體類型的相容性

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

Amazon ECS 記憶體硬性限制

描述

檢查 Amazon ECS 任務定義是否為其容器定義設定了記憶體限制。為任務中所有容器預訂的記憶體總量必須低於任務記憶體值。

如需詳細資訊，請參閱容器定義。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`c18d2gz176`

來源

AWS Config受管規則： ecs-task-definition-memory-硬性限制

警示條件

黃色：未設定 Amazon ECS 記憶體硬性限制。

建議的動作

為您的 Amazon ECS 任務配置記憶體以避免記憶體不足。如果您的容器嘗試使用超過指定的記憶體，則會終止容器。

如需詳細資訊，請參閱如何將記憶體分配給 Amazon ECS 中的任務？。

其他資源

叢集保留

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則

- 輸入參數
- 上次更新時間

Amazon EFS 輸送量模式最佳化

描述

檢查客戶的 Amazon EFS 檔案系統目前是否設定為使用「爆量輸送量」模式。

EFS 的「爆量輸送量」模式 [1] 中的檔案系統可提供一致的基準輸送量 (EFS 標準儲存體中每 GiB 資料 50 KiB/s)，且在有「爆量點數」可用時，使用點數模式來提供更高級別的「爆量輸送量」效能。當您耗盡爆量點數時，您的檔案系統效能會限流到這個較低的基準，如此可能會對使用者或應用程式造成緩慢、逾時或其他形式的效能影響。

檢查 ID

`c1dfprch02`

警示條件

- 黃色：檔案系統正在使用爆量輸送量模式。

建議的動作

若要讓您的使用者和應用程式皆能達到所需的輸送量，建議您將檔案系統組態更新為彈性輸送量模式 [2]。在彈性輸送量模式下，您的檔案系統最多可以達到 10 Gib/s 的讀取輸送量或 3 Gib/s 的寫入輸送量 (視 AWS 區域 [3] 而定)，且您僅需支付所使用的輸送量。請注意，您可以根據需要更新檔案系統組態，在彈性和爆量輸送量模式之間切換，而在彈性輸送量模式下的檔案系統會產生額外的資料傳輸費用 [4]。

其他資源

- [1] Amazon EFS 效能輸送量模式
- [2] Amazon EFS 效能彈性輸送量模式
- [3] Amazon EFS 配額和限制
- [4] Amazon EFS 定價

報告欄位

- Status
- 區域
- EFS 檔案系統 ID
- 輸送量模式

- 上次更新時間

Amazon RDS 自動真空參數已關閉

描述

資料庫執行個體的自動真空參數已關閉。關閉自動真空可增加工作台和指數膨脹並影響效能。

建議您在資料庫參數群組中開啟自動真空。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

`c1qf5bt025`

警示條件

黃色：DB 參數組已關閉自動真空。

建議的動作

開啟資料庫參數群組中的自動真空參數。

其他資源

PostgreSQL 數據庫需要定期維護，這就是所謂的吸塵。PostgreSQL 中的自動真空可自動執行真空和分析指令。此程序會收集資料表統計資料並刪除無效資料列。當 auto真空關閉時，表的增加，索引膨脹，陳舊的統計數據都會影響數據庫的性能。

如需詳細資訊，請參閱了解 Amazon RDS for PostgreSQL 環境中的自動真空。

報告欄位

- Status
- 區域
- 資源
- 參數名稱
- 建議值
- 上次更新時間

Amazon RDS 資料庫叢集僅支援最多 64 TiB 磁碟區

描述

您的資料庫叢集支援高達 64 TiB 的磁碟區。最新的引擎版本支援高達 128 TiB 的磁碟區。建議您將資料庫叢集的引擎版本升級至最新版本，以支援高達 128 TiB 的磁碟區。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

```
c1qf5bt017
```

警示條件

黃色：資料庫叢集僅支援最多 64 TiB 的磁碟區。

建議的動作

升級資料庫叢集的引擎版本，以支援高達 128 TiB 的磁碟區。

其他資源

在單一 Amazon Aurora 資料庫叢集上擴展應用程式時，如果儲存限制為 128 TiB，則可能無法達到此限制。增加的儲存限制有助於避免刪除資料或將資料庫分割到多個執行個體。

如需詳細資訊，請參閱 Amazon Aurora 大小限制。

報告欄位

- Status
- 區域
- 資源
- 引擎名稱
- 引擎版本目前
- 建議值
- 上次更新時間

叢集中具有異質執行個體類別的 Amazon RDS 資料庫執行個體

描述

建議您對資料庫叢集中的所有資料庫執行個體使用相同的資料庫執行個體類別和大小。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。

如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

`c1qf5bt009`

警示條件

紅色：資料庫叢集的資料庫執行個體具有異質執行個體類別。

建議的動作

對資料庫叢集中的所有資料庫執行個體使用相同的執行個體類別和大小。

其他資源

當資料庫叢集中的資料庫執行個體使用不同的資料庫執行個體類別或大小時，資料庫執行個體的工作負載可能會發生不平衡。容錯移轉期間，其中一個讀取器資料庫執行個體會變更為寫入器資料庫執行個體 如果資料庫執行個體使用相同的資料庫執行個體類別和大小，則可以針對資料庫叢集中的資料庫執行個體平衡工作負載。

如需詳細資訊，請參閱 Aurora 複本。

報告欄位

- Status
- 區域
- 資源
- 建議值
- 引擎名稱
- 上次更新時間

叢集中具有異質執行個體大小的 Amazon RDS 資料庫執行個體

描述

建議您對資料庫叢集中的所有資料庫執行個體使用相同的資料庫執行個體類別和大小。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

`c1qf5bt008`

警示條件

紅色：資料庫叢集的資料庫執行個體具有異質執行個體大小。

建議的動作

對資料庫叢集中的所有資料庫執行個體使用相同的執行個體類別和大小。

其他資源

當資料庫叢集中的資料庫執行個體使用不同的資料庫執行個體類別或大小時，資料庫執行個體的工作負載可能會發生不平衡。容錯移轉期間，其中一個讀取器資料庫執行個體會變更為寫入器資料庫執行個體 如果資料庫執行個體使用相同的資料庫執行個體類別和大小，則可以針對資料庫叢集中的資料庫執行個體平衡工作負載。

如需詳細資訊，請參閱 Aurora 複本。

報告欄位

- Status
- 區域
- 資源
- 建議值

- 引擎名稱
- 上次更新時間

Amazon RDS 數據庫內存參數與默認值不同

描述

資料庫執行個體的記憶體參數與預設值明顯不同。這些設定可能會影響效能並導致錯誤。

建議您將資料庫執行個體的自訂記憶體參數重設為資料庫參數群組中的預設值。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

`c1qf5bt020`

警示條件

黃色：資料庫參數群組的記憶體參數與預設值有很大差異。

建議的動作

將記憶體參數重設為預設值。

其他資源

如需詳細資訊，請參閱設定適用於 Amazon RDS for MySQL 參數的最佳實務，第 1 部分：與效能相關的參數。

報告欄位

- Status
- 區域
- 資源
- 參數名稱
- 建議值
- 上次更新時間

Amazon RDS 啟用索引訪問參數已關閉

描述

查詢規劃工具或最佳化工具在關閉時無法使用僅索引掃描計劃類型。

我們建議您將啟用參數值設定為 1。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

```
c1qf5bt028
```

警示條件

黃色：資料庫參數群組已關閉啟用 _ 索引連結掃描參數。

建議的動作

將參數啟用 _ 索引連結掃描設定為 1。

其他資源

當您關閉 enable_indexonlyscan 參數時，它會防止查詢規劃工具選取最佳執行計畫。查詢規劃工具使用不同的計劃類型，例如索引掃描，可增加查詢成本和執行時間。索引僅掃描計劃類型會擷取資料而不存取資料表資料。

如需詳細資訊，請參閱 PostgreSQL 文件網站上的啟用索引連結掃描 (布林值)。

報告欄位

- Status
- 區域
- 資源
- 參數名稱
- 建議值
- 上次更新時間

Amazon RDS 啟用索引掃描參數已關閉

描述

查詢規劃工具或最佳化工具在關閉索引掃描計劃類型時無法使用。

我們建議您將啟用 _ 索引掃描參數值設定為 1。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。

如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

`c1qf5bt029`

警示條件

黃色：資料庫參數群組已關閉啟用 _ 索引掃描參數。

建議的動作

將參數啟用 _ 索引掃描設定為 1。

其他資源

當您關閉 enable_indexscan 參數時，它會防止查詢規劃工具選取最佳執行計畫。查詢規劃工具使用不同的計劃類型，例如索引掃描，可增加查詢成本和執行時間。

如需詳細資訊，請參閱 PostgreSQL 文件網站上的啟用索引掃描 (布林值)。

報告欄位

- Status
- 區域
- 資源
- 參數名稱
- 建議值
- 上次更新時間

Amazon RDS 一般記錄參數已打開

描述

資料庫執行個體的一般記錄已開啟。此設定在疑難排解資料庫問題時很有用。不過，開啟一般記錄會增加 I/O 作業和配置的儲存空間量，這可能會導致爭用和效能降低。

檢查您的一般記錄用法需求。我們建議您將一般記錄參數值設定為 0。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

`c1qf5bt037`

警示條件

黃色：資料庫參數群組已開啟一般記錄。

建議的動作

檢查您的一般記錄用法需求。如果不是強制性的，我們建議您將一般記錄參數值設定為 0。

其他資源

一般查詢記錄檔會在一般記錄參數值為 1 時開啟。一般查詢記錄檔包含資料庫伺服器作業的記錄。當用戶端連線或中斷連線時，伺服器會將資訊寫入此記錄檔，而且記錄檔包含從用戶端接收到的每個 SQL 陳述式。當您懷疑用戶端發生錯誤，而且想要尋找用戶端傳送至資料庫伺服器的資訊時，一般查詢記錄檔非常有用。

如需詳細資訊，請參閱適用於 MySQL 的 RDS 資料庫記錄檔概觀。

報告欄位

- Status
- 區域
- 資源

- 參數名稱
- 建議值
- 上次更新時間

Amazon RDS 使用小於最佳值的 InnoDB 更改緩衝參數

描述

變更緩衝可讓 MySQL 資料庫執行個體延遲幾次寫入，這是維護次要索引所需的寫入。此功能在磁碟速度較慢的環境中非常有用。變更緩衝組態稍微改善了資料庫效能，但在升級期間造成當機復原延遲和較長的關機時間。

我們建議您將 Innodb_change_ 緩衝參數的值設定為無。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

```
c1qf5bt021
```

警示條件

黃色：資料庫參數群組的 Innodb_change_緩衝參數設定為低的最佳值。

建議的動作

在數據庫參數組中將 INNODB_CHANGE 緩衝參數值設置為無。

其他資源

如需詳細資訊，請參閱設定適用於 Amazon RDS for MySQL 參數的最佳實務，第 1 部分：與效能相關的參數。

報告欄位

- Status
- 區域
- 資源
- 參數名稱
- 建議值
- 上次更新時間

Amazon RDS 開啟文件參數低

描述

該 INNODB 文件參數控制 InnoDB 可以在同一時間打開的文件的數量。InnoDB 打開所有的日誌和系統表空間文件時 mysqld 正在運行。

針對 InnoDB 一次能開啟的最大檔案數量，您的資料庫執行個體設定值很低。我們建議您將 Innodb_open_files 參數設定為最小值 65。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

c1qf5bt033

警示條件

黃色：資料庫參數群組的 InnoDB 開啟檔案設定配置錯誤。

建議的動作

將檔案參數設定為 65 的最小值。

其他資源

該 INNODB 文件參數控制 InnoDB 可以在同一時間打開的文件的數量。InnoDB 保持所有的日誌文件和系統表空間文件打開時 mysqld 正在運行。如果使用 file-per-table 存儲模型，InnoDB 還需要打開一些 .ibd 文件。當 innodb_open_files 設置很低時，它會影響數據庫性能，並且服務器可能無法啟動。

如需詳細資訊，請參閱文件網站上的 InnoDB 啟動選項和系統變數-innodb_open_ file。 MySql

報告欄位

- Status
- 區域
- 資源
- 參數名稱
- 建議值
- 上次更新時間

Amazon RDS 統計持久參數已關閉

描述

您的資料庫執行個體未設定將 InnoDB 統計資料保留於磁碟。如果不儲存統計資料，則每次執行個體重新啟動並存取資料表時，都會重新計算這些統計資料。這會導致查詢執行計劃的變化。您可以在資料表層級修改此全域參數的值。

我們建議您將 Innodb_stats_持久性參數值設定為開啟。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

`c1qf5bt032`

警示條件

黃色：資料庫參數群組具有未保留在磁碟的最佳化處理程式統計資料。

建議的動作

將永久性參數值設定為「開啟」。

其他資源

如果 innodb_stats_持久參數設定為ON，則在執行個體重新啟動時，最佳化程式統計資料會持續存在。這提高了執行計劃的穩定性和一致的查詢性能。您可以在建立或變更資料表時，使用子句 STATS_ PERTION，在資料表層次修改全域統計資料保存。

如需詳細資訊，請參閱設定適用於 Amazon RDS for MySQL 參數的最佳實務，第 1 部分：與效能相關的參數。

報告欄位

- Status
- 區域
- 資源

- 參數名稱
- 建議值
- 上次更新時間

針對系統容量佈建不足的 Amazon RDS 執行個體

描述

檢查 Amazon RDS 執行個體或 Amazon Aurora 資料庫執行個體是否具有操作所需的系統容量。

檢查 ID

`c1qf5bt039`

警示條件

黃色：

O ut-of-memory 殺死：當數據庫主機上的進程因為操作系統級別的內存減少而停止時，內存不足（OOM）殺死計數器增加。

過度交換：記憶體交換和記憶體交換度量值很高。

建議的動作

建議您調整查詢以使用較少的記憶體，或使用配置記憶體較高的資料庫執行個體類型。當執行個體的記憶體不足時，會影響資料庫效能。

其他資源

檢測到 O ut-of-memory 殺死：當主機上運行的進程需要超過操作系統實際可用的內存時，Linux 內核調用內存不足（OOM）殺手。在這種情況下，OOM Killer 審查所有正在運行的進程，並停止一個或多個進程，以釋放系統內存並保持系統運行。

偵測到交換：當資料庫主機上的記憶體不足時，作業系統會將一些最少使用的分頁傳送到交換空間中的磁碟。此卸載程序會影響資料庫效能。

如需詳細資訊，請參閱 Amazon RDS 執行個體類型和擴展您的 RDS 執行個體。

報告欄位

- Status
- 區域

- 資源
- O ut-of-memory 殺人數（計數）
- 過度交換（計數）
- 上次偵測週期
- 上次更新時間

Amazon RDS 磁碟區正在使用

描述

您的資料庫執行個體使用磁性儲存。不建議大多數資料庫執行個體使用磁性儲存。選擇不同的儲存類型：一般用途 (SSD) 或佈建 IOPS。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

`c1qf5bt000`

警示條件

黃色：Amazon RDS 資源正在使用磁性儲存。

建議的動作

選擇不同的儲存類型：一般用途 (SSD) 或佈建 IOPS。

其他資源

磁性儲存是較早一代的儲存類型。一般用途 (SSD) 或佈建 IOPS 是針對新儲存需求的建議儲存類型。這些儲存類型可提供更高且一致的效能，並改善儲存大小選項。

如需詳細資訊，請參閱上一代磁碟區。

報告欄位

- Status
- 區域
- 資源
- 建議值
- 引擎名稱
- 上次更新時間

Amazon RDS 參數組不使用大型頁面

描述

大型分頁可以增加資料庫延展性，但您的資料庫執行個體並未使用大型分頁。建議您在資料庫執行個體的資料庫參數群組中，將 use_large_pages 參數值設定為「僅限」。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

c1qf5bt024

警示條件

黃色：資料庫參數群組不使用大型頁面。

建議的動作

在資料庫參數群組中，將使用大型頁面參數值設定為「僅」。

其他資源

如需詳細資訊，請參閱開啟 HugePages 適用於 Oracle 執行個體的 RDS。

報告欄位

- Status
- 區域
- 資源
- 參數名稱
- 建議值
- 上次更新時間

Amazon RDS 查詢緩存參數已打開

描述

當變更需要清除查詢快取時，您的資料庫執行個體將會停止。大部分工作負載並不會受益於查詢快取。MySQL 8.0 版已移除查詢快取。我們建議您將查詢 _ 快取類型參數設定為 0。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

`c1qf5bt022`

警示條件

黃色：資料庫參數群組已開啟查詢快取。

建議的動作

在資料庫參數群組中，將查詢 _cache_type 參數值設定為 0。

其他資源

如需詳細資訊，請參閱設定適用於 Amazon RDS for MySQL 參數的最佳實務，第 1 部分：與效能相關的參數。

報告欄位

- Status
- 區域
- 資源
- 參數名稱
- 建議值
- 上次更新時間

需要更新 Amazon RDS 資源執行個體類別

描述

您的資料庫正在執行上一代資料庫執行個體類別。我們已將上一代的資料庫執行個體類別取代為具有更高成本、效能或兩者兼具的資料庫執行個體類別。建議您使用新一代的資料庫執行個體類別執行資料庫執行個體。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

`c1qf5bt015`

警示條件

紅色：資料庫執行個體使用終止支援資料庫執行個體類別。

建議的動作

升級至最新資料庫執行個體類別。

其他資源

如需詳細資訊，請參閱資料庫執行個體類別的支援資料庫引擎。

報告欄位

- Status
- 區域
- 資源
- 資料庫執行個體類別
- 建議值
- 引擎名稱
- 上次更新時間

需要更新 Amazon RDS 資源主要版本

描述

不支援資料庫引擎目前主要版本的資料庫。我們建議您升級至包含新功能和增強功能的最新主要版本。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

`c1qf5bt014`

警示條件

紅色：RDS 資源使用終止支援主要版本。

建議的動作

升級至資料庫引擎的最新主要版本。

其他資源

Amazon RDS 針對支援的資料庫引擎發行新版本，以維護資料庫的最新版本。新發布的版本可能包括對數據庫引擎的錯誤修復，安全性增強和其他改進。您可以使用藍/綠部署，將資料庫執行個體升級所需的停機時間降至最低。

如需詳細資訊，請參閱下列資源：

- 升級資料庫執行個體引擎版本

- Amazon Aurora 更新
- 使用 Amazon RDS 藍色/綠色部署進行資料庫更新

報告欄位

- Status
- 區域
- 資源
- 引擎名稱
- 引擎目前版本
- 建議值
- 上次更新時間

Amazon RDS 資源使用已包含授權的終止支援引擎版本

描述

建議您將主要版本升級至 Amazon RDS 支援的最新引擎版本，以繼續使用目前的授權支援。目前的授權不支援資料庫的引擎版本。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

```
c1qf5bt016
```

警示條件

紅色：Amazon RDS 資源在包含授權的模式下使用終止支援引擎版本。

建議的動作

我們建議您將資料庫升級到 Amazon RDS 中的最新支援版本，以繼續使用授權模型。

其他資源

如需詳細資訊，請參閱 Oracle 主要版本升級。

報告欄位

- Status
- 區域
- 資源
- 引擎名稱
- 引擎版本目前
- 建議值
- 引擎名稱
- 上次更新時間

Amazon Route 53 別名資源記錄集

描述

檢查是否有資源記錄集可變更為別名資源記錄集，以改善效能並節省成本。

別名資源記錄集會將 DNS 查詢路由至 AWS 資源 (例如 Elastic Load Balancing 負載平衡器或 Simple Storage Service (Amazon S3) 儲存貯體) 或其他 Route 53 資源記錄集。使用別名資源記錄集時，Route 53 會免費將您的 DNS 查詢路由至 AWS 資源。

AWS 服務建立的託管區域不會出現在您的檢查結果中。

檢查 ID

`B913Ef6fb4`

警示條件

- 黃色：資源記錄集是 Amazon S3 網站的 CNAME。
- 黃色：資源記錄集是 Amazon CloudFront 分佈的 CNAME。

- 黃色：資源記錄集是 Elastic Load Balancing 負載平衡器的 CNAME。

建議的動作

以別名資源記錄集取代列出的 CNAME 資源記錄集；請參閱選擇別名或非別名資源記錄集。

您還需要根據 AWS 資源，將記錄類型從 CNAME 變更為 A 或 AAAA。請參閱您在建立或編輯 Amazon Route 53 資源記錄集時指定的值。

其他資源

將查詢路由至 AWS 資源

報告欄位

- Status
- 託管區域名稱
- 託管區域 ID
- 資源記錄集名稱
- 資源記錄集類型
- 資源記錄集識別碼
- 別名目標

AWS Lambda 佈建不足的函數 (對於記憶體大小)

描述

檢查回顧期間已呼叫至少一次的 AWS Lambda 函數。此檢查會提醒您任何 Lambda 函數在記憶體大小佈建不足的情形。當您的 Lambda 函數在記憶體大小佈建不足時，這些函數會需要更長的時間才能完成。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`C0r6dfpM06`

警示條件

黃色：在回顧期間記憶體大小佈建不足的 Lambda 函數。若要判斷 Lambda 函數是否佈建不足，我們會考慮該函數的所有預設 CloudWatch 指標。用於識別記憶體大小佈建不足的 Lambda 函數的演算法是依據 AWS 最佳實務。找出新的模式時，該演算法會更新。

建議的動作

請考慮增加 Lambda 函數的記憶體大小。

如需詳細資訊，請參閱 對於 AWS Compute Optimizer 檢查，選擇使用 Trusted Advisor。

報告欄位

- Status
- 區域
- 函數名稱
- 函數版本
- 記憶體大小 (MB)
- 建議的記憶體大小 (MB)
- 回顧期間 (天)
- 效能風險
- 上次更新時間

沒有設定並行限制的 AWS Lambda 函數

描述

檢查 AWS Lambda 函數是否已設定函數層級的並行執行限制。

並行是 AWS Lambda 函數可同時處理的傳輸中請求數量。Lambda 會針對每個並行請求佈建個別的執行環境執行個體。

您可以使用AWS Config規則中的和ConcurrencyLimitHigh參數來指定最小concurrencyLimitLow和最大並行限制。

如需詳細資訊，請參閱 Lambda 函數擴展。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

c18d2gz181

來源

AWS Config受管規則： lambda-concurrency-check

警示條件

黃色：Lambda 函數並未設定並行限制。

建議的動作

請確定您的 Lambda 函數已設定並行功能。Lambda 函數的並行限制有助於確保您的函數可靠且可預測地處理請求。並行限制減少了因流量突然激增而導致功能不堪負荷的風險。

如需詳細資訊，請參閱設定預留並行。

其他資源

- Lambda 函數擴展
- 設定預留並行

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

AWS Well-Architected 效能的高風險問題

描述

檢查效能支柱中，工作負載是否有高風險問題 (HRI)。這項檢查是以您的 AWS-Well Architected 檢閱為基礎。您的檢查結果取決於您是否使用 AWS Well-Architected 完成工作負載評估。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`Wxdfp4B1L2`

警示條件

- 紅色：在 AWS Well-Architected 的性能支柱中發現至少一個待處理的高風險問題。
- 綠色：在 AWS Well-Architected 的效能支柱中未發現任何待處理的高風險問題。

建議的動作

AWS Well-Architected 在工作負載評估期間偵測到高風險問題。解決這些問題，可能有機會降低風險和節省成本。登入 AWS Well-Architected 工具，檢閱答案並採取行動，解決待處理的問題。

報告欄位

- Status
- 區域
- 工作負載 ARN
- 工作負載名稱
- 檢閱者姓名
- 工作負載類型
- 工作負載開始日期
- 工作負載上次修改日期
- 效能方面已識別的高風險問題數量
- 效能方面已解決的高風險問題數量
- 效能方面已回答的問題數量

- 效能支柱中的問題總數
- 上次更新時間

CloudFront 替代網域名稱

描述

檢查 Amazon CloudFront 分發是否有錯誤設定 DNS 設定的備用網域名稱 (CNAME)。

如果 CloudFront 發行版包含替代網域名稱，則網域的 DNS 組態必須將 DNS 查詢路由到該散發。

> **Note**
>
> 此檢查假設 Amazon 路線 53 DNS 和 Amazon CloudFront 分佈在相同的配置AWS 帳戶。因此，由於這個 AWS 帳戶 之外的 DNS 設定，提醒清單可能包含原本會如預期般運作的資源。

檢查 ID

`N420c450f2`

警示條件

- 黃色： CloudFront 散佈包含替代網域名稱，但 DNS 組態未正確設定為 CNAME 記錄或 Amazon Route 53 別名資源記錄。
- 黃色： CloudFront 發行版包含替代網域名稱，但Trusted Advisor無法評估 DNS 組態，因為重新導向太多。
- 黃色： CloudFront 發行版包含替代網域名稱，但由於某些其他原因而無法評估 DNS 組態，最有Trusted Advisor可能是因為逾時。

建議的動作

更新 DNS 組態，以將 DNS 查詢路由到 CloudFront 分佈；請參閱使用備用網域名稱 (CNAME)。

如果您使用 Amazon Route 53 做為 DNS 服務，請參閱使用您的 CloudFront 網域名稱將流量路由到 Amazon 網路分發。如果檢查已逾時，請嘗試重新整理檢查。

其他資源

Amazon CloudFront 開發指南

報告欄位

- Status
- 分佈 ID
- 分佈網域名稱
- 備用網域名稱
- 原因

CloudFront 內容傳遞最佳化

描述

檢查使用 Amazon (AWS全球內容交付服務) 是否可以加速從 Amazon 簡單儲存服務 (Amazon CloudFront S3) 儲存貯體傳輸資料的情況。

當您設定 CloudFront 為傳送內容時，對內容的要求會自動路由到最近的節點，其中快取內容。此路由能以最佳的效能將內容交付給您的使用者。與儲存貯體中儲存的資料相比，傳出的資料比例很高，表示您可以從使用 Amazon CloudFront 交付資料中受益。

檢查 ID

796d6f3D83

警示條件

- 黃色：在檢查前 30 天內，透過 GET 請求從儲存貯體傳輸至使用者的資料量，至少是儲存在儲存貯體中平均資料量的 25 倍。
- 紅色：在檢查前 30 天內，透過 GET 請求從儲存貯體傳輸給使用者的資料量至少為 10 TB，至少是儲存在儲存貯體中平均資料量的 25 倍。

建議的動作

考慮使用 CloudFront 以獲得更好的性能。請參閱 Amazon CloudFront 產品詳情。

如果傳輸的資料為每月 10 TB 或更多，請參閱 Amazon CloudFront 定價以探索可能節省的成本。

其他資源

- Amazon CloudFront 開發指南
- AWS 案例研究：PBS

報告欄位

- Status

- 區域
- 儲存貯體名稱
- S3 儲存體 (GB)
- 資料傳出 (GB)
- 傳輸與儲存的比率

CloudFront 標頭轉送和快取命中率

描述

檢查目 CloudFront 前從用戶端接收並轉寄至原始伺服器的 HTTP 要求標頭。

某些標頭 (例如日期或使用者代理程式) 會大幅降低快取命中率 (從 CloudFront 邊緣快取提供的要求比例)。這會增加原始伺服器的負載並降低效能，因為 CloudFront 必須將更多要求轉寄給您的來源。

檢查 ID

`N415c450f2`

警示條件

黃色： CloudFront 轉寄至來源的一或多個要求標頭可能會大幅降低快取命中率。

建議的動作

考慮使用請求標頭的好處是否足夠抵消對快取命中率的負面影響。如果您的 origin 返回相同的對象，而不管給定標頭的值如何，我們建議您不 CloudFront 要配置將該標頭轉發到 origin。如需詳細資訊，請參閱 CloudFront 根據要求標頭設定快取物件。

其他資源

- 增加從 CloudFront 邊緣快取提供的請求比例
- CloudFront 快取統計值報表
- HTTP 要求標頭和 CloudFront 行為

報告欄位

- 分佈 ID
- 分佈網域名稱
- 快取行為路徑模式

- 標頭

Amazon EC2 執行個體高使用率

描述

檢查過去 14 天內在任何時間執行的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體。如果四天或以上天數的每日 CPU 使用率超過 90%，則會傳送提醒。

穩定的高使用率可能表示最佳化、穩定的效能。不過也可能表示應用程式的資源不足。若要取得每日 CPU 使用率資料，請下載此檢查的報告。

檢查 ID

`ZRxQlPsb6c`

警示條件

黃色：在過去 14 天中，至少有 4 天執行個體每日平均 CPU 使用率超過 90%。

建議的動作

請考慮新增更多執行個體。如需有關根據需求調整執行個體數量的詳細資訊，請參閱 Auto Scaling 是什麼？

其他資源

- 監控 Amazon EC2
- 執行個體中繼資料與使用者資料
- Amazon CloudWatch 用戶指南
- 《Amazon EC2 Auto Scaling 使用者指南》

報告欄位

- 區域/可用區域
- 執行個體 ID
- 執行個體類型
- 執行個體名稱
- 14 天平均 CPU 使用率
- CPU 使用率超過 90% 的天數

大量 EC2 安全群組規則套用至執行個體

描述

檢查是否有 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體具有大量安全群組規則。如果執行個體具有大量規則，可能會降低效能。

檢查 ID

`j3DFqYTe29`

警示條件

- 黃色： Amazon EC2-VPC 執行個體具有 50 個以上的安全群組規則。
- 黃色：Amazon EC2-Classic 執行個體具有 100 個以上的安全群組規則。

建議的動作

刪除不必要或重複的規則，以減少與執行個體相關聯的規則數量。如需詳細資訊，請參閱刪除安全群組的規則。

其他資源

Amazon EC2 安全群組

報告欄位

- 區域
- 執行個體 ID
- 執行個體名稱
- VPC ID
- 傳入規則總計
- 傳出規則總計

EC2 安全群組中有大量規則

描述

檢查每個 Amazon Elastic Compute Cloud (Amazon EC2) 安全群組是否具有過量的規則。

如果安全群組具有大量的規則，可能會降低效能。

檢查 ID

`tfg86AVHAZ`

警示條件

- 黃色：Amazon EC2-VPC 安全群組具有 50 個以上的規則。
- 黃色：Amazon EC2-Classic 安全群組具有 100 個以上的規則。

建議的動作

刪除不必要或重複的規則，以減少安全群組中的規則數量。如需詳細資訊，請參閱刪除安全群組的規則。

其他資源

Amazon EC2 安全群組

報告欄位

- 區域
- 安全群組名稱
- 群組 ID
- 描述
- 執行個體計數
- VPC ID
- 傳入規則總計
- 傳出規則總計

利用率過高的 Amazon EBS 磁帶磁碟區

描述

檢查是否有 Amazon Elastic Block Store (Amazon EBS) 磁帶磁碟區可能受益於更高效的組態。

磁帶磁碟區適用於具有中等或突增輸入/輸出 (I/O) 需求的應用程式，而不能保證 IOPS 速率。平均可提供約 100 IOPS，而最佳作業能力可突增至數百 IOPS。若要穩定維持較高的 IOPS，您可以使用佈建 IOPS (SSD) 磁碟區。針對突增的 IOPS，您可以使用一般用途 (SSD) 磁碟區。如需詳細資訊，請參閱 Amazon EBS 磁碟區類型。

如需支援 EBS 最佳化行為的執行個體類型清單，請參閱 Amazon EBS 最佳化執行個體。

若要取得每日使用率指標，請下載此檢查的報告。詳細報告會顯示過去 14 天的情況 (一欄一天)。如果沒有作用中的 EBS 磁碟區，則儲存格為空白。如果沒有足夠的資料進行可靠的測量，則儲存

格會顯示 N/A。如果有足夠的資料，儲存格會顯示每日中位數和變異數相對於中位數的百分比 (例如，256 / 20%)。

檢查 ID

k3J2hns32g

警示條件

黃色：Amazon EBS 磁帶磁碟區連接到可進行 EBS 最佳化的執行個體，或屬於叢集運算網路的一部分，其每日中位數超過 95 個 IOPS，在過去 14 天中，至少有 7 天變化程度不到中位數的 10%。

建議的動作

若要穩定維持較高的 IOPS，您可以使用佈建 IOPS (SSD) 磁碟區。針對突增的 IOPS，您可以使用一般用途 (SSD) 磁碟區。如需詳細資訊，請參閱 Amazon EBS 磁碟區類型。

其他資源

Amazon Elastic Block Store (Amazon EBS)

報告欄位

- Status
- 區域
- 磁碟區 ID
- 磁碟區名稱
- 過去的天數
- 每日最大中位數

> **Note**
>
> 如果您選擇使用 AWS Compute Optimizer 專用帳戶，建議您改用 Amazon EBS 佈建不足的磁碟區檢察。如需更多詳細資訊，請參閱 對於 AWS Compute Optimizer 檢查，選擇使用 Trusted Advisor。

安全

您可以針對安全類別使用下列檢查。

> **Note**
>
> 如果您啟用了帳戶 AWS 帳戶 的 Security Hub，則可以在 Trusted Advisor 主控台中檢視問題清單。如需相關資訊，請參閱 檢視 AWS Security Hub 中的 AWS Trusted Advisor 控制項。您可以在 AWS 基礎安全最佳實務安全標準中檢視所有控制項，具有 Category: Recover > Resilience (類別：復原 > 恢復力)的控制項除外。如需支援的控制項清單，請參閱《AWS Security Hub 使用者指南》中的 AWS 基礎安全最佳實務控制項。

檢查名稱

- Amazon CloudWatch 日誌群組保留期
- Microsoft SQL 伺服器終止支援的 Amazon EC2 執行個體
- Microsoft Windows Server 終止支援的 Amazon EC2 執行個體
- 具有 Ubuntu LTS 標準支援的 Amazon EC2 執行個體結束
- Amazon EFS 用戶端未使用 data-in-transit 加密
- Amazon EBS 公有快照
- Amazon RDS Aurora 存儲加密已關閉
- Amazon RDS 引擎次要版本升級是必需的
- Amazon RDS 公有快照
- Amazon RDS 安全群組存取風險
- Amazon RDS 儲存加密已關閉
- Amazon 路線 53 不匹配的 CNAME 記錄直接指向 S3 存儲桶
- Amazon Route 53 MX 資源記錄集和寄件者政策架構
- Amazon S3 儲存貯體許可
- 已停用具有 DNS 解析的 Amazon VPC 對等互連
- 沒有資源型政策來防止刪除復原點的 AWS Backup Vault
- AWS CloudTrail 日誌
- 使用已棄用執行階段的 AWS Lambda 函數
- AWS Well-Architected 安全性的高風險問題
- CloudFrontIAM 憑證存放區中的自訂 SSL 憑證
- CloudFront 原始伺服器上的 SSL 憑證
- ELB 接聽程式安全性

- ELB 安全群組
- 存取金鑰已暴露
- IAM 存取金鑰輪換
- IAM 密碼政策
- IAM 使用情形
- 根帳戶的 MFA
- 安全群組—— 不受限制的特定連接埠
- 安全群組 - 不受限制的存取

Amazon CloudWatch 日誌群組保留期

描述

檢查 Amazon 日 CloudWatch 誌群組保留期是否設定為 365 天或其他指定的數字。

根據預設，日誌將無限期保留且永遠不會過期。不過，您可以調整每個日誌群組的保留原則，以符合特定期間的產業法規或法律要求。

您可以使用AWS Config規則中的和MinRetentionTime參數來指定最短保留時間LogGroupNames和記錄群組名稱。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz186
```

來源

```
AWS Config Managed Rule: cw-loggroup-retention-period-check
```

警示條件

黃色：Amazon 日 CloudWatch 誌群組的保留期間小於所需的最短天數。

建議的動作

為儲存在 Amazon CloudWatch Logs 中的日誌資料設定超過 365 天的保留期，以符合合規要求。

如需詳細資訊，請參閱變更 CloudWatch 記錄檔中的記錄檔資料保留。

其他資源

更改 CloudWatch 日誌保留

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

Microsoft SQL 伺服器終止支援的 Amazon EC2 執行個體

描述

檢查過去 24 小時內用於執行 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 SQL 伺服器版本。這項檢查會在版本接近或已達到終止支援時發出提醒。每個 SQL 伺服器版本都提供 10 年的支援，包括 5 年的主流支援和 5 年的延長支援。終止支援後，SQL 伺服器版本將不會收到定期的安全更新。使用不支援的 SQL 伺服器版本執行應用程式可能會帶來安全或法規遵循風險。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`Qsdfp3A4L3`

警示條件

- 紅色：EC2 執行個體具有已終止支援的 SQL Server 版本。

- 黃色：EC2 執行個體具有即將在 12 個月終止支援的 SQL Server 版本。

建議的動作

若要將 SQL Server 工作負載現代化，請考慮將其重構到 AWS 雲端 原生資料庫，如 Amazon Aurora。如需詳細資訊，請參閱使用 AWS 實現 Windows 工作負載現代化。

若要移至全受管資料庫，請考慮將其平台轉換為 Amazon Relational Database Service (Amazon RDS)。如需詳細資訊，請參閱 Amazon RDS for SQL Server。

若要在 Amazon EC2 上升級您的 SQL Server，請考慮使用自動化 Runbook 簡化您的升級。如需詳細資訊，請參閱 AWS Systems Manager 文件。

如果您無法在 Amazon EC2 上升級 SQL Server，請考慮使用 Windows Server 的終止支援遷移計劃 (EMP)。如需詳細資訊，請參閱 EMP 網站。

其他資源

- 透過 AWS 為 SQL Server 終止支援做好準備
- 將 Microsoft SQL Server 遷移至 AWS

報告欄位

- Status
- 區域
- 執行個體 ID
- SQL Server 版本
- 支援週期
- 終止支援
- 上次更新時間

Microsoft Windows Server 終止支援的 Amazon EC2 執行個體

描述

這項檢查會在版本接近或已達到終止支援時發出提醒。每個 Windows Server 版本都提供 10 年的支援。這包括 5 年的主流支援和 5 年的延長支援。終止支援後，Windows Server 版本將不會收到定期的安全更新。如果您使用不支援的 Windows Server 版本執行應用程式，則會危及這些應用程式的安全性或法規遵循。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`Qsdfp3A4L4`

警示條件

- 紅色：EC2 執行個體的 Windows Server 版本已達到終止支援階段 (Windows Server 2003、2003 R2、2008 和 2008 R2)。
- 黃色：EC2 執行個體的 Windows Server 版本將在不到 18 個月內達到終止支援階段 (Windows Server 2012 和 2012 R2)。

建議的動作

若要將您的 Windows Server 工作負載現代化，請考慮使用 AWS 實現 Windows 工作負載現代化中的幾個可用選項。

若要升級您的 Windows Server 工作負載，以便在更新版本的 Windows Server 上執行，您可以使用自動化 Runbook。如需詳細資訊，請參閱 AWS Systems Manager 文件。

請按照以下步驟操作：

- a. 升級視窗伺服器版本
- b. 硬停止並在升級時啟動
- c. 如果使用 EC2Config，請移轉至 EC2 啟動

報告欄位

- Status
- 區域
- 執行個體 ID
- Windows Server 版本
- 支援週期
- 終止支援
- 上次更新時間

具有 Ubuntu LTS 標準支援的 Amazon EC2 執行個體結束

描述

如果版本接近或已達到標準支援結束，則此檢查會提醒您。採取行動很重要-通過遷移到下一個 LTS 或升級到 Ubuntu Pro。支援結束後，您的 18.04 LTS 電腦將不會收到任何安全性更新。使用 Ubuntu 專業版訂閱，您的 Ubuntu 18.04 LTS 部署可以收到擴展的安全性維護（ESM），直到 2028 年。仍未修補的安全漏洞會使您的系統對黑客開放，並且可能發生重大漏洞。

檢查 ID

```
c1dfprch15
```

警示條件

紅色：Amazon EC2 實例具有達到標準支持結束的 Ubuntu 版本（Ubuntu 18.04 LTS，18.04.1 LTS，18.04.2 LTS，18.04.3 LTS，18.04.4 LTS，18.04.4 LTS，18.04.5 LTS 和 18.04.6 LTS）。

黃色：Amazon EC2 實例具有 Ubuntu 版本，該版本將在不到 6 個月內達到標準支持的結束（Ubuntu 20.04 LTS，20.04.1 LTS，20.04.2 LTS，20.04.3 LTS，20.04.4 LTS，20.04.5 LTS 和 20.04.6 LTS）。

綠色：所有 Amazon EC2 執行個體都符合規定。

建議的動作

若要將 Ubuntu 18.04 LTS 執行個體升級為受支援的 LTS 版本，請依照本文中提到的步驟執行。要將 Ubuntu 18.04 LTS 實例升級到 Ubuntu 專業版，請訪問AWS License Manager控制台並按照AWS License Manager用戶指南中提到的步驟進行操作。您還可以參考 Ubuntu 博客，其中顯示了將 Ubuntu 實例升級到 Ubuntu Pro 的一步一步演示。

其他資源

如需定價的相關資訊，請聯絡AWS Support。

報告欄位

- Status
- 區域
- Ubuntu 的 LTS 版本
- 預期終止 Support 日期
- 執行個體 ID

- 支援週期
- 上次更新時間

Amazon EFS 用戶端未使用 data-in-transit 加密

描述

檢查 Amazon EFS 檔案系統是否已使用 data-in-transit 加密裝載。 AWS建議客戶對所有資料流程使用 data-in-transit 加密，以保護資料免於意外外洩或未經授權的存取。Amazon EFS 建議用戶端使用 Amazon EFS 掛載協助程式使用「-o tls」掛載設定，使用 TLS 1.2 版加密傳輸中的資料。

檢查 ID

`c1dfpnchv1`

警示條件

黃色：Amazon EFS 檔案系統的一或多個 NFS 用戶端未使用提供 data-in-transit 加密的建議掛載設定。

綠色：Amazon EFS 檔案系統的所有 NFS 用戶端都使用提供 data-in-transit 加密的建議掛載設定。

建議的動作

若要利用 Amazon EFS 上的 data-in-transit 加密功能，建議您使用 Amazon EFS 掛載協助程式和建議的掛載設定重新掛接檔案系統。

> **Note**
>
> 某些 Linux 發行版本不包含預設支援 TLS 功能的暫停版本。如果您使用的是不受支援的 Linux 發行版本 (請參閱此處支援的發行版)，建議您在使用建議的掛載設定重新掛載之前先升級它。

其他資源

- 加密傳輸中的資料

報告欄位

- Status
- 區域

- EFS 檔案系統 ID
- 具有未加密連線的 AZ
- 上次更新時間

Amazon EBS 公有快照

描述

檢查 Amazon Elastic Block Store (Amazon EBS) 磁碟區快照的權限設定，並在有任何快照可公開存取時提醒您。

將快照標示為公有時，會提供所有 AWS 帳戶 和使用者快照上所有資料的存取權。如果您只想與特定使用者或帳戶共用快照，請將快照標示為私有。然後指定您要共用快照資料的使用者或帳戶。請注意，如果您在「封鎖所有共用」模式中啟用了封鎖公開存取，您的公開快照將無法公開存取，也不會顯示在檢查結果中。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會出現。

檢查 ID

`ePs02jT06w`

警示條件

紅色：可公開存取 EBS 磁碟區快照。

建議的動作

除非您確定要與所有 AWS 帳戶 和使用者共用快照中的所有資料，否則請修改許可：將快照標記為私有，然後指定您要授予許可的帳戶。如需詳細資訊，請參閱共用 Amazon EBS 快照。使用 EBS 快照的封鎖公用存取來控制允許公開存取資料的設定。無法從 Trusted Advisor 主控台檢視中排除此檢查。

若要直接修改快照的許可，您可以在 AWS Systems Manager 主控台中使用 Runbook。如需詳細資訊，請參閱`AWSSupport-ModifyEBSSnapshotPermission`。

其他資源

Amazon EBS 快照

報告欄位

- Status
- 區域
- 磁碟區 ID
- 快照 ID
- 描述

Amazon RDS Aurora 存儲加密已關閉

描述

Amazon RDS 使用您管理的金鑰，支援所有資料庫引擎的靜態加密AWS Key Management Service。在具有 Amazon RDS 加密的作用中資料庫執行個體上，儲存在儲存中的靜態資料會加密，類似於自動備份、僅供讀取複本和快照。

如果在建立 Aurora DB 叢集時未開啟加密，則必須將解密的快照還原到加密的資料庫叢集。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

```
c1qf5bt005
```

警示條件

紅色：Amazon RDS Aurora 資源未啟用加密。

建議的動作

開啟資料庫叢集的靜態資料加密。

其他資源

您可以在建立資料庫執行個體時開啟加密，或使用因應措施在作用中資料庫執行個體上開啟加密。您無法將解密的資料庫叢集修改為加密的資料庫叢集。不過，您可以將解密的快照還原到加密的資料庫叢集。從解密的快照還原時，必須指定AWS KMS金鑰。

如需詳細資訊，請參閱加密 Amazon Aurora 資源。

報告欄位

- Status
- 區域
- 資源
- 引擎名稱
- 上次更新時間

Amazon RDS 引擎次要版本升級是必需的

描述

您的資料庫資源沒有執行最新的次要資料庫引擎版本。最新的次要版本包含最新的安全性修正和其他改進。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。

如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

`c1qf5bt003`

警示條件

紅色：Amazon RDS 資源未執行最新的次要資料庫引擎版本。

建議的動作

升級至最新的引擎版本。

其他資源

我們建議您使用最新的 DB Engine 次要版本來維護資料庫，因為此版本包含最新的安全性和功能修正。數據庫引擎次要版本升級僅包含與相同主要版本的數據庫引擎的早期次要版本向後兼容的更改。

如需詳細資訊，請參閱升級資料庫執行個體引擎版本。

報告欄位

- Status
- 區域
- 資源
- 引擎名稱
- 引擎版本目前
- 建議值
- 上次更新時間

Amazon RDS 公有快照

描述

檢查 Amazon Relational Database Service (Amazon RDS) 資料庫快照的許可設定，並在任何快照標示為公有時發出提醒。

將快照標示為公有時，會提供所有 AWS 帳戶 和使用者快照上所有資料的存取權。如果您只想與特定使用者或帳戶共用快照，請將快照標示為私有。然後指定您要共用快照資料的使用者或帳戶。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會出現。

檢查 ID

`rSs93HQwa1`

警示條件

紅色：Amazon RDS 快照標記為公有。

建議的動作

除非您確定要與所有 AWS 帳戶 和使用者共用快照中的所有資料，否則請修改許可：將快照標記為私有，然後指定您要授予許可的帳戶。如需詳細資訊，請參閱共用資料庫快照或資料庫叢集快照。無法從 Trusted Advisor 主控台檢視中排除此檢查。

若要直接修改快照的許可，您可以在 AWS Systems Manager 主控台中使用 Runbook。如需詳細資訊，請參閱`AWSSupport-ModifyRDSSnapshotPermission`。

其他資源

備份與還原 Amazon RDS 資料庫執行個體

報告欄位

- Status
- 區域
- 資料庫執行個體或叢集 ID
- 快照 ID

Amazon RDS 安全群組存取風險

描述

檢查 Amazon Relational Database Service (Amazon RDS) 的安全群組組態，並在安全群組規則授予過度寬鬆的資料庫許可存取權時發出警告。建議的安全群組規則組態是僅允許從特定的 Amazon Elastic Compute Cloud (Amazon EC2) 安全群組或特定 IP 地址存取。

檢查 ID

```
nNauJisYIT
```

警示條件

- 黃色：資料庫安全群組規則參考的 Amazon EC2 安全群組會授予對下列其中一個連接埠的全域存取權：20、21、22、1433、1434、3306、3389、4333、5432、5500。
- 黃色：資料庫安全群組規則會授予對多個單一 IP 地址的存取權 (CIDR 規則尾碼不是 /0 或 /32)。
- 紅色：資料庫安全群組規則會授予全域存取權 (CIDR 規則尾碼為 /0)。

建議的動作

檢閱您的安全群組規則，並將存取權設定為僅限授權的 IP 地址或 IP 範圍使用。若要編輯安全性群組，請使用授權 SecurityGroupIngress API 或. AWS Management Console 如需詳細資訊，請參閱使用資料庫安全群組。

其他資源

- Amazon RDS 安全群組
- 無類別網域間路由
- TCP 和 UDP 連接埠號碼清單

報告欄位

- Status
- 區域
- RDS 安全群組名稱
- 輸入規則
- 原因

Amazon RDS 儲存加密已關閉

描述

Amazon RDS 使用您管理的金鑰，支援所有資料庫引擎的靜態加密AWS Key Management Service。在具有 Amazon RDS 加密的作用中資料庫執行個體上，儲存在儲存中的靜態資料會加密，類似於自動備份、僅供讀取複本和快照。

如果在建立資料庫執行個體時未開啟加密，則必須先還原已解密快照的加密副本，然後再開啟加密。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

`c1qf5bt006`

警示條件

紅色：Amazon RDS 資源未啟用加密。

建議的動作

為資料庫執行個體開啟靜態資料加密。

其他資源

只有在建立資料庫執行個體時，才能加密資料庫執行個體。若要加密現有作用中資料庫執行個體：

建立原始資料庫執行個體的加密副本

1. 建立資料庫執行個體的快照。
2. 為步驟 1 中建立的快照建立加密副本。
3. 從加密的快照還原資料庫執行個體。

如需詳細資訊，請參閱下列資源：

- 加密 Amazon RDS 資源
- 複製資料庫快照

報告欄位

- Status
- 區域
- 資源
- 引擎名稱
- 上次更新時間

Amazon 路線 53 不匹配的 CNAME 記錄直接指向 S3 存儲桶

描述

檢查具有直接指向 Amazon S3 儲存貯體主機名稱的 CNAME 記錄的 Amazon Route 53 託管區域，如果您的 CNAME 與您的 S3 儲存貯體名稱不符，則會發出警示。

檢查 ID

```
c1ng44jvbm
```

警示條件

紅色：Amazon Route 53 託管區域的 CNAME 記錄指向 S3 存儲桶主機名稱不匹配。

綠色：在您的 Amazon 路線 53 託管區域中找不到不匹配的 CNAME 記錄。

建議的動作

將 CNAME 記錄指向 S3 儲存貯體主機名稱時，您必須確定您設定的任何 CNAME 或別名記錄都有相符的儲存貯體。這樣可以避免 CNAME 記錄被欺騙的風險。您還可以防止任何未經授權的AWS用戶在您的域中託管錯誤或惡意的 Web 內容。

若要避免將 CNAME 記錄直接指向 S3 儲存貯體主機名稱，請考慮使用來源存取控制 (OAC) 透過 Amazon 存取 S3 儲存貯體 Web 資產。 CloudFront

如需將 CNAME 與 Amazon S3 儲存貯體主機名稱建立關聯的詳細資訊，請參閱使用 CNAME 記錄自訂 Amazon S3 URL。

其他資源

- 如何將主機名稱與 Amazon S3 儲存貯體建立關聯
- 限制對 Amazon S3 來源的訪問 CloudFront

報告欄位

- Status
- 託管區域 ID
- 託管區域
- 符合 CNAME 記錄
- CNAME 記錄不相符
- 上次更新時間

Amazon Route 53 MX 資源記錄集和寄件者政策架構

描述

針對每個 MX 資源記錄集，檢查 TXT 或 SPF 資源記錄集是否包含有效的 SPF 記錄。記錄開頭必須為「v=spf1」。SPF 記錄會指定已授權為您的網域傳送電子郵件的伺服器，這有助於偵測和阻止電子郵件地址詐騙，並減少垃圾郵件。Route 53 建議您使用 TXT 記錄而非 SPF 記錄。只要每個 MX 資源記錄集至少有一筆 SPF 或 TXT 記錄，Trusted Advisor 就會將此檢查報告為綠色。

檢查 ID

c9D319e7sG

警示條件

黃色：MX 資源記錄集沒有包含有效 SPF 值的 TXT 或 SPF 資源記錄。

建議的動作

針對每個 MX 資源記錄集，建立包含有效 SPF 值的 TXT 或 SPF 資源記錄集。如需詳細資訊，請參閱 Sender Policy Framework: SPF Record Syntax (寄件者政策架構：SPF 記錄語法) 和 Creating

Resource Record Sets By Using the Amazon Route 53 Console (使用 Amazon Route 53 主控台來建立資源記錄集)。

其他資源

- 寄件者政策架構
- MX 記錄

報告欄位

- 託管區域名稱
- 託管區域 ID
- 資源記錄集名稱
- Status

Amazon S3 儲存貯體許可

描述

檢查 Amazon Simple Storage Service (Amazon S3) 中的儲存貯體是否具有開放存取許可，或允許存取任何通過驗證的 AWS 使用者。

此檢查會檢查明確的儲存貯體許可，以及可能會覆寫這些許可的儲存貯體政策。建議不要將 Amazon S3 儲存貯體的 List 存取權授予所有使用者。這些許可有可能導致非預期的使用者以高頻率列出儲存貯體中的物件，進而造成費用高於預期。授予上傳和刪除存取權給所有人的許可，可能會導致儲存貯體中出現安全漏洞。

檢查 ID

`Pfx0RwqBli`

警示條件

- 黃色：儲存貯體 ACL 授予每個人或者任何已驗證的 AWS 使用者 List 存取權。
- 黃色：儲存貯體政策授予任何類型的開放式存取權。
- 黃色：儲存貯體政策具有授予公開存取權的陳述式。封鎖對具有公用政策的儲存貯體的公開與跨帳戶存取權設定已開啟，並且將存取權設定為僅限該帳戶的授權使用者使用，直到公開陳述式已遭移除。
- 黃色：Trusted Advisor 沒有檢查政策的許可，或者由於其他原因無法評估該政策。
- 紅色：儲存貯體 ACL 授予每個人或者任何已驗證的 AWS 使用者 Upload 和 Delete 存取權。

建議的動作

如果儲存貯體授予開放式存取權，請確定是否真的需要開放式存取權。如果不需要，請更新儲存貯體許可，以將存取權設定為僅限擁有者或特定使用者使用。使用 Amazon S3 封鎖公開存取，控制允許公開存取資料的設定。設定設定儲存貯體及物件存取許可。

其他資源

管理對您 Amazon S3 資源的存取許可

報告欄位

- Status
- 區域名稱
- 區域 API 參數
- 儲存貯體名稱
- ACL 允許 List 存取權
- ACL 允許 Upload 和 Delete 存取權
- 政策允許存取權

已停用具有 DNS 解析的 Amazon VPC 對等互連

描述

檢查您的 VPC 對等互連是否同時為接受者和請求者 VPC 開啟 DNS 解析。

VPC 對等互連的 DNS 解析可在從 VPC 查詢時，將公用 DNS 主機名稱解析為私有 IPv4 地址。這允許使用 DNS 名稱在對等 VPC 中的資源之間進行通訊。VPC 對等互連中的 DNS 解析可讓應用程式開發和管理變得更簡單、更不容易出錯，並確保資源一律會透過 VPC 對等互連進行私密通訊。

您可以使用 AWS Config 規則中的 vpcIds 參數來指定 VPC ID。

如需詳細資訊，請參閱啟用 VPC 對等互連的 DNS 解析。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

c18d2gz124

來源

AWS Config Managed Rule: vpc-peering-dns-resolution-check

警示條件

黃色：VPC 對等互連中的接受者和請求者 VPC 皆未啟用 DNS 解析。

建議的動作

開啟 VPC 對等互連的 DNS 解析。

其他資源

- 修改 VPC 對等互連連線選項
- VPC 中的 DNS 屬性

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

沒有資源型政策來防止刪除復原點的 AWS Backup Vault

描述

檢查 AWS Backup 保存庫是否具有可防止復原點刪除的已附加資源型政策。

資源型政策可防止意外刪除復原點，讓您以最低權限對備份資料強制執行存取控制。

您可以指定不希望AWS Config規則簽入規則principalArnList參數的 AWS Identity and Access Management ARN。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`c18d2gz152`

來源

`AWS Config Managed Rule: backup-recovery-point-manual-deletion-disabled`

警示條件

黃色：有些 AWS Backup Vault 沒有可防止刪除復原點的資源型政策。

建議的動作

為您的 AWS Backup 文件庫建立資源型政策，以防止意外刪除復原點。

此原則必須包含具備備份:DeleteRecoveryPoint、備份:和備份:UpdateRecoveryPointLifecyclePutBackupVaultAccessPolicy 權限的「拒絕」陳述式。

如需詳細資訊，請參閱設定備份文件庫的存取政策。

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

AWS CloudTrail 日誌

描述

檢查您使用的AWS CloudTrail. CloudTrail AWS 帳戶透過記錄在帳戶上進行的 AWS API 呼叫的相關資訊，提高對您的活動的可見度。例如，您可以使用這些日誌來判斷特定使用者在指定時段內採取的動作，或是哪些使用者在指定時段內對特定資源採取了動作。

由於將日誌檔 CloudTrail 交付到 Amazon Simple Storage Service (Amazon S3) 儲存貯體，因此 CloudTrail 必須具有儲存貯體的寫入許可。如果某筆追蹤記錄會套用到所有區域 (建立新追蹤記錄時的預設值)，該追蹤記錄會多次出現在 Trusted Advisor 報告中。

檢查 ID

`vjafUGJ9H0`

警示條件

- 黃色： CloudTrail 報告追蹤的記錄傳送錯誤。
- 紅色：尚未為區域建立追蹤，或已關閉追蹤的記錄功能。

建議的動作

若要從主控台建立追蹤並開始記錄，請移至 AWS CloudTrail 主控台。

若要開始記錄，請參閱停止和開始追蹤記錄。

如果您收到日誌交付錯誤，請檢查以確認儲存貯體存在，且必要的政策已連接至儲存貯體。請參閱 Amazon S3 儲存貯體政策。

其他資源

- AWS CloudTrail使用者指南
- 支援的區域
- 支援的服務

報告欄位

- Status
- 區域
- 追蹤記錄名稱
- 記錄狀態
- 儲存貯體名稱
- 上次交付日期

使用已棄用執行階段的 AWS Lambda 函數

描述

檢查是否有 Lambda 函數設為使用即將棄用或已棄用的執行階段。已棄用的執行時間不符合安全性更新或技術支援的資格。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

已發佈的 Lambda 函數版本是不可變的，這表示可以叫用它們，但無法更新它們。只能更新 Lambda 函數的 $LATEST 版本。如需詳細資訊，請參閱 Lambda 函數版本。

檢查 ID

L4dfs2Q4C5

警示條件

- 紅色：函數正在已棄用的執行階段上執行。
- 黃色：函數在將在 180 天內棄用的執行階段上執行。

建議的動作

如果您有函數正在接近棄用的執行階段上執行，您應該準備將這些函數遷移至受支援的執行階段。如需詳細資訊，請參閱執行階段支援政策。

建議您刪除已不再使用的先前函數版本。

其他資源

Lambda 執行階段

報告欄位

- Status
- 區域
- 函數 ARN
- 執行期
- 距離棄用的天數
- 取代日期
- 平均每日叫用次數
- 上次更新時間

AWS Well-Architected 安全性的高風險問題

描述

檢查安全性支柱中，工作負載是否有高風險問題 (HRI)。這項檢查是以您的 AWS-Well Architected 檢閱為基礎。您的檢查結果取決於您是否使用 AWS Well-Architected 完成工作負載評估。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`Wxdfp4B1L3`

警示條件

- 紅色：在 AWS Well-Architected 的安全支柱中發現至少一個待處理的高風險問題。
- 綠色：在 AWS Well-Architected 的安全支柱中未發現到任何待處理的高風險問題。

建議的動作

AWS Well-Architected 在工作負載評估期間偵測到高風險問題。解決這些問題，可能有機會降低風險和節省成本。登入 AWS Well-Architected 工具，檢閱答案並採取行動，解決待處理的問題。

報告欄位

- Status
- 區域
- 工作負載 ARN
- 工作負載名稱
- 檢閱者姓名
- 工作負載類型
- 工作負載開始日期
- 工作負載上次修改日期
- 安全性方面已識別的高風險問題數量
- 安全性方面已解決的高風險問題數量

- 安全性方面的問題數量
- 安全性支柱中的問題總數
- 上次更新時間

CloudFrontIAM 憑證存放區中的自訂 SSL 憑證

描述

檢查 IAM 憑證存放區中的 CloudFront 替代網域名稱的 SSL 憑證。這項檢查會在憑證過期、即將過期、使用過期的加密或未正確設定分佈時發出提醒。

當替代網域名稱的自訂憑證到期時，顯示您 CloudFront 內容的瀏覽器可能會顯示有關您網站安全性的警告訊息。Chrome 和 Firefox 等 Web 瀏覽器已棄用使用 SHA-1 雜湊演算法加密的憑證。

憑證包含的網域名稱，必須與原始網域名稱或檢視者請求之主機標頭中的網域名稱相符。如果不匹配，則向用戶 CloudFront 返回 502（錯誤網關）的 HTTP 狀態碼。如需詳細資訊，請參閱使用備用網域名稱與 HTTPS。

檢查 ID

N425c450f2

警示條件

- 紅色：自訂 SSL 憑證已過期。
- 黃色：自訂 SSL 憑證會在接下來的七天內到期。
- 黃色：自訂 SSL 憑證使用 SHA-1 雜湊演算法加密。
- 黃色：分佈中的一個或多個備用網域名稱沒有出現在自訂 SSL 憑證的 Common Name (通用名稱) 欄位或 Subject Alternative Names (主體備用名稱) 欄位中。

建議的動作

更新過期的憑證或即將到期的憑證。

以使用 SHA-256 雜湊演算法加密的憑證，取代使用 SHA-1 雜湊演算法加密的憑證。

以 Common Name (通用名稱) 欄位或 Subject Alternative Names (主體備用網域名稱) 欄位中有適用值的憑證來取代該憑證。

其他資源

使用 HTTPS 連線存取物件

報告欄位

- Status
- 分佈 ID
- 分佈網域名稱
- 憑證名稱
- 原因

CloudFront 原始伺服器上的 SSL 憑證

描述

檢查原始伺服器是否有已過期、即將過期、遺失或使用過期加密的 SSL 憑證。如果憑證有其中一個問題，請使用 HTTP 狀態碼 502「錯誤的閘道」來 CloudFront 回應內容的要求。

Chrome 和 Firefox 等 Web 瀏覽器已棄用使用 SHA-1 雜湊演算法加密的憑證。根據您與 CloudFront分發相關聯的 SSL 憑證數量而定，此檢查每月可能會增加幾美分的費用，例AWS如，如果您使用 Amazon EC2 或 Elastic Load Balancing 作為 CloudFront 分發的來源。此檢查不會驗證您的原始伺服器憑證鏈結或憑證授權單位。您可以在 CloudFront 配置中檢查這些內容。

檢查 ID

N430c450f2

警示條件

- 紅色：您原始伺服器上的 SSL 憑證已過期或遺失。
- 黃色：您原始伺服器上的 SSL 憑證會在三十天後到期。
- 黃色：您原始伺服器上的 SSL 憑證使用 SHA-1 雜湊演算法加密。
- 黃色：找不到您原始伺服器上的 SSL 憑證。連線可能因為逾時或其他 HTTPS 連線問題而失敗。

建議的動作

如果您原始伺服器上的憑證已過期或即將到期，請更新憑證。

如果憑證不存在，則新增憑證。

以使用 SHA-256 雜湊演算法加密的憑證，取代使用 SHA-1 雜湊演算法加密的憑證。

其他資源

使用備用網域名稱和 HTTPS

報告欄位

- Status
- 分佈 ID
- 分佈網域名稱
- Origin
- 原因

ELB 接聽程式安全性

描述

針對未使用建議的安全性組態進行加密通訊的接聽程式，檢查負載平衡器。 AWS建議使用安全協議（HTTPS 或 SSL）， up-to-date 安全策略以及安全的密碼和協議。

針對前端連線 (用戶端連至負載平衡器) 使用安全通訊協定時，用戶端與負載平衡器之間的請求會經過加密，藉此建立更安全的環境。Elastic Load Balancing 提供預先定義的安全政策，其加密和通訊協定符合 AWS 安全最佳實務。預先定義政策的新版本會隨著新組態開放使用而發佈。

檢查 ID

```
a2sEc6ILx
```

警示條件

- 黃色：負載平衡器沒有使用安全通訊協定 (HTTPS 或 SSL) 的接聽程式。
- 黃色：負載平衡器接聽程式使用了過期的預先定義 SSL 安全政策。
- 黃色：負載平衡器接聽程式使用了不建議使用的密碼或通訊協定。
- 紅色：負載平衡器接聽程式使用了不安全的密碼或通訊協定。

建議的動作

如果到負載平衡器的流量必須是安全的，請使用 HTTPS 或 SSL 通訊協定進行前端連線。

將負載平衡器升級至最新版本的預先定義 SSL 安全政策。

僅使用建議的密碼和通訊協定。

如需詳細資訊，請參閱 Elastic Load Balancing 的接聽程式組態。

其他資源

- 接聽程式組態快速參考

- 更新負載平衡器的 SSL 溝通組態
- Elastic Load Balancing 的 SSL 溝通組態
- SSL 安全政策表

報告欄位

- Status
- 區域
- 負載平衡器名稱
- 負載平衡器連接埠
- 原因

ELB 安全群組

描述

檢查是否有負載平衡器設定了遺失的安全群組，或是允許存取未針對負載平衡器設定之連接埠的安全群組。

如果刪除與負載平衡器相關聯的安全群組，負載平衡器將無法如預期運作。如果安全群組允許存取未針對負載平衡器設定的連接埠，資料遺失或遭受惡意攻擊的風險就會增加。

檢查 ID

xSqX82fQu

警示條件

- 黃色：與負載平衡器相關聯的 Amazon VPC 安全群組的傳入規則，允許存取未在負載平衡器的接聽程式組態中定義的連接埠。
- 紅色：與負載平衡器相關聯的安全群組不存在。

建議的動作

設定安全群組規則，將存取權設定為僅限僅負載平衡器接聽程式組態中定義的連接埠和通訊協定可以使用，以及支援 Path MTU 探索的 ICMP 通訊協定可以使用。請參閱 Classic Load Balancer 的接聽程式和在 VPC 中負載平衡器的安全群組。

如果遺失安全群組，請將新的安全群組套用至負載平衡器。建立安全群組規則，將存取權設定為僅限僅負載平衡器接聽程式組態中定義的連接埠和通訊協定可以使用。請參閱在 VPC 中負載平衡器的安全群組。

其他資源

- Elastic Load Balancing User Guide (《Elastic Load Balancing 使用者指南》)
- 設定 Classic Load Balancer

報告欄位

- Status
- 區域
- 負載平衡器名稱
- 安全群組 ID
- 原因

存取金鑰已暴露

描述

檢查常用的程式碼存放庫是否有已遭暴露的存取金鑰，以及可能因為存取金鑰遭入侵而造成的不正常的 Amazon Elastic Compute Cloud (Amazon EC2) 用量。

存取金鑰由存取金鑰 ID 和對應的私密存取金鑰組成。遭暴露的存取金鑰會對您的帳戶和其他使用者構成安全風險，可能會導致未經授權的活動或濫用而產生過多費用，以及違反 AWS 客戶協議。

如果您的存取金鑰已遭暴露，請立即採取行動來保護您的帳戶。為避免您的帳戶被收取過高費用，AWS 會暫時限制您建立某些 AWS。這無法確保您的帳戶安全。只能限制部分您可能需支付費用的未經授權使用。

> **Note**
>
> 此檢查並不保證能識別遭暴露的存取金鑰或遭入侵的 EC2 執行個體。保您存取金鑰和 AWS 資源安全無虞的責任最終落在您肩上。
> 此檢查的結果會自動重新整理，且不允許重新整理請求。目前，您無法從此檢查中排除資源。

如果顯示存取金鑰有截止日期，且在該日期之前沒有停止未經授權的使用，則 AWS 可能會暫停 AWS 帳戶。如果您認為警示有誤，請聯絡 AWS Support。

Trusted Advisor 中顯示的資訊可能無法反映您帳戶的最新狀態。在帳戶上所有公開的存取金鑰都解決之前，不會將公開的存取金鑰標記為已解決。此資料同步最多可能需要一週的時間。

檢查 ID

12Fnkpl8Y5

警示條件

- 紅色：可能已遭到入侵 – AWS 已識別到已經在網際網路上公開且可能已遭到入侵 (已使用) 的存取金鑰 ID 及其對應的私密存取金鑰。
- 紅色：公開 – AWS 已識別已在網際網路上公開的存取金鑰 ID 及其對應的私密存取金鑰。
- 紅色：可疑 – 異常的 Amazon EC2 使用情況表示存取金鑰可能已遭到入侵，但尚未被識別為已在網際網路上公開。

建議的動作

儘快刪除受影響的存取金鑰。如果金鑰與 IAM 使用者相關聯，請參閱管理 IAM 使用者的存取金鑰。

檢查您的帳戶是否有未經授權的使用。登入 AWS Management Console 並檢查每個服務控制台是否存在可疑資源。請特別注意正在執行中的 Amazon EC2 執行個體、Spot 執行個體請求、存取金鑰和 IAM 使用者。您還可以在帳單和成本管理主控台上檢查整體使用情況。

其他資源

- 《管理 AWS 存取金鑰的最佳實務》
- 《AWS 安全性稽核指南》

報告欄位

- 存取金鑰 ID
- 使用者名稱 (IAM 或根)
- 詐騙類型
- 案例 ID
- 更新時間
- 位置
- 截止日期
- 用量 (美元/日)

IAM 存取金鑰輪換

描述

檢查是否有作用中 IAM 存取金鑰過去 90 天內未輪換。

若定期輪換存取金鑰，可以減少在您不知情的情況下使用遭入侵的金鑰來存取資源的機會。就這項檢查的目的而言，上次輪換日期和時間指的是建立存取金鑰或上次啟用的時間。存取金鑰編號和日期來自最新 IAM 憑證報告中的 `access_key_1_last_rotated` 和 `access_key_2_last_rotated` 資訊。

由於憑證報告的重新產生頻率受到限制，因此重新整理此檢查可能不會反映最近的變更。如需詳細資訊，請參閱取得 AWS 帳戶 帳戶的憑證報告。

若要建立和輪換存取金鑰，使用者必須擁有相應的許可。如需詳細資訊，請參閱允許使用者管理自己的密碼、存取金鑰和 SSH 金鑰。

檢查 ID

`DqdJqYeRm5`

警示條件

- 綠色：存取金鑰處於作用中狀態，並在過去的 90 天內輪換過。
- 黃色：存取金鑰處於作用中狀態，並在過去 2 年內輪換過，但輪換時間已超過 90 天。
- 紅色：存取金鑰處於作用中狀態，但在過去 2 年內沒有輪換過。

建議的動作

定期輪換存取金鑰。請參閱輪換存取金鑰和管理 IAM 使用者的存取金鑰。

其他資源

- IAM 最佳實務
- 如何輪換 IAM 使用者的存取金鑰

報告欄位

- Status
- IAM 使用者
- 存取金鑰
- 上次輪換的金鑰
- 原因

IAM 密碼政策

描述

檢查帳戶的密碼策略，並在密碼政策未啟用或密碼內容要求未啟用時發出警告。

密碼內容要求可藉由強制建立高強度使用者密碼，提高您 AWS 環境的整體安全性。建立或變更密碼政策時，對立即為新的使用者強制執行該項變更，但不會要求現有使用者變更密碼。

檢查 ID

Yw2K9puPzl

警示條件

- 黃色：已啟用密碼政策，但至少有一項內容要求未啟用。
- 紅色：未啟用密碼政策。

建議的動作

如果未啟用某些內容要求，請考慮啟用它們。如果未啟用密碼政策，請建立並設定一個密碼政策。請參閱設定 IAM 使用者的帳戶密碼政策。

其他資源

管理密碼

報告欄位

- 密碼政策
- 大寫
- 小寫
- Number
- 非英數字元

IAM 使用情形

描述

檢查您的 IAM 使用情形。您可以使用 IAM 在 AWS 中建立使用者、群組和角色。您還可以使用許可來控制對 AWS 資源的存取。這項檢查的目的是透過檢查是否存在至少一位 IAM 使用者，來阻止使用根存取權。如果您遵循在外部身分提供者或者 AWS IAM Identity Center 中集中身分並設定使用者的最佳實務，則可以忽略警示。

檢查 ID

zXCkfM1nI3

警示條件

黃色：尚未為此帳戶建立任何 IAM 使用者。

建議的動作

建立 IAM 使用者或使用 AWS IAM Identity Center 建立其他使用者，確保這些使用者僅限於可在 AWS 環境中執行特定任務。

其他資源

- 什麼是 AWS IAM Identity Center？
- 什麼是 IAM？

根帳戶的 MFA

描述

檢查根帳戶，並在未啟用多重要素驗證 (MFA) 時發出警告。

為了提高安全性，建議您使用 MFA 來保護您的帳戶，此功能會要求使用者在與 AWS Management Console 及關聯網站互動時，從其 MFA 硬體或虛擬裝置輸入唯一身分驗證代碼。

檢查 ID

7DAFEmoDos

警示條件

紅色：根帳戶上未啟用 MFA。

建議的動作

登入您的根帳戶並啟動 MFA 裝置。請參閱檢查 MFA 狀態和設定 MFA 裝置。

其他資源

在 AWS 中使用多重要素驗證 (MFA) 裝置

安全群組–– 不受限制的特定連接埠

描述

檢查安全群組的規則是否允許對特定連接埠進行無限制存取 (0.0.0.0/0)。

不受限制的訪問增加了惡意活動（黑客 denial-of-service 攻擊，攻擊，數據丟失）的機會。風險最高的連接埠會標示為紅色，而風險較低的連接埠會標示為黃色。標示為綠色的連接埠通常由需要不受限制存取的應用程式 (例如 HTTP 和 SMTP) 使用。

如果您刻意以這種方式設定安全群組，建議您使用其他安全措施來保護基礎設施 (例如 IP 表)。

> **Note**
>
> 此檢查只會評估您為 IPv4 地址建立的安全群組及其傳入規則。AWS Directory Service 建立的安全群組會標記為紅色或黃色，但它們不會構成安全風險，且可以安全地忽略或排除。如需詳細資訊，請參閱 Trusted Advisor 常見問答集。

> **Note**
>
> 此檢查不包括當客戶管理前綴清單授與存取 0.0.0.0/0 的存取權，而且用作具有安全性群組的來源時的使用案例。

檢查 ID

HCP4007jGY

警示條件

- 綠色：連接埠 80、25、443 或 465 的存取不受限制。
- 紅色：連接埠 20、21、1433、1434、3306、3389、4333、5432 或 5500 的存取不受限制。
- 黃色：任何其他連接埠的存取不受限制。

建議的動作

將存取權設定為僅限需要存取權的 IP 地址使用。若要將存取權設定為僅限特定 IP 地址使用，請將尾碼設定為 /32 (例如 192.0.2.10/32)。建立更嚴格的規則之後，請務必刪除過於寬鬆的規則。

其他資源

- Amazon EC2 安全群組

  TCP 和 UDP 連接埠號碼清單
- 無類別網域間路由

報告欄位

- Status
- 區域

- 安全群組名稱
- 安全群組 ID
- 通訊協定
- 從連接埠
- 到連接埠

安全群組 - 不受限制的存取

描述

檢查安全群組的規則是否允許不受限制存取資源。

不受限制的訪問增加了惡意活動（黑客 denial-of-service 攻擊，攻擊，數據丟失）的機會。

> **Note**
>
> 此檢查只會評估您為 IPv4 地址建立的安全群組及其傳入規則。AWS Directory Service 建立的安全群組會標記為紅色或黃色，但它們不會構成安全風險，且可以安全地忽略或排除。如需詳細資訊，請參閱 Trusted Advisor 常見問答集。

> **Note**
>
> 此檢查不包括當客戶管理前綴清單授與存取 0.0.0.0/0 的存取權，而且用作具有安全性群組的來源時的使用案例。

檢查 ID

`1iG5NDGVre`

警示條件

紅色：安全群組規則的來源 IP 地址的連接埠尾碼為 /0，而不是 25、80 或 443。

建議的動作

將存取權設定為僅限需要存取權的 IP 地址使用。若要將存取權設定為僅限特定 IP 地址使用，請將尾碼設定為 /32 (例如 192.0.2.10/32)。建立更嚴格的規則之後，請務必刪除過於寬鬆的規則。

其他資源

- Amazon EC2 安全群組
- 無類別網域間路由

報告欄位

- Status
- 區域
- 安全群組名稱
- 安全群組 ID
- 通訊協定
- 從連接埠
- 到連接埠
- IP 範圍

容錯能力

您可以針對容錯能力類別使用下列檢查。

檢查名稱

- ALB 異地同步備份
- 未啟用 Amazon Aurora MySQL 叢集回溯功能
- Amazon Aurora 資料庫執行個體存取性
- Amazon CloudFront 原始容錯
- Amazon Comprehend 端點存取風險
- Amazon DocumentDB 單一可用區叢集
- Amazon DynamoDB P 復原 oint-in-time
- Amazon DynamoDB 資料表並未包含在備份計畫中
- Amazon EBS 不包括在計劃中 AWS Backup
- Amazon EBS 快照
- Amazon EC2 Auto Scaling 未啟用 ELB 運作狀態檢查
- Amazon EC2 Auto Scaling 群組已啟用了容量重新平衡
- Amazon EC2 Auto Scaling 未部署在多個 AZ 中，或不符合最少 AZ 數量

- Amazon EC2 可用區域平衡
- 未啟用 Amazon EC2 詳細監控
- Amazon ECS AWS記錄驅動程式處於封鎖模式
- Amazon ECS 服務使用單一 AZ
- Amazon ECS Multi-AZ 放置策略
- Amazon EFS 無掛載目標備援
- Amazon EFS 不在 AWS Backup 計劃中
- Amazon ElastiCache 異地同步備份叢集
- Amazon ElastiCache Redis 集群自動 Backup
- Amazon MemoryDB Multi-AZ 叢集
- Amazon MSK 代理程式託管過多分割區
- 具有少於三個資料節點的 Amazon OpenSearch 服務網域
- Amazon RDS 備份
- Amazon RDS 資料庫叢集有一個資料庫執行個體
- 具有所有執行個體位於相同可用區域的 Amazon RDS 資料庫叢集
- Amazon RDS 資料庫叢集，所有讀取器執行個體都位於相同可用區域
- 未啟用 Amazon RDS 資料庫執行個體增強型監控
- Amazon RDS 資料庫執行個體已關閉儲存自動調度資源
- 不使用異地同步備份部署的 Amazon RDS 資料庫執行
- Amazon RDS DiskQueueDepth
- Amazon RDS FreeStorageSpace
- Amazon RDS 日誌輸出參數設置為表
- Amazon RDS 默認 _ 行格式參數設置不安全
- Amazon RDS 信息 _ 刷新 _ 日誌 _ 提交參數不是 1
- Amazon RDS 最大用戶 _ 連接參數很低
- Amazon RDS Multi-AZ
- Amazon RDS 不在 AWS Backup 計劃中
- Amazon RDS 僅供讀取複本以可寫入模式開啟
- Amazon RDS 資源自動備份已關閉

- Amazon RDS 同步記錄參數已關閉
- RDS 資料庫叢集未啟用 Multi-AZ 複寫
- 未啟用 RDS Multi-AZ 備用執行個體
- Amazon RDS ReplicaLag
- Amazon RDS 同步提交參數已關閉
- Amazon Redshift 叢集自動快照
- Amazon Route 53 已刪除運作狀態檢查
- Amazon Route 53 容錯移轉資源記錄集
- Amazon Route 53 高 TTL 資源記錄集
- Amazon Route 53 名稱伺服器委派
- Amazon Route 53 Resolver 端點可用區域備援
- Simple Storage Service (Amazon S3) 儲存貯體記錄
- 未啟用 Amazon S3 儲存貯體複寫
- Amazon S3 Bucket Versioning
- 應用程式、網路及閘道負載平衡器未跨多個可用區域
- Auto Scaling 在子網路中的可用 IP
- Auto Scaling 群組運作狀態檢查
- Auto Scaling 群組資源
- 在單一可用區域中執行 HSM 執行個體的AWS CloudHSM 叢集
- AWS Direct Connect 連線備援
- AWS Direct Connect 位置冗餘
- AWS Direct Connect 位置彈性
- AWS Direct Connect 虛擬介面備援
- AWS Lambda 沒有配置無效字母隊列的函數
- AWS Lambda 失敗時事件目的地
- 不含多可用區域備援且支援 VPC 的AWS Lambda 函數
- AWS Resilience Hub 違反政策
- AWS Resilience Hub 彈性分數
- AWS Resilience Hub 評估年齡

- AWS Site-to-Site VPN 至少有一個通道處於「關閉」狀態
- AWS Well-Architected 可靠性的高風險問題
- Classic Load Balancer 未設定多個 AZ
- ELB 連接耗盡
- ELB 跨區域負載平衡
- 負載平衡器最佳化
- NAT Gateway AZ 獨立性
- 跨負載平衡的 Network Load Balancer
- NLB-私有子網路中的網際網路對向資源
- NLB 異地同步備份
- 事件管理員複製組 AWS 區域 中的數目
- 單一 AZ 應用程式檢查
- 多個 AZ 中的 VPC 介面端點網路介面
- VPN 通道備援
- ActiveMQ 可用區域備援
- RabbitMQ 可用區域備援

ALB 異地同步備份

描述

檢查您的應用程式負載平衡器是否設定為使用一個以上的可用區域 (AZ)。AZ 是明顯與其他區域中的故障隔絕開來的地點。在相同區域的多個 AZ 中設定負載平衡器，以協助改善工作負載可用性。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c1dfprch08
```

警示條件

黃色：ALB 位於單一 AZ 中。

綠色：ALB 具有兩個或兩個以上的 AZ。

建議的動作

請確定您的負載平衡器至少設定了兩個可用區域。

如需詳細資訊，請參閱《Application Load Balancer 的可用區域》。

其他資源

如需詳細資訊，請參閱下列 文件：

- Elastic Load Balancing 的運作方式
- 區域、可用區域和本地區域

報告欄位

- Status
- 區域
- ALB 名稱
- ALB 法則
- 阿爾布 ARN
- AZ 數量
- 上次更新時間

未啟用 Amazon Aurora MySQL 叢集回溯功能

描述

檢查 Amazon Aurora MySQL 叢集是否已啟用回溯功能。

Amazon Aurora MySQL 叢集回溯是一項功能，可讓您將 Aurora 資料庫叢集還原到先前的時間點，而無需建立新叢集。它可讓您將資料庫復原到保留期間內的特定時間點，而無需從快照還原。

您可以在 AWS Config 規則BacktrackWindowInHours參數中調整回溯時間範圍 (小時)。

如需詳細資訊，請參閱恢復 Aurora 資料庫叢集。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz131
```

來源

```
AWS Config Managed Rule: aurora-mysql-backtracking-enabled
```

警示條件

黃色：未啟用 Amazon Aurora MySQL 叢集回溯功能。

建議的動作

開啟 Amazon Aurora MySQL 叢集的回溯功能。

如需詳細資訊，請參閱恢復 Aurora 資料庫叢集。

其他資源

回溯 Aurora 資料庫叢集

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

Amazon Aurora 資料庫執行個體存取性

描述

檢查是否有 Amazon Aurora 資料庫叢集同時具備私有執行個體和公有執行個體。

如果主要資料庫執行個體失敗，可將複本提升為主要執行個體。如果該複本是私有的，則只具公有存取權的使用者在容錯移轉後將無法再連線至資料庫。建議叢集中的所有資料庫執行個體都具有相同的存取性。

檢查 ID

`xuy7H1avtl`

警示條件

黃色：Aurora 資料庫叢集中的執行個體具有不同的可存取性 (混合公有和私有)。

建議的動作

修改資料庫叢集中執行個體的 `Publicly Accessible` 設定，使其全部為公有或私有。如需詳細資訊，請參閱修改執行 MySQL 資料庫引擎的資料庫執行個體中關於 MySQL 執行個體的指示。

其他資源

Aurora 資料庫叢集的容錯能力

報告欄位

- Status
- 區域
- 叢集
- 公有資料庫執行個體
- 私有資料庫執行個體
- 原因

Amazon CloudFront 原始容錯

描述

檢查原始群組是否已針對在 Amazon 中包含兩個起源的散佈進行設定 CloudFront。

如需詳細資訊，請參閱使用 CloudFront 來源容錯移轉最佳化高可用性

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz112
```

來源

```
AWS Config Managed Rule: cloudfront-origin-failover-enabled
```

警示條件

黃色：未啟用 Amazon CloudFront 原始容錯移轉。

建議的動作

請務必為您的 CloudFront 發佈開啟來源容錯移轉功能，以協助確保您的內容設定對使用者的高可用性。當您開啟此功能時，如果主要原始伺服器無法使用，流量會自動路由到備份原始伺服器。如此能讓潛在的停機時間降至最低，並確保內容的持續可用性。

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

Amazon Comprehend 端點存取風險

描述

針對使用客戶管理金鑰加密基礎模型的端點檢查 AWS Key Management Service (AWS KMS) 金鑰權限。如果客戶管理的金鑰已停用、或金鑰政策已變更而改變了 Amazon Comprehend 允許的權限，則端點可用性可能會受到影響。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

Cm24dfsM13

警示條件

紅色：如果客戶管理金鑰已停用，或金鑰政策已變更，從而改變了對 Amazon Comprehend 的存取權限。

建議的動作

如果客戶管理金鑰已停用，建議您啟用金鑰。如需詳細資訊，請參閱啟用金鑰。如果金鑰原則已變更，而您想繼續使用端點，建議您更新 AWS KMS 金鑰原則。如需詳細資訊，請參閱變更金鑰政策。

其他資源

AWS KMS 許可

報告欄位

- Status
- 區域
- 端點 ARN
- 模型 ARN
- 公里 KeyId
- 上次更新時間

Amazon DocumentDB 單一可用區叢集

描述

檢查是否有設定為單一可用區的 Amazon DocumentDB 叢集。

在單一可用區架構中執行 Amazon DocumentDB 工作負載並不足以處理高度關鍵的工作負載，而且從元件故障中復原最多可能需要 10 分鐘的時間。客戶應在其他可用區域部署複本執行個體，以確保維護、執行個體故障、元件故障或可用區域故障期間的可用性。

> **Note**
>
> 此檢查的結果會每天自動重新整理一次或多次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

c15vnddn2x

警示條件

黃色：Amazon DocumentDB 叢集的執行個體位於不到三個可用區域。

綠色：Amazon DocumentDB 叢集在三個可用區域中具有執行個體。

建議的動作

如果您的應用程式需要高可用性，請修改資料庫執行個體，以使用複本執行個體啟用異地 請參閱 Amazon DocumentDB 的高可用性和複寫

其他資源

了解 Amazon DocumentDB 叢集容錯

區域與可用區域

報告欄位

- Status
- 區域
- 可用區域
- DB Cluster Identifier (資料庫叢集識別符)
- 資料庫叢集 ARN
- 上次更新時間

Amazon DynamoDB P 復原 oint-in-time

描述

檢查是否為 Amazon DynamoDB 資料表啟用了時間點復原。

時間點復原有助於保護您的 DynamoDB 資料表免遭意外寫入或刪除操作。有了時間點復原，就無需為建立、維護或排程隨需備份而煩惱。時間點復原可將該資料表還原到過去 35 天內的任何時間點。DynamoDB 維護您資料表的增量備份。

如需詳細資訊，請參閱適用於 DynamoDB 的 P oint-in-time 復原。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`c18d2gz138`

來源

`AWS Config Managed Rule: dynamodb-pitr-enabled`

警示條件

黃色：未為您的 DynamoDB 資料表啟用 P oint-in-time 復原功能。

建議的動作

在 Amazon DynamoDB 中開啟 point-in-time 復原功能，以持續備份您的表格資料。

如需詳細資訊，請參閱 P oint-in-time 復原：其運作方式。

其他資源

適用於 DynamoDB 的 P oint-in-time 復原

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

Amazon DynamoDB 資料表並未包含在備份計畫中

描述

檢查 Amazon DynamoDB 料表是否屬於計劃的一 AWS Backup 部分。

AWS Backup 為 DynamoDB 資料表提供增量備份，這些表格可擷取自上次備份以來所做的變更。在 AWS Backup 計劃中包含 DynamoDB 表可協助保護您的資料免受意外資料遺失情況的影響，並將備份程序自動化。這可以為 DynamoDB 資料表提供可靠且可擴展的備份解決方案，協助確保您寶貴的資料獲得妥善保護，並可視需要進行復原。

如需詳細資訊，請參閱使用以下方式建立 DynamoDB 資料表的備份 AWS Backup

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz107
```

來源

```
AWS Config Managed Rule: dynamodb-in-backup-plan
```

警示條件

黃色：計劃中 AWS Backup 不包含 Amazon DynamoDB 表格。

建議的動作

確保您的 Amazon DynamoDB 表格屬於計劃的一 AWS Backup 部分。

其他資源

排程備份

什麼是 AWS Backup？

使用 AWS Backup 主控台建立備份計畫

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

Amazon EBS 不包括在計劃中 AWS Backup

描述

檢查備份計劃中是否存在 Amazon EBS 磁碟區。 AWS Backup

在 AWS Backup 計劃中包含 Amazon EBS 磁碟區，以自動化存放在這些磁碟區上的資料的定期備份。如此可保護您不受資料遺失的影響，讓資料管理更加輕鬆，並可在需要時進行資料復原。備份計畫有助於確保您的資料安全，並且能夠滿足應用程式和服務的復原時間和點目標 (RT/RPO)。

如需詳細資訊，請參閱建立備份計畫

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz106
```

來源

```
AWS Config Managed Rule: ebs-in-backup-plan
```

警示條件

黃色： AWS Backup 計劃中不包含 Amazon EBS 卷。

建議的動作

請確定您的 Amazon EBS 磁碟區是 AWS Backup 方案的一部分。

其他資源

使用 AWS Backup 主控台建立備份計劃

什麼是 AWS Backup？

開始使用 3：建立排程備份

報告欄位

- Status
- 區域

- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

Amazon EBS 快照

描述

檢查 Amazon Elastic Block Store (Amazon EBS) 磁碟區的快照存留期 (可用或使用中)。

即使已複寫 Amazon EBS 磁碟區，仍可能發生故障。快照會保留在 Amazon Simple Storage Service (Amazon S3)，以提供持久的儲存和 point-in-time復原。

檢查 ID

`H7IgTzjTYb`

警示條件

- 黃色：最新的磁碟區快照已存在 7 到 30 天。
- 紅色：最新的磁碟區快照已存在超過 30 天。
- 紅色：磁碟區沒有快照。

建議的動作

每週或每月建立磁碟區快照。如需詳細資訊，請參閱建立 Amazon EBS 快照。

其他資源

Amazon Elastic Block Store (Amazon EBS)

報告欄位

- Status
- 區域
- 磁碟區 ID
- 磁碟區名稱
- 快照 ID
- 快照名稱
- 快照存在時間
- 磁碟區連接

- 原因

Amazon EC2 Auto Scaling 未啟用 ELB 運作狀態檢查

描述

檢查與 Classic Load Balancer 關聯的 Amazon EC2 Auto Scaling 群組是否使用 Elastic Load Balancing 運作狀態檢查。Auto Scaling 群組的預設運作狀態檢查只會檢查 Amazon EC2 狀態。如果執行個體未通過這些運作狀態檢查，則會標記為運作狀態不佳並予以終止。Amazon EC2 Auto Scaling 會啟動全新替代執行個體。Elastic Load Balancing 運作狀態檢查會定期監控 Amazon EC2 執行個體，以偵測和終止運作狀態不良的執行個體，然後啟動新的執行個體。

如需詳細資訊，請參閱新增 Elastic Load Balancing 健康狀態檢查。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz104
```

來源

```
AWS Config Managed Rule: autoscaling-group-elb-healthcheck-required
```

警示條件

黃色：附加至 Classic Load Balancer 的 Amazon EC2 Auto Scaling 群組未啟用 Elastic Load Balancing 運作狀態檢查。

建議的動作

確保與 Classic Load Balancer 關聯的 Auto Scaling 群組使用 Elastic Load Balancing 運作狀態檢查。

Elastic Load Balancing 運作狀態檢查報告負載平衡器是否運作狀態良好且可用於處理請求。如此可確保應用程式的高可用性。

如需詳細資訊，請參閱將 Elastic Load Balancing 運作狀態檢查新增至 Auto Scaling 群組

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

Amazon EC2 Auto Scaling 群組已啟用了容量重新平衡

描述

檢查是否為使用多個執行個體類型的 Amazon EC2 Auto Scaling 群組啟用了容量重新平衡。

透過容量重新平衡設定 Amazon EC2 Auto Scaling 群組，有助於確保 Amazon EC2 執行個體均勻分佈在可用區域，無論執行個體類型和購買選項為何。它會使用與群組關聯的目標追蹤政策，例如 CPU 使用率或網路流量。

如需詳細資訊，請參閱具備多個執行個體類型及購買選項的 Auto Scaling 群組。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
AWS Config c18d2gz103
```

來源

AWS Config 受管規則： autoscaling-capacity-rebalancing

警示條件

黃色：未啟用 Amazon EC2 Auto Scaling 群組容量重新平衡。

建議的動作

確保已為使用多個執行個體類型的 Amazon EC2 Auto Scaling 群組啟用了容量重新平衡。

如需詳細資訊，請參閱啟用容量重新平衡 (主控台)

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

Amazon EC2 Auto Scaling 未部署在多個 AZ 中，或不符合最少 AZ 數量

描述

檢查 Amazon EC2 Auto Scaling 群組是否部署在多個可用區域之中，或是否部署在指定的可用區域的最小數量之中。在多個可用區域中部署 Amazon EC2 執行個體以確保高可用性。

您可以使用 AWS Config 規則中的參數調整可用區域的最小minAvailibilityZones數目。

如需詳細資訊，請參閱具備多個執行個體類型及購買選項的 Auto Scaling 群組。

檢查 ID

```
c18d2gz101
```

來源

```
AWS Config Managed Rule: autoscaling-multiple-az
```

警示條件

紅色：Amazon EC2 Auto Scaling 群組並未設定多個 AZ，或不符合指定的 AZ 的最小數量。

建議的動作

請確定您的 Amazon EC2 Auto Scaling 群組已設定多個 AZ。在多個可用區域中部署 Amazon EC2 執行個體以確保高可用性。

其他資源

使用啟動範本建立 Auto Scaling 群組

使用啟動組態建立 Auto Scaling 群組

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

Amazon EC2 可用區域平衡

描述

檢查 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體在一個區域中可用區域之間的分配。

可用區域為不同位置，可以隔離其他可用區域的故障。這為同一區域中其他可用區域提供實惠、低延遲的網路連線能力。藉由在同一區域的多個可用區域中啟動執行個體，您可以保護應用程式免於發生單點故障情形。

檢查 ID

```
wuy7G1zxql
```

警示條件

- 黃色：該區域在多個區域中有執行個體，但分佈不均衡 (已使用的可用區域中的最大執行個體數量與最少執行個體數量之間的差異大於 20%)。
- 紅色：該區域只在單一可用區域內有執行個體。

建議的動作

在多個可用區域內均衡分佈 Amazon EC2 執行個體。您可以手動啟動執行個體來執行此操作或使用 Auto Scaling 來自動執行此操作。如需詳細資訊，請參閱啟動您的執行個體和平衡您的 Auto Scaling 群組負載。

其他資源

《Amazon EC2 Auto Scaling 使用者指南》

報告欄位

- Status
- 區域

- 區域 a 執行個體
- 區域 b 執行個體
- 區域 c 執行個體
- 區域 e 執行個體
- 區域 f 執行個體
- 原因

未啟用 Amazon EC2 詳細監控

描述

檢查您的 Amazon EC2 執行個體是否啟用詳細監控。

Amazon EC2 詳細監控提供時間間隔更小的指標，發佈間隔為一分鐘，而 Amazon EC2 基本監控的發佈間隔為五分鐘。啟用 Amazon EC2 的詳細監控，可幫助您更完善管理 Amazon EC2 資源，以便您可以更快地尋找趨勢並採取行動。

如需詳細資訊，請參閱基本監控和詳細監控。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
AWS Config c18d2gz144
```

來源

AWS Config 受管規則：ec2-instance-detailed-monitoring-enabled

警示條件

黃色：Amazon EC2 執行個體未啟用詳細監控功能。

建議的動作

開啟 Amazon EC2 執行個體的詳細監控功能，以增加 Amazon EC2 指標資料發佈到 Amazon 的頻率 CloudWatch (每隔 5 分鐘到 1 分鐘)。

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

Amazon ECS AWS記錄驅動程式處於封鎖模式

描述

檢查使用 AWS日誌記錄驅動程式設定為封鎖模式的 Amazon ECS 任務定義。在封鎖模式中設定的驅動程式會造成系統可用性風險

> **Note**
>
> 此檢查的結果會每天自動重新整理一次或多次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`c1dvkm4z6b`

警示條件

黃色：awslogs 驅動程式記錄組態參數模式設定為封鎖或遺失。遺失 mode 參數表示預設的封鎖組態。

綠色：Amazon ECS 任務定義未使用 awslog 驅動程式，或者 awslog 驅動程式是以非封鎖模式設定的。

建議的動作

若要降低可用性風險，請考慮將作業定義 AWS記錄驅動程式組態從封鎖變更為非封鎖。在非阻塞模式下，您將必須為 max-buffer-size 參數設置一個值。如需有關組態參數的詳細資訊和指導，請參閱。請參閱防 AWS護記錄檔容器記錄驅動程式中的非封鎖模式防止記錄遺失

其他資源

使用 AWS 記錄檔記錄驅動程式

選擇容器記錄選項以避免背壓

防止記錄檔容器記錄檔驅動程式中的非封鎖模式遺失 AWS記錄

報告欄位

- Status
- 區域
- 作業定義 ARN
- 容器定義名稱
- 上次更新時間

Amazon ECS 服務使用單一 AZ

描述

檢查您的服務組態是否使用單一可用區域 (AZ)。

AZ 是明顯與其他區域中的故障隔絕開來的地點。這種做法可以支援位於相同 AWS 區域內可用區域之間不昂貴、低延遲的網路連線能力。藉由在同一區域的多個 AZ 中啟動執行個體，您可以保護應用程式免於發生單點故障情形。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`c1z7dfpz01`

警示條件

- 黃色：Amazon ECS 服務正在單一 AZ 中執行所有任務。
- 綠色：Amazon ECS 服務至少正在兩個不同的 AZ 中執行任務。

建議的動作

在不同的 AZ 中為服務至少再建立一個任務。

其他資源

Amazon ECS 容量和可用性

報告欄位

- Status
- 區域
- ECS 叢集名稱/ECS 服務名稱
- 可用區域的數量
- 上次更新時間

Amazon ECS Multi-AZ 放置策略

描述

檢查您的 Amazon ECS 服務是否使用以可用區域 (AZ) 為基礎的分散置放策略。此策略會以相同方式將工作分配到可用區域， AWS 區域 並協助保護您的應用程式不受單點故障影響。

對於作為 Amazon ECS 服務一部分來執行的任務，分散會是預設任務置放策略。

此檢查還會驗證分散是否為已啟用置放策略清單中的第一個策略或唯一策略。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`c1z7dfpz02`

警示條件

- 黃色：依可用區域分散已停用，或不是 Amazon ECS 服務已啟用置放策略清單中的第一個策略。

- 綠色：依可用區域分散是 Amazon ECS 服務已啟用置放策略清單中的第一個策略，或是唯一啟用的置放策略。

建議的動作

啟用分散任務置放策略，以便於多個 AZ 之間分佈任務。確認依可用區域分散是所有已啟用任務置放策略的第一個策略，或是唯一使用的策略。如果您選擇管理 AZ 置放，則可以在另一個 AZ 中使用鏡像服務來減輕這些風險。

其他資源

Amazon ECS 任務置放策略

報告欄位

- Status
- 區域
- ECS 叢集名稱/ECS 服務名稱
- 正確啟用並套用分散任務置放策略
- 上次更新時間

Amazon EFS 無掛載目標備援

描述

檢查 Amazon EFS 檔案系統的掛載目標是否於多個可用區域中存在。

可用區域是明顯與其他區域中的故障隔絕開來的地點。透過在 AWS 區域內的多個不同地理位置的可用區域中建立掛載目標，您可以為 Amazon EFS 檔案系統達到最高等級的可用性和耐久性。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c1dfprch01
```

警示條件

- 黃色：檔案系統在單一可用區域中建立了 1 個掛載目標。

綠色：檔案系統在多個可用區域中建立了 2 或多個掛載目標。

建議的動作

對於使用 One Zone 儲存類別的 EFS 檔案系統，建議您透過將備份還原至新檔案系統的方式來建立使用 Standard 儲存類別的新檔案系統。然後在多個可用區域中建立掛載目標。

對於使用標準儲存類別的 EFS 檔案系統，我們建議您在多個可用區域中建立掛載目標。

其他資源

- 使用 Amazon EFS 主控台管理掛載目標
- Amazon EFS 配額和限制

報告欄位

- Status
- 區域
- EFS 檔案系統 ID
- 掛載目標的數量
- AZ 數量
- 上次更新時間

Amazon EFS 不在 AWS Backup 計劃中

描述

檢查 Amazon EFS 檔案系統是否包含在備份計劃中 AWS Backup。

AWS Backup 是一種統一的備份服務，旨在簡化備份的建立、遷移、還原和刪除作業，同時提供更好的報告和稽核功能。

如需詳細資訊，請參閱備份您的 Amazon EFS 檔案系統。

檢查 ID

```
c18d2gz117
```

來源

```
AWS Config Managed Rule: EFS_IN_BACKUP_PLAN
```

警示條件

紅色：Amazon EFS 不包括在 AWS Backup 計劃中。

建議的動作

確保您的 Amazon EFS 檔案系統包含在您的 AWS Backup 計劃中，以防止意外的資料遺失或資料損毀。

其他資源

備份 Amazon EFS 檔案系統

Amazon EFS Backup 和還原使用 AWS Backup.

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

Amazon ElastiCache 異地同步備份叢集

描述

檢查是否在單一可用區域 (AZ) 中部署的 ElastiCache 叢集。如果 Multi-AZ 在叢集中處於非作用中狀態，則此檢查會提醒您。

多個 AZ 中的部署可透過非同步方式複寫至不同 AZ 中的唯讀複本來增強 ElastiCache 叢集可用性。進行計畫的叢集維護或主節點無法使用時， ElastiCache 會自動將複本提升為主節點。此容錯移轉允許繼續執行叢集寫入操作，而且不需要管理員介入。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

ECHdfsQ402

警示條件

- 綠色：Multi-AZ 在叢集中處於作用中狀態。
- 黃色：Multi-AZ 在叢集中處於非作用中狀態。

建議的動作

在與主碎片不同的可用區域中，為每個碎片至少建立一個複本。

其他資源

如需詳細資訊，請參閱使用異地同步備份 ElastiCache 的 Redis 最小化停機時間。

報告欄位

- Status
- 區域
- 叢集名稱
- 上次更新時間

Amazon ElastiCache Redis 集群自動 Backup

描述

檢查 Amazon ElastiCache for Redis 叢集是否已開啟自動備份，以及快照保留期限是否超過指定或 15 天預設限制。啟用自動備份後，每天都 ElastiCache 會建立叢集備份。

您可以使用規則的snapshotRetentionPeriod參數指定所需的快照保留限 AWS Config 制。

如需詳細資訊，請參閱 Redis 的 ElastiCache Backup 和還原。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

c18d2gz178

來源

AWS Config Managed Rule: elasticache-redis-cluster-automatic-backup-check

警示條件

紅色：Amazon ElastiCache for Redis 叢集未開啟自動備份，或快照保留期限低於限制。

建議的動作

請確定 Amazon ElastiCache for Redis 叢集已開啟自動備份，且快照保留期限超過指定或 15 天預設限制。自動備份可協助防止資料遺失。如果發生失敗，您可以建立新的叢集，從最新的備份還原您的資料。

如需詳細資訊，請參閱 Redis 的 ElastiCache Backup 和還原。

其他資源

如需詳細資訊，請參閱排程自動備份。

報告欄位

- Status
- 區域
- 叢集名稱
- 上次更新時間

Amazon MemoryDB Multi-AZ 叢集

描述

檢查是否有 MemoryDB 叢集部署在單一可用區域 (AZ) 中。如果 Multi-AZ 在叢集中處於非作用中狀態，則此檢查會提醒您。

在多可用區進行部署，可以非同步方式複寫至不同可用區域中的唯讀複本，從而增強 MemoryDB 叢集可用性。進行計畫的叢集維護或主節點無法使用時，MemoryDB 會自動將複本提升為主節點。此容錯移轉允許繼續執行叢集寫入操作，而且不需要管理員介入。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

MDBdfsQ401

警示條件

- 綠色：Multi-AZ 在叢集中處於作用中狀態。
- 黃色：Multi-AZ 在叢集中處於非作用中狀態。

建議的動作

在與主碎片不同的可用區域中，為每個碎片至少建立一個複本。

其他資源

如需詳細資訊，請參閱在 Minimizing downtime in MemoryDB with Multi-AZ (使用 Multi-AZ 將 MemoryDB 中的停機時間降至最低)。

報告欄位

- Status
- 區域
- 叢集名稱
- 上次更新時間

Amazon MSK 代理程式託管過多分割區

描述

檢查 Managed Streaming for Kafka (MSK) 叢集的代理程式沒有超過指派的建議分割區數量。

檢查 ID

Cmsvnj8vf1

警示條件

- 紅色：您的 MSK 代理程式已超過建議最大分割區限制的 100%
- 黃色：您的 MSK 已達到建議最大分割區限制的 80%

建議的動作

依照 MSK 建議的最佳實務來擴展 MSK 叢集或刪除任何未使用的分割區。

其他資源

- 調整您叢集的大小

報告欄位

- Status
- 區域
- 叢集 ARN
- 中介裝置 ID
- 分割區計數

具有少於三個資料節點的 Amazon OpenSearch 服務網域

描述

檢查 Amazon OpenSearch 服務網域是否設定至少有三個資料節點且 ZoneAwarenessEnabled 為真。 ZoneAwarenessEnabled 啟用後，Amazon Ser OpenSearch vice 可確保在不同的可用區域中分配每個主要碎片及其對應複本。

如需詳細資訊，請參閱在 Amazon OpenSearch 服務中設定異地同步備份網域。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz183
```

來源

```
AWS Config Managed Rule: opensearch-data-node-fault-tolerance
```

警示條件

黃色：Amazon OpenSearch 服務網域設定的資料節點少於三個。

建議的動作

確保 Amazon OpenSearch 服務網域設定至少有三個資料節點。設定異地同步備份網域，透過在同一區域內的三個可用區域中配置節點和複寫資料，以增強 Amazon Ser OpenSearch vice 叢集的可用性。如此可避免在發生節點和資料中心 (AZ) 故障的情況下造成資料遺失，且將停機時間降到最低。

如需詳細資訊，請參閱透過在三個可用區域部署來提高 Amazon OpenSearch 服務的可用性。

其他資源

- 透過在三個可用區域部署，提高 Amazon OpenSearch 服務的可用性

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

Amazon RDS 備份

描述

檢查 Amazon RDS 資料庫執行個體的自動備份。

備份功能預設為啟用，保留期間為一天。備份可降低意外資料遺失的風險，並允許 point-in-time復原。

檢查 ID

opQPADkZvH

警示條件

紅色：資料庫執行個體的備份保留期間設為 0 天。

建議的動作

根據應用程式的需求，將自動化資料庫執行個體備份的保留期間設為 1 到 35 天。請參閱使用自動備份。

其他資源

Amazon RDS 入門

報告欄位

- Status
- 區域/可用區域

- 資料庫執行個體
- VPC ID
- 備份保留期間

Amazon RDS 資料庫叢集有一個資料庫執行個體

描述

至少將另一個資料庫執行個體新增至資料庫叢集，以提高可用性和效能。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用 Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

`c1qf5bt011`

警示條件

黃色：資料庫叢集只有一個資料庫執行個體。

建議的動作

將讀取器資料庫執行個體新增至資料庫叢集。

其他資源

在目前的組態中，一個資料庫執行個體同時用於讀取和寫入作業。您可以新增另一個資料庫執行個體，以允許讀取重新分配和容錯移轉選項。

如需詳細資訊，請參閱 Amazon Aurora 的高可用性。

報告欄位

- Status
- 區域
- 資源
- 引擎名稱
- 資料庫執行個體類別
- 上次更新時間

具有所有執行個體位於相同可用區域的 Amazon RDS 資料庫叢集

描述

資料庫叢集目前位於單一可用區域中。使用多個可用區域來提高可用性。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用 Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

```
c1qf5bt007
```

警示條件

黃色：資料庫叢集的所有執行個體都位於相同的可用區域中。

建議的動作

將資料庫執行個體新增至資料庫叢集中的多個可用區域。

其他資源

建議您將資料庫執行個體新增至資料庫叢集中的多個可用區域。將資料庫執行個體新增至多個可用區域，可改善資料庫叢集的可用性。

如需詳細資訊，請參閱 Amazon Aurora 的高可用性。

報告欄位

- Status
- 區域
- 資源
- 引擎名稱
- 上次更新時間

Amazon RDS 資料庫叢集，所有讀取器執行個體都位於相同可用區域

描述

在您的資料庫叢集之中，所有讀取器執行個體都位於相同的可用區域。建議您將 Reader 執行個體散佈到資料庫叢集中的多個可用區域。

散發可增加資料庫的可用性，並藉由減少用戶端與資料庫之間的網路延遲來改善回應時間。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用 Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。

如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

`c1qf5bt018`

警示條件

紅色：資料庫叢集的讀取器執行個體位於相同的可用區域。

建議的動作

將讀取器執行個體散佈到多個可用區域。

其他資源

可用區域 (AZ) 是彼此不同的位置，以便在每個區域內發生中斷時提供隔離。 AWS 建議您將資料庫叢集中的主要執行個體和讀取器執行個體分配到多個 AZ，以提高資料庫叢集的可用性。您可以在建立叢集時使用 AWS Management Console AWS CLI、或 Amazon RDS API 建立異地同步備份叢集。您可以透過新增讀取器執行個體並指定不同的 AZ，將現有的 Aurora 叢集修改為異地同步備份叢集。

如需詳細資訊，請參閱 Amazon Aurora 的高可用性。

報告欄位

- Status
- 區域
- 資源
- 引擎名稱
- 上次更新時間

未啟用 Amazon RDS 資料庫執行個體增強型監控

描述

檢查是否已啟用 Amazon RDS 資料庫執行個體增強型監控。

Amazon RDS 增強型監控會即時提供執行資料庫執行個體在其上執行之作業系統 (OS) 的指標。您可以在 Amazon RDS 主控台上檢視 Amazon RDS 資料庫執行個體的所有系統指標和處理資訊。此

外，您還可以自訂儀表板。透過增強型監控，您幾乎可以即時掌握 Amazon RDS 執行個體操作狀態，讓您更快回應操作問題。

您可以使用規則的 monitoringInterval 參數來指定所需的 AWS Config 監視間隔。

如需詳細資訊，請參閱增強型監視概觀和增強型監控中的 OS 指標。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz158
```

來源

```
AWS Config Managed Rule: rds-enhanced-monitoring-enabled
```

警示條件

黃色：您的 Amazon RDS 資料庫執行個體未啟用增強型監控，或未設定所需的時間間隔。

建議的動作

為 Amazon RDS 資料庫執行個體啟用增強型監控功能，藉此改善 Amazon RDS 執行個體操作狀態的可見性。

如需詳細資訊，請參閱使用增強型監控來監控 OS 指標。

其他資源

增強型監控中的作業系統指標

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數

- 上次更新時間

Amazon RDS 資料庫執行個體已關閉儲存自動調度資源

描述

您的資料庫執行個體尚未開啟 Amazon RDS 儲存自動調度資源功能。當資料庫工作負載增加時，RDS 儲存區自動調度資源會自動擴展儲存容量，且無停機時間。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用 Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

`c1qf5bt013`

警示條件

紅色：資料庫執行個體未開啟儲存自動調度資源功能。

建議的動作

使用指定的最大儲存臨界值開啟 Amazon RDS 儲存自動調度資源。

其他資源

當資料庫工作負載增加時，Amazon RDS 儲存自動擴展儲存容量，而不會停機。儲存自動調度資源可監控儲存使用情況，並在使用量接近佈建的儲存容量時自動擴展容量。您可以指定 Amazon RDS 可分配給資料庫執行個體的儲存上限。儲存自動調度資源不會產生額外費用。您只需為配置給資料庫執行個體的 Amazon RDS 資源付費。我們建議您開啟 Amazon RDS 儲存自動調度資源功能。

如需詳細資訊，請參閱使用 Amazon RDS 儲存體自動調整規模自動管理容量。

報告欄位

- Status
- 區域
- 資源
- 建議值
- 引擎名稱
- 上次更新時間

不使用異地同步備份部署的 Amazon RDS 資料庫執行

描述

建議您使用多可用區部署。多可用區部署可增強資料庫執行個體的可用性和耐久性。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用 Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

```
c1qf5bt019
```

警示條件

黃色：資料庫執行個體未使用異地同步備份部署。

建議的動作

為受影響的資料庫執行個體設定異地同步備份。

其他資源

在 Amazon RDS 異地同步備份部署中，Amazon RDS 會自動建立主資料庫執行個體，並將資料複寫到不同可用區域中的執行個體。當它偵測到故障時，Amazon RDS 會自動容錯移轉到備用執行個體，無需手動介入。

如需詳細資訊，請參閱 定價。

報告欄位

- Status
- 區域
- 資源
- 引擎名稱
- 上次更新時間

Amazon RDS DiskQueueDepth

描述

檢查 CloudWatch 測量結果是否 DiskQueueDepth 顯示 RDS 執行處理資料庫儲存體的佇列寫入次數是否已增加到建議進行作業調查的層次。

檢查 ID

`Cmsvnj8db3`

警示條件

- 紅色： DiskQueueDepth CloudWatch 量度已超過 10
- 黃色： DiskQueueDepth CloudWatch 量度大於 5 但小於或等於 10
- 綠色: DiskQueueDepth CloudWatch 量度小於或等於 5

建議的動作

請考慮移至支援讀取/寫入特性的執行個體和儲存磁碟區。

報告欄位

- Status

- 區域
- 資料庫執行個體 ARN
- DiskQueueDepth 公制

Amazon RDS FreeStorageSpace

描述

檢查 RDS 資料庫執行個體的 FreeStorageSpace CloudWatch 指標是否已增加超過作業上合理的臨界值。

檢查 ID

`Cmsvnj8db2`

警示條件

- 紅色： FreeStorageSpace 已達/超過總容量的 90%
- 黃色：介 FreeStorageSpace 於總容量的 80% 至 90% 之間
- 綠色：小 FreeStorageSpace 於總容量的 80%

建議的動作

使用 Amazon RDS 管理主控台、Amazon RDS API 或 AWS 命令列界面，為可用儲存空間不足的 RDS 資料庫執行個體擴展儲存空間。

報告欄位

- Status
- 區域
- 資料庫執行個體 ARN
- FreeStorageSpace 公制 (MB)
- 資料庫執行個體分配的儲存空間 (MB)
- 資料庫執行個體儲存空間用量百分比

Amazon RDS 日誌輸出參數設置為表

描述

當 log_output 被設置為表時，比 log_output 被設置為文件時使用更多的存儲空間。建議您將參數設定為 FILE，以避免達到儲存區大小限制。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用 Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

`c1qf5bt023`

警示條件

黃色：資料庫參數群組的日誌輸出參數設定為表格。

建議的動作

在資料庫參數群組中將 log_output 參數值設定為「檔案」。

其他資源

如需詳細資訊，請參閱 MySQL 資料庫記錄檔。

報告欄位

- Status
- 區域
- 資源
- 參數名稱
- 建議值
- 上次更新時間

Amazon RDS 默認 _ 行格式參數設置不安全

描述

您的資料庫執行個體遇到一個已知問題：當索引超過 7 67 個位元組時，資料庫執行個體在 MySQL 版本低於 8.0.26 的情況下建立的資料表無法存取且無法復原。

我們建議您將 「預設 _ 格式」參數值設定為「動態」。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用 Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

```
c1qf5bt036
```

警示條件

紅色：資料庫參數群組對於 Innodb_default_row_ format 參數有不安全的設定。

建議的動作

將 「預設 _ 列格式」參數設定為「動態」。

其他資源

當使用 MySQL 版本低於 8.0.26 且 ROW_format 設置為緊湊或冗餘創建表時，不會強制使用 key prefix 短於 767 字節創建索引。資料庫重新啟動之後，就無法存取或復原這些資料表。

如需詳細資訊，請參閱 MySQL 文件網站上的 MySQL 變更。

報告欄位

- Status
- 區域
- 資源
- 參數名稱
- 建議值
- 上次更新時間

Amazon RDS 信息 _ 刷新 _ 日誌 _ 提交參數不是 1

描述

資料庫執行個體的 In nodb_flush_log_at_trx_ commit 參數的值不是安全值。此參數控制提交操作至磁碟的持續性。

我們建議您將 Innodb_Flush_log_at_trx_commit 參數設定為 1。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用 Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

```
c1qf5bt030
```

警示條件

黃色：資料庫參數群組的資料庫參數群組已設定為 1 以外的設定。

建議的動作

設置知識庫 _ 刷新 _ 日誌 _ 提交參數值為 1

其他資源

將記錄緩衝區儲存至耐久性儲存時，資料庫交易是持久性的。但是，儲存到磁碟會影響效能。根據針對 Innodb_flush_log_at_trx_commit 參數設定的值而定，記錄檔寫入和儲存到磁碟的行為可能會有所不同。

- 當參數值為 1 時，記錄會在每次認可的交易之後寫入並儲存到磁碟中。
- 當參數值為 0 時，記錄檔會每秒寫入一次並儲存到磁碟。
- 當參數值為 2 時，會在認可每個交易後寫入記錄檔，並每秒儲存一次至磁碟。數據從 InnoDB 存儲器緩衝區移動到操作系統的緩存，這也是在存儲器中。

> **Note**
>
> 當參數值不是 1 時，InnoDB 不保證 ACID 屬性。數據庫崩潰時，最近的交易可能會丟失最後一秒鐘。

如需詳細資訊，請參閱設定適用於 Amazon RDS for MySQL 參數的最佳實務，第 1 部分：與效能相關的參數。

報告欄位

- Status
- 區域
- 資源
- 參數名稱
- 建議值
- 上次更新時間

Amazon RDS 最大用戶 _ 連接參數很低

描述

針對每個資料庫帳戶能同時連線的數量上限，您的資料庫執行個體設定值很低。

我們建議將 max_user_connect 參數設定為大於 5 的數字。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用 Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

`c1qf5bt034`

警示條件

黃色：資料庫參數群組的 max_user_連接設定錯誤。

建議的動作

將最大值使用者 _ 連接參數的值增加到大於 5 的數字。

其他資源

max_user_ connect 設定可控制 MySQL 使用者帳戶允許的同時連線數目上限。達到此連線限制會導致 Amazon RDS 執行個體管理操作失敗，例如備份、修補和參數變更。

如需詳細資訊，請參閱 MySQL 文件網站上的設定帳號資源限制。

報告欄位

- Status

- 區域
- 資源
- 參數名稱
- 建議值
- 上次更新時間

Amazon RDS Multi-AZ

描述

檢查是否有資料庫執行個體部署在單一可用區域 (AZ) 中。

Multi-AZ 部署會同步複寫至不同可用區域中的備用執行個體，以增強資料庫的可用性。在規劃的資料庫維護期間，或在資料庫執行個體或可用區域故障期間，Amazon RDS 會自動容錯移轉到備用執行個體。此容錯移轉可讓資料庫作業快速恢復，無需系統管理介入。由於 Amazon RDS 不支援適用於 Microsoft SQL 伺服器的 Multi-AZ 部署，因此這項檢查不會對 SQL 伺服器執行個體進行檢查。

檢查 ID

`f2iK5R6Dep`

警示條件

黃色：資料庫執行個體部署在單一可用區域。

建議的動作

如果您的應用程式需要高可用性，請修改資料庫執行個體以啟用 Multi-AZ 部署。請參閱高可用性 (Multi-AZ)。

其他資源

區域與可用區域

報告欄位

- Status
- 區域/可用區域
- 資料庫執行個體
- VPC ID
- Multi-AZ

Amazon RDS 不在 AWS Backup 計劃中

描述

檢查您的 Amazon RDS 資料庫執行個體是否包含在 AWS Backup的備份計畫中。

AWS Backup 這是一項全受管備份服務，可讓您輕鬆集中管理並自動化跨 AWS 服務備份資料。

在備份計畫中包含 Amazon RDS 資料庫執行個體對於監管法規遵循義務、災難復原、資料保護的業務政策和業務持續性目標而言非常重要。

如需詳細資訊，請參閱什麼是 AWS Backup？。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz159
```

來源

```
AWS Config Managed Rule: rds-in-backup-plan
```

警示條件

黃色：使用的備份計劃不包含 Amazon RDS 資料庫執行個體 AWS Backup。

建議的動作

將您的 Amazon RDS 資料庫執行個體包含在備份計劃中 AWS Backup。

如需詳細資訊，請參閱使用 AWS Backup 進行 Amazon RDS 備份和還原。

其他資源

指派資源至備份計畫

報告欄位

- Status
- 區域

- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

Amazon RDS 僅供讀取複本以可寫入模式開啟

描述

您的資料庫執行個體具有可寫入模式的僅供讀取複本，可從用戶端進行更新。

我們建議您將 read_only 參數設定為，TrueIfReplica以便僅供讀取複本不處於可寫入模式。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用 Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

`c1qf5bt035`

警示條件

黃色：資料庫參數群組為僅供讀取複本開啟可寫入模式。

建議的動作

將只讀參數值設定為。TrueIfReplica

其他資源

read_only 參數控制從用戶端到資料庫執行個體的寫入權限。此參數的預設值為 TrueIfReplica。對於複本執行個體，請將 read_only 值TrueIfReplica設定為 ON (1)，並停用來自用戶端的任何寫入活動。對於主/寫入器執行個體，請將值TrueIfReplica設定為 OFF (0)，並啟用來自用戶端執行個體的寫入活動。以可寫入模式開啟僅供讀取複本時，儲存在此執行個體中的資料可能會與主要執行個體不同，導致複寫錯誤。

如需詳細資訊，請參閱設定適用於 MySQL 的 Amazon RDS 參數的最佳實務，第 2 部分：MySQL 文件網站上與複寫相關的參數。

報告欄位

- Status
- 區域
- 資源
- 參數名稱
- 建議值
- 上次更新時間

Amazon RDS 資源自動備份已關閉

描述

數據庫資源上的自動備份已禁用。自動備份可讓您 point-in-time 復原資料庫執行個體。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用 Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。

如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

`c1qf5bt001`

警示條件

紅色：Amazon RDS 資源沒有開啟自動備份

建議的動作

開啟保留期最多 14 天的自動備份。

其他資源

自動備份可讓您 point-in-time 復原資料庫執行個體。我們建議您開啟自動備份。當您為資料庫執行個體開啟自動備份時，Amazon RDS 會在您偏好的備份時段期間，每天自動執行資料的完整備份。備份會在資料庫內容有更新時擷取交易記錄。您可以獲得高達資料庫執行個體儲存大小的備份儲存體，無需額外費用。

如需詳細資訊，請參閱下列資源：

- 啟用自動備份
- 揭開 Amazon RDS 備份儲存成本的神秘面紗

報告欄位

- Status
- 區域
- 資源
- 建議值
- 引擎名稱
- 上次更新時間

Amazon RDS 同步記錄參數已關閉

描述

在資料庫執行個體中確認交易確認之前，不會強制執行二進位記錄到磁碟的同步處理。

我們建議您將 sync_binlog 參數值設定為 1。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用 Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

`c1qf5bt031`

警示條件

黃色：資料庫參數群組已關閉同步二進位記錄。

建議的動作

將同步處理參數設定為 1。

其他資源

sync_binlog 參數可控制 MySQL 將二進位記錄檔推送至磁碟的方式。當此參數的值設為 1 時，它會在認可交易之前開啟磁碟的二進位記錄同步處理。當此參數的值設定為 0 時，會關閉磁碟的二進位記錄同步處理。通常情況下，MySQL 服務器依賴於操作系統將二進制日誌定期推送到磁盤類似於其他文件。將 sync_binlog 參數值設定為 0 可以增強效能。不過，在電源故障或作業系統當機期間，伺服器會遺失所有未同步處理至二進位記錄的已認可交易。

如需詳細資訊，請參閱設定適用於 Amazon RDS for MySQL 參數的最佳實務，第 2 部分：與複寫相關的參數。

報告欄位

- Status

- 區域
- 資源
- 參數名稱
- 建議值
- 上次更新時間

RDS 資料庫叢集未啟用 Multi-AZ 複寫

描述

檢查您的 Amazon RDS 資料庫叢集是否已啟用 Multi-AZ 複寫。

Multi-AZ 資料庫叢集在三個不同的可用區域中有一個寫入器資料庫執行個體和兩個讀取器資料庫。Multi-AZ 資料庫叢集相較於 Multi-AZ 部署，可提供高可用性、增加讀取工作負載的容量以及更低的延遲。

如需詳細資訊，請參閱建立 Multi-AZ 資料庫叢集。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz161
```

來源

```
AWS Config Managed Rule: rds-cluster-multi-az-enabled
```

警示條件

黃色：您的 Amazon RDS 資料庫叢集未設定 Multi-AZ 複寫

建議的動作

在建立 Amazon RDS 資料庫叢集時，開啟 Multi-AZ 資料庫叢集部署。

如需詳細資訊，請參閱建立 Multi-AZ 資料庫叢集。

其他資源

Multi-AZ 資料庫叢集部署

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

未啟用 RDS Multi-AZ 備用執行個體

描述

檢查 Amazon RDS 資料庫執行個體是否已設定 Multi-AZ 備用複本。

Amazon RDS Multi-AZ 會將資料複寫到不同可用區域中的備用複本，為資料庫執行個體提供高可用區域和耐用性。如此可提供自動容錯移轉、改善效能並增強資料耐久性。在 Multi-AZ 資料庫執行個體部署中，Amazon RDS 會自動佈建，並在不同的可用區域中維持同步待命複本。主要資料庫執行個體會跨可用區域，同步複寫到待命複本，提供資料備援並且降低系統備份時的延遲遽增發生等功能。執行具有高可用性的資料庫執行個體，可在規劃好的系統維護期間增強可用性。它還有助於在資料庫執行個體失敗和可用區域中斷時保護資料庫。

如需詳細資訊，請參閱 Multi-AZ 資料庫執行個體部署。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

c18d2gz156

來源

AWS Config Managed Rule: rds-multi-az-support

警示條件

黃色：Amazon RDS 資料庫執行個體未設定 Multi-AZ 複本。

建議的動作

在建立 Amazon RDS 資料庫執行個體時，開啟 Multi-AZ 部署。

此檢查無法從 Trusted Advisor 主控台的檢視中排除。

其他資源

Multi-AZ 資料庫執行個體部署

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

Amazon RDS ReplicaLag

描述

檢查 RDS 資料庫執行個體的 ReplicaLag CloudWatch 指標是否在過去一週增加超過操作上合理的臨界值。

ReplicaLag 指標測量僅供讀取複本落後於主要執行個體的秒數。當對僅供讀取複本進行的非同步更新無法跟上主要資料庫執行個體上發生的更新時，就會發生複寫延遲。如果主執行個體發生故障，如果超過操作上合理的閾 ReplicaLag 值，則僅供讀取複本中可能會遺失資料。

檢查 ID

Cmsvnj8db1

警示條件

- 紅色： ReplicaLag 量度在一週內至少超過 60 秒一次。

- 黃色： ReplicaLag 量度在一週內至少超過 10 秒一次。
- 綠色： ReplicaLag 小於 10 秒。

建議的動作

有幾個可能的原因導致增 ReplicaLag 加超出操作安全水平。例如，這可能是因為最近從舊版備份取代/啟動的複本執行個體，以及這些複本需要大量時間才能「catch-up」主要資料庫執行個體和即時交易所導致。隨著 catch 的發生，這 ReplicaLag 可能會隨著時間的推移而減少。另一個範例可能是：主要資料庫執行個體上能夠達到的交易速度，高於複寫處理或複本基礎結構能趕上的速度。隨著複寫無法跟上主要資料庫效能的速度，這 ReplicaLag 可能會隨著時間的推移而增加。最後，工作量可能會在一天/月/等的不同時期突發，導致偶爾 ReplicaLag 落後。您的小組應該調查哪些可能的根本原因導致資料庫高 ReplicaLag ，並可能變更資料庫執行個體類型或工作負載的其他特性，以確保複本上的資料連續性符合您的需求。

其他資源

- 使用 Amazon RDS for PostgreSQL 的僅供讀取複本
- 在 Amazon RDS 中使用 MySQL 複寫
- 使用 MySQL 僅供讀取複本

報告欄位

- Status
- 區域
- 資料庫執行個體 ARN
- ReplicaLag 公制

Amazon RDS 同步提交參數已關閉

描述

當同步提交參數關閉時，資料庫損毀時可能會遺失資料。資料庫的耐久性存在風險。

我們建議您打開同步 _ 提交參數。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用 Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

`c1qf5bt026`

警示條件

紅色：資料庫參數群組已關閉同步 _ 提交參數。

建議的動作

開啟資料庫參數群組中的同步提交參數。

其他資源

synchronized ous_commit 參數會定義資料庫伺服器傳送成功通知給用戶端之前的預寫記錄 (WAL) 處理程序完成。此提交被稱為異步提交，因為客戶端在 WAL 將事務保存在磁盤之前確認提交。如果已關閉 ynchronous_commit 參數，則交易可能會遺失、資料庫執行個體耐久性可能會受到影響，而且資料庫當機時可能會遺失資料。

如需詳細資訊，請參閱 MySQL 資料庫記錄檔。

報告欄位

- Status
- 區域
- 資源
- 參數名稱
- 建議值
- 上次更新時間

Amazon Redshift 叢集自動快照

描述

檢查您的 Amazon Redshift 叢集是否已啟用自動化快照。

Amazon Redshift 會自動取得增量快照，以追蹤自上一個自動快照以來對叢集的變更。自動快照會保留所有需要的資料以從快照還原叢集。若要停用自動快照，請將保留期間設定為 zero (零)。您無法停用 RA3 節點類型的自動快照。

您可以使用 AWS Config 規則的 and MaxRetentionPeriod參數來指定所需的最短MinRetentionPeriod和最長保留期。

Amazon Redshift 快照和備份

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz135
```

來源

```
AWS Config Managed Rule: redshift-backup-enabled
```

警示條件

紅色：Amazon Redshift 並未在所需的保留期間內設定自動快照。

建議的動作

確定您的 Amazon Redshift 叢集已啟用自動化快照。

如需詳細資訊，請參閱使用主控台管理快照。

其他資源

Amazon Redshift 快照和備份

如需詳細資訊，請參閱使用備份。

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

Amazon Route 53 已刪除運作狀態檢查

描述

檢查是否有資源記錄集與已刪除的運作狀態檢查相關聯。

Route 53 不會阻止您刪除與一或多個資源記錄集相關聯的運作狀態檢查。如果您刪除運作狀態檢查而沒有更新相關聯的資源記錄集，DNS 備援組態的 DNS 查詢路由將無法如預期運作。

由 AWS 服務建立的託管區域不會顯示在您的檢查結果中。

檢查 ID

Cb877eB72b

警示條件

黃色：資源記錄集與已刪除的運作狀態檢查相關聯。

建議的動作

建立新的運作狀態檢查，並將其與資源記錄集建立關聯。請參閱建立、更新和刪除運作狀態檢查和將運作狀態檢查新增到資源記錄集。

其他資源

- Amazon Route 53 運作狀態檢查和 DNS 備援
- 簡單 Amazon Route 53 組態中運作狀態檢查的運作方式

報告欄位

- 託管區域名稱

- 託管區域 ID
- 資源記錄集名稱
- 資源記錄集類型
- 資源記錄集識別碼

Amazon Route 53 容錯移轉資源記錄集

描述

檢查是否有 Amazon Route 53 容錯移轉資源記錄集設定錯誤。

Amazon Route 53 運作狀態檢查判斷主要資源運作狀況不良時，Amazon Route 53 會以次要備份資源記錄集回應查詢。您必須建立正確設定的主要和次要資源記錄集，容錯移轉才能運作。

由 AWS 服務建立的託管區域不會顯示在您的檢查結果中。

檢查 ID

`b73EEdD790`

警示條件

- 黃色：主要容錯移轉資源記錄集沒有對應的次要資源記錄集。
- 黃色：次要容錯移轉資源記錄集沒有對應的主要資源記錄集。
- 黃色：具有相同名稱的主要與次要資源記錄集與相同的運作狀態檢查相關聯。

建議的動作

如果遺失容錯移轉資源集，請建立對應的資源記錄集。請參閱建立容錯移轉資源記錄集。

如果您的資源記錄集與相同的運作狀態檢查相關聯，請為每個記錄集建立個別的運作狀態檢查。請參閱建立、更新和刪除運作狀態檢查。

其他資源

Amazon Route 53 運作狀態檢查和 DNS 備援

報告欄位

- 託管區域名稱
- 託管區域 ID
- 資源記錄集名稱

- 資源記錄集類型
- 原因

Amazon Route 53 高 TTL 資源記錄集

描述

檢查資源記錄集是否有較低的 time-to-live (TTL) 值。

TTL 是 DNS 解析器快取資源記錄集的秒數。指定長 TTL 時，DNS 解析器需要花較長的時間請求更新的 DNS 記錄，這可能會導致重新路由傳輸造成的不必要延遲。例如，長 TTL 會在 DNS 備援偵測到端點故障，以及透過重新路由流量進行回應的過程之間產生延遲。

由 AWS 服務建立的託管區域不會顯示在您的檢查結果中。

檢查 ID

`C056F80cR3`

警示條件

- 黃色：路由政策為容錯移轉的資源記錄集的 TTL 大於 60 秒。
- 黃色：具有關聯運作狀態檢查的資源記錄集的 TTL 大於 60 秒。

建議的動作

針對列出的資源記錄集，輸入 60 秒的 TTL 值。如需詳細資訊，請參閱使用資源記錄集。

其他資源

Amazon Route 53 運作狀態檢查和 DNS 備援

報告欄位

- Status
- 託管區域名稱
- 託管區域 ID
- 資源記錄集名稱
- 資源記錄集類型
- 資源記錄集 ID
- TTL

Amazon Route 53 名稱伺服器委派

描述

檢查您的網域註冊商或 DNS 針對哪個 Amazon Route 53 託管區域沒有使用正確的 Route 53 名稱伺服器。

建立託管區域時，Route 53 會指派一組四個名稱伺服器。這些伺服器的名稱包括 ns-###.awsdns-##.com、.net、.org 和 .co.uk，其中 ### 和 ## 通常代表不同的數字。您必須先更新註冊商的名稱伺服器組態，移除註冊商指派的名稱伺服器，Route 53 才能路由您網域的 DNS 查詢。接下來，您必須在 Route 53 委派集中新增全部四個名稱伺服器。為了提供最高的可用性，您必須新增全部四個 Route 53 名稱伺服器。

由 AWS 服務建立的託管區域不會顯示在您的檢查結果中。

檢查 ID

`cF171Db240`

警示條件

黃色：託管區域中您網域的註冊商未使用委派集中全部四個 Route 53 名稱伺服器。

建議的動作

使用您的註冊商或網域目前的 DNS 服務新增或更新名稱伺服器記錄，以包含 Route 53 委派集中的全部四個名稱伺服器。若要尋找這些值，請參閱取得託管區域的名稱伺服器。如需有關新增或更新名稱伺服器記錄的詳細資訊，請參閱建立和遷移網域與子網域至 Amazon Route 53。

其他資源

使用託管區域

報告欄位

- 託管區域名稱
- 託管區域 ID
- 已使用的委派名稱伺服器數量

Amazon Route 53 Resolver 端點可用區域備援

描述

檢查您的服務組態是否具有在至少兩個可用區域 (AZ) 中指定的 IP 地址以供備援之用。AZ 是明顯與其他區域中的故障隔絕開來的地點。藉由在同一區域的多個 AZ 中指定 IP 地址，您可以保護應用程式免於發生單點故障情形。

檢查 ID

`Chrv231ch1`

警示條件

- 黃色：IP 地址僅在一個 AZ 中指定
- 綠色：至少在兩個 AZ 中指定了 IP 地址

建議的動作

在至少兩個可用區域中指定 IP 地址以進行備援。

其他資源

- 如果您需要多個始終可用的彈性網路介面端點，建議您至少建立一個超過所需的網路介面，以確保有額外的容量可用於處理可能的流量激增。額外的網路介面也可確保維護或升級等維修作業期間的可用性。
- Resolver 端點的高可用性

報告欄位

- Status
- 區域
- 資源 ARN
- AZ 數量

Simple Storage Service (Amazon S3) 儲存貯體記錄

描述

檢查 Amazon Simple Storage Service (Amazon S3) 儲存貯體的記錄組態。

啟用伺服器存取記錄功能時，每小時都會將詳細的存取日誌傳送至您選擇的儲存貯體。存取日誌記錄包含每個請求的詳細資訊，例如請求類型、請求中指定的資源，以及處理請求的時間與日期。儲

存貯體金鑰預設為未啟用。如果您想要執行安全稽核或進一步了解使用者和使用模式，請啟用記錄功能。

一開始啟用記錄功能時，系統會自動驗證組態。不過未來的修改可能會導致記錄失敗。這項檢查會檢查明確的 Amazon S3 儲存貯體許可，但不會檢查可能覆寫儲存貯體許可的相關聯儲存貯體政策。

檢查 ID

BueAdJ7NrP

警示條件

- 黃色：儲存貯體未啟用伺服器存取記錄。
- 黃色：目標儲存貯體權限不包含根帳戶，因此 Trusted Advisor 無法檢查它。
- 紅色：目標儲存貯體不存在。
- 紅色：目標儲存貯體和來源儲存貯體擁有者不同。
- 紅色：日誌交付者沒有目標儲存貯體的寫入許可。

建議的動作

為大多數儲存貯體啟用儲存貯體記錄功能。請參閱使用主控台啟用記錄和以程式設計方式啟用記錄。

如果目標值區權限不包含根帳戶，而您想 Trusted Advisor 要檢查記錄狀態，請將根帳戶新增為受權者。請參閱編輯儲存貯體許可。

如果目標儲存貯體不存在，請選取現有儲存貯體作為目標儲存貯體，或建立新儲存貯體然後加以選取。請參閱管理儲存貯體記錄。

如果目標和來源儲存貯體的擁有者不同，請將目標儲存貯體變更為與來源儲存貯體有相同擁有者的儲存貯體。請參閱管理儲存貯體記錄。

如果日誌交付者沒有目標儲存貯體的寫入許可 (未啟用寫入)，請將上傳/刪除許可授予給日誌交付群組。請參閱編輯儲存貯體許可。

其他資源

- 使用儲存貯體
- 伺服器存取記錄
- 伺服器存取日誌格式

- 刪除日誌檔案

報告欄位

- Status
- 區域
- 儲存貯體名稱
- 目標名稱
- 目標已存在
- 相同擁有者
- 已啟用寫入
- 原因

未啟用 Amazon S3 儲存貯體複寫

描述

檢查您的跨區域複寫、相同區域複寫或兩者是否均已啟用 Amazon S3 儲存貯體複寫規則。

複製是在相同或不同區域中跨值 AWS 區域的物件自動非同步複製。複寫會將來源儲存貯體中新建立的物件和物件更新複製至目的地儲存貯體。使用 Amazon S3 儲存貯體複寫來協助改善應用程式和資料儲存的彈性與法規遵循。

如需詳細資訊，請參閱複製物件。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz119
```

來源

```
AWS Config Managed Rule: s3-bucket-replication-enabled
```

警示條件

黃色：跨區域複寫、相同區域複寫或兩者皆未啟用 Amazon S3 儲存貯體複寫規則。

建議的動作

開啟 Amazon S3 儲存貯體複寫規則來改善應用程式和資料儲存的彈性與法規遵循。

如需詳細資訊，請參閱檢視備份工作和復原點及設定複寫。

其他資源

逐步解說：設定複寫的範例

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

Amazon S3 Bucket Versioning

描述

檢查是否有 Amazon Simple Storage Service 儲存貯體未啟用或已暫停版本控制功能。

啟用版本控制功能時，您可以輕鬆復原失誤的使用者動作和應用程式故障。版本控制功能可用來保留、擷取和恢復儲存貯體中所存放任何物件的任何版本。透過自動將物件封存至 Glacier 儲存類別，您可以使用生命週期規則來管理物件的所有版本及其相關成本。您也可以設定規則，在指定的期間過後移除物件的版本。您也可以針對儲存貯體的任何物件刪除或組態變更，要求使用多重要素驗證 (MFA)。

啟用版本控制功能後無法停用。但是可以暫停此功能，防止建立物件的新版本。使用版本控制功能可能會增加 Simple Storage Service (Amazon S3) 的成本，因為您需為同一個物件支付多個版本的儲存費用。

檢查 ID

```
R365s2Qddf
```

警示條件

- 綠色：啟用儲存貯體中的版本控制。
- 黃色：未啟用儲存貯體的版本控制。
- 黃色：已暫停儲存貯體的版本控制。

建議的動作

在大多數儲存貯體上啟用儲存貯體版本控制，防止意外刪除或覆寫。請參閱使用版本控制和以程式設計方式啟用版本控制。

如果已暫停儲存貯體版本控制，請考慮重新啟用版本控制。如需有關使用暫停版本控制之儲存貯體中的物件的詳細資訊，請參閱管理暫停版本控制之儲存貯體中的物件。

啟用或暫停版本控制後，您可以定義生命週期組態規則，將某些物件版本標記為過期，或永久移除不需要的物件版本。如需詳細資訊，請參閱物件生命週期管理。

變更儲存貯體的版本控制狀態或刪除物件版本時，MFA Delete 需要進行額外的驗證。這會要求使用者輸入憑證和經批准的驗證裝置提供的代碼。如需詳細資訊，請參閱 MFA Delete。

其他資源

使用儲存貯體

報告欄位

- Status
- 區域
- 儲存貯體名稱
- 版本控制
- MFA Delete 已啟用

應用程式、網路及閘道負載平衡器未跨多個可用區域

描述

檢查您的負載平衡器 (應用程式、網路和閘道負載平衡器) 是否設定了跨多個可用區域的子網路。

您可以在 AWS Config 規則的minAvailabilityZones參數中指定所需的最小可用區域。

如需詳細資訊，請參閱 Application Load Balancer 的可用區域、可用區域 - Network Load Balancer，以及建立 Gateway Load Balancer。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`c18d2gz169`

來源

`AWS Config Managed Rule: elbv2-multiple-az`

警示條件

黃色：在少於兩個可用區域中設定子網路的應用程式、網路或閘道負載平衡器。

建議的動作

使用跨多個可用區域的子網路來設定您的應用程式、網路和閘道負載平衡器。

其他資源

Application Load Balancer 的可用區域

可用區域 (Elastic Load Balancing)

建立 Gateway Load Balancer

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

Auto Scaling 在子網路中的可用 IP

描述

檢查目標子網路中是否仍有足夠的可用 IP。當 Auto Scaling 群組達到其大小上限且需要啟動其他執行個體時，有足夠的 IP 可供使用會很有幫助。

檢查 ID

Cjxm268ch1

警示條件

- 紅色：ASG 可建立的執行個體和 IP 地址數量上限超過所設定之子網路中剩餘的 IP 地址數量。
- 綠色：有足夠的 IP 地址可供 ASG 中的剩餘擴展使用。

建議的動作

增加可用 IP 地址的數量

報告欄位

- Status
- 區域
- 資源 ARN
- 可建立的執行個體上限
- 可用執行個體的數量

Auto Scaling 群組運作狀態檢查

描述

檢查 Auto Scaling 群組的運作狀態檢查組態。

如果 Auto Scaling 群組使用 Elastic Load Balancing，建議的組態是啟用 Elastic Load Balancing 運作狀態檢查。如果沒有使用 Elastic Load Balancing 運作狀態檢查，則 Auto Scaling 只能在 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的運作狀態良好的情況下執行作業。Auto Scaling 不會對執行個體上執行的應用程式執行作業。

檢查 ID

CL0G40CD08

警示條件

- 黃色：Auto Scaling 群組具有相關聯的負載平衡器，但未啟用 Elastic Load Balancing 運作狀態檢查。
- 黃色：Auto Scaling 群組不具有相關聯的負載平衡器，但已啟用 Elastic Load Balancing 運作狀態檢查。

建議的動作

如果 Auto Scaling 群組具有相關的負載平衡器，但未啟用 Elastic Load Balancing 運作狀態檢查，請參閱將 Elastic Load Balancing 運作狀態檢查新增至您的 Auto Scaling 群組。

如果已啟用 Elastic Load Balancing 運作狀態檢查，但 Auto Scaling 群組沒有相關聯的負載平衡器，請參閱設定自動擴展和負載平衡應用程式。

其他資源

《Amazon EC2 Auto Scaling 使用者指南》

報告欄位

- Status
- 區域
- Auto Scaling 群組名稱
- 關聯的負載平衡器
- 運作狀態檢查

Auto Scaling 群組資源

描述

檢查與啟動組態和 Auto Scaling 群組相關聯資源的可用性。

若 Auto Scaling 群組指向無法使用的資源，便無法啟動新的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體。如果正確設定，Auto Scaling 可讓 Amazon EC2 執行個體的數量在需求尖峰期間順暢增加，並在需求低落期間自動減少。若 Auto Scaling 群組和啟動組態指向無法使用的資源，便無法如預期運作。

檢查 ID

```
8CNsSllI5v
```

警示條件

- 紅色：Auto Scaling 群組與已刪除的負載平衡器相關聯。
- 紅色：啟動組態與已刪除的 Amazon Machine Image (AMI) 相關聯。

建議的動作

如果負載平衡器已刪除，您可以建立新的負載平衡器或目標群組，然後將其關聯至 Auto Scaling 群組，或建立不帶負載平衡器的新 Auto Scaling 群組。如需有關建立帶新負載平衡器的新 Auto Scaling 群組的詳細資訊，請參閱設定自動擴展和負載平衡應用程式。如需有關建立不帶負載平衡器的新 Auto Scaling 群組的詳細資訊，請參閱 Auto Scaling 入門 (使用主控台) 中的「建立 Auto Scaling 群組」。

如果已刪除 AMI，請使用有效的 AMI 建立新的啟動範本或啟動範本版本，然後將其與 Auto Scaling 群組關聯。請參閱 Auto Scaling 入門 (使用主控台)中的「建立啟動組態」。

其他資源

- Auto Scaling 疑難排解：Amazon EC2 AMI
- Auto Scaling 疑難排解：負載平衡器組態
- 《Amazon EC2 Auto Scaling 使用者指南》

報告欄位

- Status
- 區域
- Auto Scaling 群組名稱
- 啟動類型
- 資源類型
- 資源名稱

在單一可用區域中執行 HSM 執行個體的AWS CloudHSM 叢集

描述

檢查在單一可用區域 (AZ) 中執行的 HSM 執行個體的叢集。如果您的叢集存在沒有最新備份的風險，則此檢查會提醒您。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`hc0dfs7601`

警示條件

- 黃色：CloudHSM 叢集正在執行單一可用區域中的所有 HSM 執行個體超過 1 小時。
- 綠色：CloudHSM 叢集正在執行至少兩個不同的可用區域中的所有 HSM 執行個體。

建議的動作

在不同的可用區域中為叢集至少再建立一個執行個體。

其他資源

的最佳做法 AWS CloudHSM

報告欄位

- Status
- 區域
- 叢集 ID
- HSM 執行個體的數量
- 上次更新時間

AWS Direct Connect 連線備援

描述

檢查 AWS 區域 是否只有一個 AWS Direct Connect 連接。與 AWS 資源的連線應始終設定兩個 Direct Connect 連線，以便在裝置無法使用時提供備援。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會出現。

檢查 ID

0t121N1Ty3

警示條件

黃色：只 AWS 區域 有一個 AWS Direct Connect 連線。

建議的動作

在此設定其他直 Connect 連線連線， AWS 區域 以防止裝置無法使用。如需詳細資訊，請參閱使用 AWS Direct Connect來設定備援連線。若要防止站台無法使用並新增位置備援，請設定至不同 Direct Connect 位置的其他 Direct Connect 連線。

其他資源

- 開始使用 AWS Direct Connect
- AWS Direct Connect 常見問答集

報告欄位

- Status
- 區域
- 時間戳記
- 位置
- 連線 ID

AWS Direct Connect 位置冗餘

描述

檢查是否 AWS 區域 有一個或多個 AWS Direct Connect 連接，而且只有一個 AWS Direct Connect 位置。與 AWS 資源的連線應該已將「直 Connect 連線」連線設定至不同的「直 Connect 線」位置，以便在某個位置無法使用時提供備援。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會出現。

檢查 ID

8M012Ph3U5

警示條件

黃色：中的「直 Connect 連線」連線 AWS 區域 未設定至不同的位置。

建議的動作

設定使用不同 Direct Connect 位置的 Direct Connect 連線，以防止位置無法使用。如需詳細資訊，請參閱入門 AWS Direct Connect。

其他資源

- 開始使用 AWS Direct Connect
- AWS Direct Connect 常見問答集

報告欄位

- Status
- 區域
- 時間戳記
- 位置
- 連線詳細資訊

AWS Direct Connect 位置彈性

描述

檢查與每個虛擬私有閘道或傳輸閘道相關聯的 AWS Direct Connect 位置恢復能力。

如果您的任何虛擬私有閘道或 Direct Connect 閘道未設定為使用至少兩個直接 Connect 位置，則此檢查會提醒您。缺乏位置恢復能力可能會導致意外的停機時間和不良的連接體驗。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會出現。

檢查 ID

```
c1dfpnchv2
```

警示條件

紅色：虛擬私人閘道或 Direct Connect 閘道沒有設定為跨多個 Direct Connect 位置連線裝置的虛擬介面。

黃色：虛擬私人閘道或 Direct Connect 閘道設定為具有多個虛擬介面，以連接至相同 Direct Connect 位置內的不同裝置。但它並未設定為跨多個直 Connect 位置連線至裝置。

綠色：虛擬私人閘道或直 Connect 閘道設定為使用至少兩個直 Connect 位置。

建議的動作

若要建立 Direct Connect 位置恢復能力，您可以將虛擬私有閘道或 Direct Connect 閘道設定為 Connect 至少兩個不同的直接連線位置。如需詳細資訊，請參閱AWS Direct Connect 復原建議。

其他資源

AWS Direct Connect 彈性建議

AWS Direct Connect 容錯移轉測

報告欄位

- Status
- 區域
- 上次更新時間
- 恢復狀態
- 位置
- 連線 ID
- 閘道 ID

AWS Direct Connect 虛擬介面備援

描述

檢查具有虛擬介面 (VIF) 的 AWS Direct Connect 虛擬私有閘道，而這些虛擬介面 (VIF) 未在至少兩個 AWS Direct Connect 連線上設定。連至您虛擬私有閘道的連線功能應該在多個 Direct Connect 連線和位置設定多個 VIF。這麼做可在裝置或位置無法使用時提供備援。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會出現。

檢查 ID

4g3Nt5M1Th

警示條件

黃色：虛擬私有閘道的虛擬介面少於兩個，或是介面未設定多個 Direct Connect 連線。

建議的動作

設定至少兩個設定有兩個 Direct Connect 連線的虛擬介面，以防止裝置或位置無法使用。請參閱 Create a Virtual Interface (建立虛擬介面)。

其他資源

- 開始使用 AWS Direct Connect
- AWS Direct Connect 常見問答集
- 使用 AWS Direct Connect 虛擬介面

報告欄位

- Status
- 區域
- 時間戳記
- 閘道 ID
- VIF 的位置
- VIF 的連線 ID

AWS Lambda 沒有配置無效字母隊列的函數

描述

檢查 AWS Lambda 函數是否配置了無效字母隊列。

無效字母佇列是可讓您擷取和分析失敗事件的 AWS Lambda 一項功能，提供相應地處理這些事件的方法。您的程式碼可能會引發例外狀況、逾時或記憶體不足，導致 Lambda 函數的非同步執行

失敗。無效字母佇列會儲存來自失敗調用的訊息，提供一種方式來處理訊息並疑難排解這些故障情況。

您可以使用規則中的 DLQarns 參數來指定要檢查的無效字母佇列資源。 AWS Config

如需詳細資訊，請參閱無效字母佇列。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz182
```

來源

```
AWS Config Managed Rule: lambda-dlq-check
```

警示條件

黃色： AWS Lambda 函數沒有配置無效字母隊列。

建議的動作

請確定您的 AWS Lambda 函數具有設定為控制所有失敗非同步叫用的訊息處理的無效字母佇列。

如需詳細資訊，請參閱無效字母佇列。

其他資源

- 採用 AWS Lambda 無效字母佇列的強大無伺服器應用程式設計

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數

- 上次更新時間

AWS Lambda 失敗時事件目的地

描述

檢查帳戶中的 Lambda 函數是否已針對非同步調用設定「失敗時」事件目的地或無效字母佇列 (DLQ)，以便將失敗調用的記錄路由至目的地以供進一步調查或處理。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`c1dfprch05`

警示條件

- 黃色：函數沒有任何已設定的「失敗時」事件目的地或 DLQ。

建議的動作

請為 Lambda 函數設定「失敗時」事件目的地或 DLQ，以便將失敗的調用及其他詳細資訊傳送至其中一個可用的目的地 AWS 服務，以供進一步偵錯或處理。

其他資源

- 非同步調用
- AWS Lambda 失敗時事件目的地

報告欄位

- Status
- 區域
- 具有已標記之版本的函數。
- 當天非同步請求下降百分比
- 當天非同步請求
- 平均每日非同步請求下降百分比

- 平均每日非同步請求
- 上次更新時間

不含多可用區域備援且支援 VPC 的AWS Lambda 函數

描述

檢查是否有支援 VPC 的 Lambda 函數在單一可用區域中容易發生服務中斷情形。建議將支援 VPC 的函數連接至多個可用區域以達到高可用性。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`L4dfs2Q4C6`

警示條件

黃色：已啟用 VPC 的 Lambda 函數連接到單一可用區域內的子網。

建議的動作

設定函數對 VPC 的存取權時，請選擇多個可用區域內的子網以確保高可用性。

其他資源

- 設定 Lambda 函數以存取 VPC 中的資源
- 韌性在 AWS Lambda

報告欄位

- Status
- 區域
- 函數 ARN
- VPC ID
- 平均每日叫用次數

- 上次更新時間

AWS Resilience Hub 違反政策

描述

檢查 Resilience Hub 是否存在不符合政策定義的復原時間點目標 (RTO) 和復原點目標 (RPO) 的應用程式。如果您的應用程式不符合您為 Resilience Hub 中的應用程式設定的 RTO 和 RPO 目標，則檢查會提醒您。

> **Note**
>
> 此檢查的結果會自動重新整理，且不允許重新整理請求。目前，您無法從此檢查中排除資源。

檢查 ID

`RH23stmM02`

警示條件

- 綠色：應用程式具有政策並符合 RTO 和 RPO 目標。
- 黃色：應用程式尚未進行評定。
- 紅色：應用程式具有政策，但不符合 RTO 和 RPO 目標。

建議的動作

登入 Resilience Hub 主控台並檢閱建議，讓您的應用程式符合 RTO 和 RPO 目標。

其他資源

Resilience Hub 概念

報告欄位

- Status
- 區域
- Application Name (應用程式名稱)
- 上次更新時間

AWS Resilience Hub 彈性分數

描述

檢查您是否已在 Resilience Hub 中對應用程式執行評估。如果您的彈性分數低於特定值，則此檢查會提醒您。

> **Note**
>
> 此檢查的結果會自動重新整理，且不允許重新整理請求。目前，您無法從此檢查中排除資源。

檢查 ID

`RH23stmM01`

警示條件

- 綠色：您的應用程式的彈性分數為 70 或更高。
- 黃色：您的應用程式的彈性分數為 40 至 69。
- 黃色：應用程式尚未進行評定。
- 紅色：您的應用程式的彈性分數低於 40。

建議的動作

登入 Resilience Hub 主控台並為您的應用程式執行評估。檢閱建議以提高彈性分數。

其他資源

Resilience Hub 概念

報告欄位

- Status
- 區域
- Application Name (應用程式名稱)
- 應用程式彈性分數
- 上次更新時間

AWS Resilience Hub 評估年齡

描述

檢查自上次執行應用程式評估之後經過多少時間。如果您在指定天數內未執行應用程式評估，此檢查會提醒您。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`RH23stmM03`

警示條件

- 綠色：您的應用程式評估曾在過去 30 天內執行。
- 黃色：過去 30 天未執行您的應用程式評估。

建議的動作

登入 Resilience Hub 主控台並為您的應用程式執行評估。

其他資源

Resilience Hub 概念

報告欄位

- Status
- 區域
- Application Name (應用程式名稱)
- 上次評估執行後的天數
- 上次評估執行時間
- 上次更新時間

AWS Site-to-Site VPN 至少有一個通道處於「關閉」狀態

描述

檢查每個作用中的通道數 AWS Site-to-Site VPN目。

VPN 應該隨時設有兩個通道。如此一來可在 AWS 端點的服務中斷時或進行預定的裝置維護期間提供備援功能。對於某些硬體，一次只會有一個通道處於作用中狀態。如果某個 VPN 沒有作用中通道，仍需支付該 VPN 的費用。

如需詳細資訊，請參閱 What is AWS Site-to-Site VPN?

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz123
```

來源

```
AWS Config Managed Rule: vpc-vpn-2-tunnels-up
```

警示條件

黃色：Site-to-Site VPN 至少有一個通道為 DOWN。

建議的動作

確保為 VPN 連線設定了兩個通道。而且，如果您的硬體支援它，那麼請確保兩個通道均處於作用中狀態。如果您不再需要 VPN 連線，那麼請予以刪除以免產生費用。

如需詳細資訊，請參閱您的客戶閘道裝置和 AWS 知識中心所提供的內容。

其他資源

- AWS Site-to-Site VPN 使用者指南
- 將虛擬私有閘道新增到您的 VPC

報告欄位

- Status

- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

AWS Well-Architected 可靠性的高風險問題

描述

檢查可靠性支柱中，工作負載是否有高風險問題 (HRI)。這項檢查是以您的 AWS-Well Architected 檢閱為基礎。您的檢查結果取決於您是否使用 AWS Well-Architected 完成工作負載評估。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`Wxdfp4B1L4`

警示條件

- 紅色：在 AWS Well-Architected 的可靠性支柱中發現至少一個活躍的高風險問題。
- 綠色： AWS Well-Architected 的可靠性支柱未偵測到任何有效的高風險問題。

建議的動作

AWS Well-Architected，在您的工作負載評估期間偵測到高風險問題。解決這些問題，可能有機會降低風險和節省成本。登入 AWS Well-Architected 工具，檢閱答案並採取行動，解決待處理的問題。

報告欄位

- Status
- 區域
- 工作負載 ARN
- 工作負載名稱

- 檢閱者姓名
- 工作負載類型
- 工作負載開始日期
- 工作負載上次修改日期
- 可靠性方面已識別的高風險問題數量
- 可靠性方面已解決的高風險問題數量
- 可靠性方面已回答的問題數量
- 可靠性支柱中的問題總數
- 上次更新時間

Classic Load Balancer 未設定多個 AZ

描述

檢查 Classic Load Balancer 是否跨越多個可用區域 (AZ)。

負載平衡器會將傳入的應用程式流量分散到多個可用區域中的多個 Amazon EC2 執行個體。根據預設，負載平衡器橫跨您為負載平衡器啟用的可用區域平均分派流量。如果一個可用區域發生中斷情形，負載平衡器節點會自動將請求轉送到一或多個可用區域中運作狀態良好的已註冊執行個體。

您可以使用 AWS Config 規則中的參數調整可用區域的最小minAvailabilityZones數目

如需詳細資訊，請參閱什麼是 Classic Load Balancer？。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz154
```

來源

```
AWS Config Managed Rule: clb-multiple-az
```

警示條件

黃色：Classic Load Balancer 未設定 Multi-AZ，或不符合指定的 AZ 的最小數量。

建議的動作

請確定您的 Classic Load Balancer 已設定多個可用區域。將負載平衡器跨越多個 AZ，以確保您的應用程式具有高可用性。

如需詳細資訊，請參閱教學課程：建立 Classic Load Balancer。

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

ELB 連接耗盡

描述

檢查是否有負載平衡器未啟用連接耗盡功能。

當連接耗盡功能沒有啟用，且您從負載平衡器取消註冊 Amazon EC2 執行個體時，負載平衡器會停止將流量路由到該執行個體並關閉連線。當連接耗盡功能啟用，負載平衡器會停止將新請求傳送至已取消註冊的執行個體，但會保持連線開啟以服務作用中請求。

檢查 ID

`7qGXsKIUw`

警示條件

黃色：未啟用負載平衡器的連接耗盡功能。

建議的動作

啟用負載平衡器的連接耗盡功能。如需詳細資訊，請參閱 Connection Draining (連接耗盡) 和 Enable or Disable Connection Draining for Your Load Balancer (為您的負載平衡器啟用或停用連接耗盡功能)。

其他資源

彈性負載平衡概念

報告欄位

- Status
- 區域
- 負載平衡器名稱
- 原因

ELB 跨區域負載平衡

描述

關閉跨區域負載平衡功能後，會出現因流量分配不均或後端超載而導致服務無法使用的風險。當用戶端不正確地快取 DNS 資訊時，可能會發生這個問題。當每個可用區域中的執行個體數量不相等時 (例如如果您中斷了某些執行個體的服務以進行維護)，也可能會發生此問題。

檢查 ID

```
xdeXZKIUy
```

警示條件

黃色：負載平衡器未啟用跨區域負載平衡功能。

建議的動作

確認向負載平衡器註冊的 Amazon EC2 執行個體已在多個可用區域中啟動，然後為該負載平衡器啟用跨區域負載平衡。如需詳細資訊，請參閱 Availability Zones and Regions (可用區域和區域) 以及 Enable or Disable Cross-Zone Load Balancing for Your Load Balancer (為您的負載平衡器啟用或停用跨區域負載平衡)。

其他資源

- 要求路由
- 彈性負載平衡概念

報告欄位

- Status
- 區域

- 負載平衡器名稱
- 原因

負載平衡器最佳化

描述

檢查您的負載平衡器組態。

為了協助在使用 Elastic Load Balancing 時提高 Amazon Elastic Compute Cloud (Amazon EC2) 的容錯能力，建議在一個區域的多個可用區域中執行相同數量的執行個體。設定完畢的負載平衡器會產生費用，因此這也是一項成本最佳化檢查。

檢查 ID

`iqdCTZKCUp`

警示條件

- 黃色：單一可用區域啟用了負載平衡器。
- 黃色：沒有作用中執行個體的可用區域啟用了負載平衡器。
- 黃色：向負載平衡器註冊的 Amazon EC2 執行個體在可用區域間分佈不均衡。(已使用的可用區域中的最大執行個體數量與最少執行個體數量之間的差異大於 1，而差異超過最大執行個體數量的 20% 以上。)

建議的動作

請確保您的負載平衡器指向至少兩個可用區域內作用中和運作狀態良好的執行個體。如需詳細資訊，請參閱新增可用區域。

如果您的負載平衡器是設定用於沒有運作狀態良好執行個體的可用區域，或是可用區域間中的執行個體的分佈不均衡，請判斷是否這些可用區域都是需要的。請省略任何不必要的可用區域，並確保在剩餘的可用區域之間均衡分配執行個體。如需更多詳細資訊，請參閱移除可用區域。

其他資源

- 可用區域和區域
- 管理負載平衡器
- Elastic Load Balancing 評估的最佳實務

報告欄位

- Status

- 區域
- 負載平衡器名稱
- 區域數量
- 區域 a 執行個體
- 區域 b 執行個體
- 區域 c 執行個體
- 區域 d 執行個體
- 區域 e 執行個體
- 區域 f 執行個體
- 原因

NAT Gateway AZ 獨立性

描述

檢查您的 NAT Gateway 是否設定為可用區域 (AZ) 獨立性。

NAT Gateway 可讓私有子網路中的資源使用 NAT Gateway 的 IP 地址安全地連線至子網路外部的服務，並捨棄任何來路不明的傳入流量。每個 NAT Gateway 皆在指定的可用區域 (AZ) 內運作，並且僅在該 AZ 中以備援建置。因此，您在特定 AZ 中的資源應該使用相同 AZ 中的 NAT Gateway，如此在 NAT Gateway 或其 AZ 發生任何潛在中斷的情況下，就不會影響其他 AZ 中的資源。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c1dfptbg10
```

警示條件

- 紅色：來自某個 AZ 中子網路的流量會透過其他 AZ 中的 NATGW 來路由。
- 綠色：來自某個 AZ 中子網路的流量會透過相同 AZ 中的 NATGW 來路由。

建議的動作

請檢查子網路的 AZ，並透過相同 AZ 中的 NAT Gateway 路由傳送流量。

如果 AZ 中沒有 NATGW，請建立一個，然後透過它來路由子網路流量。

如果您在不同 AZ 的子網路之間有相同的路由表關聯，請將此路由表保持與 NAT Gateway 位於相同 AZ 中的子網路的關聯，而對於另一個 AZ 中的子網路，請將個別路由表與至此其他 AZ 中 NAT Gateway 的路由建立關聯。

我們建議您為 Amazon VPC 中的架構變更選擇維護時段。

其他資源

- 如何建立 NAT Gateway
- 如何設定 NAT Gateway 使用案例的路由

報告欄位

- Status
- 區域
- NAT 可用區域
- NAT ID
- 子網路可用區域
- 子網路 ID
- 路由表 ID
- NAT ARN
- 上次更新時間

跨負載平衡的 Network Load Balancer

描述

檢查跨區域負載平衡是否已在 Network Load Balancer 上啟用。

跨區域負載平衡有助於在不同可用區域中的執行個體之間維持連入流量的均勻分佈。這樣可防止負載平衡器將所有流量路由到相同可用區域中的執行個體，這可能會導致流量分佈不均和潛在的超載問題。在單一可用區域故障的情況下，此功能也會自動將流量路由到其他可用區域中運作狀態良好的執行個體，有助於提升應用程式的可靠性。

如需詳細資訊，請參閱跨區域負載平衡。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz105
```

來源

```
AWS Config Managed Rule: nlb-cross-zone-load-balancing-enabled
```

警示條件

- 黃色：Network Load Balancer 未啟用跨區域負載平衡。

建議的動作

確保跨區域負載平衡是否已在 Network Load Balancer 上啟用。

其他資源

跨區域負載平衡 (Network Load Balancer)

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

NLB-私有子網路中的網際網路對向資源

描述

檢查網際網路對向網路的 Network Load Balancer (NLB) 是否已設定為私有子網路。必須在公用子網路中設定面向網際網路的 Network Load Balancer (NLB)，才能接收流量。公用子網路定義為具有直接路由至網際網路閘道的子網路。如果子網路設定為私有，則其可用區域 (AZ) 不會接收流量，這可能會造成可用性問題。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

c1dfpnchv4

警示條件

紅色：NLB 設定為一或多個私有子網路

綠色：沒有為面向網際網路的 NLB 設定私有子網路

建議的動作

確認網際網路對向負載平衡器中設定的子網路是公用的。公用子網路定義為具有直接路由至網際網路閘道的子網路。使用下列其中一個選項：

- 建立新的負載平衡器，並選取具有直接路由到網際網路閘道的其他子網路。
- 將目前連接到負載平衡器的子網路從私人變更為公用。若要這麼做，請變更其路由表並關聯網閘道。

其他資源

- 設定負載平衡器和監聽器
- VPC 適用的子網路
- 將閘道與路由表建立關聯

報告欄位

- Status
- 區域
- NLB 阿恩
- NLB 名稱
- 子網路 ID
- NLB 計劃
- 子網路類型
- 上次更新時間

NLB 異地同步備份

描述

檢查您的網路負載平衡器是否設定為使用多個可用區域 (AZ)。AZ 是明顯與其他區域中的故障隔絕開來的地點。在相同區域的多個 AZ 中設定負載平衡器，以協助改善工作負載可用性。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`c1dfprch09`

警示條件

黃色：NLB 位於單一 AZ 中。

綠色：NLB 有兩個或更多個 AZ。

建議的動作

請確定您的負載平衡器至少設定了兩個可用區域。

其他資源

如需詳細資訊，請參閱下列 文件：

- 可用區域
- AWS Well-Architected-將工作負載部署到多個位置
- 區域與可用區域

報告欄位

- Status
- 區域
- AZ 數量
- NLB ARN
- NLB 名稱

- 上次更新時間

事件管理員複製組 AWS 區域 中的數目

描述

檢查事件管理員複製組的組態是否使用多個組態 AWS 區域 來支援區域容錯移轉和回應。針對 CloudWatch 警示或事件所產生的 EventBridge 事件，事件管理員會以警示或事件規則 AWS 區域 相同的方式建立事件。如果該區域暫時無法使用 Incident Manager，則系統會嘗試在複製集的另一個區域中建立事件。如果複製集僅包含一個區域，則系統無法在 Incident Manager 無法使用時建立事件記錄。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`cIdfp1js9r`

警示條件

- 綠色：複寫集包含超過一個的區域。
- 黃色：複本集包含一個區域。

建議的動作

至少新增一個區域至複寫集。

其他資源

如需詳細資訊，請參閱跨區域事件管理。

報告欄位

- Status
- 多區域
- 複寫集
- 上次更新時間

單一 AZ 應用程式檢查

描述

檢查網路模式是否透過單一可用區域 (AZ) 路由您的輸出網路流量。

AZ 是明顯與其他區域中的任何影響隔絕開來的地點。透過將您的服務分散到多個 AZ，您可以限制 AZ 故障的衝擊半徑。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`c1dfptbg11`

警示條件

- 黃色：根據觀察到的輸出網路模式，您的應用程式僅能部署在一個 AZ 中。如果這是真的，而且您的應用程式預期高可用性，建議您佈建應用程式資源並實作網路流程來運用多個可用區域。

建議的動作

如果您的應用程式需要高可用性，請考慮實作多可用區域架構來獲得更高的可用性。

報告欄位

- Status
- 區域
- VPC ID
- 上次更新時間

多個 AZ 中的 VPC 介面端點網路介面

描述

檢查您的 AWS PrivateLink VPC 介面端點是否設定為使用多個可用區域 (AZ)。AZ 是明顯與其他區域中的故障隔絕開來的地點。這支援相 AWS 同區域中 AZ 之間經濟實惠、低延遲的網路連線。在建立介面端點時選取多個 AZ 中的子網路，以協助保護您的應用程式不受單點故障影響。

> **Note**
>
> 此檢查目前僅包含介面端點。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`c1dfprch10`

警示條件

黃色：VPC 端點位於單一可用區中。

綠色：VPC 端點至少位於兩個 AZ 中。

建議的動作

請確定您的 VPC 介面端點已設定至少兩個可用區域。

其他資源

如需詳細資訊，請參閱下列 文件：

- 使用介面 VPC 端點存取 AWS 服務
- 端點網路介面的私有 IP 位址
- AWS PrivateLink 概念
- 區域與可用區域

報告欄位

- Status
- 區域
- VPC 端點識別碼
- 是異同步備份

- 上次更新時間

VPN 通道備援

描述

檢查每個 VPN 的作用中通道數。

VPN 應該隨時設有兩個通道。如此一來可在 AWS 端點的服務中斷時或進行預定的裝置維護期間提供備援功能。對於某些硬體，一次只會有一個通道處於作用中狀態。如果某個 VPN 沒有作用中通道，仍需支付該 VPN 的費用。如需詳細資訊，請參閱 AWS Client VPN 管理員指南。

檢查 ID

`S45wrEXrLz`

警示條件

- 黃色：VPN 有一個作用中的通道 (這對於某些硬體而言是正常的)。
- 黃色：VPN 沒有作用中的通道。

建議的動作

請確保已為您的 VPN 連線設定兩個通道，並且兩個通道都在作用中 (如果您的硬體支援這種情形)。您可以刪除不再需要的 VPN 連線以避免產生費用。如需詳細資訊，請參閱客戶閘道或者刪除 VPN 連線。

其他資源

- AWS 網 Site-to-Site VPN 使用者指南
- 「將硬體虛擬私有閘道新增到您的 VPC」

報告欄位

- Status
- 區域
- VPN ID
- VPC
- 虛擬私有閘道
- 客戶閘道
- 作用中通道

- 原因

ActiveMQ 可用區域備援

描述

檢查 Amazon MQ for ActiveMQ 代理程式是否已為多個可用區域中的作用中/待命的代理程式設定高可用性。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`c1t3k8mqv1`

警示條件

- 黃色：Amazon MQ for ActiveMQ 代理程式是在單一可用區域中設定。

  綠色：Amazon MQ for ActiveMQ 代理程式是在至少兩個可用區域中設定。

建議的動作

建立具有作用中/待命部署模式的新代理程式。

其他資源

- 建立 ActiveMQ 中介裝置

報告欄位

- Status
- 區域
- ActiveMQ 代理程式 ID
- 中介裝置引擎類型
- 部署模式
- 上次更新時間

RabbitMQ 可用區域備援

描述

檢查 Amazon MQ for RabbitMQ 代理程式是否已為多個可用區域中的叢集執行個體設定高可用性。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`c1t3k8mqv2`

警示條件

- 黃色：Amazon MQ for RabbitMQ 代理程式是在單一可用區域中設定。

  綠色：Amazon MQ for RabbitMQ 代理程式是在多個可用區域中設定。

建議的動作

建立具有叢集部署模式的新代理程式。

其他資源

- 建立 RabbitMQ 代理程式

報告欄位

- Status
- 區域
- RabbitMQ 代理程式 ID
- 中介裝置引擎類型
- 部署模式
- 上次更新時間

服務限制

請參閱下列適用於服務配額 (也稱為配額) 類別的檢查。

此類別中的所有檢查都有以下描述：

警示條件

- 黃色：已達到上限的 80%。
- 紅色：已達到上限的 100%。
- 藍色：Trusted Advisor 無法擷取一個或多個 AWS 區域 的使用率或限額。

建議的動作

如果您預期超過服務限額，請直接在 Service Quotas 主控台請求提高限額。如果 Service Quotas 尚不支援您的服務，您可以在支援中心建立支援案例。

報告欄位

- Status
- 服務
- 區域
- 限額
- 目前用量

> **Note**
>
> - 這些值是以快照為基礎，因此您目前的用量可能會有所不同。配額和用量資料最多可能需要 24 小時才會反映任何變更。若最近剛提高配額，您可能會暫時看到用量超過配額的情形。

檢查名稱

- Auto Scaling 群組
- Auto Scaling 啟動組態
- CloudFormation 堆疊
- DynamoDB 讀取容量
- DynamoDB 寫入容量
- EBS 作用中快照
- EBS 冷 HDD (sc1) 磁碟區儲存
- EBS 一般用途 SSD (gp2) 磁碟區儲存

- EBS 一般用途 SSD (gp3) 磁碟區儲存
- EBS 磁帶 (標準) 磁碟區儲存
- EBS 佈建 IOPS (SSD) 磁碟區彙總 IOPS
- EBS 佈建 IOPS SSD (io1) 磁碟區儲存
- EBS 佈建 IOPS SSD (io2) 磁碟區儲存
- EBS 輸送量最佳化 HDD (st1) 磁碟區儲存
- EC2 隨需執行個體
- EC2 預留執行個體租用
- EC2-Classic 彈性 IP 地址
- EC2-VPC 彈性 IP 地址
- ELB Application Load Balancer
- ELB Classic Load Balancer
- ELB Network Load Balancer
- IAM 群組
- IAM 執行個體描述檔
- IAM 政策
- IAM 角色
- IAM 伺服器憑證
- IAM 使用者
- 每個區域的 Kinesis 碎片
- Lambda 程式碼儲存用量
- RDS 叢集參數群組
- RDS 叢集角色
- RDS 叢集
- RDS 資料庫執行個體
- RDS 資料庫手動快照
- RDS 資料庫參數群組
- RDS 資料庫安全群組
- RDS 事件訂閱
- 每個安全群組的 RDS 驗證上限

- RDS 選項群組
- 每個主資料的 RDS 僅供讀取複本
- RDS 預留執行個體
- RDS 子網路群組
- 每個子網路群組的 RDS 子網路
- RDS 總儲存配額
- Route 53 託管區域
- Route 53 運作狀態檢查上限
- Route 53 可重複使用的委派集
- Route 53 流量政策
- Route 53 流量政策執行個體
- SES 每日傳送份額
- VPC
- VPC 網際網路閘道

Auto Scaling 群組

描述

檢查是否有用量超過 Auto Scaling 群組配額的 80%。

檢查 ID

`fW7HH0l7J9`

其他資源

Auto Scaling 配額

Auto Scaling 啟動組態

描述

檢查是否有用量超過 Auto Scaling 啟動組態配額的 80%。

檢查 ID

`aW7HH0l7J9`

其他資源

Auto Scaling 配額

CloudFormation 堆疊

描述

檢查使用量是否超過 CloudFormation 堆疊配額的 80%。

檢查 ID

gW7HH0l7J9

其他資源

AWS CloudFormation 配額

DynamoDB 讀取容量

描述

檢查是否有用量超過 DynamoDB 為每個 AWS 帳戶所佈建讀取輸送量限額的 80%。

檢查 ID

6gtQddfEw6

其他資源

DynamoDB 配額

DynamoDB 寫入容量

描述

檢查是否有用量超過 DynamoDB 為每個 AWS 帳戶所佈建寫入輸送量限額的 80%。

檢查 ID

c5ftjdfkMr

其他資源

DynamoDB 配額

EBS 作用中快照

描述

檢查是否有用量超過 EBS 作用中快照配額的 80%。

檢查 ID

`eI7KK0l7J9`

其他資源

Amazon EBS 限額

EBS 冷 HDD (sc1) 磁碟區儲存

描述

檢查是否有用量超過 EBS 冷 HDD (sc1) 磁碟區儲存配額的 80%。

檢查 ID

`gH5CC0e3J9`

其他資源

Amazon EBS 限額

EBS 一般用途 SSD (gp2) 磁碟區儲存

描述

檢查是否有用量超過 EBS 一般用途 SSD (gp2) 磁碟區儲存配額的 80%。

檢查 ID

`dH7RR0l6J9`

其他資源

Amazon EBS 限額

EBS 一般用途 SSD (gp3) 磁碟區儲存

描述

檢查是否有用量超過 EBS 一般用途 SSD (gp3) 磁碟區儲存配額的 80%。

檢查 ID

dH7RR0l6J3

其他資源

Amazon EBS 限額

EBS 磁帶 (標準) 磁碟區儲存

描述

檢查是否有用量超過 EBS 磁帶 (標準) 磁碟區儲存配額的 80%。

檢查 ID

cG7HH0l7J9

其他資源

Amazon EBS 限額

EBS 佈建 IOPS (SSD) 磁碟區彙總 IOPS

描述

檢查是否有用量超過 EBS 佈建 IOPS (SSD) 磁碟區彙總 IOPS 配額的 80%。

檢查 ID

tV7YY0l7J9

其他資源

Amazon EBS 限額

EBS 佈建 IOPS SSD (io1) 磁碟區儲存

描述

檢查是否有用量超過 EBS 佈建 IOPS SSD (io1) 磁碟區儲存配額的 80%。

檢查 ID

gI7MM0l7J9

其他資源

Amazon EBS 限額

EBS 佈建 IOPS SSD (io2) 磁碟區儲存

描述

檢查是否有用量超過 EBS 佈建 IOPS SSD (io2) 磁碟區儲存配額的 80%。

檢查 ID

gI7MM0l7J2

其他資源

Amazon EBS 限額

EBS 輸送量最佳化 HDD (st1) 磁碟區儲存

描述

檢查是否有用量超過 EBS 輸送量最佳化 HDD (st1) 磁碟區儲存配額的 80%。

檢查 ID

wH7DD0l3J9

其他資源

Amazon EBS 限額

EC2 隨需執行個體

描述

檢查是否有用量超過 EC2 隨需執行個體配額的 80%。

檢查 ID

`0Xc6LMYG8P`

其他資源

Amazon EC2 配額

EC2 預留執行個體租用

描述

檢查是否有用量超過 EC2 預留執行個體租用配額的 80%。

檢查 ID

`iH7PP0l7J9`

其他資源

Amazon EC2 配額

EC2-Classic 彈性 IP 地址

描述

檢查是否有用量超過 EC2-Classic 彈性 IP 地址配額的 80%。

檢查 ID

`aW9HH0l8J6`

其他資源

Amazon EC2 配額

EC2-VPC 彈性 IP 地址

描述

檢查是否有用量超過 EC2-VPC 彈性 IP 地址配額的 80%。

檢查 ID

`lN7RR0l7J9`

其他資源

VPC 彈性 IP 配額

ELB Application Load Balancer

描述

檢查是否有用量超過 ELB Application Load Balancer 配額的 80%。

檢查 ID

`EM8b3yLRTr`

其他資源

Elastic Load Balancing 配額

ELB Classic Load Balancer

描述

檢查是否有用量超過 ELB Classic Load Balancer 配額的 80%。

檢查 ID

`iK7O00l7J9`

其他資源

Elastic Load Balancing 配額

ELB Network Load Balancer

描述

檢查是否有用量超過 ELB Network Load Balancer 配額的 80%。

檢查 ID

8wIqYSt25K

其他資源

Elastic Load Balancing 配額

IAM 群組

描述

檢查是否有用量超過 IAM 群組配額的 80%。

檢查 ID

sU7XX0l7J9

其他資源

IAM 配額

IAM 執行個體描述檔

描述

檢查是否有用量超過 IAM 執行個體描述檔配額的 80%。

檢查 ID

n07SS0l7J9

其他資源

IAM 配額

IAM 政策

描述

檢查是否有用量超過 IAM 政策配額的 80%。

檢查 ID

pR7UU0l7J9

其他資源

IAM 配額

IAM 角色

描述

檢查是否有用量超過 IAM 角色配額的 80%。

檢查 ID

oQ7TT0l7J9

其他資源

IAM 配額

IAM 伺服器憑證

描述

檢查是否有用量超過 IAM 伺服器憑證配額的 80%。

檢查 ID

rT7WW0l7J9

其他資源

IAM 配額

IAM 使用者

描述

檢查是否有用量超過 IAM 使用者配額的 80%。

檢查 ID

`qS7VV0l7J9`

其他資源

IAM 配額

每個區域的 Kinesis 碎片

描述

檢查是否有用量超過每個區域 Kinesis 碎片配額的 80%。

檢查 ID

`bW7HH0l7J9`

其他資源

Kinesis 配額

Lambda 程式碼儲存用量

描述

檢查是否有程式碼用量超過帳戶限制的 80%。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`c1dfprch07`

警示條件

- 黃色：已達到上限的 80%。

建議的動作

請找出未使用的 Lambda 函數或版本然後移除它們，藉此釋出您在該區域帳戶的程式碼儲存空間。如果您需要額外的儲存空間，請在支援中心裡建立支援案例。如果您預期超過服務限額，請直接在 Service Quotas 主控台請求提高限額。如果 Service Quotas 尚不支援您的服務，您可以在支援中心建立支援案例。

其他資源

- Lambda 程式碼儲存用量

報告欄位

- Status
- 區域
- 此資源的合格函數 ARN。
- 函數代碼存儲使用情況 MegaBytes 與 2 位小數。
- 函數中版本的數量
- 上次更新時間

RDS 叢集參數群組

描述

檢查是否有用量超過 RDS 叢集參數群組配額的 80%。

檢查 ID

`jtlIMO3qZM`

其他資源

Amazon RDS 配額

RDS 叢集角色

描述

檢查是否有用量超過 RDS 叢集角色配額的 80%。

檢查 ID

7fuccf1Mx7

其他資源

Amazon RDS 配額

RDS 叢集

描述

檢查是否有用量超過 RDS 叢集配額的 80%。

檢查 ID

gjqMBn6pjz

其他資源

Amazon RDS 配額

RDS 資料庫執行個體

描述

檢查是否有用量超過 RDS 資料庫執行個體配額的 80%。

檢查 ID

XG0aXHpIEt

其他資源

Amazon RDS 配額

RDS 資料庫手動快照

描述

檢查是否有用量超過 RDS 資料庫手動快照配額的 80%。

檢查 ID

dV84wpqRUs

其他資源

Amazon RDS 配額

RDS 資料庫參數群組

描述

檢查是否有用量超過 RDS 資料庫參數群組配額的 80%。

檢查 ID

jEECYg2YVU

其他資源

Amazon RDS 配額

RDS 資料庫安全群組

描述

檢查是否有用量超過 RDS 資料庫安全群組配額的 80%。

檢查 ID

gfZAn3W7wl

其他資源

Amazon RDS 配額

RDS 事件訂閱

描述

檢查是否有用量超過 RDS 事件訂閱配額的 80%。

檢查 ID

keAhfbH5yb

其他資源

Amazon RDS 配額

每個安全群組的 RDS 驗證上限

描述

檢查是否有用量超過每個安全群組 RDS 驗證上限配額的 80%。

檢查 ID

dBkuNCvqn5

其他資源

Amazon RDS 配額

RDS 選項群組

描述

檢查是否有用量超過 RDS 選項群組配額的 80%。

檢查 ID

3Njm0DJQO9

其他資源

Amazon RDS 配額

每個主資料的 RDS 僅供讀取複本

描述

檢查是否有用量超過每個主資料 RDS 僅供讀取複本配額的 80%。

檢查 ID

pYW8UkYz2w

其他資源

Amazon RDS 配額

RDS 預留執行個體

描述

檢查是否有用量超過 RDS 預留執行個體配額的 80%。

檢查 ID

UUDv0a5r34

其他資源

Amazon RDS 配額

RDS 子網路群組

描述

檢查是否有用量超過 RDS 子網路群組配額的 80%。

檢查 ID

dYWBaXaaMM

其他資源

Amazon RDS 配額

每個子網路群組的 RDS 子網路

描述

檢查是否有用量超過每個子網路群組 RDS 子網路配額的 80%。

檢查 ID

jEhCtdJK0Y

其他資源

Amazon RDS 配額

RDS 總儲存配額

描述

檢查是否有用量超過 RDS 總儲存配額的 80%。

檢查 ID

`P1jhKWEmLa`

其他資源

Amazon RDS 配額

Route 53 託管區域

描述

檢查是否有用量超過每個帳戶 Route 53 託管區域配額的 80%。

檢查 ID

`dx3xfcdfMr`

其他資源

Route 53 配額

Route 53 運作狀態檢查上限

描述

檢查是否有用量超過每個帳戶 Route 53 運作狀態檢查配額的 80%。

檢查 ID

`ru4xfcdfMr`

其他資源

Route 53 配額

Route 53 可重複使用的委派集

描述

檢查是否有用量超過每個帳戶 Route 53 可重複使用委派集配額的 80%。

檢查 ID

`ty3xfcdfMr`

其他資源

Route 53 配額

Route 53 流量政策

描述

檢查是否有用量超過每個帳戶 Route 53 流量政策配額的 80%。

檢查 ID

`dx3xfbjfMr`

其他資源

Route 53 配額

Route 53 流量政策執行個體

描述

檢查是否有用量超過每個帳戶 Route 53 流量政策執行個體配額的 80%。

檢查 ID

`dx8afcdfMr`

其他資源

Route 53 配額

SES 每日傳送份額

描述

檢查是否有用量超過 Amazon SES 每日傳送份額的 80%。

檢查 ID

hJ7NN0l7J9

其他資源

Amazon SES 配額

VPC

描述

檢查是否有用量超過 VPC 配額的 80%。

檢查 ID

jL7PP0l7J9

其他資源

VPC 配額

VPC 網際網路閘道

描述

檢查是否有用量超過 VPC 網際網路閘道配額的 80%。

檢查 ID

kM7QQ0l7J9

其他資源

VPC 配額

營運卓越

您可以針對營運卓越類別使用下列檢查。

檢查名稱

- Amazon API Gateway 未記錄執行日誌
- 未啟用 X-Ray 追蹤的 Amazon API Gateway REST API
- Amazon CloudFront 訪問日誌配置
- Amazon CloudWatch 警報操作已禁用
- Amazon EC2 執行個體並非由 AWS Systems Manager 所管理
- 已停用具有標籤不變性的 Amazon ECR 儲存庫
- 已停用具有 Container Insights 的 Amazon ECS 叢集
- 未啟用 Amazon ECS 任務日誌記錄
- CloudWatch 未設定 Amazon OpenSearch 服務記錄
- 具有異質參數群組的叢集中的 Amazon RDS 資料庫執行個體
- Amazon RDS 增強型監控已關閉
- Amazon RDS Performance Insights 已關閉
- Amazon RDS 跟踪計數參數已關閉
- Amazon Redshift 叢集稽核日誌記錄
- Amazon S3 未啟用事件通知
- Amazon SNS 主題未記錄訊息傳遞狀態
- Amazon VPC (不含流程日誌)
- 未啟用存取日誌的 Application Load Balancer 和 Classic Load Balancer
- AWS CloudFormation 堆疊通知
- S3 儲存貯體中物件的 AWS CloudTrail 資料事件日誌記錄
- AWS CodeBuild 專案日誌記錄
- 已啟用 AWS CodeDeploy 自動復原和監控
- AWS CodeDeployLambda 正在使用 all-at-once 部署組態
- 未設定 AWS Elastic Beanstalk 增強型運作狀態報告
- 已停用具有受管平台更新的 AWS Elastic Beanstalk
- AWS Fargate 平台版本並非最新
- 處於不合規狀態的 AWS Systems Manager State Manager 關聯
- CloudTrail 未使用 Amazon CloudWatch 日誌設定追蹤

- 未針對負載平衡器啟用 Elastic Load Balancing 刪除保護
- RDS 資料庫叢集刪除保護檢查
- RDS 資料庫執行個體自動微幅版本升級檢查

Amazon API Gateway 未記錄執行日誌

描述

檢查 Amazon API Gateway 是否已在所需的記錄層級開啟 CloudWatch 日誌。

在 Amazon API 閘道中開啟 REST API 方法或 WebSocket API 路由的 CloudWatch 記錄功能，以針對 API 收到的請求，在 CloudWatch 日誌中收集執行日誌。執行日誌中包含的資訊有助於找出及疑難排解與 API 相關的問題。

您可以在 AWS Config 規則的 loggingLevel 參數中指定日誌記錄層級 (ERROR, INFO) ID。

如需有關在 Amazon API 閘道中 CloudWatch 記錄的詳細資訊，請參閱 REST API 或 WebSocket API 文件。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz125
```

來源

```
AWS Config Managed Rule: api-gw-execution-logging-enabled
```

警示條件

黃色：Amazon API Gateway 的所需 CloudWatch 記錄層級未啟用執行日誌收集的日誌記錄設定。

建議的動作

為 Amazon API 閘道 REST API 或具有適當 CloudWatch 記錄層級 (錯誤、資訊) 的 WebSocket API 或 API 開啟執行日誌的記錄功能。

如需詳細資訊，請參閱建立流程日誌。

其他資源

- 在 API Gateway 中設定 REST API 的 CloudWatch 記錄
- 設定 WebSocket API 的記錄

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

未啟用 X-Ray 追蹤的 Amazon API Gateway REST API

描述

檢查 Amazon API Gateway REST API 是否已開啟 AWS X-Ray 追蹤。

開啟 REST API 的 X-Ray 追蹤功能，允許 API Gateway 使用追蹤資訊來取樣 API 調用請求。如此可讓您運用 AWS X-Ray 的優點，在請求通過 API Gateway REST API 進入下游服務時予以追蹤及分析。

如需詳細資訊，請參閱使用 X-Ray 追蹤使用者的 REST API 請求。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz126
```

來源

```
AWS Config Managed Rule: api-gw-xray-enabled
```

警示條件

黃色：未開啟 API Gateway REST API 的 X-Ray 追蹤。

建議的動作

開啟 API Gateway REST API 的 X-Ray 追蹤。

如需詳細資訊，請參閱使用 API Gateway REST API 設定 AWS X-Ray。

其他資源

- 使用 X-Ray 追蹤使用者對 REST API 的請求
- 什麼是 AWS X-Ray？

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

Amazon CloudFront 訪問日誌配置

描述

檢查 Amazon CloudFront 分發是否設定為從 Amazon S3 伺服器存取日誌擷取資訊。Amazon S3 伺服器存取日誌包含有關 CloudFront 收到的每個使用者請求的詳細資訊。

您可以使用AWS Config規則中的 S3 BucketName 參數調整用於存放伺服器存取日誌的 Amazon S3 儲存貯體名稱。

如需詳細資訊，請參閱設定和使用標準日誌 (存取日誌)。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

c18d2gz110

來源

AWS Config Managed Rule: cloudfront-accesslogs-enabled

警示條件

黃色：未啟用 Amazon CloudFront 存取記錄

建議的動作

請務必開啟 CloudFront 存取記錄功能，以擷取有關 CloudFront 接收之每個使用者要求的詳細資訊。

您可以在建立或更新分佈時開啟標準日誌。

如需詳細資訊，請參閱在建立或更新分佈時您指定的值。

其他資源

- 您在建立或更新分佈時指定的值
- 設定和使用標準日誌 (存取日誌)

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

Amazon CloudWatch 警報操作已禁用

描述

檢查您的 Amazon CloudWatch 警示動作是否處於停用狀態。

您可以使用 AWS CLI 來啟用或停用警示中的動作功能。或者，您可以使用 AWS SDK 以程式設計的方式來停用或啟用動作功能。警示動作功能關閉時， CloudWatch 不會在任何狀態下執行任何已定義的動作 (正常、不足資料、鬧鐘)。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz109
```

來源

```
AWS Config Managed Rule: cloudwatch-alarm-action-enabled-check
```

警示條件

黃色：未啟用 Amazon CloudWatch 警示動作。在任何警示狀態下均不會執行任何動作。

建議的動作

在 CloudWatch 警報中啟用動作，除非您有正當理由停用它們，例如用於測試目的。

如果不再需要 CloudWatch 警報，請將其刪除以避免產生不必要的成本。

如需詳細資訊，請參閱 enable-alarm-actionsGo API 參考 AWS SDK EnableAlarmActions 中的 AWS CLI命令參考和 func (*CloudWatch) 中的。

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

Amazon EC2 執行個體並非由 AWS Systems Manager 所管理

描述

檢查您帳戶中的 Amazon EC2 執行個體是否由 AWS Systems Manager 管理。

Systems Manager 可協助您瞭解和控制 Amazon EC2 執行個體和 OS 組態的目前狀態。有了 Systems Manager，您可以收集有關執行個體機群的軟體組態和庫存資訊，包含安裝在執行個體上的軟體。這可讓您追蹤詳細的系統組態、OS 修補程式等級、應用程式組態，以及有關部署的其他詳細資訊。

如需詳細資訊，請參閱設定 EC2 執行個體的 Systems Manager。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz145
```

來源

```
AWS Config Managed Rule: ec2-instance-managed-by-systems-manager
```

警示條件

黃色：Amazon EC2 執行個體不是由 Systems Manager 管理。

建議的動作

設定 Amazon EC2 執行個體，使其由 Systems Manager 所管理。

無法從 Trusted Advisor 主控台檢視中排除此檢查。

如需詳細資訊，請參閱為何我的 EC2 執行個體未顯示為受管節點，或在 Systems Manager 中顯示「連線中斷」狀態？。

其他資源

設定 EC2 執行個體的 Systems Manager

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則

- 輸入參數
- 上次更新時間

已停用具有標籤不變性的 Amazon ECR 儲存庫

描述

檢查私有 Amazon ECR 儲存庫是否已開啟映像標籤不變性。

開啟私有 Amazon ECR 儲存庫的映像標籤不變性，以防止映像標籤遭覆寫。這可讓您依賴描述性標籤作為追蹤和唯一識別映像的可靠機制。例如，倘若開啟了映像標籤不變性，則使用者便能可靠地使用映像標籤，將已部署的映像版本與產生此類映像的建置版本建立關聯。

如需詳細資訊，請參閱映像標籤可變性。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz129
```

來源

```
AWS Config Managed Rule: ecr-private-tag-immutability-enabled
```

警示條件

黃色：Amazon ECR 私有儲存庫未開啟標籤不變性。

建議的動作

開啟 Amazon ECR 私有儲存庫的映像標籤不變性。

如需詳細資訊，請參閱映像標籤可變性。

報告欄位

- Status
- 區域

- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

已停用具有 Container Insights 的 Amazon ECS 叢集

描述

檢查您的 Amazon ECS 叢集是否已開啟 Amazon CloudWatch 容器深入解析。

CloudWatch Container Insights 會從您的容器化應用程式和微服務收集、彙總和摘要指標和記錄。指標包含 CPU、記憶體、磁碟和網路這類資源的使用率。

如需詳細資訊，請參閱 Amazon ECS CloudWatch 容器深入解析。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz173
```

來源

```
AWS Config Managed Rule: ecs-container-insights-enabled
```

警示條件

黃色：Amazon ECS 叢集未啟用容器洞見。

建議的動作

在 Amazon ECS 叢集上開啟 CloudWatch 容器洞見。

如需詳細資訊，請參閱使用 Container Insights。

其他資源

Amazon ECS CloudWatch 容器見解

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

未啟用 Amazon ECS 任務日誌記錄

描述

檢查日誌組態是否已在作用中的 Amazon ECS 任務定義上設定。

檢查 Amazon ECS 任務定義中的日誌組態可確保容器產生的日誌已正確設定和儲存。如此有助於更快找出問題並進行疑難排解、最佳化效能，以及遵守法規遵循要求。

在預設情況下，擷取的日誌會顯示您在本機執行容器時，通常會在互動式終端機中看見的命令輸出。awslogs 驅動程序將這些日誌從碼頭傳遞到 Amazon 日誌。 CloudWatch

如需詳細資訊，請參閱使用 awslogs 日誌驅動程式。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz175
```

來源

```
AWS Config Managed Rule: ecs-task-definition-log-configuration
```

警示條件

黃色：Amazon ECS 任務定義沒有日誌記錄組態。

建議的動作

請考慮在容器定義中指定記錄驅動程式組態，以將記錄資訊傳送至記 CloudWatch 錄檔或其他記錄驅動程式。

如需詳細資訊，請參閱LogConfiguration。

其他資源

請考慮在容器定義中指定記錄驅動程式組態，以將記錄資訊傳送至記 CloudWatch 錄檔或其他記錄驅動程式。

如需詳細資訊，請參閱任務定義範例。

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

CloudWatch 未設定 Amazon OpenSearch 服務記錄

描述

檢查 Amazon OpenSearch 服務網域是否設定為將日誌傳送到 Amazon CloudWatch 日誌。

監控記錄對於維護 OpenSearch 服務的可靠性、可用性和效能至關重要。

搜尋慢速日誌、索引慢速日誌和錯誤日誌對於疑難排解工作負載的效能和穩定性問題非常有用。必須啟用這些日誌才能擷取資料。

您可以使用 AWS Config 規則中的 logTypes 參數來指定要篩選 (錯誤、搜尋、索引) 的日誌類型。

如需詳細資訊，請參閱監控 Amazon OpenSearch 服務網域。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz184
```

來源

```
AWS Config Managed Rule: opensearch-logs-to-cloudwatch
```

警示條件

黃色：Amazon OpenSearch 服務沒有使用 Amazon CloudWatch 日誌的日誌記錄配置

建議的動作

設定 OpenSearch 服務網域以將記錄檔發佈至 CloudWatch 記錄檔。

如需詳細資訊，請參閱啟用日誌發布 (主控台)。

其他資源

- 使用 Amazon 監控 OpenSearch 服務叢集指標 CloudWatch

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

具有異質參數群組的叢集中的 Amazon RDS 資料庫執行個體

描述

建議資料庫叢集中的所有資料庫執行個體使用相同的資料庫參數群組。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

`c1qf5bt010`

警示條件

黃色：資料庫叢集的資料庫執行個體具有異質參數群組。

建議的動作

將資料庫執行個體與資料庫叢集中的寫入器執行個體相關聯的資料庫參數群組建立關聯。

其他資源

當資料庫叢集中的資料庫執行個體使用不同的資料庫參數群組時，容錯移轉期間可能會出現不一致的行為，或資料庫叢集中的資料庫執行個體之間的相容性問題。

如需詳細資訊，請參閱使用參數群組。

報告欄位

- Status
- 區域
- 資源
- 建議值
- 引擎名稱
- 上次更新時間

Amazon RDS 增強型監控已關閉

描述

您的資料庫資源未開啟增強型監控。增強型監控針對監控及疑難排解，提供即時的作業系統指標。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

`c1qf5bt004`

警示條件

黃色：Amazon RDS 資源未開啟增強型監控功能。

建議的動作

開啟增強型監控。

其他資源

Amazon RDS 的增強型監控可提供更多資料庫執行個體運作狀態的可見性。建議您開啟增強型監控。當資料庫執行個體的增強型監控選項開啟時，它會收集重要的作業系統指標和程序資訊。

如需詳細資訊，請參閱使用增強型監控來監控 OS 指標。

報告欄位

- Status
- 區域
- 資源
- 建議值
- 引擎名稱

- 上次更新時間

Amazon RDS Performance Insights 已關閉

描述

Amazon RDS Performance Insights 可監控您的資料庫執行個體負載，以協助您分析和解決資料庫效能問題。我們建議您開啟 Performance Insights。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

`c1qf5bt012`

警示條件

黃色：Amazon RDS 資源未開啟 Performance Insights。

建議的動作

開啟績效詳情。

其他資源

Performance Insights 使用不會影響應用程式效能的輕量型資料收集方法。Performance Insights 可協助您快速評估資料庫負載。

如需詳細資訊，請參閱使用 Amazon RDS 上的 Performance Insights 來監控資料庫負載。

報告欄位

- Status
- 區域
- 資源
- 建議值
- 引擎名稱
- 上次更新時間

Amazon RDS 跟踪計數參數已關閉

描述

當 track_counts 參數關閉時，資料庫不會收集資料庫活動統計資料。自動清空功能需要這些統計資料才能正常運作。

我們建議您將追蹤計數參數設定為 1

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

> **Note**
>
> 當資料庫執行個體或資料庫叢集停止時，您可以在 Trusted Advisor 3 到 5 天內檢視 Amazon RDS 建議。五天後，建議在中不可用Trusted Advisor。若要檢視建議，請開啟 Amazon RDS 主控台，然後選擇「建議」。
> 如果刪除資料庫執行個體或資料庫叢集，則與這些執行個體或叢集相關聯的建議在 Trusted Advisor Amazon RDS 管理主控台中將無法使用。

檢查 ID

```
c1qf5bt027
```

警示條件

黃色：資料庫參數群組的追蹤計數參數已關閉。

建議的動作

將跟踪計數參數設置為 1

其他資源

當 track_counts 參數關閉時，它會停用資料庫活動統計資料的集合。auto真空daemon 需要收集的統計資料，以識別用於自動真空和自動分析的表格。

如需詳細資訊，請參閱 PostgreSQL 文件網站上的執行階段統計資料。

報告欄位

- Status
- 區域
- 資源
- 參數值
- 建議值
- 上次更新時間

Amazon Redshift 叢集稽核日誌記錄

描述

檢查您的 Amazon Redshift 叢集是否已開啟資料庫稽核日誌記錄。Amazon Redshift 會記錄您資料庫中連線和使用者活動的相關資訊。

您可以在 AWS Config 規則的 bucketNames 參數中指定要符合的所需日誌記錄 Amazon S3 儲存貯體名稱。

如需詳細資訊，請參閱資料庫稽核日誌記錄。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

c18d2gz134

來源

AWS Config Managed Rule: redshift-audit-logging-enabled

警示條件

黃色：Amazon Redshift 叢集已停用資料庫稽核日誌記錄

建議的動作

開啟 Amazon Redshift 叢集的日誌記錄和監控功能。

如需詳細資訊，請參閱使用主控台來設定稽核。

其他資源

在 Amazon Redshift 中記錄和監控

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

Amazon S3 未啟用事件通知

描述

檢查 Amazon S3 事件通知是否已啟用或正確設定為所需的一或多個目的地類型。

Amazon S3 事件通知功能可在 S3 儲存貯體中發生特定事件時傳送通知。Amazon S3 可以將通知訊息傳送至 Amazon SQS 佇列、Amazon SNS 主題和 AWS Lambda 函數。

您可以使用 AWS Config 規則的 destinationArn 和 eventTypes 參數來指定所需的目的地和事件類型。

如需詳細資訊，請參閱 Amazon S3 事件通知。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz163
```

來源

```
AWS Config Managed Rule: s3-event-notifications-enabled
```

警示條件

黃色：Amazon S3 未啟用事件通知，或未設定所需的目的地或類型。

建議的動作

設定物件和儲存貯體事件的 Amazon S3 事件通知。

如需詳細資訊，請參閱使用 Amazon S3 主控台啟用和設定事件通知。

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

Amazon SNS 主題未記錄訊息傳遞狀態

描述

檢查 Amazon SNS 主題是否已開啟訊息傳遞狀態日誌記錄。

設定 Amazon SNS 主題來記錄訊息傳遞狀態，以協助提供更好的操作洞察。例如，訊息傳遞日誌記錄會驗證訊息是否已傳遞至特定 Amazon SNS 端點。此外，它還有助於識別從端點傳送的回應。

如需詳細資訊，請參閱 Amazon SNS 訊息傳遞狀態。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`c18d2gz121`

來源

`AWS Config Managed Rule: sns-topic-message-delivery-notification-enabled`

警示條件

黃色：Amazon SNS 主題未開啟訊息傳遞狀態日誌記錄。

建議的動作

開啟 SNS 主題的訊息傳遞狀態日誌記錄。

如需詳細資訊，請參閱使用 AWS 管理主控台設定傳遞狀態日誌記錄。

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

Amazon VPC (不含流程日誌)

描述

檢查系統是否已為 VPC 建立 Amazon Virtual Private Cloud Flow Logs。

您可以使用 AWS Config 規則中的 trafficType 參數來指定流量類型。

如需詳細資訊，請參閱使用 VPC 流量日誌記錄 IP 流量。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

`c18d2gz122`

來源

`AWS Config Managed Rule: vpc-flow-logs-enabled`

警示條件

黃色：VPC 沒有 Amazon VPC 流程日誌。

建議的動作

為每個 VPC 建立 VPC 流程日誌。

如需詳細資訊，請參閱建立流程日誌。

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

未啟用存取日誌的 Application Load Balancer 和 Classic Load Balancer

描述

檢查 Application Load Balancer 和 Classic Load Balancer 是否已啟用存取日誌。

Elastic Load Balancing 提供存取日誌，可針對傳送到負載平衡器的請求，擷取其詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。您可以使用這些存取日誌來分析流量模式和排除問題。

存取日誌是 Elastic Load Balancing 的選用功能，預設為停用。對負載平衡器啟動存取日誌之後，Elastic Load Balancing 會擷取日誌並存放在您指定的 Amazon S3 儲存貯體中。

您可以使用AWS Config規則中的 s3 BucketNames 參數指定要檢查的存取日誌 Amazon S3 儲存貯體。

如需詳細資訊，請參閱 Application Load Balancer 的存取日誌或 Classic Load Balancer 的存取日誌。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz167
```

來源

```
AWS Config Managed Rule: elb-logging-enabled
```

警示條件

黃色：Application Load Balancer 或 Classic Load Balancer 未啟用存取日誌功能。

建議的動作

啟用 Application Load Balancer 和 Classic Load Balancer 的存取日誌。

如需詳細資訊，請參閱啟用 Application Load Balancer 的存取日誌或啟用 Classic Load Balancer 的存取日誌。

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

AWS CloudFormation 堆疊通知

描述

檢查您的所有 AWS CloudFormation 堆疊是否都使用 Amazon SNS 在事件發生時接收通知。

您可以使用 AWS Config 規則中的參數來設定此檢查，藉此尋找特定的 Amazon SNS 主題 ARN。

如需詳細資訊，請參閱設定 AWS CloudFormation 堆疊選項。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz111
```

來源

```
AWS Config Managed Rule: cloudformation-stack-notification-check
```

警示條件

黃色：AWS CloudFormation 堆疊的 Amazon SNS 事件通知並未開啟。

建議的動作

確保您的 AWS CloudFormation 堆疊會使用 Amazon SNS 在事件發生時接收通知。

監控堆疊事件可協助您快速回應可能會改變 AWS 環境的未經授權動作。

其他資源

當我的 AWS CloudFormation 堆疊進入 ROLLBACK_IN_PROGRESS 狀態時，如何收到電子郵件警示？

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則

- 輸入參數
- 上次更新時間

S3 儲存貯體中物件的 AWS CloudTrail 資料事件日誌記錄

描述

檢查是否至少有一個 AWS CloudTrail 追蹤記錄所有 Amazon S3 儲存貯體的 Amazon S3 資料事件。

如需詳細資訊，請參閱使用 AWS CloudTrail 記錄 Amazon S3 API 呼叫。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz166
```

來源

```
AWS Config Managed Rule: cloudtrail-s3-dataevents-enabled
```

警示條件

黃色：未設定 Amazon S3 儲存貯體的 AWS CloudTrail 事件日誌記錄

建議的動作

啟用 Amazon S3 儲存貯體和物件的 CloudTrail 事件記錄，以追蹤目標儲存貯體存取的請求。

如需詳細資訊，請參閱啟用 S3 儲存貯體和物件的 CloudTrail 事件記錄。

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數

- 上次更新時間

AWS CodeBuild 專案日誌記錄

描述

檢查 AWS CodeBuild 專案環境是否使用日誌記錄。日誌記錄選項可以是 Amazon 日誌中的 CloudWatch 日誌，也可以是建立在指定的 Amazon S3 儲存貯體中，或兩者兼而有之。在 CodeBuild 專案中啟用記錄可提供數個好處，例如偵錯和稽核。

您可以使用AWS Config規則中的 s3 或 Names 參數，指定用於存放 CloudWatch 日誌的 Amazon S33 儲存貯體BucketNames或日誌群組的cloudWatchGroup名稱。

如需詳細資訊，請參閱 監控AWS CodeBuild。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz113
```

來源

```
AWS Config Managed Rule: codebuild-project-logging-enabled
```

警示條件

黃色：未啟用 AWS CodeBuild 專案日誌記錄。

建議的動作

確保您的 AWS CodeBuild 專案中已開啟日誌記錄。無法從 AWS Trusted Advisor 主控台檢視中排除此檢查。

如需詳細資訊，請參閱 AWS CodeBuild 中的日誌記錄和監控。

報告欄位

- Status
- 區域

- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

已啟用 AWS CodeDeploy 自動復原和監控

描述

檢查部署群組是否設定了自動部署復原和附加了警示的部署監視。如果部署期間出現問題，系統會自動回復，而您的應用程式則會保持在穩定狀態

如需詳細資訊，請參閱使用 CodeDeploy.

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz114
```

來源

```
AWS Config Managed Rule: codedeploy-auto-rollback-monitor-enabled
```

警示條件

黃色：未啟用 AWS CodeDeploy 自動部署復原和部署監控。

建議的動作

設定部署群組，或設定部署在部署失敗或到達您指定的監控閾值時自動轉返。

設定警示以在部署程序期間監控各種指標，例如 CPU 使用率、記憶體用量或網路流量。如果這些指標有任何一個超過特定臨界值，就會觸發警示，且部署會停止或回復。

如需為部署群組設定自動回復和設定警示的相關資訊，請參閱設定部署群組的進階選項。

其他資源

什麼是 CodeDeploy？

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

AWS CodeDeployLambda 正在使用 all-at-once 部署組態

描述

檢查AWS Lambda計算平台的AWS CodeDeploy部署群組是否正在使用 all-at-once 部署組態。

為了降低 Lambda 函數部署失敗的風險 CodeDeploy，最佳做法是使用初期測試或線性部署組態，而非預設選項，其中所有流量都會立即從原始 Lambda 函數轉移到更新的函數。

如需詳細資訊，請參閱 Lambda 函數版本和部署組態。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz115
```

來源

```
AWS Config Managed Rule: codedeploy-lambda-allatonce-traffic-shift-
disabled
```

警示條件

黃色：AWS CodeDeployLambda 部署使用 all-at-once 部署組態，將所有流量一次轉移到更新的 Lambda 函數。

建議的動作

針對 Lambda 運算平台使用部 CodeDeploy 署群組的 Canary 或線性部署組態。

其他資源

Deployment configuration (部署組態)

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

未設定 AWS Elastic Beanstalk 增強型運作狀態報告

描述

檢查 AWS Elastic Beanstalk 環境是否已針對增強型運作狀態報告設定。

Elastic Beanstalk 增強型運作狀態報告提供詳細的效能指標，例如 CPU 使用率、記憶體使用率、網路流量和基礎結構運作狀態資訊，例如執行個體數量和負載平衡器狀態。

如需詳細資訊，請參閱增強型運作狀態報告與監控。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz108
```

來源

```
AWS Config Managed Rule: beanstalk-enhanced-health-reporting-enabled
```

警示條件

黃色：Elastic Beanstalk 環境未針對增強型運作狀態報告設定

建議的動作

請確定 Elastic Beanstalk 環境已針對增強型運作狀態報告設定。

如需詳細資訊，請參閱使用 Elastic Beanstalk 主控台啟用增強型運作狀態報告。

其他資源

- 啟用 Elastic Beanstalk 增強型運作狀態報告
- 增強型運作狀態報告與監控

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

已停用具有受管平台更新的 AWS Elastic Beanstalk

描述

檢查是否已啟用 Elastic Beanstalk 環境和組態範本中的受管平台更新。

AWS Elastic Beanstalk 會定期發佈平台更新，來提供修正程式，軟體更新和新功能。有了受管平台更新，Elastic Beanstalk 可以針對新的修補程式和微幅平台版本自動執行平台更新。

您可以在AWS Config規則的UpdateLevel參數中指定所需的更新級別。

如需詳細資訊，請參閱更新 Elastic Beanstalk 環境的平台版本。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz177
```

來源

```
AWS Config Managed Rule: elastic-beanstalk-managed-updates-enabled
```

警示條件

黃色：AWS Elastic Beanstalk 受管平台更新完全未經設定，包含次要或修補程式層級在內。

建議的動作

在您的 Elastic Beanstalk 環境中啟用受管平台更新，或在微幅或更新層級予以設定。

如需詳細資訊，請參閱受管平台更新。

其他資源

- 啟用 Elastic Beanstalk 增強型運作狀態報告
- 增強型運作狀態報告與監控

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

AWS Fargate 平台版本並非最新

描述

檢查 Amazon ECS 是否正在執行最新的 AWS Fargate 之平台版本。Fargate 平台版本表示 Fargate 任務基礎結構的特定執行期環境。此為核心與容器執行期版本的結合。全新平台版本會隨著執行期環境的演進而發布。例如，是否有核心或作業系統更新、全新功能、錯誤修正或安全性更新。

如需詳細資訊，請參閱 Fargate 任務維護。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz174
```

來源

```
AWS Config Managed Rule: ecs-fargate-latest-platform-version
```

警示條件

黃色：Amazon ECS 並未於最新版本的 Fargate 平台上執行。

建議的動作

更新至最新版 Fargate 平台版本。

如需詳細資訊，請參閱 Fargate 任務維護。

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

處於不合規狀態的 AWS Systems Manager State Manager 關聯

描述

在執行個體上執行關聯後，檢查 AWS Systems Manager 關聯法規遵循的狀態為 COMPLIANT 或 NON_COMPLIANT。

狀態管理員 (AWS Systems Manager 的一項功能) 是一項安全且可擴展的組態管理服務，能夠以自動化程序使您的受管節點和其他 AWS 資源維持在您所定義的狀態。狀態管理員關聯是您指派

給 AWS 資源的組態。組態會定義您要在資源上維護的狀態，因此可協助您達成目標，例如避免 Amazon EC2 執行個體之間的組態漂移。

如需詳細資訊，請參閱 AWS Systems Manager 狀態管理員。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz147
```

來源

```
AWS Config Managed Rule: ec2-managedinstance-association-compliance-status-check
```

警示條件

黃色：AWS Systems Manager 關聯法規遵循的狀態為 NON_COMPLIANT。

建議的動作

驗證「狀態管理員」關聯的狀態，然後採取任何必要的行動讓狀態返回 COMPLIANT。

如需詳細資訊，請參閱關於狀態管理員。

其他資源

AWS Systems Manager 狀態管理員

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

CloudTrail 未使用 Amazon CloudWatch 日誌設定追蹤

描述

檢查AWS CloudTrail追蹤是否設定為將記錄檔傳送至 CloudWatch 記錄檔。

使用日 CloudTrail 誌監控 CloudWatch 日誌文件，以在中捕獲重要事件時觸發自動響應AWS CloudTrail。

如需詳細資訊，請參閱使用記 CloudTrail 錄監視 CloudWatch 記錄檔。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz164
```

來源

```
AWS Config Managed Rule: cloud-trail-cloud-watch-logs-enabled
```

警示條件

黃色：AWS CloudTrail未使用 CloudWatch 記錄整合進行設定。

建議的動作

設定 CloudTrail 追蹤以將記錄事件傳送至 CloudWatch 記錄檔。

如需詳細資訊，請參閱建立 CloudTrail 事件 CloudWatch 警示：範例。

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

未針對負載平衡器啟用 Elastic Load Balancing 刪除保護

描述

檢查負載平衡器是否已開啟刪除保護。

Elastic Load Balancing 支援 Application Load Balancer、Network Load Balancer 和 Gateway Load Balancer 的刪除保護。啟用刪除保護以避免您的負載平衡器遭意外刪除。當您建立負載平衡器時，預設會關閉刪除保護。如果您的負載平衡器是生產環境的一部分，請考慮啟用刪除保護。

存取日誌是 Elastic Load Balancing 的選用功能，預設為停用。對負載平衡器啟動存取日誌之後，Elastic Load Balancing 會擷取日誌並存放在您指定的 Amazon S3 儲存貯體中。

如需詳細資訊，請參閱 Application Load Balancer 刪除保護、Network Load Balancer 刪除保護，或 Gateway Load Balancers 刪除保護。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz168
```

來源

```
AWS Config Managed Rule: elb-deletion-protection-enabled
```

警示條件

黃色：未啟用負載平衡器的刪除保護。

建議的動作

開啟 Application Load Balancer、Network Load Balancer 和 Gateway Load Balancer 的刪除保護。

如需詳細資訊，請參閱 Application Load Balancer 刪除保護、Network Load Balancer 刪除保護，或 Gateway Load Balancers 刪除保護。

報告欄位

- Status

- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

RDS 資料庫叢集刪除保護檢查

描述

檢查 Amazon RDS 資料庫叢集是否已啟用刪除保護。

當叢集設定了刪除保護時，任何使用者皆無法刪除資料庫。

刪除保護功能可在所有 AWS 區域中的 Amazon Aurora 和 RDS for MySQL、RDS for MariaDB、RDS for Oracle、RDS for PostgreSQL，以及 RDS for SQL Server 資料庫執行個體上使用。

如需詳細資訊，請參閱 Aurora 叢集的刪除保護。

檢查 ID

```
c18d2gz160
```

來源

```
AWS Config Managed Rule: rds-cluster-deletion-protection-enabled
```

警示條件

黃色：您有未啟用刪除保護的 Amazon RDS 資料庫叢集。

建議的動作

在您建立 Amazon RDS 資料庫叢集時開啟刪除保護。

您可以僅刪除未啟用刪除保護的叢集。啟用刪除保護功能可增加額外的保護層，並避免因意外或非意外刪除資料庫執行個體而導致資料遺失。刪除保護還有助於滿足法規遵循要求，確保業務連續性。

如需詳細資訊，請參閱 Aurora 叢集的刪除保護。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

其他資源

Aurora 叢集的刪除保護

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

RDS 資料庫執行個體自動微幅版本升級檢查

描述

檢查 Amazon RDS 資料庫執行個體是否已設定自動微幅版本升級。

為 Amazon RDS 執行個體開啟自動微幅版本升級，以確保資料庫始終執行最新的安全且穩定的版本。微幅升級提供安全性更新、錯誤修正、效能改善，並維持與現有應用程式的相容性。

如需詳細資訊，請參閱升級資料庫執行個體引擎版本。

> **Note**
>
> 此檢查的結果會每天自動重新整理數次，且不允許重新整理請求。變更可能需要幾個小時才會顯示。目前，您無法從此檢查中排除資源。

檢查 ID

```
c18d2gz155
```

來源

AWS Config Managed Rule: rds-automatic-minor-version-upgrade-enabled

警示條件

黃色：RDS 資料庫執行個體未開啟自動微幅版本升級。

建議的動作

在建立 Amazon RDS 資料庫執行個體時，開啟自動微幅版本升級。

當您開啟微幅版本升級時，若資料庫版本執行的資料庫引擎微幅版本低於手動升級引擎版本，則資料庫版本會自動升級。

報告欄位

- Status
- 區域
- 資源
- AWS Config 規則
- 輸入參數
- 上次更新時間

變更的記錄 AWS Trusted Advisor

如需 Trusted Advisor 檢查的最新變更，請參閱下列主題。

> **Note**
> 如果您使用主 Trusted Advisor 控台或 AWS Support API，則已移除的檢查不會顯示在檢查結果中。如果您使用任何已移除的檢查，例如在 AWS Support API 作業或程式碼中指定檢查 ID，則必須移除這些檢查以避免 API 呼叫錯誤。

如需可用檢查的詳細資訊，請參閱「AWS Trusted Advisor 檢查參考」。

新的容錯能力檢查

Trusted Advisor 在 2024 年 2 月 29 日新增 1 項容錯檢查：

- NLB-私有子網路中的網際網路對向資源

如需更多資訊，請參閱 AWS Trusted Advisor 檢查參考。

新的容錯能力檢查

Trusted Advisor 在 2024 年 1 月 31 日新增 1 項容錯檢查：

- AWS Direct Connect 位置彈性

如需更多資訊，請參閱 AWS Trusted Advisor 檢查參考。

更新容錯檢查

Trusted Advisor 在 2024 年 1 月 8 日修正了 1 次容錯檢查：

- Amazon RDS 日誌 _ 提交參數不是 1

如需更多資訊，請參閱 AWS Trusted Advisor 檢查參考。

更新安全檢查

Trusted Advisor 修訂了 1 年 12 月 21 日的安全檢查：

- AWS Lambda 使用已停用執行階段的函

如需更多資訊，請參閱 AWS Trusted Advisor 檢查參考。

新的安全性和效能檢查

Trusted Advisor 在 2023 年 12 月 20 日增加了 2 次新的安全檢查和 2 次新的性能檢查：

- Amazon EFS 用戶端未使用 data-in-transit 加密
- 針對讀取工作負載佈建不足的 Amazon Aurora 資料庫
- 針對系統容量佈建不足的 Amazon RDS 執行個體
- 具有 Ubuntu LTS 標準支援的 Amazon EC2 執行個體結束

如需更多資訊，請參閱 AWS Trusted Advisor 檢查參考。

新的安全檢查

Trusted Advisor 已於 2023 年 12 月 15 日新增 1 項安全性檢查：

- Amazon 路線 53 不匹配的 CNAME 記錄直接指向 S3 存儲桶

如需更多資訊，請參閱 AWS Trusted Advisor 檢查參考。

新的容錯能力和成本最佳化檢查

Trusted Advisor 在 2023 年 12 月 7 日增加了 2 項新的容錯檢查和 1 項新的「成本最佳化」檢查：

- Amazon DocumentDB 單一可用區叢集
- Amazon S3 不完整的多部分上傳中止組態
- Amazon ECS AWS記錄驅動程式處於封鎖模式

如需更多資訊，請參閱 AWS Trusted Advisor 檢查參考。

新的容錯能力檢查

Trusted Advisor 在 2023 年 11 月 17 日增加了 3 項新的容錯檢查：

- ALB 異地同步備份
- NLB 異地同步備份
- 多個 AZ 中的 VPC 介面端點網路介面

如需更多資訊，請參閱 AWS Trusted Advisor 檢查參考。

Amazon RDS 的新檢查

Trusted Advisor 在 2023 年 11 月 15 日為 Amazon RDS 增加了 37 次新的檢查。

如需更多資訊，請參閱 AWS Trusted Advisor 檢查參考。

新的 AWS Trusted Advisor API

AWS Trusted Advisor 引入新的 API，可讓您以程式設計方式存取 Trusted Advisor 最佳實務檢查、建議和優先順序建議。 Trusted Advisor API 可讓您以程式設計方式 Trusted Advisor 與偏好的作業工具整

合，以大規模自動化和最佳化您的工作負載。新的 API 適用於商業、企業版 Rund 或企業 Support 客戶，可讓您存取帳戶或付款人帳戶中所有連結帳戶的 Trusted Advisor 建議。擁有管理或委派管理員帳戶存取權的 Enterprise Support 客戶，還可以透過程式設計方式擷取組織中已排定優先順

新的 Trusted Advisor API 將取代先前透過 Sup AWS port API (SAPI) 提供的 3 項功能。SAPI 將繼續提供案例和其他支持信息。

Trusted Advisor API 在美國東部 (俄亥俄)、美國東部 (維吉尼亞北部)、美國西部 (奧勒岡)、亞太區域 (首爾)、亞太區域 (雪梨) 和歐洲 (愛爾蘭) 區域一般提供。

要了解更多信息，請訪問 AWS Trusted Advisor API 頁面。

Trusted Advisor 檢查移除

Trusted Advisor 於 2023 年 11 月 9 日移除了以下檢查。

檢查名稱	檢查類別	檢查 ID
EBS 磁碟區應連接至 EC2 執行個體	安全	Hs4Ma3G119
S3 儲存貯體應啟用伺服器端加密	安全	Hs4Ma3G167
CloudFront 分佈應啟用原始訪問身份	安全	Hs4Ma3G195

將 AWS Config 檢查整合到 Trusted Advisor

Trusted Advisor 於 2023 年 10 月 30 AWS Config 日增加了 64 張新支票。

如需更多資訊，請參閱 檢視由 AWS Config 提供技術的 AWS Trusted Advisor 檢查。

新的容錯能力檢查

Trusted Advisor 於 2023 年 10 月 12 日新增了以下檢查。

- Amazon RDS ReplicaLag
- Amazon RDS FreeStorageSpace

- Amazon RDS DiskQueueDepth
- Amazon Route 53 Resolver 端點可用區域備援
- Auto Scaling 在子網路中的可用 IP
- Amazon MSK 代理程式託管過多分割區

如需詳細資訊，請參閱 容錯能力 類別。

全新服務限制檢查

Trusted Advisor 於 2023 年 8 月 17 日新增了以下檢查。

- Lambda 程式碼儲存用量

如需詳細資訊，請參閱 服務限制 類別。

新的容錯能力檢查

Trusted Advisor 於 2023 年 8 月 3 日新增下列檢查。

- AWS Lambda 失敗時事件目的地

如需詳細資訊，請參閱 容錯能力 類別。

全新容錯能力和效能檢查

Trusted Advisor 於 2023 年 6 月 1 日新增下列檢查。

- Amazon EFS 無掛載目標備援
- Amazon EFS 輸送量模式最佳化
- ActiveMQ 可用區域備援
- RabbitMQ 可用區域備援

如需詳細資訊，請參閱 容錯能力 類別和 效能 類別。

新的容錯能力檢查

Trusted Advisor 於 2023 年 5 月 16 日新增了以下檢查。

- NAT Gateway AZ 獨立性
- 單一 AZ 應用程式檢查

如需詳細資訊，請參閱 容錯能力 類別。

新的容錯能力檢查

Trusted Advisor 在 2023 年 4 月 27 日新增了以下檢查。

- 事件管理員複製組 AWS 區域 中的數目
- AWS Resilience Hub 評估年齡

如需詳細資訊，請參閱 容錯能力 類別。

Amazon ECS 容錯檢查的區域擴展

Trusted Advisor 於 2023 年 4 月 27 日將下列支票擴展至其他區域。 Trusted Advisor Amazon ECS 的檢查現在可在所有 Amazon ECS 正式推出的區域中使用。

- Amazon ECS 服務使用單一 AZ
- Amazon ECS Multi-AZ 放置策略

區域拓展至非洲 (開普敦)、亞太區域 (香港)、亞太區域 (海德拉巴)、亞太區域 (雅加達)、亞太區域 (墨爾本)、歐洲 (米蘭)、歐洲 (西班牙)、歐洲 (蘇黎世)、中東 (巴林)、中東 (阿拉伯聯合大公國)。

新的容錯能力檢查

Trusted Advisor 於 2023 年 3 月 30 日新增了以下檢查。

- Amazon ECS 服務使用單一 AZ
- Amazon ECS Multi-AZ 放置策略

如需詳細資訊，請參閱 容錯能力 類別。

新的容錯能力檢查

Trusted Advisor 於 2022 年 12 月 15 日增加了以下檢查。

- AWS CloudHSM 在單一 AZ 中執行 HSM 執行個體的叢集
- Amazon ElastiCache 異地同步備份叢集
- Amazon MemoryDB Multi-AZ 叢集

若要接收 AWS CloudHSM、 ElastiCache和 MemoryDB 叢集的結果，您的可用區域中必須有叢集。Trusted Advisor 如需詳細資訊，請參閱下列 文件：

- AWS CloudHSM 使用者指南
- Amazon MemoryDB for Redis Developer Guide (《Amazon MemoryDB for Redis 開發人員指南》)
- Amazon ElastiCache 的 Redis 用戶指南

Trusted Advisor 於 2022 年 12 月 15 日更新以下檢查資訊。

- AWS Resilience Hub 違反政策 — 應用程式名稱已更新為應用程式名稱
- AWS Resilience Hub 彈性分數 — 應用程式名稱和應用程式彈性分數已更新為應用程式名稱和應用程式彈性

如需詳細資訊，請參閱 容錯能力 類別。

與 Trusted Advisor 整合的更新 AWS Security Hub

Trusted Advisor 於二零二二年十一月十七日作出以下更新。

如果您停用 Security Hub 或 AWS Config AWS 區域， Trusted Advisor 現在會在 7-9 天 AWS 區域 內移除您的控制項發現項目。之前，移除 Security Hub 資料的時間範圍 Trusted Advisor 為 90 天。

如需詳細資訊，請參閱 疑難排解 中的下列章節：

- 我在一個區域關閉了 Security Hub 或 AWS Config
- 我的控制項封存在 Security Hub 中，但我仍然可以在 Trusted Advisor 中看到問題清單。

AWS Resilience Hub的新容錯能力檢查

Trusted Advisor 於 2022 年 11 月 17 日增加了以下檢查。

- AWS Resilience Hub 違反政策
- AWS Resilience Hub 彈性分數

您可以使用這些檢查來檢視應用程式的最新彈性政策狀態和彈性分數。Resilience Hub 可讓您在一個集中的位置，定義、追蹤和管理應用程式的彈性和可用性。

若要接收彈性中樞應 Trusted Advisor 用程式的結果，您必須部署應用 AWS 程式並使用彈性中樞來追蹤應用程式的彈性狀態。如需詳細資訊，請參閱 AWS Resilience Hub 使用者指南。

若要接收 ElastiCache 和 MemoryDB 叢集的結果，您的可用區域中必須有叢集。 Trusted Advisor 如需詳細資訊，請參閱下列 文件：

- Amazon MemoryDB for Redis Developer Guide (《Amazon MemoryDB for Redis 開發人員指南》)
- Amazon ElastiCache 的 Redis 用戶指南

如需詳細資訊，請參閱 容錯能力 類別。

更新到 Trusted Advisor 控制台

Trusted Advisor 在 2022 年 11 月 16 日增加了以下更改。

控制台中的「 Trusted Advisor 儀表板」現在是「 Trusted Advisor 建議」。 Trusted Advisor Recommendations 頁面仍會顯示檢查結果和您的 AWS 帳戶每種類別的可用檢查。

此名稱變更只會更新主 Trusted Advisor 控台。您可以像往常一樣繼續使用 Trusted Advisor 控制台和 AWS Support API 中的 Trusted Advisor 操作。

如需詳細資訊，請參閱 開始使用 Trusted Advisor Recommendations。

Amazon EC2 的新檢查

Trusted Advisor 於 2022 年 9 月 1 日增加了以下檢查。

- Microsoft Windows Server 終止支援的 Amazon EC2 執行個體

如需詳細資訊，請參閱 安全 類別。

將 Security Hub 檢查新增到 Trusted Advisor

自 2022 年 6 月 23 日起， Trusted Advisor 僅支援在 2022 年 4 月 7 日之前提供的 Security Hub 控制項。此版本支援 AWS 基礎安全性最佳作法安全性標準中的所有控制項，但類別中的控制項除外：復原 > 復原。如需詳細資訊，請參閱 檢視 AWS Security Hub 中的 AWS Trusted Advisor 控制項。

如需支援的控制項清單，請參閱《AWS Security Hub 使用者指南》中的 AWS 基礎安全最佳實務控制項。

新增檢查來源 AWS Compute Optimizer

Trusted Advisor 於 2022 年 5 月 4 日增加了以下檢查。

檢查名稱	檢查類別	檢查 ID
Amazon EBS 過度佈建的磁碟區	成本最佳化	COr6dfpM03
Amazon EBS 佈建不足的磁碟區	效能	COr6dfpM04
AWS Lambda 記憶體大小的過度佈建函數	成本最佳化	COr6dfpM05
AWS Lambda 記憶體大小佈建不足的函數	效能	COr6dfpM06

您必須選擇使 AWS 帳戶 用 Compute Optimizer，這些檢查才能從 Lambda 和 Amazon EBS 資源接收資料。如需詳細資訊，請參閱 對於 AWS Compute Optimizer 檢查，選擇使用 Trusted Advisor。

存取金鑰已暴露的檢查更新

Trusted Advisor 於 2022 年 4 月 25 日更新了以下檢查。

檢查名稱	檢查類別	檢查 ID
存取金鑰已暴露	安全	12Fnkpl8Y5

Trusted Advisor 現在會自動為您重新整理此檢查。無法從 Trusted Advisor 主控台或 AWS Support API 手動重新整理此檢查。如果您的應用程式或程式碼為您重新整理此檢查 AWS 帳戶，建議您更新它，以便不再重新整理此檢查。否則，您將收到 `InvalidParameterValue` 錯誤。

在此更新之前排除的任何存取金鑰將不再受到排除，並將顯示為受影響的資源。您無法從檢查結果中排除存取金鑰。如需詳細資訊，請參閱 存取金鑰已暴露。

> **Note**
>
> 如果您是在 2022 年 4 月 25 日 AWS 帳戶 之後建立的，則公開存取金鑰的檢查結果最初會顯示灰色圖示 ()，即使是未公開的存取金鑰也是如此。這表示 Trusted Advisor 尚未識別出檢查有任何變更。如果 Trusted Advisor 識別出有風險的資源，狀態會變更為「建議的動作」圖示 ()。修正或刪除資源後，檢查結果會顯示核取記號圖示 ()。

面向 AWS Direct Connect更新檢查

Trusted Advisor 於 2022 年 3 月 29 日更新下列檢查。

檢查名稱	檢查類別	檢查 ID
AWS Direct Connect 連線備援	容錯能力	`0t121N1Ty3`
AWS Direct Connect 位置冗餘	容錯能力	`8M012Ph3U5`
AWS Direct Connect 虛擬介面備援	容錯能力	`4g3Nt5M1Th`

- Region (區域) 欄的值現在顯示 AWS 區域 程式碼而非全名。例如，美國東部 (維吉尼亞北部) 中的資源現在將有 `us-east-1` 值。
- Time Stamp (時間戳記) 欄的值現在會以 RFC 3339 格式顯示，例如 `2022-03-30T01:02:27.000Z`。
- 未偵測到任何問題的資源現在將顯示在檢查資料表中。這些資源的旁邊將有一個核取記號圖示 ()。

  以前，只有 Trusted Advisor 建議您調查的資源才會顯示在表格中。這些資源的旁邊有一個警告圖示 ()。

AWS Security Hub 已新增至主控 AWS Trusted Advisor 台的控制項

AWS Trusted Advisor 在 2022 年 1 月 18 日，將 111 個安全 Security Hub 控制項新增至「安全性」類別。

您可以從 AWS 基礎安全性最佳作法安全性標準檢視 Security Hub 控制項的發現項目。此整合不包括具有類別：復原 > 彈性的控制項。

如需使用此功能的詳細資訊，請參閱「檢視 AWS Security Hub 中的 AWS Trusted Advisor 控制項」。

新的 Amazon EC2 和 AWS Well-Architected 檢查

Trusted Advisor 於 2021 年 12 月 20 日增加了以下檢查。

- Microsoft SQL 伺服器的 Amazon EC2 執行個體合併
- Microsoft SQL 伺服器過度佈建的 Amazon EC2 執行個體
- Microsoft SQL 伺服器終止支援的 Amazon EC2 執行個體
- AWS Well-Architected 成本最佳化的高風險問題
- AWS Well-Architected 效能的高風險問題
- AWS Well-Architected 安全性的高風險問題
- AWS Well-Architected 可靠性的高風險問題

如需詳細資訊，請參閱 AWS Trusted Advisor 檢查參考。

更新了 Amazon OpenSearch 服務的檢查名稱

Trusted Advisor 於 2021 年 9 月 8 日更新了Amazon OpenSearch Service Reserved Instance Optimization支票名稱。

檢查建議、類別和 ID 相同。

檢查名稱	檢查類別	檢查 ID
Amazon OpenSearch 服務預留實例優化	成本最佳化	7ujm6yhn5t

> **Note**
>
> 如果您用 Trusted Advisor 於 Amazon CloudWatch 指標，則此檢查的指標名稱也會更新。如需詳細資訊，請參閱 建立 Amazon CloudWatch 警示來監控 AWS Trusted Advisor 指標。

新增適用於 Amazon Elastic Block Store 磁碟區儲存的檢查

Trusted Advisor 於 2021 年 6 月 8 日新增以下檢查。

檢查名稱	檢查類別	檢查 ID
EBS 一般用途 SSD (gp3) 磁碟區儲存	服務限額	dH7RR0l6J3
EBS 佈建 IOPS SSD (io2) 磁碟區儲存	服務限制	gI7MM0l7J2

添加了檢查 AWS Lambda

Trusted Advisor 於 2021 年 3 月 8 日新增以下檢查。

檢查名稱	檢查類別	檢查 ID
AWS Lambda 超時功能	成本最佳化	L4dfs2Q3C3
AWS Lambda 具有高錯誤率的函數	成本最佳化	L4dfs2Q3C2
AWS Lambda 使用已停用執行階段的函	安全	L4dfs2Q4C5
AWS Lambda 支援 VPC 功能，不含異地同步備份備援	容錯能力	L4dfs2Q4C6

如需如何將這些檢查與 Lambda 搭配使用的詳細資訊，請參閱AWS Lambda 開發人員指南中檢視建議的範例 AWS Trusted Advisor 工作流程。

Trusted Advisor 檢查移除

Trusted Advisor 刪除了 2021 年 3 月 8 AWS GovCloud (US) Region 日的以下檢查。

檢查名稱	檢查類別	檢查 ID
EC2 彈性 IP 地址	服務限制	aW9HH0l8J6

更新適用於 Amazon Elastic Block Store 的檢查

Trusted Advisor 將 Amazon EBS 卷的單位從吉字節（GiB）更新為太字節（TiB），以便於 2021 年 3 月 5 日進行以下檢查。

> **Note**
>
> 如果您用 Trusted Advisor 於 Amazon CloudWatch 指標，這五個檢查的指標名稱也會更新。如需詳細資訊，請參閱 建立 Amazon CloudWatch 警示來監控 AWS Trusted Advisor 指標。

檢查名稱	檢查類別	檢查 ID	已更新的 CloudWatch 量度 ServiceLimit
EBS 冷 HDD (sc1) 磁碟區儲存	服務限制	gH5CC0e3J9	冷 HDD (sc1) 磁碟區儲存 (TiB)
EBS 一般用途 SSD (gp2) 磁碟區儲存	服務限制	dH7RR0l6J9	一般用途 SSD (gp2) 磁碟區儲存 (TiB)
EBS 磁帶 (標準) 磁碟區儲存	服務限制	cG7HH0l7J9	磁帶 (標準) 磁碟區儲存 (TiB)
EBS 佈建 IOPS SSD (io1) 磁碟區儲存	服務限制	gI7MM0l7J9	佈建 IOPS (SSD) 儲存 (TiB)
EBS 輸送量最佳化 HDD (st1) 磁碟區儲存	服務限制	wH7DD0l3J9	輸送量最佳化 HDD (st1) 磁碟區儲存 (TiB)

Trusted Advisor 檢查移除

> **Note**
>
> Trusted Advisor 於 2020 年 11 月 18 日移除了以下檢查。

2020 年 11 月 18 日已移除檢查	檢查類別	檢查 ID
適用於 EC2 Windows 執行個體的 EC2Config 服務	容錯能力	V77iOLlBqz
適用於 EC2 Windows 執行個體的 ENA 驅動程式版本	容錯能力	TyfdMXG69d
適用於 EC2 Windows 執行個體的 NVMe 驅動程式版本	容錯能力	yHAGQJV9K5
適用於 EC2 Windows 執行個體的 PV 驅動程式版本	容錯能力	Wnwm9Il5bG
EBS 作用中磁碟區	服務限制	fH7LL0l7J9

Amazon Elastic Block Store 不再針對您可以佈建的磁碟區數量限制配額。

您可以監控 Amazon EC2 執行個體，並使用 AWS Systems Manager Distributor 或其他第三方工具，或撰寫您自己的指令碼來傳回 Windows Management Instrumentation (WMI) 的驅動程式資訊。

Trusted Advisor 檢查移除

Trusted Advisor 於 2020 年 2 月 18 日移除以下檢查。

檢查名稱	檢查類別	檢查 ID
服務配額	效能	eW7HH0l7J9

Slack 中的 AWS Support 應用程式

您可以使用 AWS Support 應用程式在 Slack 中管理您的 AWS 支援案例。您可以邀請團隊成員加入聊天頻道、回應案例更新以及直接與支援客服人員聊天。AWS Support 應用程式可幫助您在 Slack 中快速且直接地管理支援案例。

您可以使用 AWS Support 應用程式執行下列動作：

- 在 Slack 頻道中建立、更新、搜尋和解決支援案例
- 將檔案附加至支援案例
- 從 Service Quotas 中請求配額增加
- 在不離開 Slack 頻道的情況下，與您的團隊分享支援案例詳細資訊
- 與支援客服人員開始即時聊天工作階段

如果您在 AWS Support 應用程式中建立、更新或解決支援案例，AWS Support Center Console 中的案例也會更新。您不需要登入支援中心主控台即可單獨管理您的支援案例。

> **備註**
>
> - 無論您是從 Slack 中還是從支援中心主控台中建立案例，支援案例的回應時間都相同。
> - 您可以建立帳戶和帳單支援、服務配額增加以及技術支援的支援案例。

主題

- 在 Slack 中重新開啟支援案例
- 請求增加服務配額
- 從 AWS Support 應用程式中刪除 Slack 頻道組態
- 從 AWS Support 應用程式中刪除 Slack 工作區組態
- Slack 命令中的 AWS Support 應用程式
- 在 AWS Support Center Console 中檢視 AWS Support 應用程式通訊
- 使用 AWS CloudFormation 在 Slack 資源中建立 AWS Support 應用程式

先決條件

您必須符合下述要求，才能在 Slack 中使用 AWS Support 應用程式：

- 您具備商業、Enterprise On-Ramp 或企業支援計劃。您可以在 AWS Support Center Console 中或支援計劃頁面中找到您的支援計劃。如需詳細資訊，請參閱比較 AWS Support 計劃。
- 您有一個適合您組織的 Slack 工作區和頻道。您必須是 Slack 工作區管理員，或具有將應用程式新增至該 Slack 工作區的許可。如需詳細資訊，請參閱 Slack 說明中心。
- 您作為擁有所需許可的 AWS Identity and Access Management (IAM) 使用者或角色登入 AWS 帳戶。如需更多詳細資訊，請參閱 管理 AWS Support 應用程式小工具的存取權。
- 您將需要建立 IAM 角色，該角色具有所需的許可，以便為您執行動作。AWS Support 應用程式使用此角色對不同的服務進行 API 呼叫。如需更多詳細資訊，請參閱 管理 AWS Support 應用程式的存取權。

主題

- 管理 AWS Support 應用程式小工具的存取權
- 管理 AWS Support 應用程式的存取權

管理 AWS Support 應用程式小工具的存取權

您可以連接 AWS Identity and Access Management (IAM) 政策，授予 IAM 使用者在 AWS Support Center Console 中設定 AWS Support 應用程式小工具的許可。

如需有關如何將政策新增至 IAM 實體的詳細資訊，請參閱《IAM 使用者指南》中的新增 IAM 身分許可 (主控台)。

> **Note**
>
> 您也可以在 AWS 帳戶 中以根使用者身分登入，但我們不建議您這麼做。如需根使用者存取權的詳細資訊，請參閱《IAM 使用者指南》中的保護您的根使用者憑證，不要將其用於日常任務。

IAM 政策範例

您可以將以下政策連接至實體，例如 IAM 使用者或群組。此政策可讓使用者授權 Slack 工作區，並在支援中心主控台中設定 Slack 頻道。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportapp:GetSlackOauthParameters",
                "supportapp:RedeemSlackOauthCode",
                "supportapp:DescribeSlackChannels",
                "supportapp:ListSlackWorkspaceConfigurations",
                "supportapp:ListSlackChannelConfigurations",
                "supportapp:CreateSlackChannelConfiguration",
                "supportapp:DeleteSlackChannelConfiguration",
                "supportapp:DeleteSlackWorkspaceConfiguration",
                "supportapp:GetAccountAlias",
                "supportapp:PutAccountAlias",
                "supportapp:DeleteAccountAlias",
                "supportapp:UpdateSlackChannelConfiguration",
                "iam:ListRoles"
            ],
            "Resource": "*"
        }
    ]
}
```

將 AWS Support 應用程式連接至 Slack 所需的許可

該 AWS Support 應用程式包含非直接對應至 API 操作的僅限許可動作。這些動作在《服務授權參考》中以 [僅限許可] 標示。

該 AWS Support 應用程式使用以下 API 動作連接至 Slack，然後在AWS Support Center Console 中列出您的 公有 Slack 通道：

- `supportapp:GetSlackOauthParameters`
- `supportapp:RedeemSlackOauthCode`
- `supportapp:DescribeSlackChannels`

這些 API 動作並非預期要由您的程式碼呼叫。因此，AWS CLI 和 AWS 軟體開發套件中未包含這些 API 動作。

管理 AWS Support 應用程式的存取權

擁有 AWS Support 應用程式小工具的許可後，您也必須建立 AWS Identity and Access Management (IAM) 角色。此角色為您執行來自其他 AWS 服務 的動作，例如 AWS Support API 和 Service Quotas。

然後，您可以將 IAM 政策附加到此角色，以便該角色擁有完成這些動作的必要許可。您可以在支援中心主控台中建立 Slack 頻道組態時選擇此角色。

Slack 頻道中的使用者擁有與您授予給 IAM 角色相同的許可。例如，如果您對支援案例指定唯讀存取權，則 Slack 頻道中的使用者可以檢視您的支援案例，但無法更新它們。

> **Important**
>
> 當您請求與支援客服人員進行即時聊天並選擇新的私有頻道作為即時聊天頻道偏好時，AWS Support 應用程式會建立個別的 Slack 頻道。此 Slack 頻道擁有與您建立案例或啟動聊天的頻道相同的許可。
>
> 如果您變更 IAM 角色或 IAM 政策，您所做的變更將套用至您設定的 Slack 頻道以及 AWS Support 應用程式為您建立的任何新的即時聊天 Slack 頻道。

請依照這些程序建立 IAM 角色和政策。

主題

使用 AWS 受管政策或建立客戶管理政策

若要授與您的角色許可，您可以使用 AWS 受管政策或者客戶管理政策。

> **Tip**
>
> 如果不想手動建立政策，則可以改用 AWS 受管政策，並跳過此程序。受管政策會自動擁有 AWS Support 應用程式的必要許可。您不需要手動更新政策。如需更多詳細資訊，請參閱 AWS 適用於 Slack 中 AWS Support 應用程式的受管政策。

請遵循此程序，為您的角色建立客戶管理政策。此程序在 IAM 主控台中使用 JSON 政策編輯器。

為 AWS Support 應用程式建立客戶管理政策

1. 登入 AWS Management Console，並開啟位於 https://console.aws.amazon.com/iam/ 的 IAM 主控台。
2. 在導覽窗格中，選擇 政策 。
3. 選擇 Create policy (建立政策)。
4. 請選擇 JSON 標籤。
5. 輸入您的 JSON，然後在編輯器中取代預設 JSON。您可以使用範例政策。
6. 選擇 下一步：標籤 。
7. (選用) 您可使用標籤作為金鑰值對，將中繼資料新增至政策。
8. 選擇 下一步：檢閱 。
9. 在 Review policy (檢閱政策) 頁面，輸入 Name (名稱) (例如 *AWSSupportAppRolePolicy*) 和 Description (說明) (選用)。
10. 檢閱 Summary (摘要) 頁面以查看政策允許的許可，然後選擇 Create policy (建立政策)。

此政策定義角色可以採取的動作。若需詳細資訊，請參閱《IAM 使用者指南》中的建立 IAM 政策 (主控台)。

IAM 政策範例

可將下列範例政策連接至您的 IAM 角色。此政策允許角色擁有 AWS Support 應用程式的所有必要動作的完整許可。使用該角色設定 Slack 頻道後，頻道中的任何使用者都擁有相同的許可。

> **Note**
>
> 如需 AWS 管理政策的清單，請參閱 AWS 適用於 Slack 中 AWS Support 應用程式的受管政策。

您可以更新政策，以便從 AWS Support 應用程式中移除許可。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "servicequotas:GetRequestedServiceQuotaChange",
                "servicequotas:GetServiceQuota",
                "servicequotas:RequestServiceQuotaIncrease",
                "support:AddAttachmentsToSet",
                "support:AddCommunicationToCase",
                "support:CreateCase",
                "support:DescribeCases",
                "support:DescribeCommunications",
                "support:DescribeSeverityLevels",
                "support:InitiateChatForCase",
                "support:ResolveCase"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"iam:AWSServiceName": "servicequotas.amazonaws.com"}
            }
        }
    ]
}
```

如需每個動作的說明，請參閱《服務授權參考》中的下列主題：

- 適用於 AWS Support 的動作、資源及條件金鑰

- Service Quotas 的動作、資源和條件金鑰
- 適用於 AWS Identity and Access Management 的動作、資源及條件金鑰

建立 IAM 角色

具有政策之後，必須建立 IAM 角色，並將政策連接到該角色。您可以在支援中心主控台中建立 Slack 頻道組態時選擇此角色。

若要為 AWS Support 應用程式建立角色

1. 登入 AWS Management Console，並開啟位於 https://console.aws.amazon.com/iam/ 的 IAM 主控台。
2. 在導覽窗格中，選擇 Roles (角色)，然後選擇 Create role (建立角色)。
3. 在 Select trusted entity (選取受信任實體) 中，請選擇 AWS 服務。
4. 選擇 AWS Support 應用程式。
5. 選擇 Next: Permissions (下一步：許可)。
6. 輸入政策名稱。您可以選擇 AWS 管理政策，或者選擇您建立的客戶管理政策，例如 *AWSSupportAppRolePolicy*。然後選取政策旁的核取方塊。
7. 選擇 下一步：標籤 。
8. (選用) 您可使用標籤作為金鑰值對，將中繼資料新增至角色。
9. 選擇 下一步：檢閱 。
10. 針對 Role name (角色名稱)，輸入名稱，例如 *AWSSupportAppRole*。
11. (選用) 在 Role description (角色說明) 中，輸入角色的說明。
12. 檢閱角色，然後選擇 Create role (建立角色)。現在可在支援中心主控台中建立 Slack 頻道時選擇此角色。請參閱 設定 Slack 頻道。

如需詳細資訊，請參閱《IAM 使用者指南》中的建立 AWS 服務的角色。

疑難排解

請參閱下列主題，以管理 AWS Support 應用程式的存取權。

內容

- 我想限制 Slack 頻道中的特定使用者執行特定動作

- 當我設定 Slack 頻道時，看不到我建立的 IAM 角色
- 我的 IAM 角色缺少許可
- Slack 錯誤表示我的 IAM 角色無效
- AWS Support 應用程式指示我缺少 Service Quotas 的 IAM 角色

我想限制 Slack 頻道中的特定使用者執行特定動作

根據預設，Slack 頻道中的使用者擁有連接到您建立的 IAM 角色的 IAM 政策中指定的相同許可。這意味著頻道中的任何人都可以讀取或寫入您的支援案例，無論他們是否擁有 AWS 帳戶 或 IAM 使用者。

建議遵循下列最佳實務：

- 使用 AWS Support 應用程式設定私有 Slack 頻道
- 僅邀請需要存取支援案例的使用者加入您的頻道
- 使用對 AWS Support 應用程式具有最低所需許可的 IAM 政策。請參閱 AWS 適用於 Slack 中 AWS Support 應用程式的受管政策。

當我設定 Slack 頻道時，看不到我建立的 IAM 角色

如果您的 IAM 角色未出現在 AWS Support 應用程式的 IAM 角色清單中，這意味著該角色沒有將 AWS Support 應用程式當作受信任的實體，或者該角色已遭刪除。您可以更新現有角色，或建立新角色。請參閱 建立 IAM 角色。

我的 IAM 角色缺少許可

您為 Slack 頻道建立的 IAM 角色需要許可才能執行您想要的動作。例如，如果您希望 Slack 中的使用者建立支援案例，則該角色必須具有 `support:CreateCase` 許可。AWS Support 應用程式承擔此角色來為您執行這些動作。

如果您收到關於 AWS Support 應用程式缺少許可的錯誤，請確認附加至您角色的政策是否具有所需許可。

請參閱之前的 IAM 政策範例。

Slack 錯誤表示我的 IAM 角色無效

請確認您為頻道組態選擇了正確的角色。

若要驗證角色

1. 在 https://console.aws.amazon.com/support/app#/config 頁面登入 AWS Support Center Console。
2. 選擇您使用 AWS Support 應用程式設定的頻道。
3. 在 Permissions (許可) 區段中，尋找您選擇的 IAM 角色名稱。
   - 若要變更角色，請選擇 Edit (編輯)，選擇其他角色，然後選擇 Save (儲存)。
   - 若要更新角色或連接至角色的政策，請登入 IAM 主控台。

AWS Support 應用程式指示我缺少 Service Quotas 的 IAM 角色

您必須在帳戶中擁有 `AWSServiceRoleForServiceQuotas` 角色，才能從 Service Quotas 中請求增加配額。如果您收到有關缺少資源的錯誤，請完成下列其中一個步驟：

- 使用 Service Quotas 主控台請求增加配額。請求成功後，Service Quotas 會自動為您建立此角色。然後，您可以使用 AWS Support 應用程式在 Slack 中請求增加配額。如需詳細資訊，請參閱請求增加配額。
- 更新連接至您角色的 IAM 政策。這會將角色許可授予給 Service Quotas。IAM 政策範例 中的以下部分允許 AWS Support 應用程式為您建立 Service Quotas 角色。

```
{
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "*",
    "Condition": {
        "StringEquals": {"iam:AWSServiceName": "servicequotas.amazonaws.com"}
     }
}
```

如果刪除您為頻道設定的 IAM 角色，則必須手動建立角色或更新 IAM 政策，以允許 AWS Support 應用程式為您建立一個角色。

授權 Slack 工作區

在您授權工作區並授予 AWS Support 應用程式存取它的許可之後，您需要一個適用於 AWS 帳戶的 AWS Identity and Access Management (IAM) 角色。AWS Support 應用程式使用此角色從 AWS

Support 和 Service Quotas 中為您呼叫 API 操作。例如，AWS Support 應用程式使用該角色來呼叫 `CreateCase` 操作，以在 Slack 中為您建立支援案例。

> **備註**
>
> - Slack 頻道會繼承 IAM 角色的許可。這意味著 Slack 頻道中的任何使用者都擁有與該角色相連的 IAM 政策中指定的相同許可。
>
> 例如，如果您的 IAM 政策允許該角色對您的支援案例具有完整讀取和寫入許可，則 Slack 頻道中的任何人都可以建立、更新和解決您的支援案例。如果您的 IAM 政策允許角色唯讀許可，則 Slack 頻道中的使用者僅具有支援案例的讀取許可。
> - 建議您新增管理支援操作所需的 Slack 工作區和頻道。建議您設定私有頻道，並僅邀請必要的使用者。

必須授權要用於您的 AWS 帳戶 之每個 Slack 工作區。如果您有多個 AWS 帳戶，您必須登入每個帳戶並重複下列程序來授權工作區。如果您的帳戶屬於 AWS Organizations 中的組織並且您想授權多個帳戶，請跳至授權多個帳戶。

若要為您的 AWS 帳戶 授權 Slack 工作區

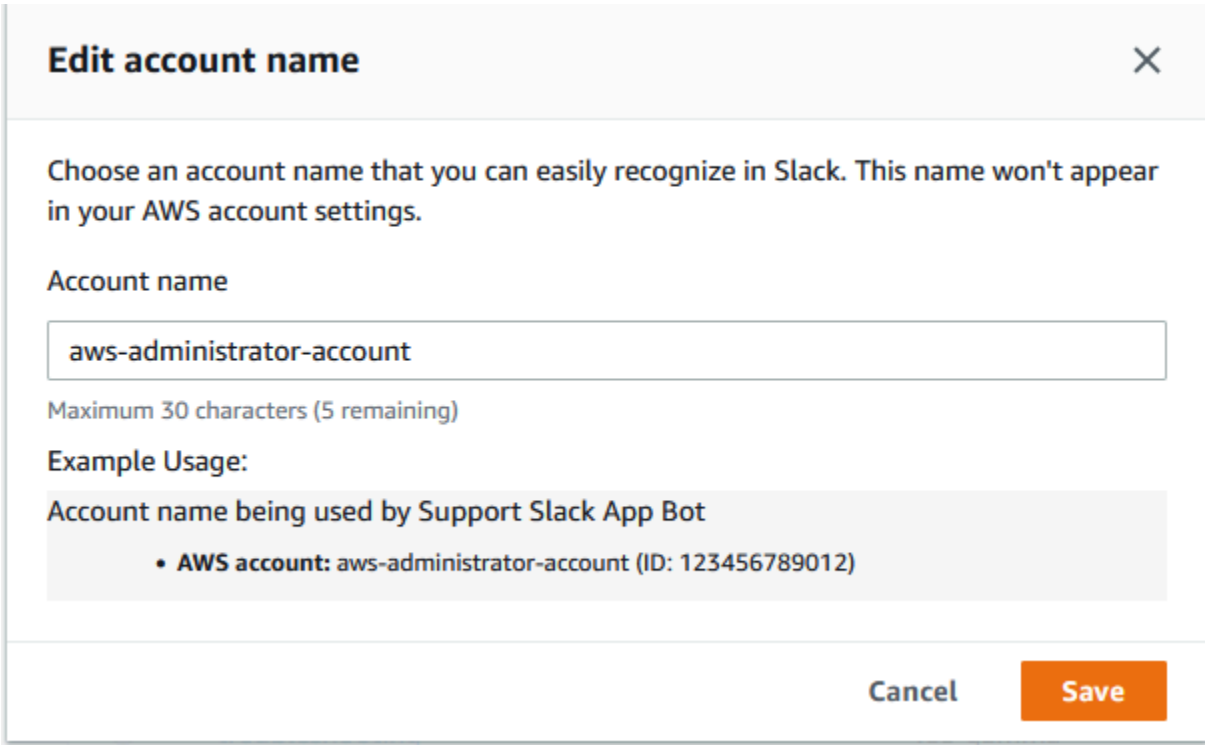
1. 登入 AWS Support Center Console 並選擇 Slack configuration (Slack 組態)。
2. 在 Getting started (入門) 頁面中，選擇 Authorize workspace (授權工作區)。
3. 如果您尚未登入 Slack，在 Sign in to your workspace (登入工作區) 頁面中，輸入您的工作區名稱，然後選擇 Continue (繼續)。
4. 在 AWS Support 正在請求許可來存取 your-workspace-name Slack 頁面中，選擇允許。

   > **Note**
   >
   > 如果您無法允許 Slack 存取您的工作區，請確認您擁有 Slack 管理員的許可，以便將 AWS Support 應用程式新增至工作區。請參閱 先決條件。

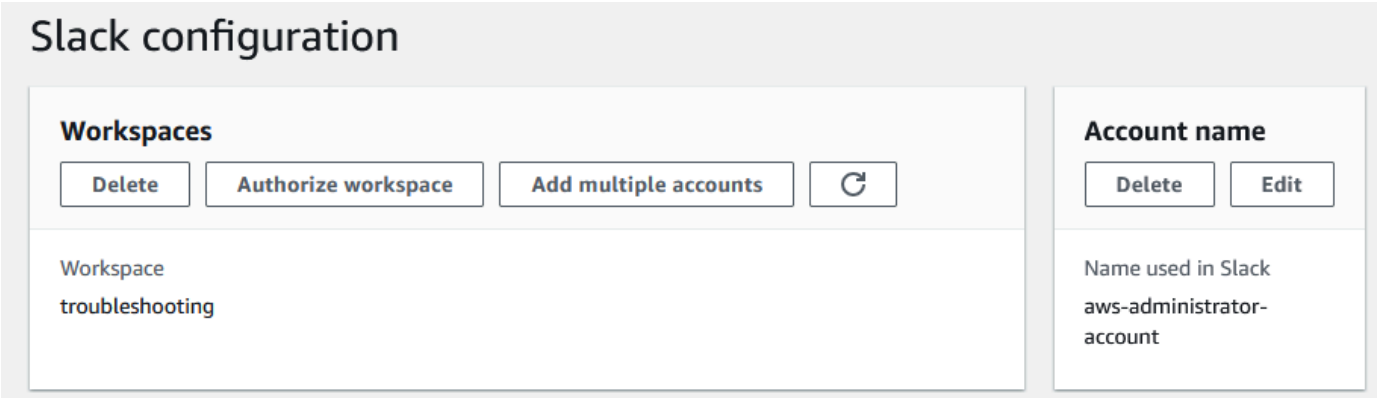
   在 Slack configuration (Slack 組態) 頁面中，您的工作區名稱會出現在 Workspaces (工作區) 中。
5. (選用) 若要新增更多工作區，請選擇 Authorize workspace (授權工作區) 並重複步驟 3-4。您最多可以將五個工作區新增到您的帳戶。

6. (選用) 根據預設，您的 AWS 帳戶 ID 號碼會在 Slack 頻道中顯示為帳戶名稱。若要變更此值，請在 Account name (帳戶名稱) 中，選擇 Edit (編輯)，輸入您的帳戶名稱，然後選擇 Save (儲存)。

> **Tip**
>
> 使用您和您的團隊可以輕鬆識別的名稱。AWS Support 應用程式會使用此名稱來識別您在 Slack 頻道中的帳戶。您可隨時更新此名稱。



您的工作區和帳戶名稱會顯示在 Slack configuration (Slack 組態) 頁面中。



授權多個帳戶

若要授權多個 AWS 帳戶 使用 Slack 工作區，您可以使用 AWS CloudFormation 或 Terraform 來建立您的 AWS Support 應用程式資源。

設定 Slack 頻道

授權 Slack 工作區後，您可以設定 Slack 頻道以使用 AWS Support 應用程式。

您可以在邀請並新增 AWS Support 應用程式的頻道中建立和搜尋案例，並接收案例通知。此頻道會顯示案例更新，例如新建立或已解決的案例、新增的通訊以及共用的案例詳細資訊。

Slack 頻道會繼承 IAM 角色的許可。這意味著 Slack 頻道中的任何使用者都擁有與該角色相連的 IAM 政策中指定的相同許可。

例如，如果您的 IAM 政策允許該角色對您的支援案例具有完整讀取和寫入許可，則 Slack 頻道中的任何人都可以建立、更新和解決您的支援案例。如果您的 IAM 政策允許角色唯讀許可，則 Slack 頻道中的使用者僅具有支援案例的讀取許可。

一個帳戶最多可新增 20 個頻道。Slack 頻道最多擁有 100 個 AWS 帳戶。這意味著只有 100 個帳戶可以將相同的 Slack 頻道新增到 AWS Support 應用程式。我們建議您只新增管理組織支援案例所需的帳戶。這樣可以減少您在頻道中收到的通知數量，從而減少您和團隊的干擾。

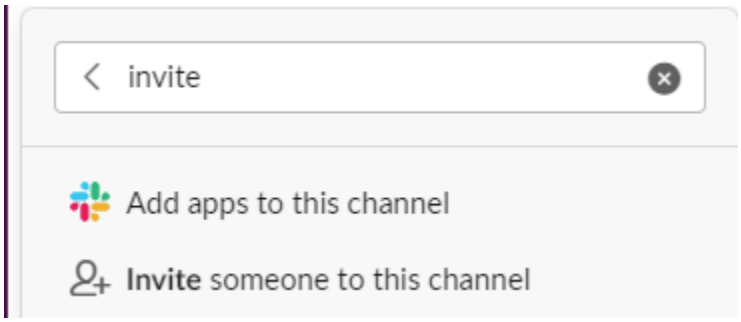
每個 AWS 帳戶 必須在 AWS Support 應用程式中分別設定 Slack 頻道。這樣，AWS Support 應用程式就可在 AWS 帳戶 中存取支援案例。如果組織中的另一個 AWS 帳戶 已將 AWS Support 應用程式邀請至 Slack 頻道，請跳至步驟 3。

> **Note**
>
> 您可以設定屬於 Slack Connect 一部分的頻道，以及與多個工作區共用的頻道。不過，只有第一個設定了 AWS 帳戶 共用頻道的工作區可以使用 AWS Support 應用程式。如果您嘗試為另一個工作區設定相同的 Slack 頻道，AWS Support 應用程式會傳回錯誤訊息。

若要設定 Slack 頻道

1. 在您的 Slack 應用程式中，選擇要與 AWS Support 應用程式搭配使用的 Slack 頻道。
2. 完成以下步驟，將 AWS Support 應用程式邀請到您的頻道：

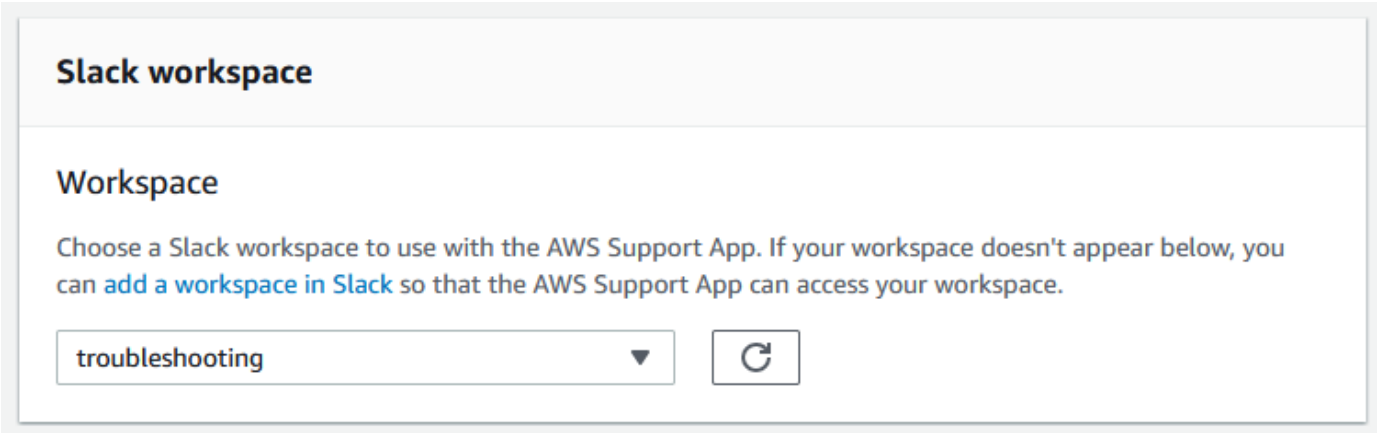
a. 選擇 + 圖示並輸入 `invite`，然後在出現提示時選擇 Add apps to this channel (將應用程式新增至此頻道)。



b. 若要搜尋應用程式，請在 Add apps to channelName (將應用程式新增至 channelName) 中輸入 AWS Support App。

c. 選擇 AWS Support 應用程式旁的新增。

3. 登入支援中心主控台並選擇Slack configuration (Slack 組態)。
4. 選擇 Add channel (新增頻道)。
5. 在 Add channel (新增頻道) 頁面的 Workspace (工作區) 中，選擇您先前授權的工作區名稱。如果工作區名稱未出現在清單中，您可以選擇重新整理圖示。



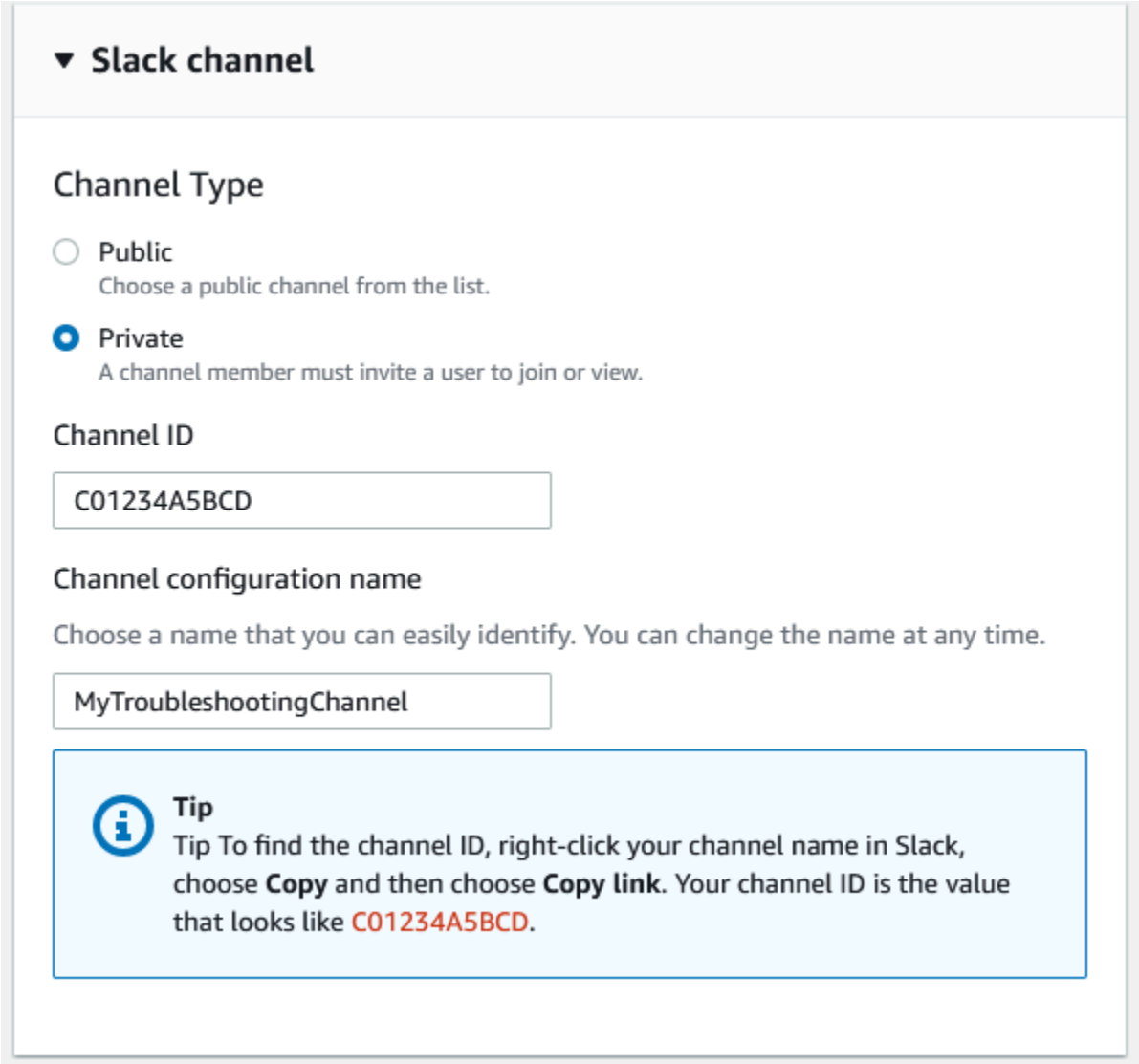
6. 在 Slack channel (Slack 頻道) 中，針對 Channel type (頻道類型)，選擇下列其中一項：
   - public (公有) - 在 Public channel (公有頻道) 中，選擇您為其邀請 AWS Support 應用程式的 Slack 頻道 (步驟 2)。如果您的頻道未出現在清單中，請選擇重新整理圖示，然後再試一次。

- Private (私有) - 在 Channel ID (頻道 ID) 中，輸入您為其邀請 AWS Support 應用程式的 Slack 頻道的 ID 或 URL。

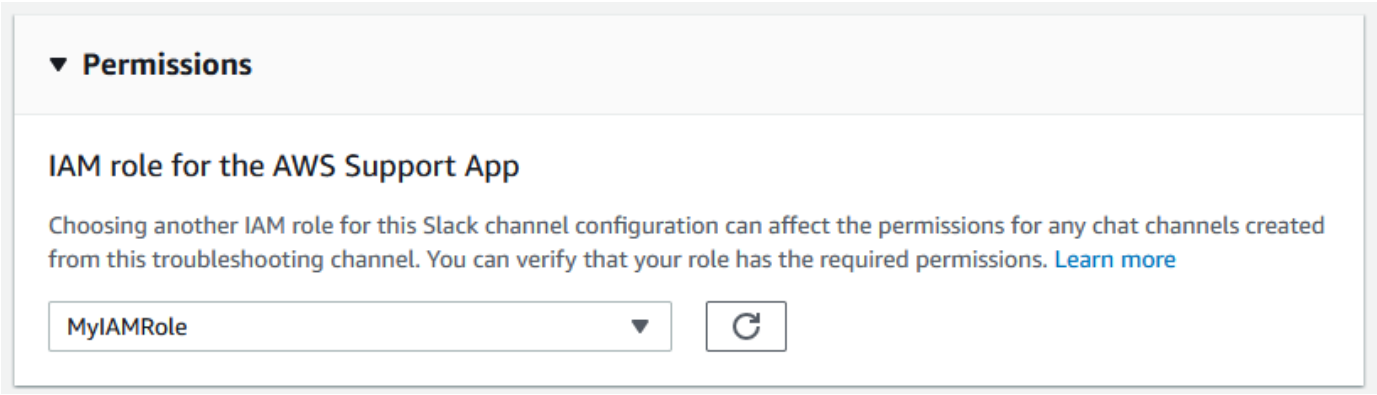
  > **Tip**
  >
  > 若要尋找頻道 ID，請在 Slack 中開啟頻道名稱的內容 (按一下滑鼠右鍵) 選單，選擇 Copy (複製)，然後選擇 Copy link (複製連結)。頻道 ID 是看起來像 *C01234A5BCD* 的值。

7. 在 Channel configuration name (頻道組態名稱) 中，輸入可輕鬆識別 AWS Support 應用程式的 Slack 頻道組態的名稱。此名稱僅出現在您的 AWS 帳戶 中，不會出現在 Slack 中。您可以稍後重新命名頻道組態。

   Slack 頻道類型看起來可能如以下範例所示。



8. 在許可下，針對適用於 Slack 中 AWS Support 應用程式的 IAM 角色，選擇您為 AWS Support 應用程式建立的角色。清單中只會顯示將 AWS Support 應用程式作為受信任實體的角色。



> **Note**
>
> 如果您尚未建立角色或在清單中看不到您的角色，請參閱 管理 AWS Support 應用程式的存取權。

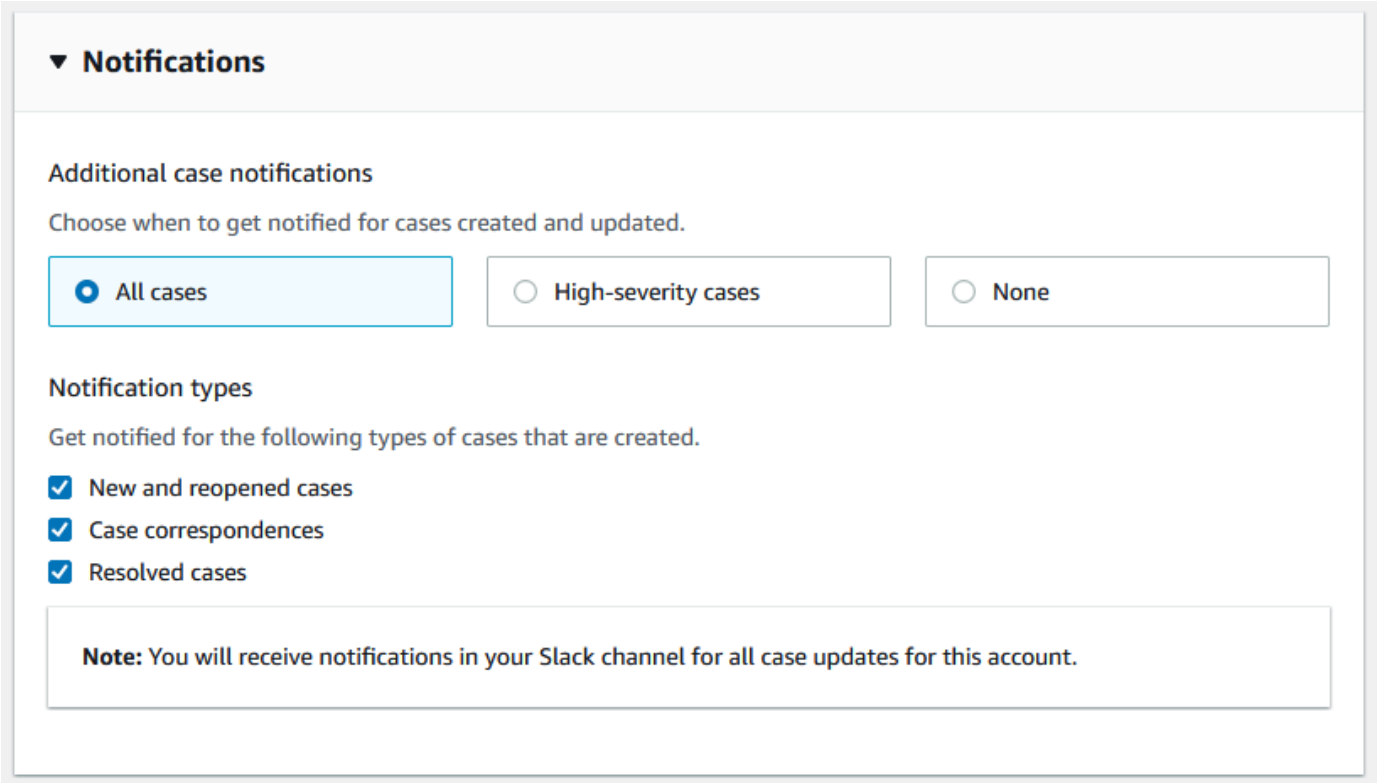
9. 在 Notifications (通知) 中，指定如何獲取案例通知。

   - All cases (所有案例) - 獲取所有案例更新的通知。
   - High-severity cases (高嚴重性案例) - 僅獲取影響生產系統或更嚴重情況的案例通知。如需更多詳細資訊，請參閱 選擇嚴重性。
   - None (無) - 不獲取案例更新的通知。

10. (選用) 如果您選擇 All cases (所有案例) 或者 High-severity cases (高嚴重性案例)，您必須至少選取下列其中一個選項：

    - New and reopened cases (新的和重新開啟的案例)
    - Case correspondences (案例通訊)
    - Resolved cases (已解決的案例)

    下列頻道會收到 Slack 中所有案例更新的案例通知。



11. 檢閱您的組態並選擇 Add channel (新增頻道)。您的頻道會顯示在 Slack configuration (Slack 組態) 頁面中。

更新您的 Slack 頻道組態

設定 Slack 頻道後，您可以稍後更新它們以變更 IAM 角色或案例通知。

若要更新您的 Slack 頻道組態

1. 登入支援中心主控台並選擇Slack configuration (Slack 組態)。
2. 在 Channels (頻道) 中，選擇您想要的頻道組態。
3. 在 ***channelName*** (頻道名稱) 頁面中，您可以執行下列任務：
   - 選擇 Rename (重新命名) 更新您的頻道組態名稱。此名稱僅出現在您的 AWS 帳戶 中，不會出現在 Slack 中。
   - 選擇 Delete (刪除)，從 AWS Support 應用程式中刪除頻道組態。請參閱 從 AWS Support 應用程式中刪除 Slack 頻道組態。
   - 選擇 Open in Slack (在 Slack 中開啟)，在瀏覽器中開啟 Slack 頻道。
   - 選擇 Edit (編輯)，變更 IAM 角色或通知。

在 Slack 頻道中建立支援案例

在您授權 Slack 工作區並新增 Slack 頻道後，可以在 Slack 頻道中建立支援案例。

若要在 Slack 中建立支援案例

1. 在 Slack 頻道中，輸入下列命令：

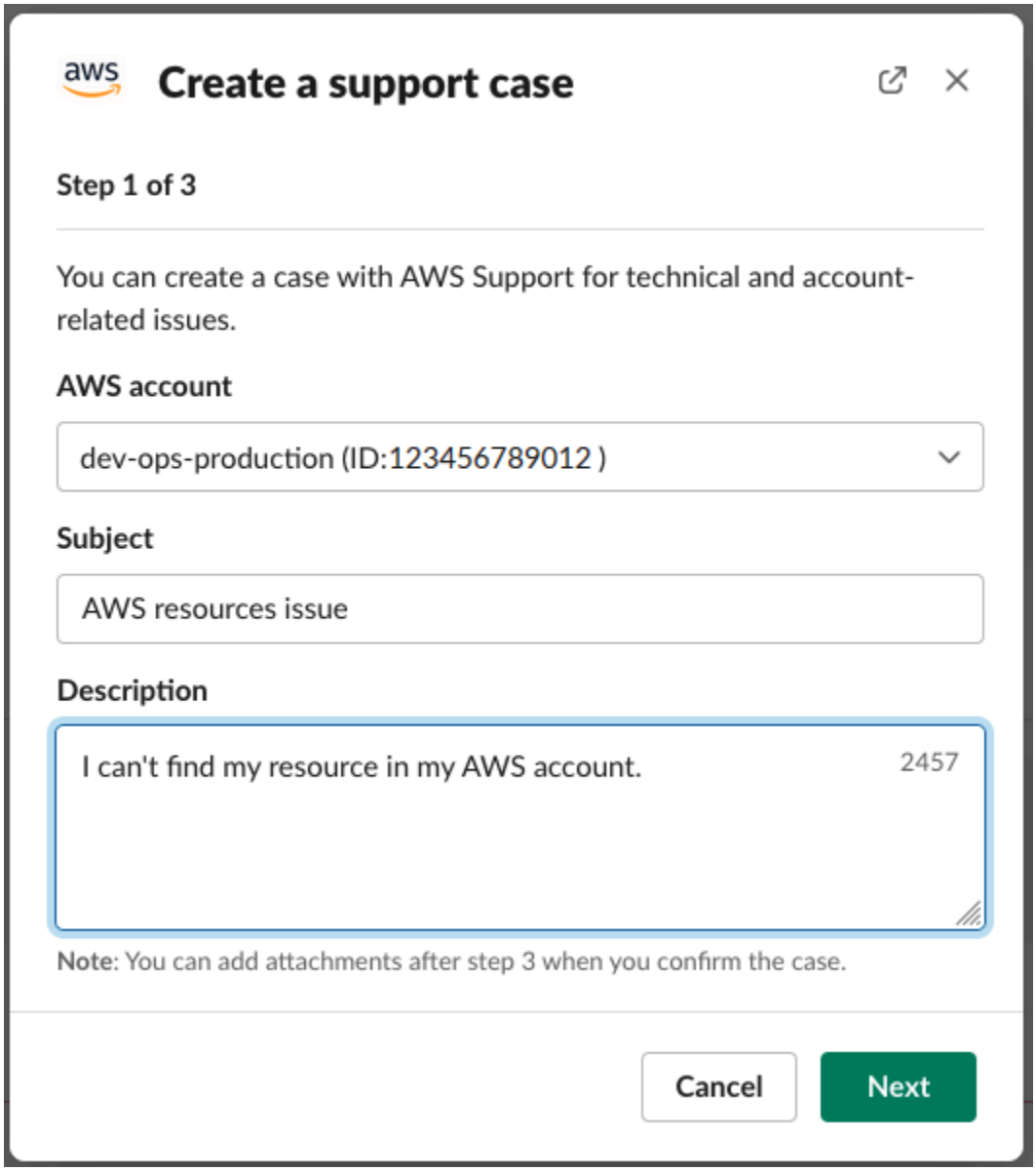
   ```
   /awssupport create
   ```

2. 在 Create a support case (建立支援案例) 對話方塊中，執行下列動作：

   a. 如果您為此 Slack 頻道設定了多個帳戶，對於 AWS 帳戶，請選擇帳戶 ID。如果您已建立帳戶名稱，此值會顯示在帳戶 ID 旁邊。如需更多詳細資訊，請參閱 授權 Slack 工作區。

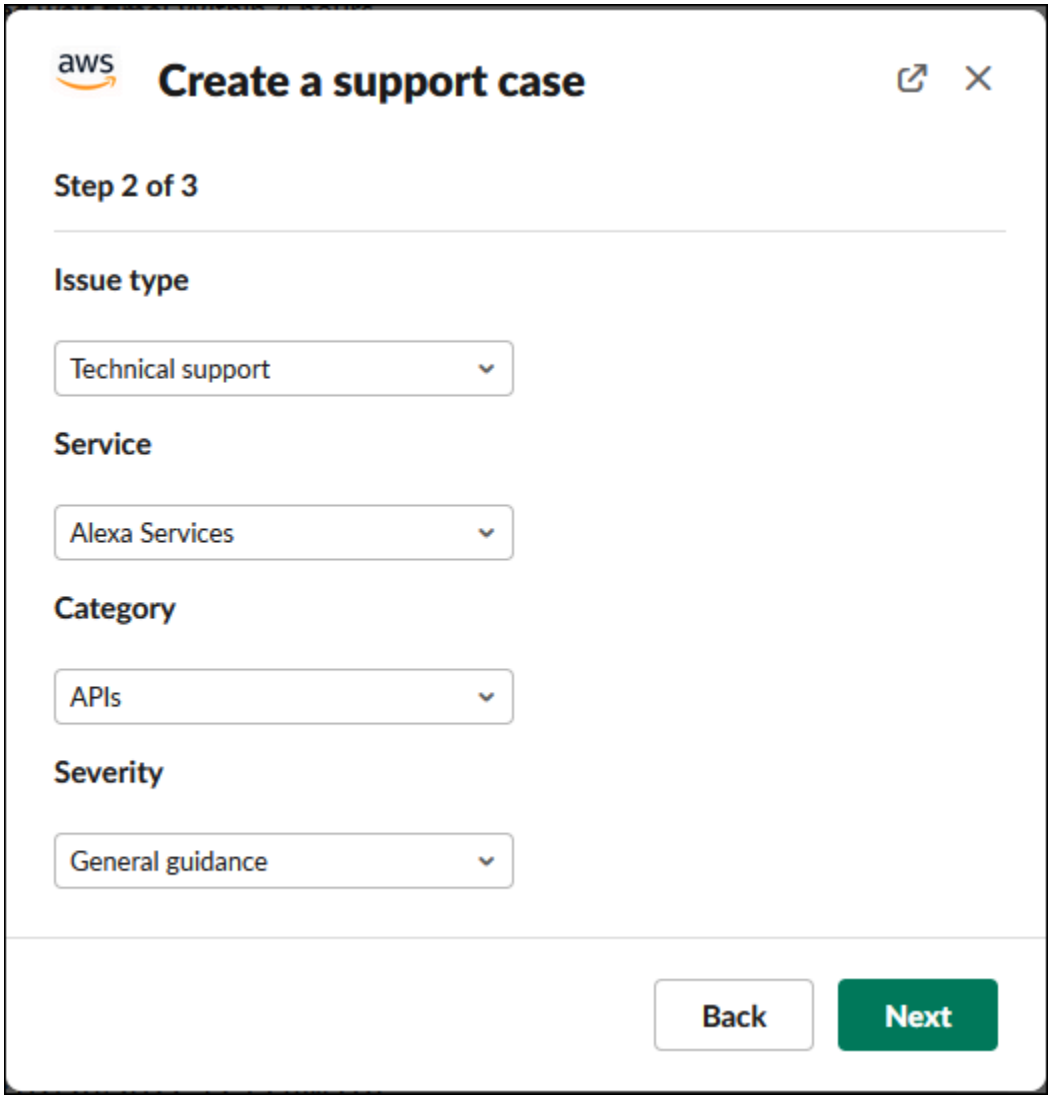
   b. 對於 Subject (主旨)，輸入支援案例的標題。

   c. 對於 Description (說明)，請說明您的支援案例。提供詳細資訊，例如您使用 AWS 服務 的方式，以及嘗試的疑難排解步驟。



3. 選擇 Next (下一步)。
4. 在 Create a support case (建立支援案例) 對話方塊中，指定下列選項：
   a. 選擇 Issue type (問題類型)。
   b. 選擇 Service (服務)。
   c. 選擇 Category (類別)。
   d. 選擇 Severity (嚴重性)。
   e. 檢閱您的案例詳細資訊，然後選擇 Next (下一步)。

   下列範例顯示 Alexa 服務的技術支援案例。

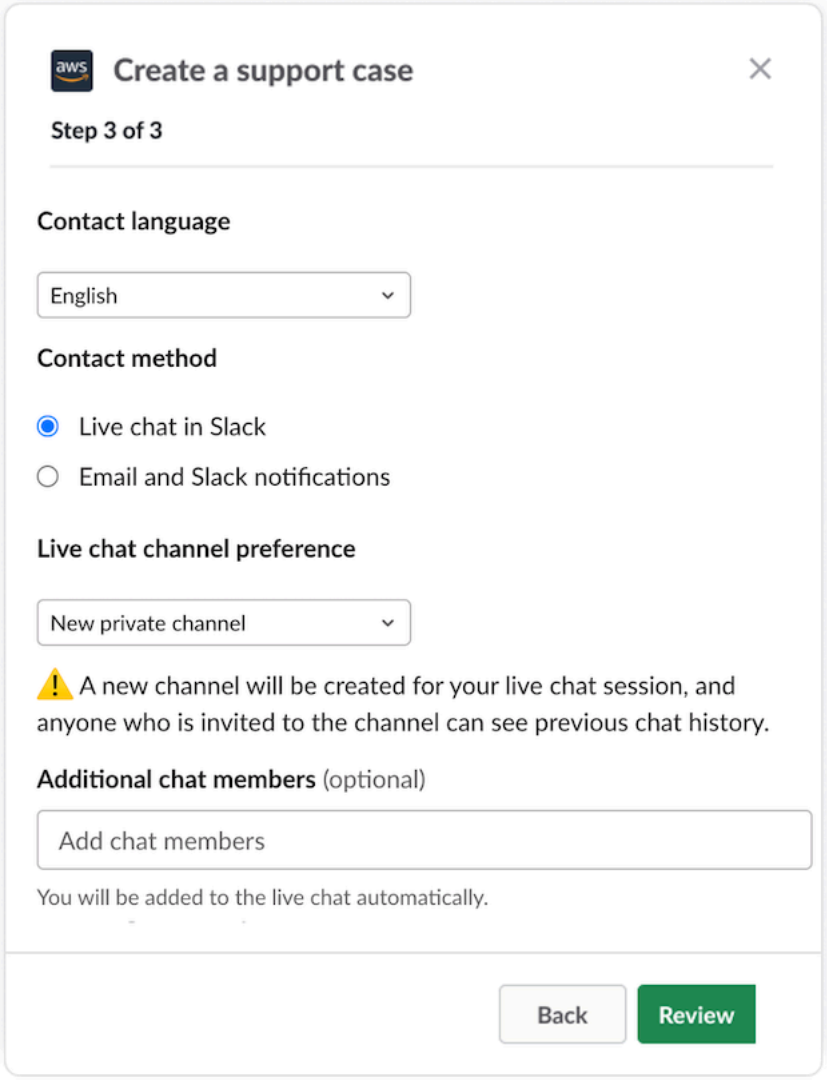


5. 針對 Contact language (聯絡語言)，為您的支援案例選擇您偏好的語言。

> **Note**
>
> Slack 中的帳戶和帳單案例的即時聊天不支援日文語言。

6. 對於 Contact method (聯絡方式)，選擇 Email and Slack notifications (電子郵件和 Slack 通知) 或者 Live chat in Slack (在 Slack 中進行即時聊天)。

   下列範例顯示如何在 Slack 中選擇即時聊天。



a. 如果您選擇在 Slack 中進行即時聊天，請選擇新的私有頻道或目前頻道作為您的即時聊天頻道偏好。新的私有頻道會建立一個單獨的私有頻道來讓您與 AWS Support 客服人員對談，目前頻道則會使用目前頻道中的討論串來讓您與 AWS Support 客服人員對談。

b. (選用) 如果選擇 Live chat in Slack (在 Slack 中進行即時聊天)，您可以輸入其他 Slack 成員的名稱。對於新的私有頻道，AWS Support 應用程式會自動將您與所選的成員加入這個全新頻道中。對於目前頻道，當 AWS Support 客服人員加入時，AWS Support 應用程式會自動標記您與聊天討論串中選取的成員。

> **Important**
>
> - 建議僅新增您希望其存取您的支援案例詳細資訊和聊天歷史記錄的聊天成員。

- 如果您為現有支援案例開始新的即時聊天工作階段，AWS Support 應用程式會使用以前的即時聊天所用的相同聊天頻道或討論串。AWS Support 應用程式也會使用先前使用的相同即時聊天頻道偏好。
- 唯有當聊天是從私有頻道請求時，才能使用目前頻道選項。我們建議，只有在您想要讓所有頻道成員均能存取聊天的情況下，才使用此選項。

7. (選用) 對於 Additional contacts to notify (要通知的其他聯絡人)，輸入電子郵件地址以接收有關此支援案例的更新。您最多可新增 10 個電子郵件地址。
8. 選擇 Review (檢閱)。
9. 在 Slack 頻道中，檢閱案例詳細資訊。您可以執行下列作業：
   - 選擇 Edit (編輯) 以變更案例詳細資訊。
   - 將檔案新增至您的案例。若要執行此作業，請依照下列步驟進行：
     a. 選擇 Attach file (附加檔案)，在 Slack 中選擇 + 圖示，然後選擇 Your computer (您的電腦)。
     b. 導覽到您的檔案並選擇。
     c. 在 Upload a file (上傳檔案) 對話方塊中，輸入 `@awssupport`，然後按傳送訊息

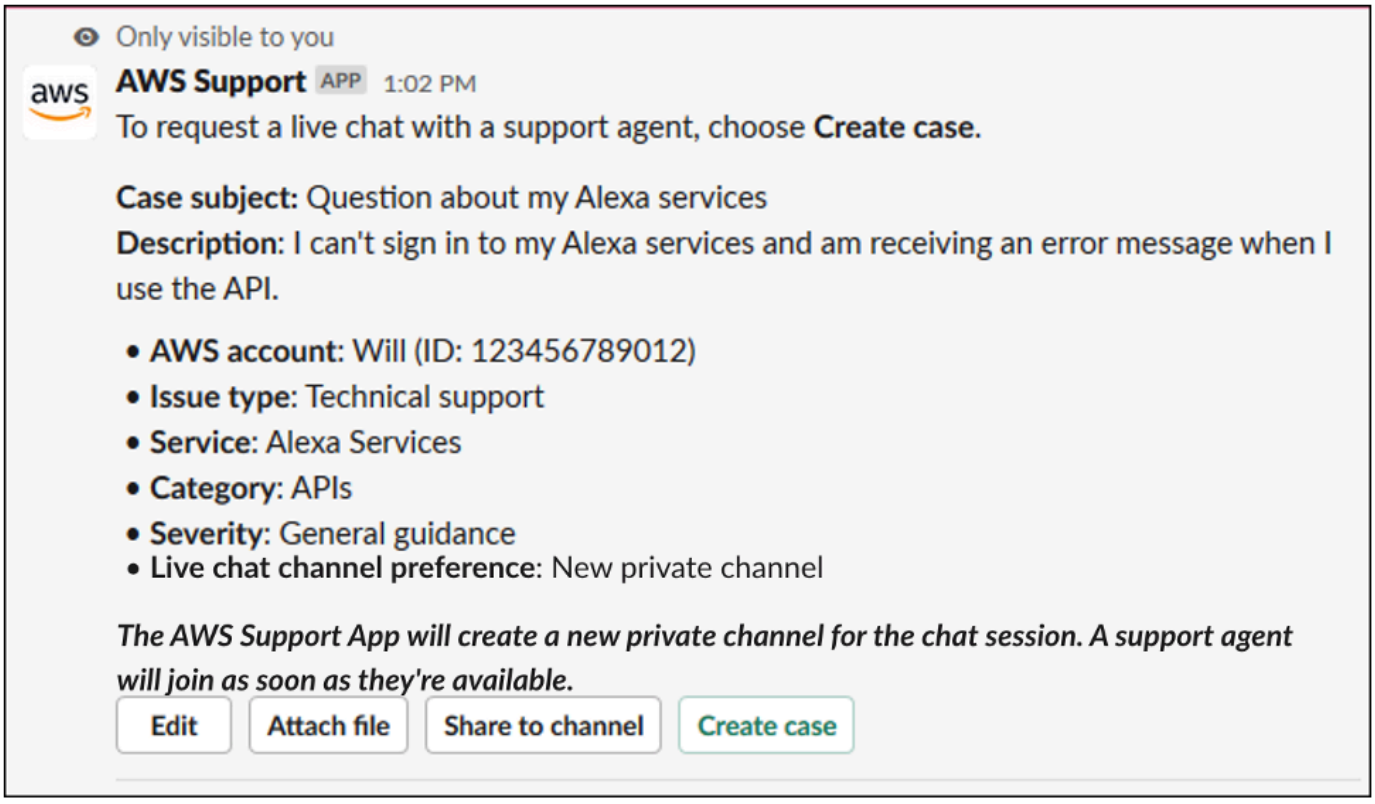
     

     圖示。

     備註

     - 您最多可以連接三個檔案。每個檔案最多可達 5 MB。
     - 如果您對支援案例附加檔案，則必須在 1 小時內提交案例。否則，必須再次新增檔案。
   - 選擇 Share to channel (分享至頻道)，與 Slack 頻道中的其他人分享案例詳細資訊。在建立案例之前，您可以使用此選項與團隊分享案例詳細資訊。
10. 檢閱您的案例詳細資訊，然後選擇 Create case (建立案例)。

下列範例顯示 Alexa 服務的技術支援案例。



建立支援案例後，案例詳細資訊可能需要幾分鐘才能顯示。

11. 當更新支援案例時，您可以選擇 See details (請參閱詳細資訊) 來檢視您的案例資訊。然後，您可以執行下列作業：
    - 選擇 Share to channel (分享至頻道)，與 Slack 頻道中的其他人分享案例詳細資訊。
    - 選擇 Reply (回覆) 可新增通訊。
    - 選擇 Resolve case (解決案例)。

> **Note**
>
> 如果沒有選擇在 Slack 中接收自動案例更新，您可以搜尋支援案例以尋找 See details (請參閱詳細資訊) 選項。

在 Slack 中回覆支援案例

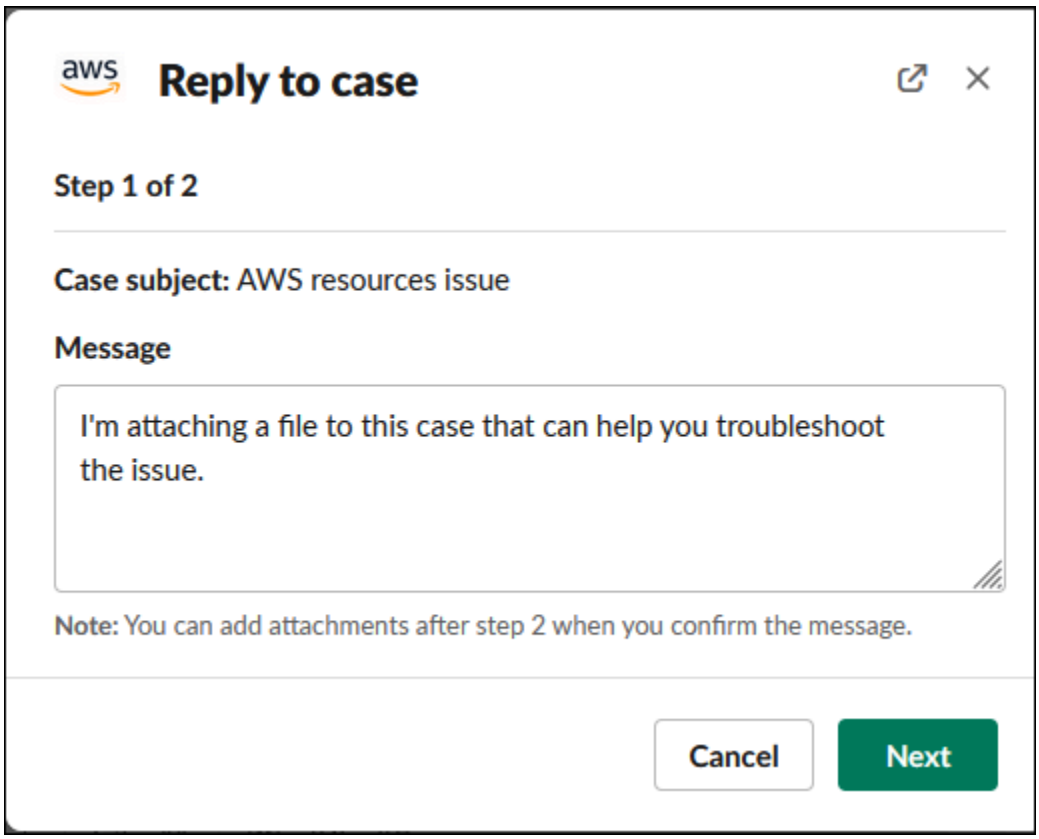
您可將更新新增到案例，例如案例詳細資訊和附件，並對支援客服人員的回應進行回覆。

> **Note**
>
> - 您也可使用 AWS Support Center Console 回覆支援客服人員。如需更多詳細資訊，請參閱更新、解決及重新開啟您的案例。
> - 您無法將通訊新增至來自 AWS Support 應用程式所建立之聊天頻道的案例。即時聊天頻道僅會在即時聊天期間向客服人員發送訊息。

若要在 Slack 中回覆支援案例

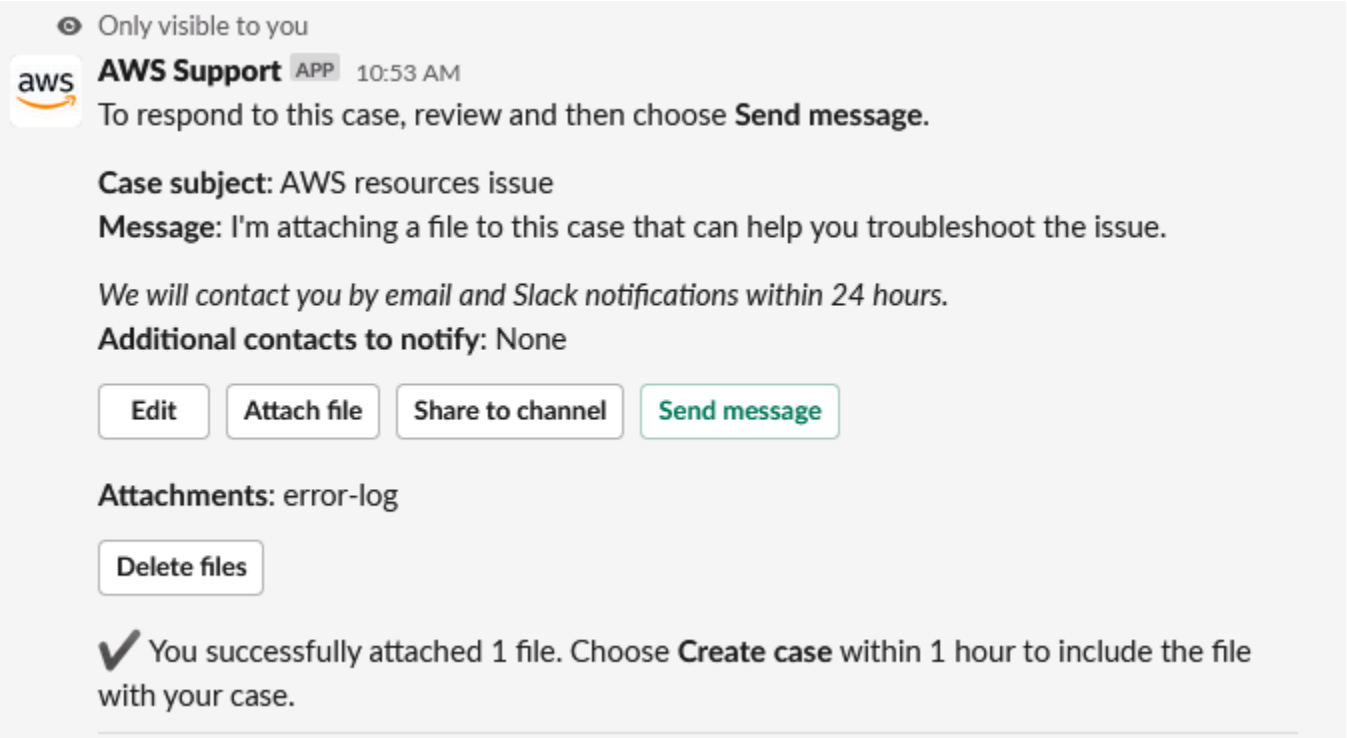
1. 在 Slack 頻道中，選擇您要回應的案例。您可以輸入 `/awssupport search` 以尋找您的支援案例。
2. 選擇所需案例旁邊的 See details (請參閱詳細資訊)。
3. 在案例詳細資訊的底部，選擇 Reply (回覆)。

4. 在 Reply to case (回覆案例) 對話方塊的 Message (訊息) 欄位中輸入問題的簡短描述。然後選擇 Next (下一步)。



5. 選擇聯絡方式。可用的聯絡方式取決於您的案例類型和支援計劃。
6. (選用) 對於 Additional contacts to notify (要通知的其他聯絡人)，輸入您想要接收有關此支援案例更新的其他電子郵件地址。您最多可新增 10 個電子郵件地址。
7. 選擇 Review (檢閱)。然後，您可以選擇是否要編輯回覆，是否附加檔案，或者是否分享至頻道。
8. 準備好回覆後，請選擇 Send message (傳送訊息)。
9. (選用) 若要檢視案例的先前通訊，請選擇 Previous correspondence (先前通訊)。若要檢視縮短訊息，請選擇 Show full message (顯示完整訊息)。

Example ：在 Slack 中回覆案例



使用 AWS Support 加入即時聊天工作階段

當您為案例請求即時聊天時，您可以為您和 AWS Support 客服人員選擇使用新的聊天頻道或目前頻道中的討論串。使用此聊天頻道或討論串來與支援客服人員以及您邀請參加即時聊天的任何其他人通訊。

Important

任何人加入具有即時聊天的頻道，都可以檢視有關此特定支援案例和聊天歷史紀錄的詳細資訊。建議您只新增需要存取支援案例的使用者。聊天頻道或討論串的任何成員也可以參與作用中的聊天。

Note

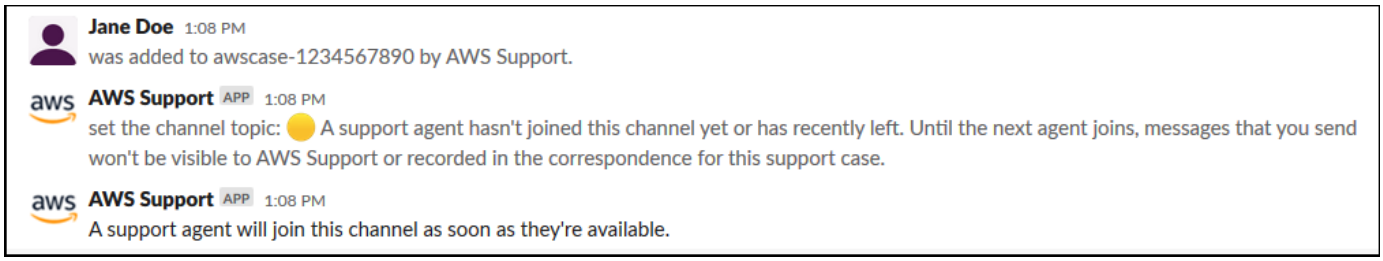
新增通訊到即時聊天工作階段之外的案例中時，即時聊天頻道和討論串也將收到通知。這會在聊天工作階段之前、期間和之後發生，因此您可以使用聊天頻道或討論串來監控案例的所有更新。如果您選擇使用新的聊天頻道，請使用您邀請 AWS Support 應用程式的來回覆這些通訊的組態頻道。

若要使用 AWS Support 在新頻道中加入即時聊天工作階段

1. 在 Slack 應用程式中，瀏覽至 AWS Support 應用程式為您建立的頻道。頻道名稱包含您的支援案例 ID，例如 *awscase-1234567890*。

   > **Note**
   >
   > AWS Support 應用程式會將固定消息新增到即時聊天頻道，其中包含有關您的支援案例的詳細資訊。在固定訊息中，您可以結束聊天或解決案例。您可以在頻道名稱下找到此頻道中的所有固定消息。

2. 當支援客服人員加入頻道時，您可以談談您的支援案例。在支援客服人員加入頻道之前，客服人員看不到聊天訊息，而且這些訊息也不會出現在您的案例通訊中。

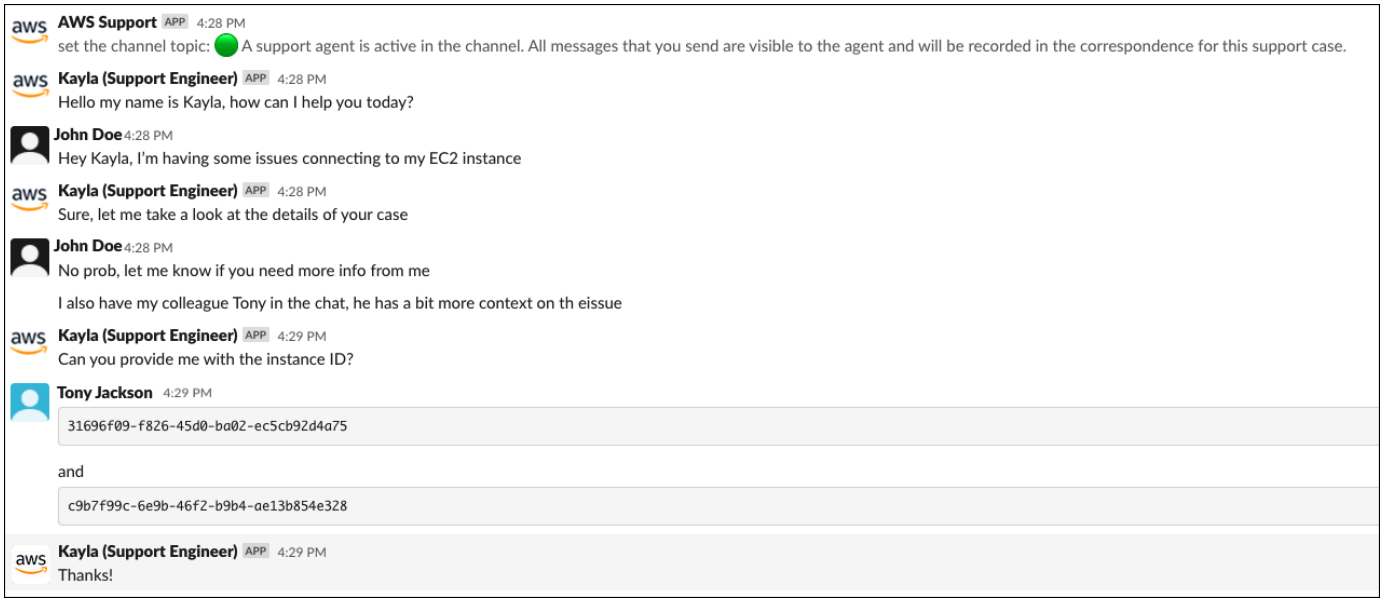
3. (選用) 將其他成員新增至聊天頻道。聊天頻道預設為私有。
4. 支援客服人員加入聊天後，聊天頻道處於活動狀態，AWS Support 應用程式會記錄聊天內容。

   您可以與客服人員討論支援案例，並將任何檔案附件上傳到該頻道。AWS Support 應用程式會自動將您的檔案和聊天記錄儲存到您的案例通訊中。

   > **Note**
   >
   > 當您與支援客服人員聊天時，請注意 Slack 中 AWS Support 應用程式的以下差異：
   >
   > - 支援客服人員無法檢視共用訊息或執行緒。若要共用訊息或執行緒中的文字，請將文字作為新訊息輸入。
   > - 如果您編輯或刪除訊息，客服人員仍會看到原始訊息。您必須再次輸入新訊息才能顯示修訂。

Example ：即時聊天工作階段

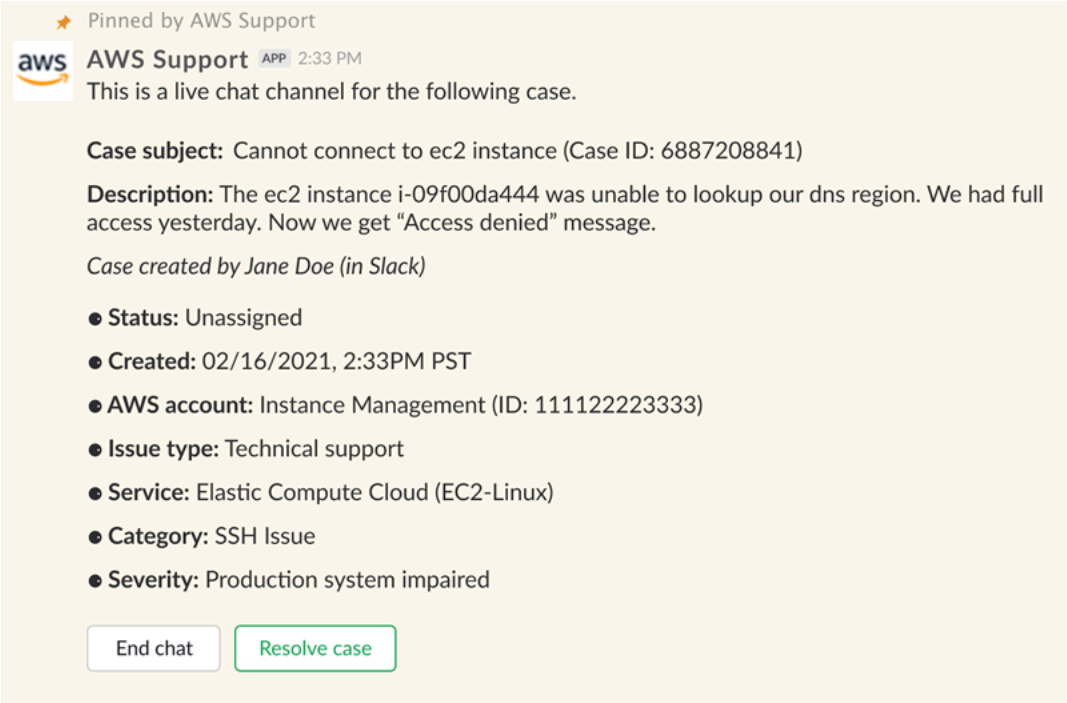
下面是為了解決兩個 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的連線問題而與支援客服人員進行的即時聊天工作階段的範例。



5. (選用) 若要停止即時聊天，請選擇 End chat (結束聊天)。支援客服人員離開頻道，AWS Support 應用程式停止錄製即時聊天。您可以找到此支援案例的案例通訊附加的聊天歷史記錄。
6. 如果問題已解決，您可以從固定訊息中選擇 Resolve case (解決案例) 或輸入 `/awssupport resolve`。

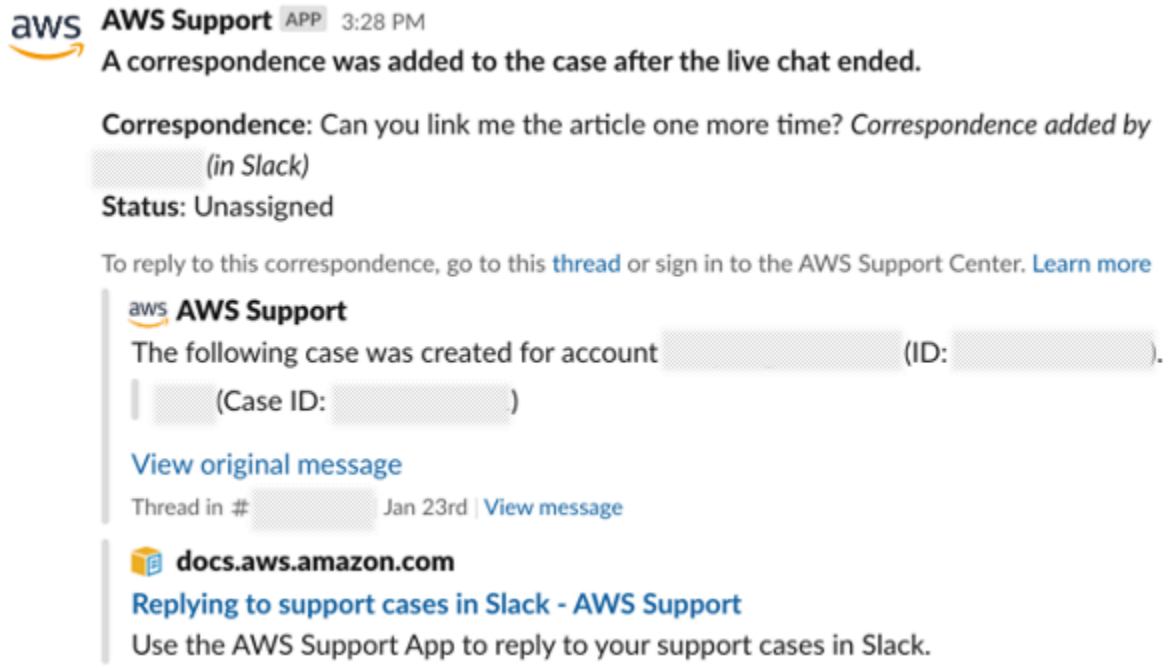
Example ：結束即時聊天

下列固定訊息顯示有關 Amazon EC2 執行個體的案例詳細資訊。您可以在 Slack 頻道名稱下找到固定訊息。



Example ：聊天頻道中的通訊通知

以下是另一個協同合作者在對話結束後新增更新時，即時聊天頻道會收到通知的範例。

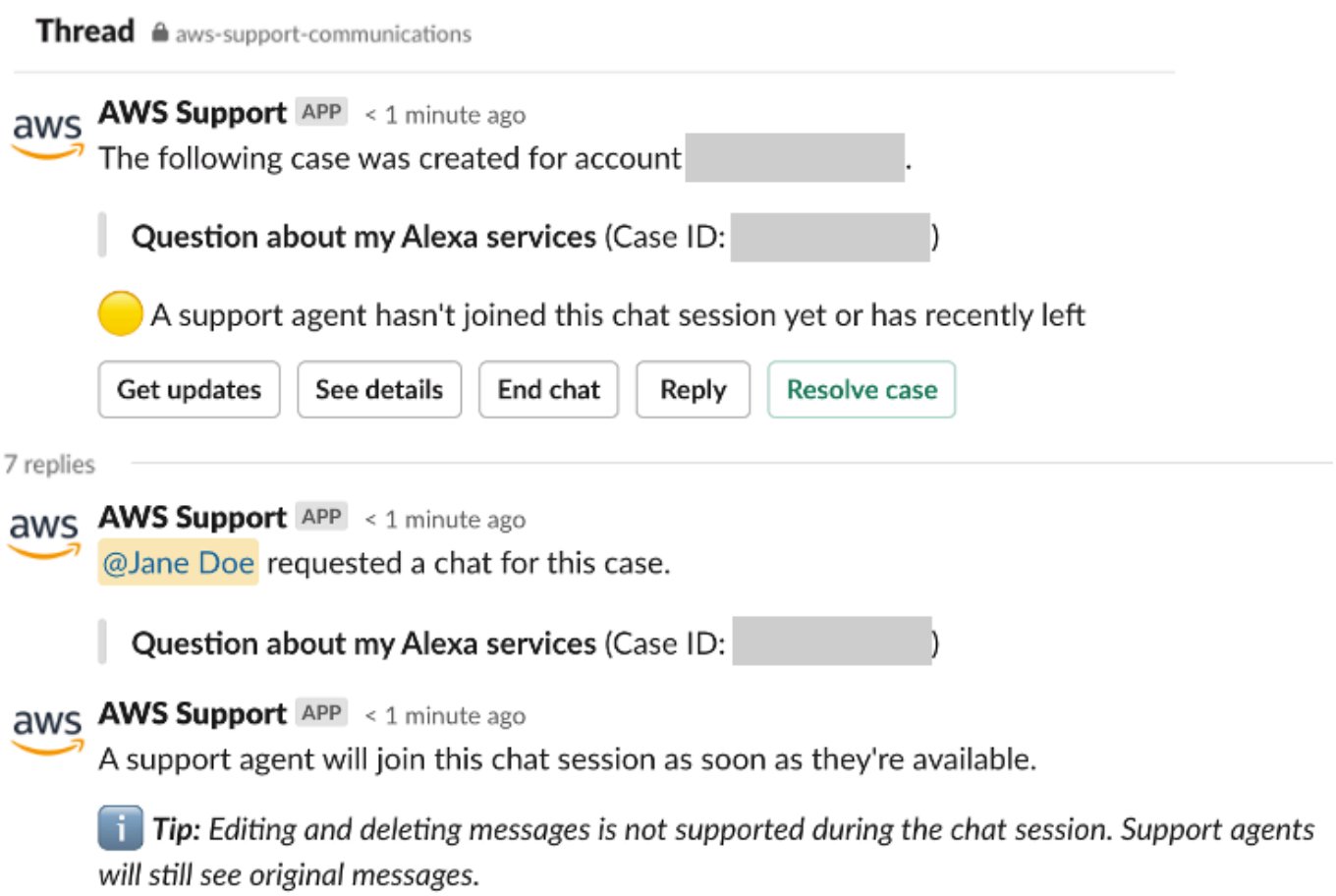


通知將顯示聊天狀態（已請求、正在進行中或已結束），以及通訊是由客服人員還是由其他協同合作者新增。Support 應用程式也會嘗試連回請求此聊天的原始 Slack 執行緒或頻道。您可以從該頻道或任何其他可以存取此案例的頻道回覆此案例。

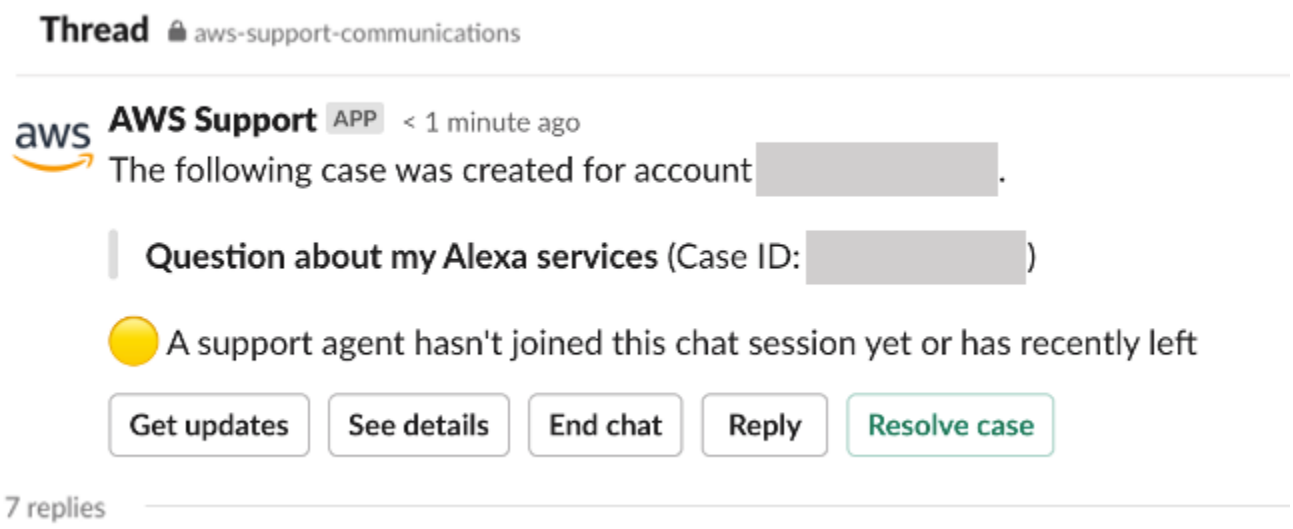
若要使用 AWS Support 在目前頻道中加入即時聊天工作階段

1. 在 Slack 應用程式中，瀏覽至 AWS Support 應用程式用於聊天的目前頻道中的討論串。在大多數情況下，這會是首次建立案例時開始的討論串。
2. 當支援客服人員加入討論串時，您可以談談您的支援案例。在支援客服人員加入討論串之前，客服人員不會看見該討論串中的訊息，且當聊天結束時，這些訊息也不會出現在您的案例通訊中。

> **Note**
>
> 即使聊天處於作用中狀態，AWS Support 也絕不會看見傳送到此頻道以外的訊息。



3. (選用) 標記其他頻道成員以便於聊天討論串通知他們。
4. 支援客服人員加入聊天後，聊天討論串會處於作用中狀態，AWS Support 應用程式會記錄聊天內容。與全新聊天頻道選項相似，您可以與客服人員討論支援案例，並將任何檔案附件上傳到該討論串。AWS Support 應用程式會自動將您的檔案和聊天記錄儲存到您的案例通訊中。
5. (選用) 若要停止即時聊天，請在此討論串的初始訊息中選擇「結束聊天」。支援客服人員離開討論串，AWS Support 應用程式停止錄製即時聊天。您可以找到此支援案例的案例通訊附加的聊天歷史記錄。
6. 如果問題已解決，您可以從初始訊息中選擇「解決」案例。



在 Slack 中搜尋支援案例

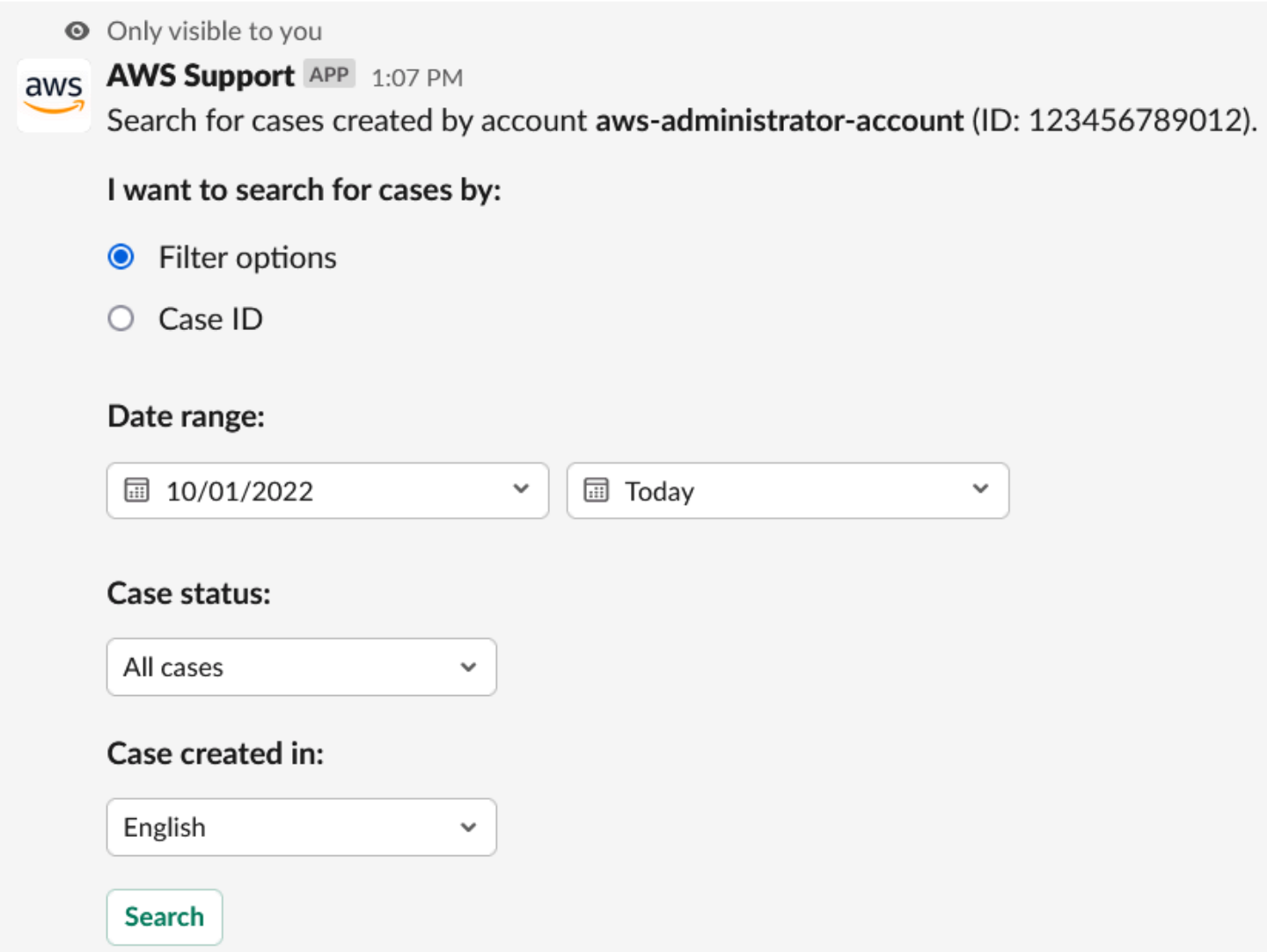
在 Slack 頻道中，可以從您的 AWS 帳戶 以及也設定了相同頻道和工作區的其他帳戶中搜尋支援案例。例如，如果您的帳戶 (123456789012) 和同事的帳戶 (111122223333) 都在 AWS Support Center Console 中設定了相同的工作區和通道，你們可以使用 AWS Support 應用程式來搜尋彼此的支援案例。

若要篩選結果，您可以使用下列選項：

- 帳戶 ID
- 案例 ID
- 案例狀態
- 聯絡語言
- 日期範圍

Example ：在 Slack 中搜尋案例

下列範例顯示如何透過指定日期範圍、案例狀態和聯絡語言，依 Filter options (篩選選項) 搜尋單一帳戶。



在 Slack 中搜尋支援案例

1. 在 Slack 頻道中，輸入下列命令：

   ```
   /awssupport search
   ```

2. 對於 I want to search for cases by: (我想透過以下方式搜尋案例：) 選項，請選擇下列其中一項：

   A. Filter options (篩選選項) – 您可以使用下列選項來篩選案例：

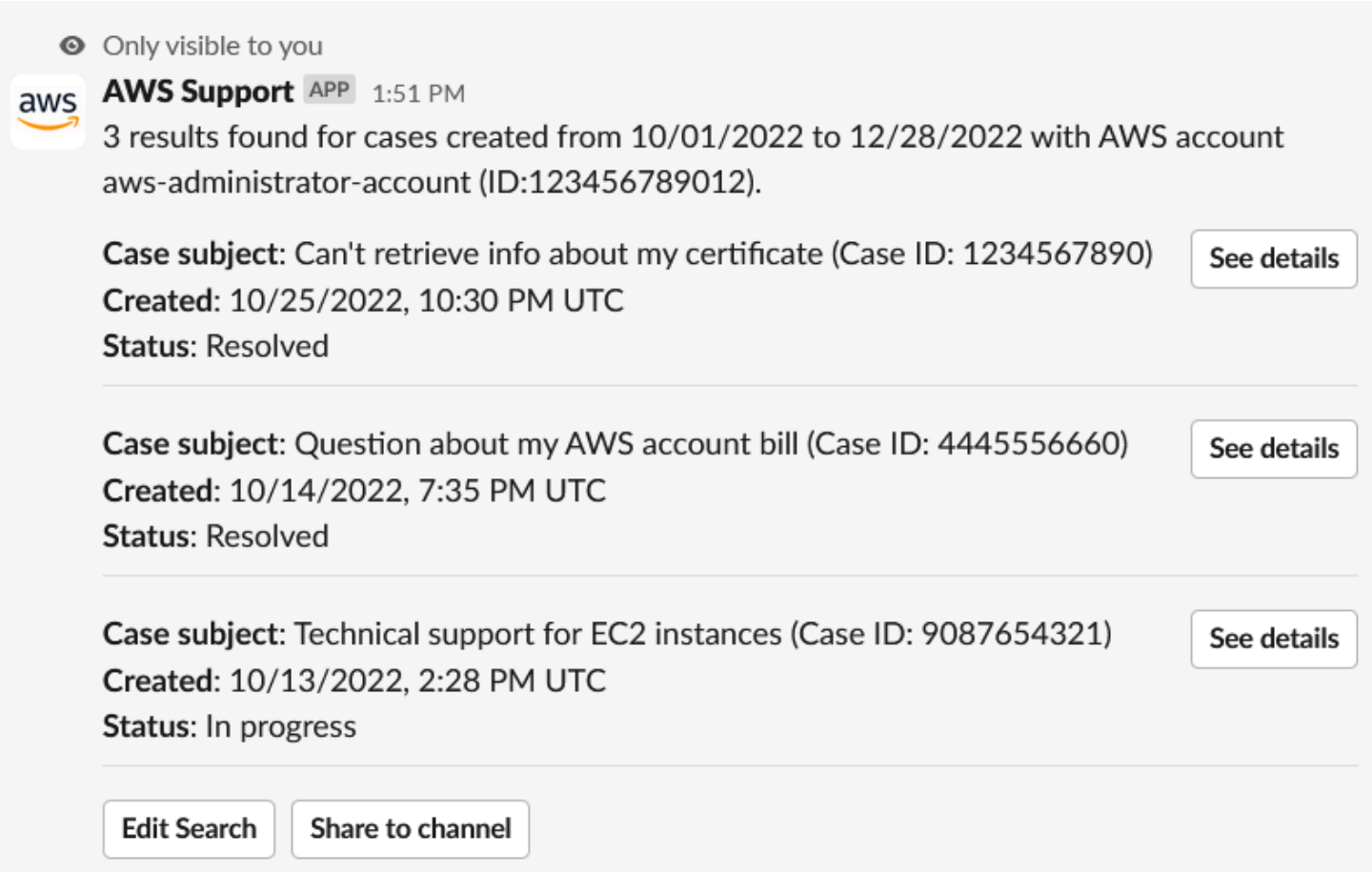
   - AWS 帳戶 – 當您在此頻道中有多個帳戶時，此清單才會出現。
   - Date range (日期範圍) - 案例的建立日期。
   - Case status (案例狀態) - 目前案例狀態，例如 All open cases (所有開啟的案例) 或 Resolved (已解決)。
   - Case created in (案例建立語言) - 案例的聯絡語言。

B. Case ID (案例 ID) - 輸入案例 ID。您一次只能輸入一個案例 ID。如果您在頻道中有多個帳戶，則請選擇 AWS 帳戶 以搜尋案例。

3. 選擇 Search (搜尋)。您的搜尋結果會顯示在 Slack 中。

使用您的搜尋結果

下列範例會從一個 AWS 帳戶 中傳回三個支援案例。



收到搜尋結果之後，您可以執行下列操作：

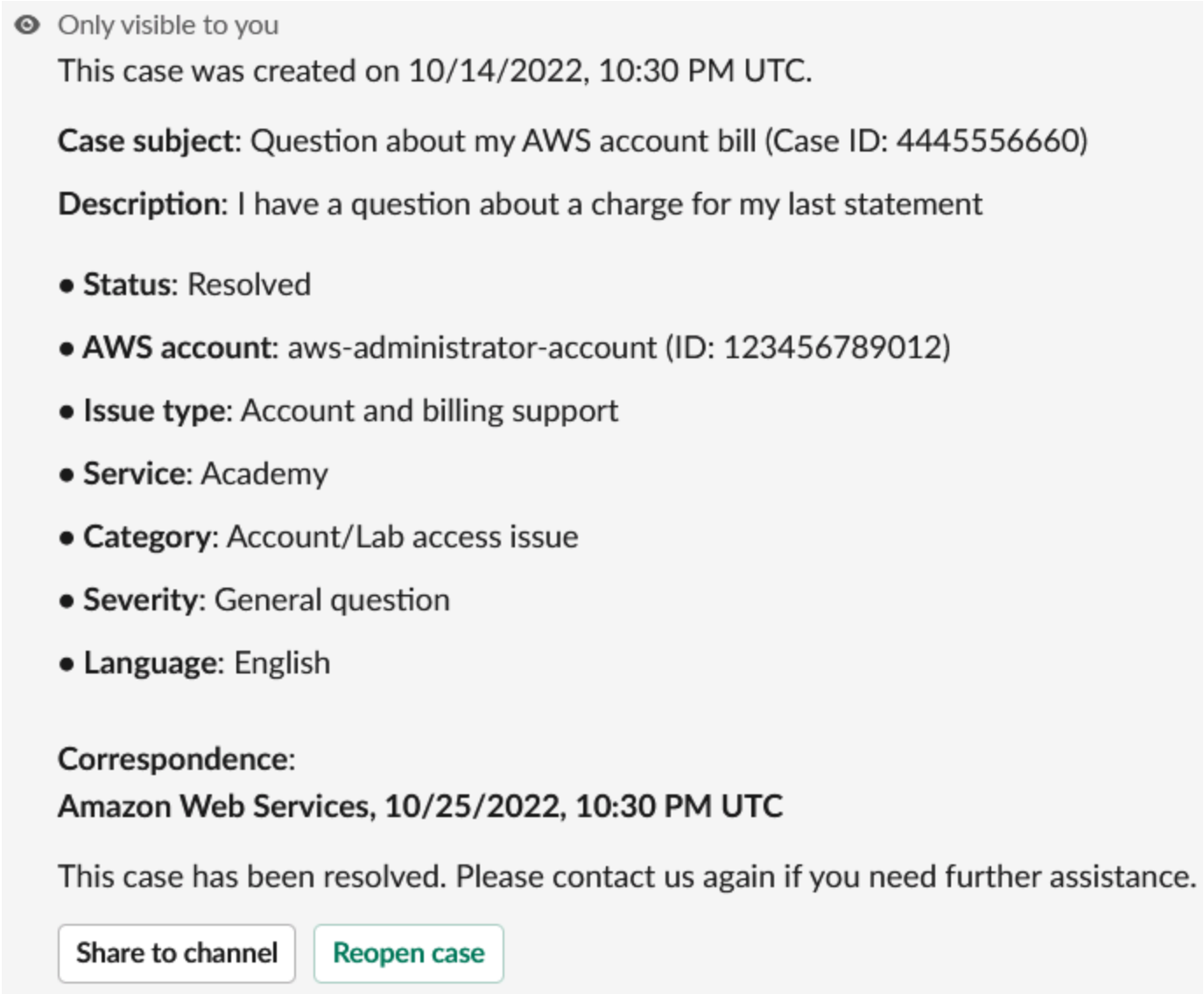
使用您的搜尋結果

1. 選擇 Edit Search (編輯搜尋) 以變更先前的篩選選項或案例 ID。
2. 選擇 Share to channel (分享到頻道)，與頻道分享搜尋結果。
3. 選擇 See details (查看詳細資訊)，以取得有關案例的詳細資訊。您可以選擇 Show full message (顯示完整訊息)，查看其餘的最新通訊。

4. 如果您依 Filter options (篩選選項) 進行搜尋，搜尋結果可能會傳回多個案例。選擇 Next 5 results (下 5 個結果) 或 Previous 5 results (上 5 個結果)，以檢視下 5 個或上 5 個案例。

Example ：已解決支援案例

下列範例在選擇 See details (查看詳細資訊) 後，顯示已解決帳戶和帳單問題的支援案例。

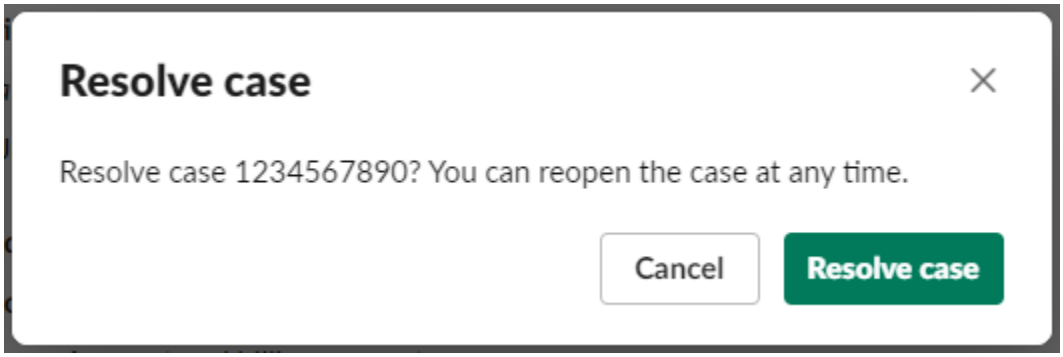


在 Slack 中解決支援案例

如果您不再需要支援案例，或已修正問題，您可以直接在 Slack 中解決支援案例。這也會在 AWS Support Center Console 中解決案例。解決案例後，可稍後重新開啟案例。

若要在 Slack 中解決支援案例

1. 在您的 Slack 頻道中導覽至支援案例。請參閱 在 Slack 中搜尋支援案例。
2. 針對該案例，選擇 See details (請參閱詳細資訊)。
3. 選擇 Resolve case (解決案例)。
4. 在 Resolve case (解決案例) 對話方塊中，選擇 Resolve case (解決案例)。您可以在 Slack 頻道中或從支援中心主控台中重新開啟案例。

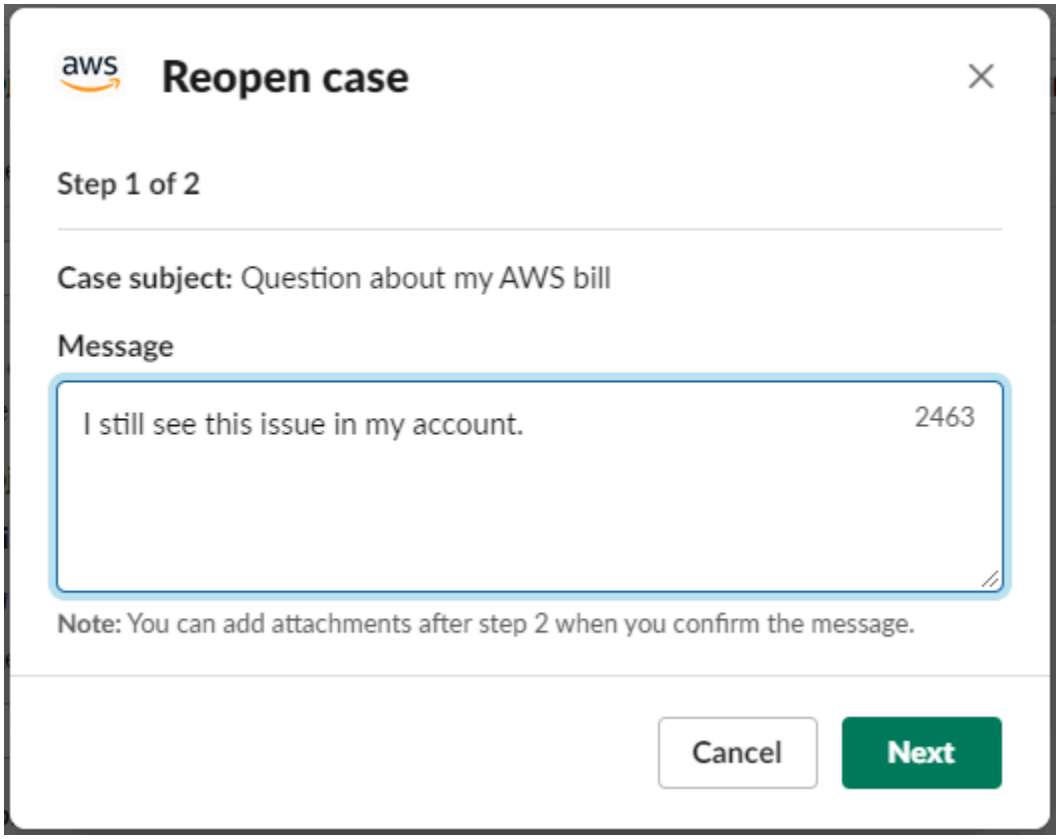


在 Slack 中重新開啟支援案例

解決支援案例後，您可以從 Slack 重新開啟案例。

若要在 Slack 中重新開啟支援案例

1. 尋找要在 Slack 中重新開啟的支援案例。請參閱 在 Slack 中搜尋支援案例。
2. 選擇 See details (請參閱詳細資訊)。
3. 選擇 Reopen case (重新開啟案例)。
4. 在 Reopen case (重新開啟案例) 對話方塊的 Message (訊息) 欄位中輸入問題的簡短描述。
5. 選擇 Next (下一步)。



6. (選用) 輸入其他聯絡人。
7. 選擇 Review (檢閱)。
8. 檢閱您的案例詳細資訊，然後選擇 Send message (傳送訊息)。您的案例會重新開啟。如果您要求與支援客服人員進行新的即時聊天，Slack 會使用與先前即時聊天所用的相同聊天頻道或討論串。如果您在新的頻道請求即時聊天，但到目前為止還沒有進行，則會開啟一個新的聊天頻道。如果您在目前頻道中請求即時聊天但目前為止仍未獲得回應，則會使用目前聊天中的討論串。

請求增加服務配額

您可以從 Slack 頻道中請求增加帳戶的服務配額。

若要請求增加服務配額

1. 在 Slack 頻道中，輸入下列命令：

   ```
   /awssupport quota
   ```

2. 在 Increase service quota (增加服務配額) 對話方塊中，輸入下列資訊：

   a. 選擇 AWS 帳戶。

b. 選擇 AWS 區域。

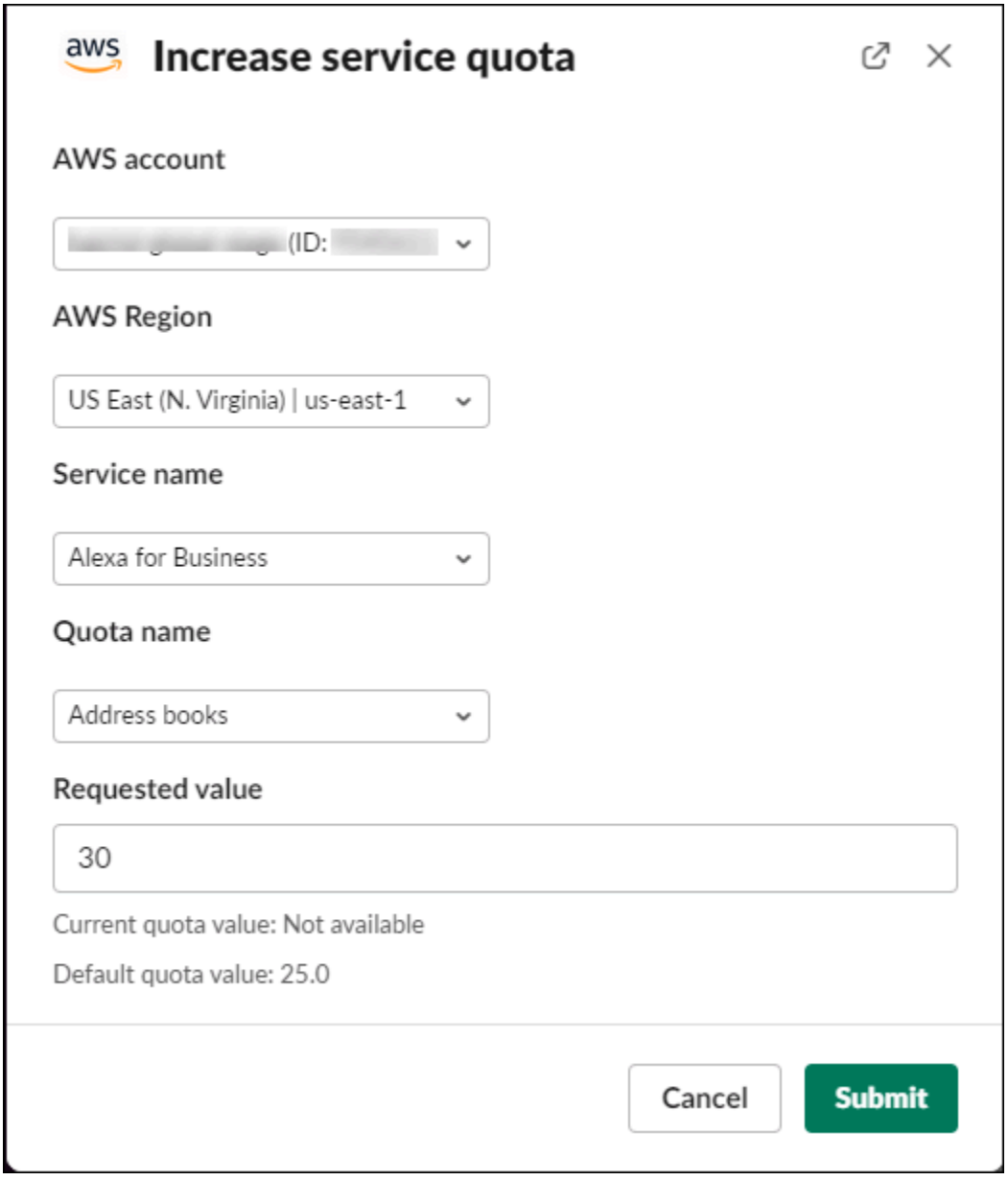
c. 選擇 Service name (服務名稱)。

d. 選擇 Quota name (配額名稱)。

e. 對配額增加輸入 Requested value (請求值)。您必須輸入大於預設配額的值。

3. 選擇 Submit (提交)。

Example ：企業版 Alexa 的配額增加



您也可以從 Service Quotas 主控台中檢視請求。如需詳細資訊，請參閱《Service Quotas 使用者指南》中的請求提高配額。

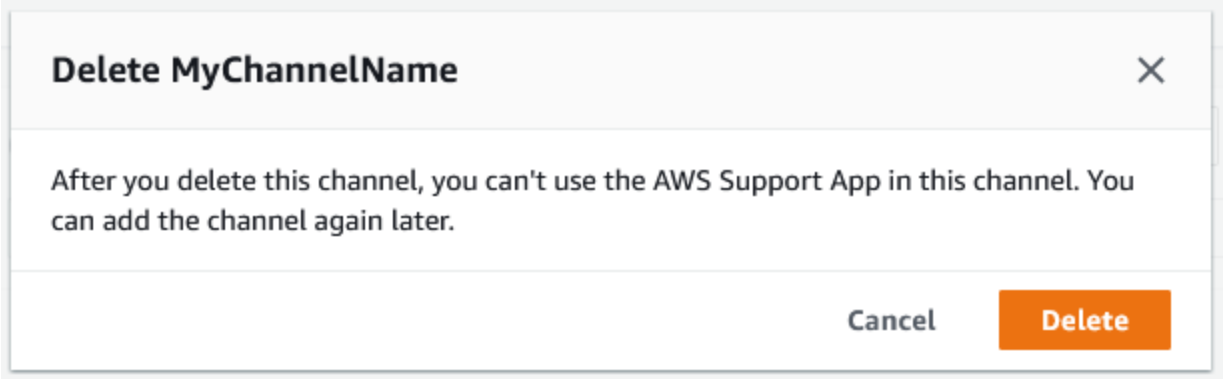
從 AWS Support 應用程式中刪除 Slack 頻道組態

如果您不需要頻道組態，可以從 AWS Support 應用程式中刪除它。此動作只會從 AWS Support 應用程式和 AWS Support Center Console 中移除頻道。不會從 Slack 中刪除您的頻道。

可為您的 AWS 帳戶 最多新增 20 個頻道。如果已達到此配額，您必須先刪除頻道，才能新增其他頻道。

若要刪除 Slack 頻道組態

1. 登入支援中心主控台並選擇Slack configuration (Slack 組態)。
2. 在 Slack configuration (Slack 組態) 頁面的 Channels (頻道) 中，選擇頻道名稱，然後選擇 Delete (刪除)。
3. 在 Delete channel name (刪除頻道名稱) 對話方塊中，選擇 Delete (刪除)。您稍後可以再次將此頻道新增至 AWS Support 應用程式。



從 AWS Support 應用程式中刪除 Slack 工作區組態

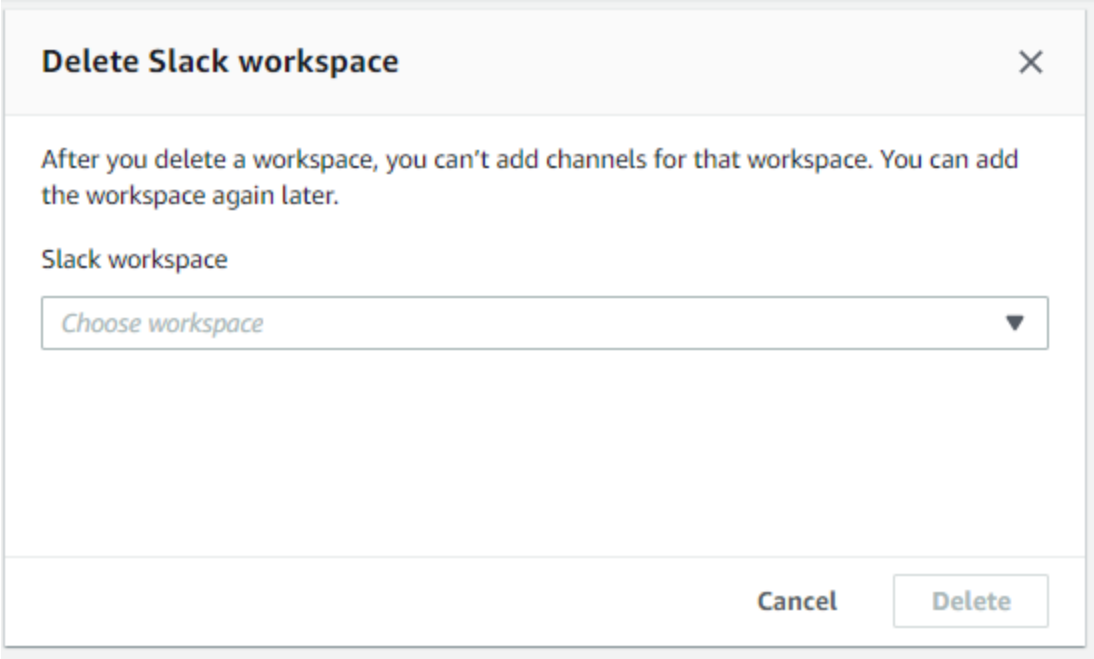
如果您不需要工作區組態，可以從 AWS Support 應用程式中刪除它。此動作只會從 AWS Support 應用程式和 AWS Support Center Console 中移除工作區。不會從 Slack 中刪除您的工作區。

最多可為您的 AWS 帳戶 新增 5 個工作區。如果已達到此配額，您必須先刪除 Slack 工作區，才能新增其他工作區。

> **Note**
>
> 如果您將頻道從此工作區新增至 AWS Support 應用程式，必須先刪除這些頻道才能刪除工作區。請參閱 從 AWS Support 應用程式中刪除 Slack 頻道組態。

若要刪除 Slack 工作區組態

1. 登入 AWS Support Center Console 並選擇 Slack configuration (Slack 組態)。
2. 在 Slack configuration (Slack 組態) 頁面的 Slack workspaces (Slack 工作區) 中，選擇 Delete a workspace (刪除工作區)。
3. 在 Delete Slack workspace (刪除 Slack 工作區) 對話方塊中，選擇 Slack 工作區名稱，然後選擇 Delete (刪除)。您可以稍後再次將工作區新增到 AWS 帳戶。



Slack 命令中的 AWS Support 應用程式

Slack 頻道命令

可以在您邀請 AWS Support 應用程式的 Slack 頻道中輸入以下命令。此 Slack 頻道名稱也會在 AWS Support Center Console 中顯示為已設定的頻道。

`/awssupport create` 或 `/awssupport create-case`

建立支援案例。

`/awssupport search` 或 `/awssupport search-case`

搜尋案例。您可以搜尋 AWS 帳戶 的支援案例，已針對相同 Slack 頻道設定 AWS Support 應用程式。

`/awssupport quota` 或 `/awssupport service-quota-increase`

請求服務配額增加。

即時聊天頻道命令

您可以在即時聊天頻道中輸入以下命令。如果您為與 AWS Support 的聊天選擇新的頻道，那麼這會是 AWS Support 應用程式為您建立的頻道。聊天頻道包含您的支援案例 ID，例如 *awscase-1234567890*。

> **Note**
>
> 在目前即時聊天的頻道中使用討論串時，無法使用下列命令。請改用附加到初始討論串訊息的按鈕來結束聊天、邀請新的客服人員，或解決案例。

`/awssupport endchat`

移除支援客服人員並結束即時聊天工作階段。

`/awssupport invite`

邀請新的支援客服人員加入此頻道。

`/awssupport resolve`

解決此支援案例。

在 AWS Support Center Console 中檢視 AWS Support 應用程式通訊

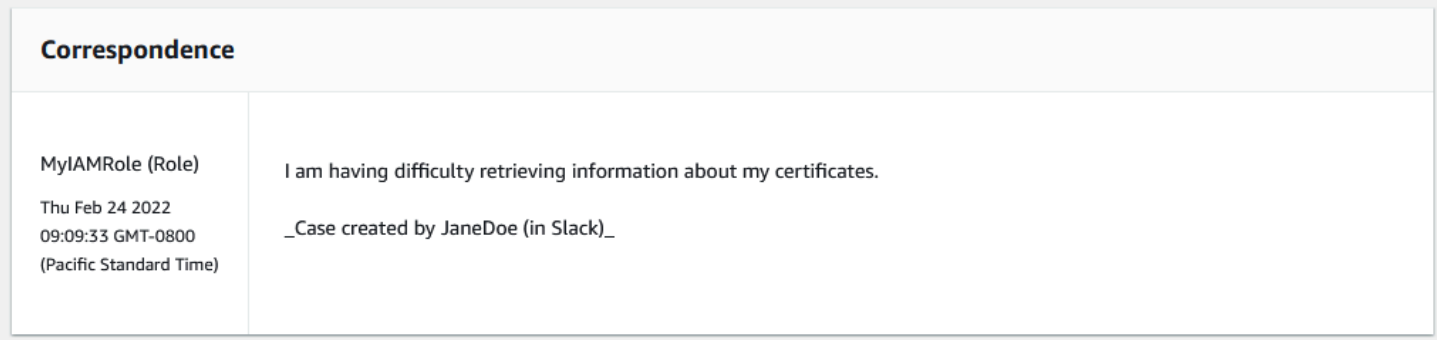
當您在 Slack 頻道中建立、更新或解決帳戶的支援案例時，您也可以登入支援中心主控台以檢視您的案例。您可以在 Slack 頻道中檢視案例通訊以判斷案例是否已更新，檢視與支援客服人員的聊天記錄，以及尋找您從 Slack 上傳的任何附件。

若要檢視來自 Slack 的通訊

1. 登入帳戶的 AWS Support Center Console。
2. 選擇您的支援案例。
3. 在 Correspondence (通訊) 中，您可以檢視是否已從 Slack 頻道建立和更新案例。

Example ：支援案例

在下列螢幕擷取畫面中，Jane Doe 在 Slack 中重新開啟了支援案例。支援案例的通訊會顯示在支援中心主控台中。



使用 AWS CloudFormation 在 Slack 資源中建立 AWS Support 應用程式

Slack 中的 AWS Support 應用程式已與 AWS CloudFormation 整合，這項服務可協助您建立 AWS 資源的模型並進行設定，以減少建立和管理資源和基礎設施的時間。您可以建立一個範本，描述您需要的所有 AWS 資源 (例如 AccountAlias 和 SlackChannelConfiguration)，AWS CloudFormation 會為您佈建和設定這些資源。

當您使用 AWS CloudFormation 時，您可以重複使用您的範本，重複且一致地設定您的 AWS Support 應用程式資源。只需描述一次您的資源，即可在多個 AWS 帳戶 帳戶與區域內重複佈建相同資源。

AWS Support 應用程式和 AWS CloudFormation 模板

若要佈建和設定 AWS Support 應用程式與相關服務的資源，您必須了解 AWS CloudFormation 範本。範本是以 JSON 或 YAML 格式化的文本檔案。而您亦可以透過這些範本的說明，了解欲在 AWS CloudFormation 堆疊中佈建的資源。如果您不熟悉 JSON 或 YAML，您可以使用 AWS CloudFormation Designer 協助您開始使用 AWS CloudFormation 範本。如需詳細資訊，請參閱 AWS CloudFormation 使用者指南中的什麼是 AWS CloudFormation Designer？。

AWS Support 應用程式支援在 AWS CloudFormation 中建立您的 AccountAlias 和 SlackChannelConfiguration。如需詳細資訊 (包括 AccountAlias 和 SlackChannelConfiguration 資源的 JSON 和 YAML 範本範例)，請參閱《AWS CloudFormation 使用者指南》中的 AWS Support 應用程式資源類型參考。

為您的組織建立 Slack 組態資源

您可以使用 CloudFormation 範本建立 AWS Support 應用程式所需的資源。如果您是組織的管理帳戶，則可以使用範本為 AWS Organizations 中的成員帳戶建立這些資源。

例如，您可以使用範本為組織中的所有帳戶建立相同的 Slack 工作區組態，然後使用不同的範本為特定 AWS 帳戶 或組織單位 (OU) 建立不同的 Slack 頻道組態。您也可以使用範本來建立 Slack 工作區組態，以便成員帳戶接著可以為其 AWS 帳戶 設定想要的 Slack 頻道。

您可以選擇是否使用 CloudFormation 範本。如果您不使用 CloudFormation 範本，則可以改為手動完成下列步驟：

- 在 AWS Support Center Console 中建立 AWS Support 應用程式資源。
- 使用 AWS Support 建立支援案例，以授權多個帳戶使用 AWS Support 應用程式。
- 呼叫 RegisterSlackWorkspaceForOrganization API 操作為您的帳戶註冊 Slack 工作區。CloudFormation 堆疊會為您呼叫此 API 操作。

請遵循下列程序，將 CloudFormation 範本上傳至您的組織。您可以使用 AWS Support 應用程式資源類型參考頁面中的範例範本。

範本會通知 CloudFormation 建立以下資源：

- Slack 頻道組態。
- Slack 工作區組態。
- 具有 `AWSSupportSlackAppCFNRole` 名稱的 IAM 角色。系統會連接 AWSSupportAppFullAccess AWS 受管政策。

內容

更新適用於 Slack 的 CloudFormation 範本

若要開始使用，請使用下列範本建立您的堆疊。您必須將範本取代為 Slack 工作區和頻道的有效值。

> **Note**
>
> 我們不建議使用範本為您的組織建立 AccountAlias 資源。AccountAlias 資源可唯一識別 AWS Support 應用程式中的 AWS 帳戶。您的成員帳戶可以在 Support Center Console 中輸入帳戶名稱。如需更多詳細資訊，請參閱 授權 Slack 工作區。

更新適用於 Slack 的 CloudFormation 範本

1. 如果您是組織的管理帳戶，則必須先手動授權帳戶的 Slack 工作區，然後您的成員帳戶才能使用 CloudFormation 來建立資源。如果您尚未這麼做，則請參閱 授權 Slack 工作區。
2. 從 AWS Support 應用程式資源類型參考頁面複製所需資源的 JSON 或 YAML 範本。
3. 在文字編輯器中，將範本貼到新檔案中。
4. 在範本中，指定所需的參數。請至少取代下列欄位的值：

   - 將 `TeamId` 取代為您的 Slack 工作區 ID
   - 將 `ChannelId` 取代為 Slack 頻道 ID
   - 將 `ChannelName` 取代為可識別 Slack 頻道組態的名稱

   > **Tip**
   >
   > 若要尋找工作區和通道 ID，請在瀏覽器中開啟 Slack 通道。在 URL 中，您的工作區 ID 是第一個識別碼，而通道 ID 是第二個識別碼。例如，在 https://app.slack.com/client/T012ABCDEFG/C01234A5BCD 中，T012ABCDEFG 是工作區 ID，而 C01234A5BCD 是通道 ID。

5. 將檔案儲存為 JSON 或 YAML 檔案。

為管理帳戶建立堆疊

接下來，您必須為組織中的管理帳戶建立堆疊。此步驟會為您呼叫 RegisterSlackWorkspaceForOrganization API 操作，並使用 Slack 授權工作區。

> **Note**
>
> 建議您上傳您在上一個程序中為管理帳戶更新的 Slack 工作區組態範本。您不需要上傳 Slack 通道組態範本，除非您也將管理帳戶設定為使用 AWS Support 應用程式。

為管理帳戶建立堆疊

1. 使用組織的管理帳戶登入 AWS Management Console。
2. 在以下網址開啟 AWS CloudFormation 主控台：https://console.aws.amazon.com/cloudformation。
3. 如果您尚未執行此步驟，則請在 Region selector (區域選取器) 中選擇下列其中一個 AWS 區域：
   - 歐洲 (法蘭克福)
   - 歐洲 (愛爾蘭)
   - 歐洲 (倫敦)
   - 美國東部 (維吉尼亞北部)
   - 美國東部 (俄亥俄)
   - 美國西部 (奧勒岡)
   - 亞太區域 (新加坡)
   - 亞太區域 (東京)
   - 加拿大 (中部)
4. 遵循下列程序來建立堆疊。如需詳細資訊，請參閱在 AWS CloudFormation 主控台上建立堆疊。

   在 CloudFormation 成功建立堆疊後，您可以使用同一個範本為您的組織建立堆疊集。

為您的組織建立堆疊集

接下來，對 Slack 工作區組態使用相同的範本來建立具有 `service-managed` 許可的堆疊集。您可以使用堆疊集為您的整個組織建立堆疊，或指定所需的 OU。如需詳細資訊，請參閱建立堆疊集。

此程序也會為您呼叫 RegisterSlackWorkspaceForOrganization API 操作。此 API 操作使用 Slack 為成員帳戶授權工作區。

為您的組織建立堆疊集

1. 使用組織的管理帳戶登入 AWS Management Console。
2. 在以下網址開啟 AWS CloudFormation 主控台：https://console.aws.amazon.com/cloudformation。
3. 如果您尚未執行此步驟，則請在 Region selector (區域選取器) 中選擇您在上一個程序中使用的相同 AWS 區域。
4. 在導覽窗格中，選擇 StackSets。
5. 選擇 Create StackSet (建立 StackSet)。
6. 在 Choose a template (選擇範本) 頁面上，保留下列選項的預設選項：
   - 在 Permissions (許可) 下，保留 Service-managed permissions (服務受管許可)。
   - 對於 Prerequisite - Prepare template (先決條件 - 準備範本)，保留 Template is ready (範本已就緒)。
7. 在 Specify template (指定範本) 下，選擇 Upload a template file (上傳範本檔案)，然後選擇 Choose file (選擇檔案)。
8. 選擇檔案，然後選擇 Next (下一步)。
9. 在 Specify StackSet details (指定 StackSet 詳細資訊) 頁面上，輸入堆疊名稱 (例如 **`support-app-slack-workspace`**)，輸入描述，然後選擇 Next (下一步)。
10. 在 Configure StackSet options (設定 StackSet 選項) 頁面上，保留預設選項，然後選擇 Next (下一步)。
11. 在 Set deployment options (設定部署選項) 頁面上，對於 Add stacks to stack set (將堆疊新增至堆疊集)，保留預設 Deploy new stacks (部署新堆疊) 選項。
12. 針對 Deployment targets (部署目標)，選擇是否要為整個組織或特定 OU 建立堆疊。如果您選擇 OU，請輸入 OU ID。
13. 在 Specify regions (指定區域) 中，僅輸入下列其中一個 AWS 區域：
    - 歐洲 (法蘭克福)
    - 歐洲 (愛爾蘭)
    - 歐洲 (倫敦)
    - 美國東部 (維吉尼亞北部)

- 美國東部 (俄亥俄)
- 美國西部 (奧勒岡)
- 亞太區域 (新加坡)
- 亞太區域 (東京)
- 加拿大 (中部)

> **備註：**
>
> - 若要簡化您的工作流程，建議您使用您在步驟 3 中選擇的相同 AWS 區域。
> - 選擇一個以上 AWS 區域 可能會導致與建立堆疊發生衝突。

14. 對於部署選項的容錯能力 – 選用中，請輸入在 CloudFormation 停止操作之前堆疊可以失敗的帳戶數量。建議您輸入要新增的帳戶數量減一。例如，如果您指定的 OU 有 10 個成員帳戶，請輸入 9。這意味著，即使 CloudFormation 操作失敗 9 次，至少有一個帳戶會成功。
15. 選擇 Next (下一步)。
16. 在 Review (檢閱) 頁面上，檢閱您的選項，然後選擇 Submit (提交)。您可以在 Stack instances (堆疊執行個體) 標籤上檢查您的堆疊狀態。
17. (選用) 重複此程序以上傳 Slack 頻道組態的範本。範例範本也會建立 IAM 角色並連接 AWS 受管政策。此角色具有為您存取其他服務所需的許可。如需更多詳細資訊，請參閱 管理 AWS Support 應用程式的存取權。

    如果您沒有建立堆疊集來建立 Slack 頻道組態，則您的成員帳戶可以手動設定 Slack 頻道。如需更多詳細資訊，請參閱 設定 Slack 頻道。

在 CloudFormation 建立堆疊之後，每個成員帳戶都可以登入 Support Center Console 並尋找其設定的 Slack 工作區和通道。然後，他們可以在 AWS 帳戶 中使用 AWS Support 應用程式。請參閱 在 Slack 頻道中建立支援案例。

> **Tip**
>
> 如果您需要上傳新的範本，則建議您使用之前指定的相同 AWS 區域。

進一步了解 CloudFormation

若要進一步了解 CloudFormation，請參閱下列資源：

- AWS CloudFormation
- 《AWS CloudFormation 使用者指南》https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html
- AWS CloudFormation API 參考
- 《AWS CloudFormation 命令列介面使用者指南》https://docs.aws.amazon.com/cloudformation-cli/latest/userguide/what-is-cloudformation-cli.html

使用 Terraform 建立 AWS Support 應用程式資源

您也可以使用 Terraform 為您的 AWS 帳戶 建立 AWS Support 應用程式資源。Terraform 是一種基礎設施即程式碼工具，可用於雲端應用程式。您可以使用 Terraform 來建立 AWS Support 應用程式資源，而不是將 CloudFormation 堆疊部署至帳戶。

安裝 Terraform 之後，您可以指定所需的 AWS Support 應用程式資源。Terraform 會呼叫 RegisterSlackWorkspaceForOrganization API 操作，以為您註冊 Slack 工作區，並建立您的資源。然後，您可以登入 Support Center Console 並尋找已設定的 Slack 工作區和頻道。

> **備註**
>
> - 如果您是組織的管理帳戶，則必須先手動為您的帳戶授權 Slack 工作區，然後您的成員帳戶才能使用 Terraform 來建立資源。如果您尚未這麼做，則請參閱 授權 Slack 工作區。
> - 與 CloudFormation 堆疊集不同，您無法使用 Terraform 為組織中的 OU 建立 AWS Support 應用程式資源。
> - 您也可以在 AWS CloudTrail 中從 Terraform 尋找這些更新的事件歷史記錄。這些事件的 `eventSource` 將是 `cloudcontrolapi.amazonaws.com` 和 `supportapp.amazonaws.com`。如需更多詳細資訊，請參閱 使用 AWS CloudTrail 在 Slack API 呼叫中記錄 AWS Support 應用程式。

進一步了解

若要進一步了解 Terraform，請參閱下列主題：

- Terraform 安裝
- Terraform 教學課程：建置 AWS 的基礎設施
- awscc_support_app_account_alias
- awscc_supportapp_slack_workspace_configuration
- awscc_supportapp_slack_channel_configuration

中的安全性 AWS Support

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，該架構專為滿足對安全性最敏感的組織的需求而打造。

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

- 雲端的安全性 — AWS 負責保護在 AWS 雲端中執行 AWS 服務的基礎架構。 AWS 還為您提供可以安全使用的服務。若要了解適用於的合規計劃 AWS Support，請參閱AWS 合規計劃 Amazon Web Services 在合規計劃服務範圍。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

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

主題

資料保護 AWS Support

AWS 共用責任模型適用於中的資料保護 AWS Support。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 FIPS 和 FIPS 端點的相關資訊，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 Support 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。

為您的 AWS Support 案件提供安全

建立支援案例時，您擁有包含在支援案例中的資訊。 AWS 未經您的許可，不會訪問您的 AWS 帳戶 數據。 AWS 不會與第三方共享您的信息。

建立支援案例時，請注意下列事項：

- AWS Support 使用`AWSServiceRoleForSupport`服務連結角色中定義的權限來呼叫其他為您疑難排 AWS 服務 解客戶問題的其他權限。如需詳細資訊，請參閱使用服務連結角色以 AWS Support 及AWS 受管理的策略： AWSSupportServiceRolePolicy。
- 您可以查看 AWS Support 發生在 AWS 帳戶. 例如，您可以在帳戶中有人建立或解決支援案例時檢視日誌資訊。如需詳細資訊，請 AWS Support 參閱使用 AWS CloudTrail.
- 您可以使用 AWS Support API 來呼叫 `DescribeCases` API。此 API 會傳回支援案例資訊，例如案例 ID、建立和解決日期以及與支援客服人員的通訊。建立案例後的 12 個月內都可檢視案例詳細資訊。如需詳細資訊，請參閱 AWS Support API 參考中的 DescribeCases。
- 您的支援案例遵守 AWS Support的法規遵循驗證。
- 建立支援案例時， AWS 無法存取您的帳戶。如有必要，支援客服人員會使用螢幕共用工具從遠端檢視您的螢幕，並確定和疑難排解問題。此工具僅供檢視。 AWS Support 無法在螢幕共用工作階段期

間為您採取動作。您必須同意才能與支援客服人員共用螢幕。如需詳細資訊，請參閱 AWS Support 常見問答集。

- 您可以變更 AWS Support 方案以取得帳戶所需的協助。如需詳細資訊，請參閱比較方 AWS Support 案和變更您的 AWS Support 方案。

的身分識別與存取管理 AWS Support

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 Support 資源。IAM 是您可以使用的 AWS 服務 ，無需額外付費。

主題

- 物件
- 使用身分驗證
- 使用政策管理存取權
- 如何與 IAM AWS Support 搭配使用
- AWS Support 以識別為基礎的原則範例
- 使用服務連結角色
- AWS 受管理的政策 AWS Support
- 管理對 AWS Support 中心的存取
- 管理對 AWS Support 計劃的存取
- 管理存取 AWS Trusted Advisor
- 適用於 AWS Trusted Advisor的服務控制政策範例
- 疑難排解 AWS Support 身分和存取

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 Support。

服務使用者 — 如果您使用 AWS Support 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 Support 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 Support中的某項功能，請參閱 疑難排解 AWS Support 身分和存取。

服務管理員 — 如果您負責公司的 AWS Support 資源，您可能擁有完整的存取權 AWS Support。決定您的服務使用者應該存取哪些 AWS Support 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 Support，請參閱如何與 IAM AWS Support 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 Support存取權的詳細資訊。若要檢視可在 IAM 中使用的 AWS Support 基於身分的政策範例，請參閱。AWS Support 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您的要求。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。如需詳細資訊，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 帳號根使用者

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作業。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。

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。建議您盡可能依賴臨時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需詳細資訊，請參閱《IAM 使用者指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#rotate-credentials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。若要進一步了解，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 – 若要向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需聯合角色的相關資訊，請參閱《IAM 使用者指南》中的為第三方身分供應商建立角色。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：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。角色是授予跨帳户存取權的主要方式。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）。若要了解跨帳户存取權和資源型政策間的差異，請參閱《IAM 使用者指南》中的 IAM 角色與資源類型政策的差異。
- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。

- 轉寄存取工作階段 (FAS) — 當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。
- 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，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 執行個體內存放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臨時性憑證。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。

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

使用政策管理存取權

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

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

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

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

身分型政策

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

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

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：許可界限是一種進階功能，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的限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可邊界的相關資訊，請參閱《IAM 使用者指南》中的 IAM 實體許可邊界。
- 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身分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 Support 搭配使用

在您使用 IAM 管理存取權限之前 AWS Support，您應該瞭解哪些 IAM 功能可搭配使用 AWS Support。若要深入瞭解如何以 AWS Support 及其他 AWS 服務如何與 IAM 搭配使用，請參閱 IAM 使用者指南中的與 IAM 搭配使用的AWS 服務。

如需如何管理 AWS Support 使用 IAM 存取權的詳細資訊，請參閱管理的 AWS Support.

主題

- AWS Support 身分型政策
- AWS Support IAM 角色

AWS Support 身分型政策

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下會允許或拒絕動作。AWS Support 支援特定動作。若要了解 JSON 政策中使用的所有元素，請參閱 IAM 使用者指南中的 IAM JSON 政策元素參考。

動作

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

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

政策會使用動作來授予執行相關聯動作的許可。

中的策略動作在動作之前 AWS Support 使用下列前置詞：`support:`例如，若要授予某人使用 Amazon EC2 `RunInstances` API 作業來執行 Amazon EC2 執行個體的許可，請在其政策中加入 `ec2:RunInstances` 動作。政策陳述式必須包含 `Action` 或 `NotAction` 元素。 AWS Support 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。

若要在單一陳述式中指定多個動作，請用逗號分隔，如下所示：

```
"Action": [
      "ec2:action1",
      "ec2:action2"
```

您也可以使用萬用字元 (*) 來指定多個動作。例如，若要指定開頭是 Describe 文字的所有動作，請包含以下動作：

```
"Action": "ec2:Describe*"
```

若要查看 AWS Support 動作清單，請參閱 IAM 使用者指南 AWS Support中的定義動作。

範例

若要檢視以 AWS Support 身分為基礎的原則範例，請參閱。AWS Support 以識別為基礎的原則範例

AWS Support IAM 角色

IAM 角色是您 AWS 帳戶中具有特定許可的實體。

使用臨時登入資料 AWS Support

您可以搭配聯合使用暫時憑證、擔任 IAM 角色，或是擔任跨帳戶角色。您可以透過呼叫AssumeRole或等 AWS STS API 作業來取得臨時安全登入資料GetFederationToken。

AWS Support 支援使用臨時認證。

服務連結角色

服務連結角色可讓 AWS 服務存取其他服務中的資源，以代表您完成動作。服務連結角色會顯示在您的 IAM 帳戶中，並由該服務所擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

AWS Support 支援服務連結角色。如需有關建立或管理 AWS Support 服務連結角色的詳細資訊，請參閱使用 AWS Support的服務連結角色。

服務角色

此功能可讓服務代表您擔任服務角色。此角色可讓服務存取其他服務中的資源，以代表您完成動作。服務角色會出現在您的 IAM 帳戶中，且由該帳戶所擁有。這表示 IAM 管理員可以變更此角色的許可。不過，這樣可能會破壞此服務的功能。

AWS Support 支援服務角色。

AWS Support 以識別為基礎的原則範例

根據預設，IAM 使用者和角色不具備建立或修改 AWS Support 資源的許可。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 IAM 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 標籤上建立政策。

主題

- 政策最佳實務
- 使用 AWS Support 主控台
- 允許使用者檢視他們自己的許可

政策最佳實務

身分型政策相當強大。他們決定是否有人可以建立、存取或刪除您帳戶中的 AWS Support 資源。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：

- 使用 AWS 受管政策開始使用 — 若要 AWS Support 快速開始使用，請使用 AWS 受管理的政策為您的員工提供所需的權限。這些政策已在您的帳戶中提供，並由 AWS維護和更新。如需詳細資訊，請參閱 IAM 使用者指南中的 AWS 受管政策開始使用許可。
- 授予最低權限 – 當您建立自訂政策時，請只授予執行任務所需要的許可。以最小一組許可開始，然後依需要授予額外的許可。這比一開始使用太寬鬆的許可，稍後再嘗試將他們限縮更為安全。如需詳細資訊，請參閱《IAM 使用者指南》中的授予最低權限。
- 為敏感操作啟用 MFA – 為了增加安全，請要求 IAM 使用者使用多重驗證 (MFA) 存取敏感資源或 API 操作。如需詳細資訊，請參閱《IAM 使用者指南》中的在 AWS中使用多重要素驗證 (MFA)。
- 使用政策條件以增加安全 – 在切實可行的範圍中，請定義您身分類型政策允許存取資源的條件。例如，您可以撰寫條件，指定請求必須來自一定的允許 IP 地址範圍。您也可以撰寫條件，只在指定的日期或時間範圍內允許請求，或是要求使用 SSL 或 MFA。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 AWS Support 主控台

若要存取 AWS Support 主控台，您必須擁有最少一組權限。這些權限必須允許您列出並檢視您 AWS 帳戶中 AWS Support 資源的詳細資料。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 (IAM 使用者或角色) 而言，主控台就無法如預期運作。

為了確保這些實體仍然可以使用 AWS Support 主控台，請同時將下列 AWS 受管理的原則附加至實體。如需詳細資訊，請參閱《IAM 使用者指南》中的新增許可到使用者。

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": "*"
        }
    ]
}
```

使用服務連結角色

AWS Support 並 AWS Trusted Advisor 使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至 AWS Support 和 Trusted Advisor的唯一 IAM 角色。在每個案例中，服務連結角色是預先定義的角色。此角色包括代表您呼叫其他 AWS 服務的所有權限 AWS Support 或 Trusted Advisor 需要的權限。下列主題說明服務連結角色的作用，以及如何在 AWS Support 和 Trusted Advisor中使用這些角色。

主題

使用 AWS Support的服務連結角色

AWS Support 工具透過 API 呼叫收集資 AWS 源相關資訊，以提供客戶服務和技術支援。為了提高支援活動的透明度和可稽核性，請 AWS Support 使用 AWS Identity and Access Management (IAM) 服務連結角色。

`AWSServiceRoleForSupport`服務連結角色是直接連結到 AWS Support的唯一 IAM 角色。此服務連結角色是預先定義的，其中包含代表您呼叫其他 AWS 服務所 AWS Support 需的權限。

`AWSServiceRoleForSupport` 服務連結角色信任 `support.amazonaws.com` 服務來擔任該角色。

為了提供這些服務，角色的預先定義權限會授予資源中繼資料的 AWS Support 存取權，而非客戶資料。只有 AWS Support 工具可以擔任此角色，該角色存在於您的 AWS 帳戶中。

我們會事先刪除可能包含客戶資料的欄位。例如， AWS Step Functions API 呼叫的`Input`和`Output`欄位GetExecutionHistory對於看不見 AWS Support。我們使用 AWS KMS keys 來加密敏感欄位。這些欄位會在 API 回應中編輯，而且 AWS Support 代理程式無法看見這些欄位。

> **Note**
>
> AWS Trusted Advisor 使用個別的 IAM 服務連結角色來存取帳戶的 AWS 資源，以提供最佳實務建議和檢查。如需詳細資訊，請參閱 使用 Trusted Advisor的服務連結角色。

`AWSServiceRoleForSupport`服務連結角色可讓客戶透過 AWS CloudTrail查看所有 AWS Support API 呼叫。這有助於監視和稽核需求，因為它提供了一種透明的方式來瞭解代表您 AWS Support 執行的動作。若要取得有關資訊 CloudTrail，請參閱《AWS CloudTrail 使用指南》。

AWS Support的服務連結角色許可

此角色使用受AWSSupportServiceRolePolicy AWS 管理的策略。此受管政策會連接至角色，提供允許代表您完成動作的角色許可。

可能包括下列動作：

- 帳單、管理、支援和其他客戶服務 — AWS 客戶服務會使用受管理政策授予的權限，在您的支援方案中執行多項服務。這些包括調查和回答帳戶和帳單相關問題、為您的帳戶提供管理支援、提高服務配額，以及提供額外的客戶支援。
- 處理您 AWS 帳戶的服務屬性和使用資料 — AWS Support 可能會使用受管理策略授予的權限來存取您 AWS 帳戶的服務屬性和使用資料。此政策允許 AWS Support 為您的帳戶提供帳單、管理和技術支援。服務屬性包括您帳戶的資源識別碼、中繼資料標籤、角色和許可。用量資料包括使用政策、用量統計資料和分析。
- 維護您帳戶及其資源的運作狀態 — AWS Support 使用自動化工具執行與營運和技術支援相關的動作。

如需允許服務和動作的詳細資訊，請參閱 IAM 主控台中的 AWSSupportServiceRolePolicy 政策。

> **Note**
>
> AWS Support 每月自動更新一次AWSSupportServiceRolePolicy原則，以新增 AWS 服務和動作的權限。

如需詳細資訊，請參閱 AWS 受管理的政策 AWS Support。

建立服務連結角色 AWS Support

您無須手動建立 AWSServiceRoleForSupport 角色。當您建立 AWS 帳號時，系統會自動為您建立和設定此角色。

> **Important**
>
> 如果您在開始支援服務連結角色 AWS Support 之前使用過，則會在您的帳戶中 AWS 建立AWSServiceRoleForSupport角色。如需詳細資訊，請參閱我的 IAM 帳戶中出現新角色。

編輯和刪除下列項目的服務連結角色 AWS Support

您可以使用 IAM 來編輯 `AWSServiceRoleForSupport` 服務連結角色的說明。如需詳細資訊，請參閱 IAM 使用者指南中的編輯服務連結角色。

該`AWSServiceRoleForSupport`角色對於為您 AWS Support 的帳戶提供管理、操作和技術支援是必要的。因此，無法透過 IAM 主控台、API 或 AWS Command Line Interface (AWS CLI) 刪除此角色。這樣可保護您的 AWS 帳戶，因為您不會無意中移除管理支援服務的必要許可。

如需 `AWSServiceRoleForSupport` 角色和其使用者的詳細資訊，請聯絡 AWS Support。

使用 Trusted Advisor的服務連結角色

AWS Trusted Advisor 使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結到 AWS Trusted Advisor的唯一 IAM 角色。服務連結角色由預先定義 Trusted Advisor，包括服務代表您呼叫其他 AWS 服務所需的所有權限。 Trusted Advisor 使用此角色來檢查您的使用情況， AWS 並提供改善 AWS 環境的建議。例如， Trusted Advisor 分析 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的使用情況，以協助您降低成本、提高效能、容忍故障並改善安全性。

> **Note**
>
> AWS Support 使用個別的 IAM 服務連結角色來存取帳戶的資源，以提供帳單、管理和支援服務。如需詳細資訊，請參閱 使用 AWS Support的服務連結角色。

關於支援服務連結角色的其他服務，如需相關資訊，請參閱搭配 IAM 使用的AWS 服務。尋找服務連結角色欄中顯示 Yes (是) 的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

主題

- Trusted Advisor的服務連結角色許可
- 管理服務連結角色的許可
- 為 Trusted Advisor建立服務連結角色
- 為 Trusted Advisor編輯服務連結角色
- 為 Trusted Advisor刪除服務連結角色

Trusted Advisor的服務連結角色許可

Trusted Advisor 使用兩個服務連結角色：

- AWSServiceRoleForTrustedAdvisor— 此角色信任 Trusted Advisor 服務會擔任代表您存取 AWS 服務的角色。角色權限原則允許所有 AWS 資源的 Trusted Advisor 唯讀存取。此角色可簡化 AWS 帳戶的入門程序，因為您不需要為 Trusted Advisor. 當您開設 AWS 帳戶時，請為您 Trusted Advisor 創建此角色。已定義的許可包括信任政策和許可政策。許可政策無法連接到其他任何 IAM 實體。

  如需有關連接政策的詳細資訊，請參閱 AWSTrustedAdvisorServiceRolePolicy。

- AWSServiceRoleForTrustedAdvisorReporting - 這個角色信任 Trusted Advisor 服務擔任使用組織檢視功能的角色。此角色可在 AWS Organizations 組織中啟用 Trusted Advisor 為受信任的服務。Trusted Advisor 當您啟用組織檢視時，會為您建立此角色。

  如需有關連接政策的詳細資訊，請參閱 AWSTrustedAdvisorReportingServiceRolePolicy。

  您可以使用組織檢視來建立組織中所有帳戶的 Trusted Advisor 檢查結果報告。如需使用此功能的詳細資訊，請參閱「AWS Trusted Advisor 的組織檢視」。

管理服務連結角色的許可

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。下列範例使用 AWSServiceRoleForTrustedAdvisor 服務連結角色。

Example ：允取 IAM 實體建立 **AWSServiceRoleForTrustedAdvisor** 服務連結角色

只有在 Trusted Advisor 帳戶已停用、刪除服務連結角色，且使用者必須重新建立角色才能重 Trusted Advisor新啟用時，才需要執行此步驟。

您可將下列陳述式新增至 IAM 實體建立服務連結角色所需的許可政策。

```
{
    "Effect": "Allow",
    "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:PutRolePolicy"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/
AWSServiceRoleForTrustedAdvisor*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

Example ：允取 IAM 實體編輯 **AWSServiceRoleForTrustedAdvisor** 服務連結角色的描述

您只能編輯 AWSServiceRoleForTrustedAdvisor 角色的描述。您可將下列陳述式新增至 IAM 實體編輯服務連結角色描述所需的許可政策。

```
{
    "Effect": "Allow",
    "Action": [
        "iam:UpdateRoleDescription"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/
AWSServiceRoleForTrustedAdvisor*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

Example ：允取 IAM 實體刪除 **AWSServiceRoleForTrustedAdvisor** 服務連結角色

您可將下列陳述式新增至 IAM 實體刪除服務連結角色所需的許可政策。

```
{
    "Effect": "Allow",
    "Action": [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/
AWSServiceRoleForTrustedAdvisor*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

您也可以使用 AWS 受管理的策略，例如 AdministratorAccess，提供對的完整存取權 Trusted Advisor。

為 Trusted Advisor建立服務連結角色

您不需要手動建立 AWSServiceRoleForTrustedAdvisor 服務連結角色。當您開設 AWS 帳戶時，Trusted Advisor 會為您建立服務連結角色。

> **Important**
>
> 如果您在開始支援 Trusted Advisor 服務連結角色之前使用服務，則 Trusted Advisor 已在您的帳戶中建立該AWSServiceRoleForTrustedAdvisor角色。若要進一步了解，請參閱 IAM 使用者指南中的我的 IAM 帳戶中出現新角色。

如果您的帳戶沒有 AWSServiceRoleForTrustedAdvisor 服務連結角色， Trusted Advisor 將無法如預期運作。若您帳戶中的某個人停用 Trusted Advisor ，然後刪除服務連結角色，可能會發生此情形。在這種情況下，您可以使用 IAM 來建立 AWSServiceRoleForTrustedAdvisor 服務連結角色，然後重新啟用 Trusted Advisor。

啟用 Trusted Advisor （控制台）

1. 使用 IAM 主控 AWS CLI台或 IAM API 為 Trusted Advisor其建立服務連結角色。如需詳細資訊，請參閱建立服務連結角色。
2. 登入 AWS Management Console，然後瀏覽至的主 Trusted Advisor 控台https://console.aws.amazon.com/trustedadvisor。

   Disabled Trusted Advisor (已停用 Trusted Advisor) 狀態橫幅會顯示於主控台中。
3. 從狀態標題中選擇「啟用 Trusted Advisor 角色」。如果未偵測到必要的 AWSServiceRoleForTrustedAdvisor，將持續顯示停用狀態橫幅。

為 Trusted Advisor編輯服務連結角色

因為各種實體可能會參考角色，所以您無法變更服務連結角色的名稱。不過，您可以使用 IAM 主控台或 IAM API 編輯角色的說明。 AWS CLI如需詳細資訊，請參閱《IAM 使用者指南》中的編輯服務連結角色。

為 Trusted Advisor刪除服務連結角色

如果您不需要使用的功能或服務 Trusted Advisor，則可以刪除AWSServiceRoleForTrustedAdvisor角色。您必須 Trusted Advisor 先停用，才能刪除此服務連結角色。這可防止您移除 Trusted Advisor 操作所需的許可。停用時 Trusted Advisor，您會停用所有服務功能，包括離線處理和通知。此外，如果您停 Trusted Advisor 用某個成員帳戶，則個別付款人帳戶也會受到影響，這表示您不會收到可識別節省成本的方法的支 Trusted Advisor 票。您無法存取 Trusted Advisor 主控台。API 呼叫以 Trusted Advisor 傳回拒絕存取錯誤。

您必須重新建立 AWSServiceRoleForTrustedAdvisor 服務連結角色，才能重新啟用 Trusted Advisor。

您必須先在主控台 Trusted Advisor 中停用，才能刪除AWSServiceRoleForTrustedAdvisor服務連結角色。

若要停用 Trusted Advisor

1. 登入 AWS Management Console 並瀏覽至 Trusted Advisor 主控台，位於https://console.aws.amazon.com/trustedadvisor。
2. 在導覽窗格中，選擇偏好設定。
3. 在 Service Linked Role Permissions (服務連結角色許可) 區段中，選擇 Disable Trusted Advisor(停用 &SERVICENAME;)。
4. 在確認對話方塊中，選擇 OK (確定)，確認您要停用 Trusted Advisor。

停用之後 Trusted Advisor，所有 Trusted Advisor 功能都會停用，且 Trusted Advisor 主控台只會顯示停用狀態標題。

然後，您可以使用 IAM 主控 AWS CLI台或 IAM API 刪除名為AWSServiceRoleForTrustedAdvisor的 Trusted Advisor 服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

AWS 受管理的政策 AWS Support

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。

主題

- AWS 受管理的政策 AWS Support

- AWS 適用於 Slack 中 AWS Support 應用程式的受管政策
- AWS 受管理的政策 AWS Trusted Advisor
- AWS 受管理的 AWS Support 計劃原則

AWS 受管理的政策 AWS Support

AWS Support 具有下列受管理的策略。

內容

- AWS 受管理的策略：AWSSupportServiceRolePolicy
- AWS SupportAWS 受管理策略的更新
- AWSSupportServiceRolePolicy 的許可變更

AWS 受管理的策略：AWSSupportServiceRolePolicy

AWS Support 使用受AWSSupportServiceRolePolicy AWS 管理的策略。此受管政策連接至 `AWSServiceRoleForSupport` 服務連結角色。政策允許服務連結角色代表您完成動作。您無法將此政策連接至 IAM 實體。如需詳細資訊，請參閱 AWS Support的服務連結角色許可。

如需政策變更清單，請參閱 AWS SupportAWS 受管理策略的更新 和 AWSSupportServiceRolePolicy 的許可變更。

AWS SupportAWS 受管理策略的更新

檢視這些服務開始追蹤這些變更以 AWS Support 來 AWS 受管理政策的更新詳細資料。如需有關此頁面變更的自動提醒，請訂閱 文件歷史紀錄 頁面的 RSS 摘要。

下表說明自 2022 年 2 月 17 日起對 AWS Support 受管理策略的重要更新。

AWS Support

變更	描述	日期
AWSSupportServiceRolePolicy – 更新現有政策	為下列服務新增 17 項新權限，可執行動作，協助疑難排解與	2024年3月22 日

變更	描述	日期
	帳單、管理和技術支援相關的客戶問題： • Amazon CloudWatch 網路監控器 — 疑難排解與網路監控服務相關的問題。 • Amazon CloudWatch 日誌 — 對與 Amazon 日 CloudWatch 誌相關的問題進行除錯。 • 適用於 Apache 卡夫卡的 Amazon 受管串流 — 為 Apache 卡夫卡偵錯與 Amazon 受管串流相關的問題。 • 適用於 Prometheus 的 Amazon 受管服務 — 針對 Prometheus 的 Amazon 託管服務進行疑難排解。	

變更	描述	日期
AWSSupportServiceRolePolicy – 更新現有政策	為下列服務新增 63 個新權限，以執行動作，協助疑難排解與帳單、管理和技術支援相關的客戶問題： • AWS 無塵室 — 疑難排解與 AWS 潔淨室相關的問題。 • CodeConnections — 要解決相關問題 CodeConnections. • Amazon EKS — 調試與 Amazon EKS 相關的問題。 • Image Builder — 偵錯與 Image Builder 相關的問題。 • Amazon 檢查器 2 — 解決與 Amazon 檢查器 2 相關的問題。 • Amazon Inspector 掃描 — 調試與 Amazon Inspector 掃描相關的問題。 • Amazon CloudWatch 日誌 — 疑難排解與 Amazon CloudWatch 日誌相關的問題。 • AWS Outposts — 若要疑難排解與 AWS Outposts. • Amazon RDS - 偵錯與 Amazon RDS 相關的問題。 • AWS IAM Identity Center — 要解決相關問題 AWS IAM Identity Center. • Amazon S3 快遞 — 調試與 Amazon S3 快遞相關的問題。	2024年1月17日

變更	描述	日期
	• AWS Trusted Advisor — 要解決相關問題 AWS Trusted Advisor.	

變更	描述	日期
AWSSupportServiceRolePolicy – 更新現有政策	為下列服務新增 126 項新權限，以執行動作，協助疑難排解與帳單、管理和技術支援相關的客戶問題： • AWS Direct Connect — 解決與 AWS Direct Connect 服務相關的問題。 • Amazon SageMaker — 解決與 Amazon SageMaker 服務相關的問題。 • Amazon AppStream -調試與 Amazon 有關的問題 AppStream。 • AWS 資源總管 — 若要偵錯與 AWS 資源總管. • 亞馬遜無伺服器 — 疑難排解與亞馬遜無伺服器相關的問題。 • Amazon ElastiCache -調試與 Amazon 有關的問題 ElastiCache。 • Amazon Comprehend – 疑難排解 Amazon Comprehend 相關的問題。 • Amazon EC2 — 疑難排解與 Amazon EC2 相關的問題。 • Amazon Elastic Kubernetes Service — 調試與 Amazon Elastic Kubernetes Service 相關的問題。 • AWS Elastic Disaster Recovery — 要解決相關	2023年12月6日

變更	描述	日期
	問題 AWS Elastic Disaster Recovery. • AWS AppSync — 調試相關的問題 AWS AppSync. • Amazon CloudWatch 日誌 — 疑難排解與 Amazon CloudWatch 日誌相關的問題。 • AWS Health — 除錯與本 AWS Health 服務相關的問題。 • Amazon Connect — 調試與 Amazon Connect 相關的問題。 • AWS Snowball — 要解決相關問題 AWS Snowball. • AWS Health複製影像 — 疑難排解與 AWS Health影像相關的問題。	

變更	描述	日期
AWSSupportServiceRolePolicy – 更新現有政策	在以下服務中新增了 163 項新許可，以執行有助於解決客戶在計費、管理和技術支援方面相關問題的動作： • Amazon CloudFront — 解決與 CloudFront 服務相關的問題。 • Amazon EC2 – 疑難排解與 Amazon EC2 服務相關的問題。 • Amazon AppStream -調試與 Amazon 有關的問題 AppStream。 • AWS WAF — 偵錯與 AWS Web 應用程式防火牆相關的問題。 • Amazon Connect – 疑難排解與 Amazon Connect 相關的問題。 • AWS IoT — 若要偵錯與 AWS IoT. • Amazon Route 53 – 疑難排解與 Amazon Route 53 相關的問題。 • AWS 已驗證存取權 — 疑難排解與 AWS 已驗證存取服務相關的問題。 • Amazon Simple Email Service – 偵錯與 Amazon Simple Email Service 相關的問題。	2023 年 10 月 27 日

變更	描述	日期
	• AWS Elastic Beanstalk — 要解決相關問題 AWS Elastic Beanstalk. • Amazon DynamoDB – 偵錯與 Amazon DynamoDB 相關的問題。 • AWS EC2 Image Builder — 疑難排解與 AWS EC2 Image Builder 相關的問題。 • AWS Outposts — 除錯與本 AWS Outposts 服務相關的問題。 • AWS Glue — 若要偵錯與 AWS Glue. • AWS Directory Service — 要解決相關問題 AWS Directory Service. • AWS Elastic Disaster Recovery — 要解決相關問題 AWS Elastic Disaster Recovery. • AWS Step Functions — 調試相關的問題 AWS Step Functions. • Amazon EMR – 疑難排解與 Amazon EMR 相關的問題。 • Amazon Relational Database Service – 疑難排解與 Amazon Relational Database Service 相關的問題。 • Amazon EC2 Systems Manager – 偵錯與 Amazon	

變更	描述	日期
	EC2 Systems Manager 相關的問題。	

變更	描述	日期
AWSSupportServiceRolePolicy – 更新現有政策	在以下服務中新增了 176 項新許可，以執行有助於解決客戶在計費、管理和技術支援方面相關問題的動作： • AWS Glue — 解決與 AWS Glue 服務相關的問題 • Amazon EMR – 疑難排解與 Amazon EMR 服務相關的問題。 • Amazon Security Lake - 偵錯與 Amazon Security Lake 相關的問題。 • AWS Systems Manager — 偵錯與 Systems Manager 服務相關的問題。 • Amazon Verified Permissions – 疑難排解與 Amazon Verified Permissions 相關的問題。 • AWS IAM 存取分析器 — 偵錯與 IAM 存取分析器服務相關的問題。 • AWS Backup — 要解決相關問題 AWS Backup. • AWS Database Migration Service — 疑難排解與 DMS 服務相關的問題。 • Amazon DynamoDB – 偵錯與 DynamoDB 相關的問題。 • Amazon Elastic Container Registry (Amazon ECR) – 疑難排解與 Amazon Elastic	2023 年 8 月 28 日

變更	描述	日期
	Container Registry (Amazon ECR) 相關的問題。 • Amazon Elastic Container Service – 偵錯與 Amazon Elastic Container Service 相關的問題。 • Amazon Elastic Kubernetes Service - 疑難排解與 Amazon Elastic Kubernetes Service 相關的問題。 • Amazon EMR Serverless – 偵錯與 Amazon EMR Serverless 服務相關的問題。 • AWS Identity and Access Management — 要解決相關問題 AWS Identity and Access Management. • AWS Network Firewall — 疑難排解與 AWS Network Firewall 相關的問題。 • AWS HealthOmics — 調試相關的問題 AWS HealthOmics. • Amazon QuickSight -調試與 Amazon 有關的問題 QuickSight。 • Amazon Relational Database Service – 疑難排解與 Amazon Relational Database Service 相關的問題。	

變更	描述	日期
	• Amazon Redshift – 疑難排解與 Amazon Redshift 相關的問題。 • Amazon Redshift Serverless – 偵錯與 Amazon Redshift Serverless 相關的問題。 • Amazon SageMaker -調試與 Amazon 有關的問題 SageMaker。	

變更	描述	日期
AWSSupportServiceRolePolicy – 更新現有政策	在以下服務中新增了 141 項新許可，以執行有助於解決客戶在計費、管理和技術支援方面相關問題的動作： • Lambda – 疑難排解與 Lambda 服務相關的問題。 • Amazon Lex – 疑難排解與 Amazon Lex 服務相關的問題。 • AWS 移轉 — 偵錯與「移轉服務」相關的問題。 • AWS Amplify — 調試與 Amplify 服務相關的問題。 • Amazon EventBridge 管道 — 疑難排解與 Pipes 相關的許可和帳單問題。 • Amazon EventBridge -調試與 Amazon 有關的問題 EventBridge • Amazon CloudWatch 日誌 — 疑難排解與 Amazon CloudWatch 日誌相關的問題。 • AWS Systems Manager — 疑難排解與 Systems Manager 相關的問題。 • Amazon CloudWatch — 調試相關的問題 CloudWatch. • Amazon ElastiCache -解決與 Amazon 相關的問題 ElastiCache。	2023 年 6 月 26 日

變更	描述	日期
	• Amazon Athena – 偵錯與 Athena 相關的問題。 • AWS Elastic Disaster Recovery — 解決與彈性災難恢復相關的問題。 • Amazon CloudWatch - Amazon 的配置故障排除 CloudWatch。 • Amazon EC2 – 偵錯與 EC2 服務相關的問題。 • AWS Certificate Manager — 疑難排解與 Certificate Manager 相關的問題。 • Amazon EventBridge 排程器 — 疑難排解與 EventBridge 排程器相關的問題。 • Amazon OpenSearch 服務 — 疑難排解 OpenSearch. • Amazon EventBridge 模式 — 調試與架 EventBridge 構相關的問題。 • AWS 使用者通知 — 疑難排解與使用者通知相關的問題。 • Amazon CloudWatch 應用程式洞察 — 疑難排解與 CloudWatch 應用程式洞察相關的問題。 • Amazon DynamoDB – 疑難排解與 DynamoDB 相關的問題。 • Amazon DocumentDB 彈性叢集 – 疑難排解與	

變更	描述	日期
	DocumentDB 彈性叢集相關的問題。	

變更	描述	日期
AWSSupportServiceRolePolicy – 更新現有政策	在以下服務中新增了 53 項新許可，以執行有助於解決客戶在計費、管理和技術支援方面相關問題的動作： • Auto Scaling – 疑難排解與 Auto Scaling 服務相關的問題。 • Amazon CloudWatch -解決與 Amazon 相關的問題 CloudWatch。 • AWS Compute Optimizer — 疑難排解與 Compute Optimizer 相關的問題。 • Amazon CloudWatch 顯然-為了解決與明顯相關的問題。 • EC2 Image Builder – 疑難排解與 Image Builder 服務相關的問題。 • AWS IoT TwinMaker — 要解決相關問題 AWS IoT TwinMaker. • Amazon CloudWatch 日誌 — 疑難排解與 Amazon CloudWatch 日誌相關的問題。 • Amazon Pinpoint – 疑難排解 Amazon Pinpoint 相關的問題。 • AWS OAM 連結 — 偵錯與 OAM 資源相關的問題。	2023 年 5 月 2 日

變更	描述	日期
	• AWS Outposts — 要解決相關問題 AWS Outposts. • Amazon RDS - 偵錯與 Amazon RDS 相關的問題。 • AWS 資源總管 — 疑難排解與資源總管相關的問題。 • Amazon CloudWatch RUM — 對 RUM 服務資源的組態進行故障排除。 • Amazon SNS – 疑難排解 Amazon SNS 相關的問題。 • Amazon CloudWatch Synthetics — 解決與 S CloudWatch ynthetics 相關的問題。	

變更	描述	日期
AWSSupportServiceRolePolicy – 更新現有政策	在以下服務中新增了 52 項新許可，以執行有助於解決客戶在計費、管理和技術支援方面相關問題的動作： • AWS Backup gateway — 疑難排解與 Backup 閘道相關的問題。 • Amazon S3 – 偵錯與 Amazon S3 相關的問題。 • AWS Application Migration Service — 疑難排解與應用程式遷移服務相關的問題。 • AWS 潔淨室 — 除錯與 AWS 潔淨室有關的問題； • AWS Systems Manager 適用於 SAP — 疑難排解與 SAP 相關 AWS Systems Manager 的問題。 • Amazon VPC Lattice – 偵錯與 Amazon VPC Lattice 相關的問題。	2023 年 3 月 16 日

變更	描述	日期
AWSSupportServiceRolePolicy – 更新現有政策	在以下服務中新增了 220 項新許可，以執行有助於解決客戶在計費、管理和技術支援方面相關問題的動作： • Amazon Athena — 能 AWS Support 夠開發工具，以協助客戶處理與 Athena 相關的查詢。 • Amazon Chime – 疑難排解 Amazon Chime 相關的問題。 • Amazon CloudWatch 互聯網監控器 — 調試與互聯網監控有關的問題。 • Amazon Comprehend – 疑難排解 Amazon Comprehend 相關的問題。 • Amazon Elastic Compute Cloud – 偵錯與 Transit Gateway Connect 和多播功能相關的問題。 • Amazon EventBridge 管道 — 疑難排解與 EventBridge 管道相關的問題。 • Amazon 互動式視頻服務 — 可以查詢 Amazon IVS 資源 AWS Support 以對客戶問題進行故障排除。 • Amazon FSx — 啟用開發工具 AWS Support 以支援 Amazon FSx 資料儲存庫的匯入和匯出。	2023 年 1 月 10 日

變更	描述	日期
	• Amazon GameLift -解決與 Amazon 相關的問題 GameLift。 • AWS Glue– 疑難排解 AWS Glue Data Quality 相關的問題。 • Amazon Kinesis Video Streams – 疑難排解 Kinesis Video Streams 相關的問題。 • Amazon Managed Service-Prometheus – 疑難排解 Prometheus 的 Amazon Managed Service 相關問題。 • Amazon Managed Streaming for Apache Kafka – 疑難排解 Amazon MSK Connect 相關的問題。 • AWS Network Manager — 疑難排解與網路管理員相關的問題。 • Amazon Nimble Studio – 偵錯與 Nimble Studio 相關的問題。 • Amazon Personalize – 偵錯與 Amazon Personalize 相關的問題。 • Amazon Pinpoint – 疑難排解 Amazon Pinpoint 相關的問題。 • AWS HealthOmics — 要解決相關問題 HealthOmics.	

變更	描述	日期
	• Amazon Transcribe – 偵錯與 Amazon Transcribe 相關的問題。	
AWSSupportServiceRolePolicy – 更新現有政策	在以下服務中新增了 47 項新許可，以執行有助於解決客戶在計費、管理和技術支援方面相關問題的動作： • AWS Application Migration Service — 疑難排解複寫和啟動問題。 • AWS CloudFormation 鉤子 — 啟 AWS Support 用開發可以幫助解決問題的自動化工具。 • Amazon Elastic Kubernetes Service - 疑難排解與 Amazon EKS 相關的問題。 • AWS IoT FleetWise – 疑難排解與 AWS IoT FleetWise 相關的問題。 • AWS Mainframe Modernization — 調試與大型主機現代化相關的問題。 • AWS Outposts — 協助 AWS Support 取得專用主機和資產清單。 • AWS Private 5G – 疑難排解與 Private 5G 相關的問題。 • AWS Tiros - 偵錯與 Tiros 相關的問題。	2022 年 10 月 4 日

變更	描述	日期
AWSSupportServiceRolePolicy – 更新現有政策	在以下服務中新增了 46 項新許可，以執行有助於解決客戶在計費、管理和技術支援方面相關問題的動作： • Amazon Managed Streaming for Apache Kafka - 疑難排解與 Amazon MSK 相關的問題。 • AWS DataSync — 要解決相關問題 DataSync. • AWS Elastic Disaster Recovery — 疑難排解複寫和啟動問題。 • Amazon GameSparks — 解決相關問題 GameSparks. • AWS IoT TwinMaker — 調試相關的問題 AWS IoT TwinMaker. • AWS Lambda — 檢視函數 URL 的組態以疑難排解問題。 • Amazon Lookout for Equipment - 疑難排解與 Lookout for Equipment 相關的問題。 • Amazon 路線 53 和 Amazon 路線 53 解析器 — 獲取解析器配置，以便 AWS Support 可以檢查 VPC 的 DNS 解析行為。	2022 年 8 月 17 日

變更	描述	日期
AWSSupportServiceRolePolicy – 更新現有政策	在以下服務中新增了一些新許可，以執行相關動作，幫助疑難排解客戶在計費、管理和技術支援方面的相關問題： • Amazon CloudWatch 日誌 — 協助疑難排解 CloudWatch 日誌相關問題。 • Amazon 互動式視訊服務 — 協助 AWS Support 檢查現有的 Amazon IVS 資源，以瞭解有關詐騙或遭入侵帳戶的支援案例。 • Amazon Inspector – 疑難排解 Amazon Inspector 相關的問題。 刪除了 Amazon 等服務的許可 WorkLink。Amazon WorkLink 於 2022 年 4 月 19 日棄用。	2022 年 6 月 23 日

變更	描述	日期
AWSSupportServiceRolePolicy – 更新現有政策	在以下服務中新增了 25 項新許可，以執行有助於解決客戶在計費、管理和技術支援方面相關問題的動作： • AWS Amplify UI 生成器-解決與組件和主題生成相關的問題。 • Amazon AppStream — 擷取最近啟動的功能的資源，藉此疑難排解問題。 • AWS Backup — 疑難排解與備份工作相關的問題。 • AWS CloudFormation — 對與 IAM、擴充功能和版本控制相關的問題執行診斷。 • Amazon Kinesis – 解決與 Kinesis 有關的問題。 • AWS Transfer Family — 解決與 Transfer Family 相關的問題.	2022 年 4 月 27 日

變更	描述	日期

AWSSupportServiceRolePolicy – 更新現有政策	在以下服務中新增了 54 項新許可，以執行有助於解決客戶在計費、管理和技術支援方面相關問題的動作：
	• Amazon Elastic Compute Cloud
	  • 解決與客戶和以 AWS管理為前綴的清單有關的問題。
	  • 解決與 Amazon VPC IP Address Manager (IPAM) 有關的問題。
	• AWS 網路管理員 — 疑難排解與網路管理員相關的問題。
	• Savings Plans – 取得與未結 Savings Plan 承諾有關的中繼資料。
	• AWS Serverless Application Repository — 作為研究和解決支持案例的一部分，改善和支持響應行動。
	• Amazon WorkSpaces 網絡 — 對 WorkSpaces Web 服務的問題進行調試和故障排除。
		2022 年 3 月 14 日

變更	描述	日期
AWSSupportServiceRolePolicy – 更新現有政策	在以下服務中新增了 74 項新許可，以執行有助於解決客戶在計費、管理和技術支援方面的相關問題的動作： • AWS Application Migration Service — 支援應用程式移轉服務中的無代理程式複寫。 • AWS CloudFormation — 對 IAM、擴充功能和版本控制相關問題執行診斷。 • Amazon CloudWatch 日誌 — 驗證資源政策。 • Amazon EC2 資源回收筒 – 取得有關資源回收筒保留規則的中繼資料。 • AWS Elastic Disaster Recovery — 疑難排解客戶帳戶中的複製和啟動問題。 • Amazon FSx – 檢視 Amazon FSx 快照的描述。 • Amazon Lightsail – 檢視 Lightsail 儲存貯體的中繼資料和組態詳細資訊。 • Amazon Macie – 檢視 Macie 組態，如分類任務、自訂資料識別符、常規表達式和問題清單。 • Simple Storage Service (Amazon S3) – 收集 Simple Storage Service (Amazon	2022 年 2 月 17 日

變更	描述	日期
	S3) 儲存貯體的中繼資料和組態。 • AWS Storage Gateway — 檢視有關客戶自動磁帶建立原則的中繼資料。 • Elastic Load Balancing –在使用 Service Quotas 主控台時檢視資源限制的說明。 如需詳細資訊，請參閱 AWSSupportServiceRolePolicy 的許可變更。	
變更發佈的日誌	變更 AWS Support 受管理策略的記錄檔。	2022 年 2 月 17 日

AWSSupportServiceRolePolicy 的許可變更

添加了大多數權限， AWS Support 以AWSSupportServiceRolePolicy允許調用具有相同名稱的 API 操作。然而，某些 API 操作需要具有不同名稱的許可。

下表僅列出了需要具有不同名稱的許可的 API 操作。此表描述了從 2022 年 2 月 17 日開始的這些差異。

日期	API 操作名稱	必要的政策許可

2022 年 2 月 17 日新增了許可	`s3.GetBucketAnalyticsConfiguration`
	
	`s3.ListBucketAnalyticsConfiguration`
		`s3:GetAnalyticsConfiguration`

	`s3.GetBucketNotificationConfiguration`	`s3:GetBucketNotification`

日期	API 操作名稱	必要的政策許可
	s3.GetBucketEncryption	s3:GetEncryptionConfiguration
	s3.GetBucketIntelligentTieringConfiguration s3.ListBucketIntelligentTieringConfiguration	s3:GetIntelligentTieringConfiguration
	s3.GetBucketInventoryConfiguration s3.ListBucketInventoryConfiguration	s3:GetInventoryConfiguration
	s3.GetBucketLifecycleConfiguration	s3:GetLifecycleConfiguration
	s3.GetBucketMetricsConfiguration s3.ListBucketMetricsConfiguration	s3:GetMetricsConfiguration
	s3.GetBucketReplication	s3:GetReplicationConfiguration
	s3.HeadBucket s3.ListObjects	s3:ListBucket
	s3.ListBuckets	s3:ListAllMyBuckets
	s3.ListMultipartUploads	s3:ListBucketMultipartUploads

日期	API 操作名稱	必要的政策許可
	s3.ListObjectVersions	s3:ListBucketVersions
	s3.ListParts	s3:ListMultipartUploadParts

AWS 適用於 Slack 中 AWS Support 應用程式的受管政策

> **Note**
>
> 若要存取和檢視中的支援案例 AWS Support Center Console，請參閱管理對 AWS Support 中心的存取。

AWS Support 應用程式具有下列受管政策。

內容

- AWS 受管理的策略：AWSSupportAppFullAccess
- AWS 受管理的策略：AWSSupportAppReadOnlyAccess
- AWS SupportAWS 受管政策的應用程式更新

AWS 受管理的策略：AWSSupportAppFullAccess

您可以使用 AWSSupportAppFullAccess 受管政策，將 Slack 頻道組態的許可授予 IAM 角色。您也可將 AWSSupportAppFullAccess 政策附加至 IAM 實體。

如需詳細資訊，請參閱 Slack 中的 AWS Support 應用程式。

此政策授予允許實體執行 AWS Support AWS Support 應用程式的 Service Quotas 和 IAM 動作的許可。

許可詳細資訊

此政策包含以下許可：

- servicequotas - 說明您現有的服務配額和請求，並為您的帳戶建立服務配額增加。
- support - 建立、更新及解決您的支援案例。更新並說明案例的相關資訊，例如檔案附件、通訊和嚴重性等級。啟動與支援客服人員的即時聊天工作階段。
- iam - 建立 Service Quotas 的服務連結角色。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "servicequotas:GetRequestedServiceQuotaChange",
                "servicequotas:GetServiceQuota",
                "servicequotas:RequestServiceQuotaIncrease",
                "support:AddAttachmentsToSet",
                "support:AddCommunicationToCase",
                "support:CreateCase",
                "support:DescribeCases",
                "support:DescribeCommunications",
                "support:DescribeSeverityLevels",
                "support:InitiateChatForCase",
                "support:ResolveCase"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"iam:AWSServiceName": "servicequotas.amazonaws.com"}
            }
        }
    ]
}
```

如需詳細資訊，請參閱 管理 AWS Support 應用程式的存取權。

AWS 受管理的策略：AWSSupportAppReadOnlyAccess

此原AWSSupportAppReadOnlyAccess則會授與允許實體執行唯讀 AWS Support 應用程式動作的權限。如需詳細資訊，請參閱 Slack 中的 AWS Support 應用程式。

許可詳細資訊

此政策包含以下許可：

- `support` - 說明支援案例詳細資訊和新增至支援案例的通訊內容。

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

AWS SupportAWS 受管政策的應用程式更新

檢視有關 AWS Support 應用程式 AWS 受管政策更新的詳細資料，因為此服務開始追蹤這些變更。如需有關此頁面變更的自動提醒，請訂閱 文件歷史紀錄 頁面的 RSS 摘要。

下表說明自 2022 年 8 月 17 日起， AWS Support 應用程式管理政策的重要更新。

AWS Support 应用

變更	描述	日期
AWSSupportAppFullAccess和 AWSSupportAppReadOnlyAccess 適用於 AWS Support 應用程式的新 AWS 受管政策	您可以將這些政策用於您為 Slack 頻道組態所設定的 IAM 角色。 如需詳細資訊，請參閱 管理 AWS Support 應用程式的存取權。	2022 年 8 月 19 日
變更發佈的日誌	變更 AWS Support 應用程式管理原則的記錄檔。	2022 年 8 月 19 日

AWS 受管理的政策 AWS Trusted Advisor

Trusted Advisor 具有下列 AWS 受管理的策略。

內容

- AWS 受管理的策略：AWSTrustedAdvisorPriorityFullAccess
- AWS 受管理的策略：AWSTrustedAdvisorPriorityReadOnlyAccess
- AWS 受管政策：AWSTrustedAdvisorServiceRolePolicy
- AWS 受管理的策略：AWSTrustedAdvisorReportingServiceRolePolicy
- Trusted AdvisorAWS 受管理策略的更新

AWS 受管理的策略：AWSTrustedAdvisorPriorityFullAccess

AWSTrustedAdvisorPriorityFullAccess政策會授予「 Trusted Advisor 優先順序」的完整存取權 此原則也允許使用者新增 Trusted Advisor 為受信任的服務， AWS Organizations 並指定 Trusted Advisor 優先順序的委派管理員帳戶。

許可詳細資訊

在第一個陳述式中，政策包含 `trustedadvisor` 的以下許可：

- 說明您的帳戶和組織。
- 描述 Trusted Advisor 優先順序中識別的風險。許可允許您下載和更新風險狀態。

- 說明「 Trusted Advisor 優先順序」電子郵件通知的組態 許可允許您設定電子郵件通知，並針對委派的管理員停用這些通知。
- 設置以 Trusted Advisor 便您的帳戶可以啟用 AWS Organizations。

在第二個陳述式中，政策包含 organizations 的以下許可：

- 說明您的 Trusted Advisor 帳戶和組織。
- 列出 AWS 服務 您啟用以使用「組織」的項目。

在第三個陳述式中，政策包含 organizations 的以下許可：

- 列出「 Trusted Advisor 優先順序」的委派管理員。
- 啟用和停用 Organizations 的受信任存取權。

在第四個陳述式中，政策包含 iam 的以下許可：

- 建立 AWSServiceRoleForTrustedAdvisorReporting 服務連結角色。

在第五個陳述式中，政策包含 organizations 的以下許可：

- 允許您註冊和取消註冊 Trusted Advisor Priority 的委派管理員。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AWSTrustedAdvisorPriorityFullAccess",
   "Effect": "Allow",
   "Action": [
    "trustedadvisor:DescribeAccount*",
    "trustedadvisor:DescribeOrganization",
    "trustedadvisor:DescribeRisk*",
    "trustedadvisor:DownloadRisk",
    "trustedadvisor:UpdateRiskStatus",
    "trustedadvisor:DescribeNotificationConfigurations",
    "trustedadvisor:UpdateNotificationConfigurations",
    "trustedadvisor:DeleteNotificationConfigurationForDelegatedAdmin",
    "trustedadvisor:SetOrganizationAccess"
```

```
    ],
    "Resource": "*"
   },
   {
    "Sid": "AllowAccessForOrganization",
    "Effect": "Allow",
    "Action": [
     "organizations:DescribeAccount",
     "organizations:DescribeOrganization",
     "organizations:ListAWSServiceAccessForOrganization"
    ],
    "Resource": "*"
   },
   {
    "Sid": "AllowListDelegatedAdministrators",
    "Effect": "Allow",
    "Action": [
     "organizations:ListDelegatedAdministrators",
     "organizations:EnableAWSServiceAccess",
     "organizations:DisableAWSServiceAccess"
    ],
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "organizations:ServicePrincipal": [
       "reporting.trustedadvisor.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AllowCreateServiceLinkedRole",
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting",
    "Condition": {
     "StringLike": {
      "iam:AWSServiceName": "reporting.trustedadvisor.amazonaws.com"
     }
    }
   },
   {
    "Sid": "AllowRegisterDelegatedAdministrators",
```

```
    "Effect": "Allow",
    "Action": [
     "organizations:RegisterDelegatedAdministrator",
     "organizations:DeregisterDelegatedAdministrator"
    ],
    "Resource": "arn:aws:organizations::*:*",
    "Condition": {
     "StringEquals": {
      "organizations:ServicePrincipal": [
       "reporting.trustedadvisor.amazonaws.com"
      ]
     }
    }
   }
  ]
}
```

AWS 受管理的策略：AWSTrustedAdvisorPriorityReadOnlyAccess

此AWSTrustedAdvisorPriorityReadOnlyAccess原則會將唯讀權限授與「 Trusted Advisor 優先順序」，包括檢視委派管理員帳戶的權限。

許可詳細資訊

在第一個陳述式中，政策包含 `trustedadvisor` 的以下許可：

- 說明您的 Trusted Advisor 帳戶和組織。
- 說明「 Trusted Advisor 優先順序」中識別的風險，並可讓您下載這些風險。
- 描述 Trusted Advisor 優先順序電子郵件通知的組態。

在第二個和第三個陳述式中，政策包含 `organizations` 的以下許可：

- 使用 Organizations 說明您的組織。
- 列出 AWS 服務 您啟用以使用「組織」的項目。
- 列出 Trusted Advisor 優先順序的委派管理員

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

```
  {
   "Sid": "AWSTrustedAdvisorPriorityReadOnlyAccess",
   "Effect": "Allow",
   "Action": [
    "trustedadvisor:DescribeAccount*",
    "trustedadvisor:DescribeOrganization",
    "trustedadvisor:DescribeRisk*",
    "trustedadvisor:DownloadRisk",
    "trustedadvisor:DescribeNotificationConfigurations"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowAccessForOrganization",
   "Effect": "Allow",
   "Action": [
    "organizations:DescribeOrganization",
    "organizations:ListAWSServiceAccessForOrganization"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowListDelegatedAdministrators",
   "Effect": "Allow",
   "Action": [
    "organizations:ListDelegatedAdministrators"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "organizations:ServicePrincipal": [
      "reporting.trustedadvisor.amazonaws.com"
     ]
    }
   }
  }
 ]
}
```

AWS 受管政策：AWSTrustedAdvisorServiceRolePolicy

此政策連接至 AWSServiceRoleForTrustedAdvisor 服務連結角色。它允許服務連結角色為您執行動作。您無法將 AWSTrustedAdvisorServiceRolePolicy 連接至 AWS Identity and Access Management (IAM) 實體。如需詳細資訊，請參閱 使用 Trusted Advisor的服務連結角色。

此政策會授予管理許可，允許服務連結角色存取 AWS 服務。這些權限允許檢查 Trusted Advisor 以評估您的帳戶。

許可詳細資訊

此政策包含以下許可。

- Auto Scaling - 描述 Amazon EC2 Auto Scaling 帳戶配額和資源
- cloudformation— 描述 AWS CloudFormation (CloudFormation) 帳戶配額和堆疊
- cloudfront— 描述 Amazon CloudFront 分佈
- cloudtrail— 描述 AWS CloudTrail (CloudTrail) 軌跡
- dynamodb - 描述 Amazon DynamoDB 帳戶配額和資源
- ec2 - 描述 Amazon Elastic Compute Cloud (Amazon EC2) 帳戶配額和資源
- elasticloadbalancing - 說明 Elastic Load Balancing (ELB) 帳戶配額和資源
- iam - 取得 IAM 資源，例如憑證、密碼政策和憑證
- kinesis - 描述 Amazon Kinesis (Kinesis) 帳戶配額
- rds - 描述 Amazon Relational Database Service (Amazon RDS) 資源
- redshift - 描述 Amazon Redshift 資源
- route53 - 描述 Amazon Route 53 帳戶配額和資源
- s3 - 描述 Amazon Simple Storage Service (Amazon S3) 資源
- ses - 取得 Amazon Simple Email Service (Amazon SES) 傳送份額
- sqs - 列出 Amazon Simple Queue Service (Amazon SQS) 佇列
- cloudwatch— 獲取 Amazon CloudWatch 事件 (CloudWatch 事件) 度量統計
- ce - 取得 Cost Explorer Service (Cost Explorer) 建議
- route53resolver— 取得 Amazon Route 53 Resolver 解析器端點和資源
- kafka – 取得 Amazon Managed Streaming for Apache Kafka 資源
- ecs— 獲取 Amazon ECS 資源
- outposts— 獲取 AWS Outposts 資源

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "autoscaling:DescribeAccountLimits",
                "autoscaling:DescribeAutoScalingGroups",
                "autoscaling:DescribeLaunchConfigurations",
                "ce:GetReservationPurchaseRecommendation",
                "ce:GetSavingsPlansPurchaseRecommendation",
                "cloudformation:DescribeAccountLimits",
                "cloudformation:DescribeStacks",
                "cloudformation:ListStacks",
                "cloudfront:ListDistributions",
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:GetTrail",
                "cloudtrail:ListTrails",
                "cloudtrail:GetEventSelectors",
                "cloudwatch:GetMetricStatistics",
                "dynamodb:DescribeLimits",
                "dynamodb:DescribeTable",
                "dynamodb:ListTables",
                "ec2:DescribeAddresses",
                "ec2:DescribeReservedInstances",
                "ec2:DescribeInstances",
                "ec2:DescribeVpcs",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeImages",
                "ec2:DescribeVolumes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeRegions",
                "ec2:DescribeReservedInstancesOfferings",
                "ec2:DescribeSnapshots",
                "ec2:DescribeVpnConnections",
                "ec2:DescribeVpnGateways",
                "ec2:DescribeLaunchTemplateVersions",
                "ecs:DescribeTaskDefinition",
                "ecs:ListTaskDefinitions"
                "elasticloadbalancing:DescribeAccountLimits",
                "elasticloadbalancing:DescribeInstanceHealth",
```

```
                "elasticloadbalancing:DescribeLoadBalancerAttributes",
                "elasticloadbalancing:DescribeLoadBalancerPolicies",
                "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
                "iam:GenerateCredentialReport",
                "iam:GetAccountPasswordPolicy",
                "iam:GetAccountSummary",
                "iam:GetCredentialReport",
                "iam:GetServerCertificate",
                "iam:ListServerCertificates",
                "kinesis:DescribeLimits",
                "kafka:ListClustersV2",
                "kafka:ListNodes",
                "outposts:GetOutpost",
                "outposts:ListAssets",
                "outposts:ListOutposts",
                "rds:DescribeAccountAttributes",
                "rds:DescribeDBClusters",
                "rds:DescribeDBEngineVersions",
                "rds:DescribeDBInstances",
                "rds:DescribeDBParameterGroups",
                "rds:DescribeDBParameters",
                "rds:DescribeDBSecurityGroups",
                "rds:DescribeDBSnapshots",
                "rds:DescribeDBSubnetGroups",
                "rds:DescribeEngineDefaultParameters",
                "rds:DescribeEvents",
                "rds:DescribeOptionGroupOptions",
                "rds:DescribeOptionGroups",
                "rds:DescribeOrderableDBInstanceOptions",
                "rds:DescribeReservedDBInstances",
                "rds:DescribeReservedDBInstancesOfferings",
                "rds:ListTagsForResource",
                "redshift:DescribeClusters",
                "redshift:DescribeReservedNodeOfferings",
                "redshift:DescribeReservedNodes",
                "route53:GetAccountLimit",
                "route53:GetHealthCheck",
                "route53:GetHostedZone",
                "route53:ListHealthChecks",
                "route53:ListHostedZones",
                "route53:ListHostedZonesByName",
                "route53:ListResourceRecordSets",
```

```
                "route53resolver:ListResolverEndpoints",
                "route53resolver:ListResolverEndpointIpAddresses",
                "s3:GetAccountPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketLocation",
                "s3:GetBucketLogging",
                "s3:GetBucketVersioning",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetLifecycleConfiguration",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "ses:GetSendQuota",
                "sqs:ListQueues"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 受管理的策略：AWSTrustedAdvisorReportingServiceRolePolicy

此原則會附加至AWSServiceRoleForTrustedAdvisorReporting服務連結角色，可 Trusted Advisor 針對組織檢視功能執行動作。您無法將 AWSTrustedAdvisorReportingServiceRolePolicy 連接至 IAM 實體。如需詳細資訊，請參閱 使用 Trusted Advisor的服務連結角色。

此原則會授與允許服務連結角色執行 AWS Organizations 動作的管理權限。

許可詳細資訊

此政策包含以下許可。

- organizations - 描述您的組織，並列出服務存取權、帳戶、父系、子系和組織單位

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

```
        {
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListChildren",
                "organizations:ListParents",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Trusted AdvisorAWS 受管理策略的更新

檢視這些服務開始追蹤這些變更 AWS Support Trusted Advisor 後 AWS 受管理政策的更新詳細資料。如需有關此頁面變更的自動提醒，請訂閱 文件歷史紀錄 頁面的 RSS 摘要。

下表說明自 2021 年 8 月 10 日起對 Trusted Advisor 受管政策的重要更新。

Trusted Advisor

變更	描述	日期
AWSTrustedAdvisorServiceRolePolicy 更新為現有策略。	Trusted Advisor 添加了新的操作以cloudtrail:GetTrail cloudtrail:ListTrails cloudtrail:GetEventSelectors outposts:GetOutpost 授予outposts:ListAssets 和outposts:ListOutposts 權限。	2024年1月18日

變更	描述	日期
AWSTrustedAdvisorPriorityFullAccess 更新為現有策略。	Trusted Advisor 已更新受AWSTrustedAdvisorPriorityFullAccess AWS 管理政策以包含陳述式 ID。	2023 年 12 月 6 日
AWSTrustedAdvisorPriorityReadOnlyAccess 更新為現有策略。	Trusted Advisor 已更新受AWSTrustedAdvisorPriorityReadOnlyAccess AWS 管理政策以包含陳述式 ID。	2023 年 12 月 6 日
AWSTrustedAdvisorServiceRolePolicy – 更新現有政策	Trusted Advisor 添加了新操作以授予ec2:DescribeRegions s3:GetLifecycleConfiguration ecs:DescribeTaskDefinition 和ecs:ListTaskDefinitions 權限。	2023 年 11 月 9 日
AWSTrustedAdvisorServiceRolePolicy – 更新現有政策	Trusted Advisor 新增了新的 IAM 動作route53resolver:ListResolverEndpoints route53resolver:ListResolverEndpointIpAddresses 、ec2:DescribeSubnets 、kafka:ListNodes 以kafka:ListClustersV2 及登入新的彈性檢查。	2023 年 9 月 14 日

變更	描述	日期
AWSTrustedAdvisorReportingServiceRolePolicy 附加在 Trusted Advisor AWSServiceRoleForTrustedAdvisorReporting 服務連結角色上的受管理原則 V2	將 Trusted Advisor AWSServiceRoleForTrustedAdvisorReporting 服務連結角色的 AWS 受管理原則升級至 V2。V2 會額外新增一個 IAM 動作 organizations:ListDelegatedAdministrators	2023 年 2 月 28 日
AWSTrustedAdvisorPriorityFullAccess 和 AWSTrustedAdvisorPriorityReadOnlyAccess 新的 AWS 受管理政策 Trusted Advisor	Trusted Advisor 新增了兩個新的受管理策略，您可以用來控制對 Trusted Advisor 優先級的存取。	2022 年 8 月 17 日

變更	描述	日期
AWSTrustedAdvisorServiceRolePolicy – 更新現有政策	Trusted Advisor 添加了新操作以授予 `DescribeTargetGroups` 和 `GetAccountPublicAccessBlock` 權限。 進行 Auto Scaling 群組運作狀態檢查需要 `DescribeTargetGroup` 許可，才能擷取 Classic Load Balancer 以外連接至 Auto Scaling 群組的負載平衡器。 進行 Simple Storage Service (Amazon S3) 儲存貯體許可檢查需要 `GetAccountPublicAccessBlock` 許可，才能擷取 AWS 帳戶的區塊公有存取設定。	2021 年 8 月 10 日
變更發佈的日誌	Trusted Advisor 開始追蹤其 AWS 受管理策略的變更。	2021 年 8 月 10 日

AWS 受管理的 AWS Support 計劃原則

AWS Support 計劃具有下列受管理的策略。

內容

- AWS 受管理的策略：AWSSupportPlansFullAccess
- AWS 受管理的策略：AWSSupportPlansReadOnlyAccess
- AWS Support 計劃 AWS 受管理策略的更新

AWS 受管理的策略：AWSSupportPlansFullAccess

AWS Support 計劃使用受AWSSupportPlansFullAccess AWS 管理的策略。IAM 實體使用此政策為您完成下列 Support Plans 動作：

- 檢視您的支援計劃 AWS 帳戶
- 檢視變更支援計劃請求的狀態詳細資訊
- 變更您的支援方案 AWS 帳戶
- 建立支援計劃排程 AWS 帳戶

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportplans:GetSupportPlan",
                "supportplans:GetSupportPlanUpdateStatus",
                "supportplans:StartSupportPlanUpdate",
                "supportplans:CreateSupportPlanSchedule"
            ],
            "Resource": "*"
        }
    ]
}
```

如需政策變更清單，請參閱 AWS Support 計劃 AWS 受管理策略的更新。

AWS 受管理的策略：AWSSupportPlansReadOnlyAccess

AWS Support 計劃使用受AWSSupportPlansReadOnlyAccess AWS 管理的策略。IAM 實體使用此政策為您完成下列唯讀 Support Plans 動作：

- 檢視您的支援計劃 AWS 帳戶
- 檢視變更支援計劃請求的狀態詳細資訊

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

```
        {
            "Effect": "Allow",
            "Action": [
                "supportplans:GetSupportPlan",
                "supportplans:GetSupportPlanUpdateStatus"
            ],
            "Resource": "*"
        }
    ]
}
```

如需政策變更清單，請參閱 AWS Support 計劃 AWS 受管理策略的更新。

AWS Support 計劃 AWS 受管理策略的更新

檢視 Support 方案 AWS 受管原則更新的詳細資料，因為這些服務開始追蹤這些變更。如需有關此頁面變更的自動提醒，請訂閱 文件歷史紀錄 頁面的 RSS 摘要。

下表說明了自 2022 年 9 月 29 日起，Support Plans 受管政策的重要更新。

AWS Support

變更	描述	日期
AWSSupportPlansFullAccess - 更新現有政策	將 `CreateSupportPlanSchedule` 動作新增至 `AWSSupportPlansFullAccess` 受管政策。	2023 年 5 月 8 日
變更發佈的日誌	Support Plans 受管政策的變更日誌。	2022 年 9 月 29 日

管理對 AWS Support 中心的存取

您必須有許可才能存取支援中心和建立支援案例。

您可以使用下列其中一個選項存取支援中心：

- 使用與您 AWS 帳戶相關聯的電子郵件地址和密碼。此身份稱為 AWS 帳號根使用者。
- 使用 AWS Identity and Access Management (IAM)。

如果您擁有商業、企業上線或企業 Support 方案，您也可以使用 AWS Support API 以程式設計方式存取 AWS Support 和 Trusted Advisor 操作。如需詳細資訊，請參閱 AWS Support API 參考。

> **Note**
>
> 如果您無法登入支援中心，可以改用聯絡我們頁面。您可以使用此頁面取得帳單和帳戶問題的說明。

AWS 帳戶

您可以使用您的 AWS 帳戶電子郵件地址 AWS Management Console 和密碼登入並存取 Support 中心。此身份稱為 AWS 帳號根使用者。不過，強烈建議您不要以根使用者身分處理日常作業，即使是管理作業也一樣。建議您改用 IAM，這可讓您控制誰能在您的帳戶中執行特定任務。

AWS 支援動作

您可以在主控台中 AWS Support 執行下列動作。您也可以在 IAM 政策中指定這些 AWS Support 動作，以允許或拒絕特定動作。

> **Note**
>
> 如果您拒絕 IAM 政策中的以下任何動作，則在建立或與支援案例互動時，可能會導致支援中心出現意外行為。

動作	描述
`DescribeSupportLevel`	准許傳回 AWS 帳戶識別碼的支援層級。這是由 AWS Support 中心內部使用，以識別您的支援等級。
`InitiateCallForCase`	授予在 AWS Support 中心發起呼叫的權限。這是由 AWS Support 中心內部用來代表您開始通話。
`InitiateChatForCase`	准許在 AWS Support Center 發起呼叫。這是由 AWS Support 中心內部代表您開始聊天。

動作	描述
RateCaseCommunication	授予對 AWS Support 案例通訊評分的權限。
DescribeCaseAttributes	准許次要服務讀取 AWS Support 案例屬性。這是由 AWS Support 中心內部使用，以獲取在您的案例上標記的屬性。
DescribeIssueTypes	准許傳回 AWS Support 案例的問題類型。 AWS Support 中心會在內部使用此功能，以取得您帳戶的可用問題類型。
SearchForCases	授予返回與給定輸入匹配的 AWS Support 案例列表的權限。這是由 AWS Support 中心內部使用來查找搜索的案例。
PutCaseAttributes	授與允許次要服務將屬性附加至 AWS Support 案例的權限。這是由 AWS Support 中心內部使用，為您的 AWS Support 案例添加操作標籤。

IAM

在預設情況下，IAM 使用者無權存取支援中心。您可以使用 IAM 建立個別使用者或群組。然後，您可以將 IAM 政策附加到這些實體，以便他們有權執行動作和存取資源，例如開啟 Support 中心案例和使用 AWS Support API。

建立 IAM 使用者之後，就可以為這些使用者提供個別的密碼和帳戶專屬登入頁面。然後，他們可以登錄到您的 AWS 帳戶並在 Support 中心工作。具有 AWS Support 存取權的 IAM 使用者可以查看為該帳戶建立的所有案例。

如需詳細資訊，請參閱 IAM 使用者指南中的 IAM 使用者如何登入您的 AWS 帳戶。

授與權限最簡單的方法是將 AWS 受管理的政策附加AWSSupportAccess到使用者、群組或角色。AWS Support 允許動作層級權限來控制對特定 AWS Support 作業的存取。 AWS Support 不提供資源級訪問權限，因此Resource元素始終設置為。*您無法允許或拒絕存取特定支援案例。

Example ：允許存取所有 AWS Support 動作

受 AWS 管政策AWSSupportAccess授予 IAM 使用者的存取權 AWS Support。具有此政策的 IAM 使用者可以存取所有 AWS Support 操作和資源。

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

如需如何將 AWSSupportAccess 政策連接至實體的詳細資訊，請參閱 IAM 使用者指南中的新增 IAM 身分許可 (主控台)。

Example ：允許存取動作以外的所有 ResolveCase 動作

您也可以在 IAM 中建立客戶受管政策，指定允許或拒絕的動作。下列政策陳述式可讓 IAM 使用者在解決案例以 AWS Support 外執行所有動作。

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

如需如何建立客戶受管 IAM 政策的詳細資訊，請參閱 IAM 使用者指南中的建立 IAM 政策 (主控台)。

如果使用者或群組已有策略，您可以將 AWS Support特定政策聲明新增至該策略。

> **Important**
>
> - 如果您無法在支援中心內檢視案例，請確認您擁有必要的許可。您可能需要聯絡 IAM 管理員。如需詳細資訊，請參閱 的身分識別與存取管理 AWS Support。

訪問 AWS Trusted Advisor

在中 AWS Management Console，單獨的 `trustedadvisor` IAM 命名空間可控制對 Trusted Advisor. 在 AWS Support API 中，`support`IAM 命名空間可控制對 Trusted Advisor. 如需詳細資訊，請參閱 管理存取 AWS Trusted Advisor。

管理對 AWS Support 計劃的存取

主題

- Support Plans 主控台的許可
- Support Plans 動作
- 適用於 Support Plans 的範例 IAM 政策
- 故障診斷

Support Plans 主控台的許可

若要存取 Support Plans 主控台，使用者必須擁有最基本的一組許可。這些許可必須允許使用者列出和檢視 AWS 帳戶中 Support Plans 資源的詳細資訊。

您可以使用`supportplans`命名空間建立 AWS Identity and Access Management (IAM) 政策。您可使用此政策指定動作和資源的許可。

當您建立政策時，可以指定服務的命名空間，以允許或拒絕動作。Support Plans 的命名空間為 `supportplans`。

您可以使用 AWS 受管政策並將其附加到 IAM 實體。如需詳細資訊，請參閱 AWS 受管理的 AWS Support 計劃原則。

Support Plans 動作

您可以在主控台中執行下列 Support Plans 動作。您也可以在 IAM 政策中指定這些 Support Plans 動作，以允許或拒絕特定動作。

動作	描述
GetSupportPlan	准許檢視此 AWS 帳戶的目前支援計劃的詳細資訊。
GetSupportPlanUpdateStatus	准許檢視更新支援計劃之請求狀態的詳細資訊。
StartSupportPlanUpdate	准許啟動更新此 AWS 帳戶支援計劃之請求。
CreateSupportPlanSchedule	准許為此 AWS 帳戶建立支援計畫排程。

適用於 Support Plans 的範例 IAM 政策

您可使用以下範例政策來管理對 Support Plans 的存取。

完整存取 Support Plans

以下政策允許使用者完整存取 Support Plans。

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

唯讀存取 Support Plans

以下政策允許唯讀存取 Support Plans。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "supportplans:Get*",
```

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

拒絕存取 Support Plans

以下政策不允許使用者存取 Support Plans。

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

故障診斷

請參閱下列主題，以管理對 Support Plans 的存取。

當我嘗試檢視或變更我的支援計畫時，Support Plans 主控台會顯示我缺少 **GetSupportPlan** 許可

IAM 使用者必須具備必要的許可，才能存取 Support Plans 主控台。您可以更新 IAM 政策以包含缺失的許可，或使用 AWS 受管政策，例如 AWSSupportPlansFullAccess 或 AWSSupportPlansReadOnlyAccess。如需詳細資訊，請參閱 AWS 受管理的 AWS Support 計劃原則。

如果您無權更新 IAM 政策，請聯絡您的 AWS 帳戶 管理員。

相關資訊

如需詳細資訊，請參閱《IAM 使用者指南》中的以下主題：

- 使用 IAM 政策模擬器測試 IAM 政策
- 對拒絕存取錯誤訊息進行疑難排解

我具有正確的 Support Plans 許可，但我仍然收到相同的錯誤

如果您 AWS 帳戶 是屬於其中的成員帳戶 AWS Organizations，則可能需要更新服務控制原則 (SCP)。SCP 是一種管理組織中的許可的政策類型。

由於 Support Plans 是全域服務，因此限制 AWS 區域 的政策可能會阻止成員帳戶檢視或變更支援計畫。若要允許組織使用全域服務，例如 IAM 和 Support Plans，您必須將服務新增至任何適用 SCP 中的排除清單。這表示組織中的帳戶可以存取這些服務，即使 SCP 拒絕指定的服務。 AWS 區域

若要將 Support Plans 新增為例外狀況，請在 SCP 的 "NotAction" 清單中輸入 "supportplans:*"。

```
"supportplans:*",
```

您的 SCP 可能會顯示為下列政策程式碼片段。

Example ：允許在組織中存取 Support Plans 的 SCP

```
{ "Version":  "2012-10-17",
   "Statement": [
     { "Sid":  "GRREGIONDENY",
       "Effect":  "Deny",
       "NotAction": [
         "aws-portal:*",
         "budgets:*",
         "chime:*"
         "iam:*",
         "supportplans:*",
         ....
```

如果您具有成員帳戶，無法更新 SCP，請聯絡 AWS 帳戶 帳戶。受管帳戶可能需要更新 SCP，以便所有成員帳戶都可以存取 Support Plans。

> 的注意事項 AWS Control Tower
>
> - 如果您的組織搭配使用 SCP AWS Control Tower，您可以 AWS 根據要求的 AWS 區域控制項 (通常稱為「區域拒絕控制」) 將「拒絕存取」更新為。
> - 如果您將 SCP 更新為 AWS Control Tower 允許supportplans，修復漂移將移除您對 SCP 的更新。有關詳情，請參閱偵測和解決中的漂移 AWS Control Tower。

相關資訊

如需詳細資訊，請參閱下列主題：

- 《AWS Organizations 使用者指南》中的服務控制政策 (SCP)。
- 《AWS Control Tower 使用者指南》中的設定區域拒絕控制。
- AWS 根據AWS Control Tower 使用者指南 AWS 區域中的要求拒絕存取

管理存取 AWS Trusted Advisor

您可以 AWS Trusted Advisor 從存取 AWS Management Console. 所 AWS 帳戶 有人都可以訪問選擇的核心Trusted Advisor 檢查。如果您有商業、Enterprise On-Ramp 或企業支援計劃，可以存取所有檢查。如需詳細資訊，請參閱《AWS Trusted Advisor 檢查參考》。

您可以使用 AWS Identity and Access Management (IAM) 控制對 Trusted Advisor.

主題

- Trusted Advisor 主控台的許可
- Trusted Advisor 動作
- IAM 政策範例
- 另請參閱

Trusted Advisor 主控台的許可

若要存取 Trusted Advisor 主控台，使用者必須具有最低限度的權限集。這些權限必須允許使用者列出並檢 Trusted Advisor 視您的 AWS 帳戶.

您可以使用下列選項來控制 Trusted Advisor的存取權：

- 使用控 Trusted Advisor 制台的標籤過濾器功能。使用者或角色必須具有與標籤相關聯的許可。

  您可以使用 AWS 受管理的原則或自訂原則，依標籤指派權限。如需詳細資訊，請參閱使用標籤來控制對 IAM 使用者和角色的存取。
- 建立具有`trustedadvisor` 命名空間的 IAM 政策。您可使用此政策指定動作和資源的許可。

當您建立政策時，可以指定服務的命名空間，以允許或拒絕動作。的命名空間 Trusted Advisor 是`trustedadvisor`。但是，您無法使用`trustedadvisor`命名空間來允許或拒絕 Trusted Advisor API 中的 AWS Support API 操作。但針對 AWS Support ，您必須使用 `support` 命名空間。

> **Note**
>
> 如果您擁有 AWS SupportAPI 的權限，則中的 Trusted Advisor 小器具會 AWS Management Console 顯示 Trusted Advisor 結果的摘要檢視。若要在 Trusted Advisor 主控台中檢視結果，您必須擁有`trustedadvisor`命名空間的權限。

Trusted Advisor 動作

您可以在主控台中 Trusted Advisor 執行下列動作。您也可以在 IAM 政策中指定這些 Trusted Advisor 動作，以允許或拒絕特定動作。

動作	描述
`DescribeAccount`	授予檢視 AWS Support 計劃和各種 Trusted Advisor 偏好設定的權限。
`DescribeAccountAccess`	授予檢視的權限是否 AWS 帳戶 已啟用或停用 Trusted Advisor。
`DescribeCheckItems`	准許檢視檢查項目的詳細資訊。
`DescribeCheckRefreshStatuses`	准許檢視 Trusted Advisor 檢查的重新整理狀態。
`DescribeCheckSummaries`	授予 Trusted Advisor 檢視檢查摘要的權限。
`DescribeChecks`	授與檢視 Trusted Advisor 檢查詳細資料的權限。
`DescribeNotificationPreferences`	准許檢視 AWS 帳戶的通知偏好設定。
`ExcludeCheckItems`	准許排除 Trusted Advisor 檢查的建議。
`IncludeCheckItems`	准許包含 Trusted Advisor 檢查的建議。

動作	描述
RefreshCheck	授與重新整理 Trusted Advisor 檢查的權限。
SetAccountAccess	授予對帳戶啟用或停 Trusted Advisor 用的權限。
UpdateNotificationPreferences	准許更新 Trusted Advisor的通知偏好設定。
DescribeCheckStatusHistoryChanges	准許檢視過去 30 天內檢查的結果和變更狀態。

Trusted Advisor 組織檢視的動作

下列 Trusted Advisor 動作適用於組織檢視功能。如需詳細資訊，請參閱 AWS Trusted Advisor 的組織檢視。

動作	描述
DescribeOrganization	授予檢視權限是否 AWS 帳戶 符合啟用組織檢視功能的需求。
DescribeOrganizationAccounts	授與檢視組織中連結 AWS 帳戶的權限。
DescribeReports	准許檢視組織檢視報告的詳細資訊，例如報告名稱、執行時間、建立日期、狀態和格式。
DescribeServiceMetadata	授與檢視組織檢視報告相關資訊的權限，例如 AWS 區域、檢查類別、檢查名稱和資源狀態。
GenerateReport	授與在組織中建立 Trusted Advisor 檢查報告的權限。
ListAccountsForParent	授與在 Trusted Advisor 主控台中檢視根或 AWS 組織單位 (OU) 所包含之組織中所有帳號的權限。
ListOrganizationalUnitsForParent	授與在 Trusted Advisor 主控台中檢視父系組織單位或根目錄中所有組織單位 (OU) 的權限。

動作	描述
ListRoots	授與在 Trusted Advisor 主控台中檢視 AWS 組織中定義之所有根目錄的權限。
SetOrganizationAccess	授與啟用組織檢視功能的權限 Trusted Advisor。

Trusted Advisor 優先權動作

如果您的帳戶已啟用「 Trusted Advisor 優先順序」，您可以在主控台中 Trusted Advisor 執行下列動作。您也可以在 IAM 政策中新增這些 Trusted Advisor 動作，以允許或拒絕特定動作。如需詳細資訊，請參閱 針對 Trusted Advisor 優先權的 IAM 政策範例。

> **Note**
>
> Trusted Advisor 優先順序中顯示的風險是您的技術客戶經理 (TAM) 針對您的帳戶所識別的建議。系統會自動為您建立來自服務的建議，例如 Trusted Advisor 檢查。來自您 TAM 的建議是手動為您建立的。接下來，您的 TAM 會傳送這些建議，讓它們顯示在您帳戶的「 Trusted Advisor 優先順序」中。

如需詳細資訊，請參閱 開始使用 AWS Trusted Advisor 優先權。

動作	描述
DescribeRisks	授予檢視 Trusted Advisor 優先順序中風險的權限。
DescribeRisk	授予檢視 Trusted Advisor 優先順序中風險詳細資料的權限。
DescribeRiskResources	授予許可以檢視 Trusted Advisor 優先權中風險的受影響資源。
DownloadRisk	授予下載包含「 Trusted Advisor 優先順序」中風險詳細資料之檔案的權限。

動作	描述
UpdateRiskStatus	授予許可以更新 Trusted Advisor 優先權中的風險狀態。
DescribeNotificationConfigurations	授予取得「 Trusted Advisor 優先權」電子郵件通知偏好設定的權限。
UpdateNotificationConfigurations	准許建立或更新 Trusted Advisor Priority 的電子郵件通知偏好設定。
DeleteNotificationConfigurationForDelegatedAdmin	授與組織管理帳戶的權限，以便從「 Trusted Advisor 優先順序」的委派管理員帳戶刪除電子郵件通知偏好設定

Trusted Advisor 參與行動

如果您的帳戶已啟用 Trusted Advisor Engage，您可以在主控台中 Trusted Advisor 執行下列動作。您也可以在 IAM 政策中新增這些 Trusted Advisor 動作，以允許或拒絕特定動作。如需詳細資訊，請參閱適用於 Trusted Advisor Engage 的 IAM 政策範例。

如需詳細資訊，請參閱 開始使用 AWS Trusted Advisor Engage (預覽版)。

動作	描述
CreateEngagement	授予創建參 Trusted Advisor 與的權限。
CreateEngagementAttachment	授予在 Trusted Advisor Engage 中創建參與附件的權限。
CreateEngagementCommunication	授予在 Trusted Advisor Engage 中創建參與交流的權限。
GetEngagement	授予檢視參與活 Trusted Advisor 動的權限。
GetEngagementAttachment	授予在 Trusted Advisor Engage 中檢視參與附件的權限。

動作	描述
GetEngagementType	授予在 Trusted Advisor Engage 中檢視特定參與類型的權限。
ListEngagementCommunications	准許在 Trusted Advisor Engage 中檢視業務開發的所有通訊。
ListEngagements	授予檢視「參與」中所有參與活 Trusted Advisor 動的權限。
ListEngagementTypes	授予在 Trusted Advisor Engage 中檢視所有參與類型的權限。
UpdateEngagement	授予更新參 Trusted Advisor 與詳細資訊的權限。
UpdateEngagementStatus	授予更新參 Trusted Advisor 與活動狀態的權限。

IAM 政策範例

下列政策會告訴您如何允許和拒絕 Trusted Advisor的存取權。您可以在 IAM 主控台中使用下列其中一項政策來建立客戶受管政策。例如，您可以複製範例政策，然後貼到 IAM 主控台的 JSON 索引標籤中。然後您可以將政策連接至 IAM 使用者、群組或角色。

如需如何建立 IAM 政策的詳細資訊，請參閱 IAM 使用者指南中的建立 IAM 政策 (主控台)。

範例

- 完全存取 Trusted Advisor
- 唯讀存取 Trusted Advisor
- 拒絕存取 Trusted Advisor
- 允許和拒絕特定動作
- 控制對下列項目之 AWS Support API 作業的存取 Trusted Advisor
- 針對 Trusted Advisor 優先權的 IAM 政策範例
- 適用於 Trusted Advisor Engage 的 IAM 政策範例

完全存取 Trusted Advisor

下列原則可讓使用者檢視並對 Trusted Advisor 主控台中的所有 Trusted Advisor 檢查採取所有動作。

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

唯讀存取 Trusted Advisor

下列原則允許使用者以唯讀方式存取 Trusted Advisor 主控台。使用者無法進行變更，例如重新整理檢查或變更通知偏好設定。

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

拒絕存取 Trusted Advisor

下列原則不允許使用者在 Trusted Advisor 主控台中 Trusted Advisor 檢視或採取處理行動。

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

```
            "Effect": "Deny",
            "Action": "trustedadvisor:*",
            "Resource": "*"
        }
    ]
}
```

允許和拒絕特定動作

下列原則可讓使用者在 Trusted Advisor 主控台中 Trusted Advisor 檢視所有檢查，但不允許使用者重新整理任何檢查。

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

控制對下列項目之 AWS Support API 作業的存取 Trusted Advisor

在中 AWS Management Console，單獨的 `trustedadvisor` IAM 命名空間可控制對 Trusted Advisor. 您無法使用`trustedadvisor`命名空間來允許或拒絕 Trusted Advisor API 中的 AWS Support API 操作。相反地，您可以使用 `support` 命名空間。您必須具有 AWS Support API 的權限，才能 Trusted Advisor 以程式設計方式呼叫。

例如，如果您想要呼叫RefreshTrustedAdvisorCheck作業，您必須擁有原則中此動作的權限。

Example ：僅允許 Trusted Advisor API 作業

下列原則允許使用者存取 AWS Support API 作業的 API 作業 Trusted Advisor，但無法存取其餘的 AWS Support API 作業。例如，使用者可以使用 API 來檢視和重新整理檢查。他們無法建立、檢視、更新或解決 AWS Support 案例。

您可以使用此原則以程式設計方式呼叫 Trusted Advisor API 作業，但無法使用此原則在 Trusted Advisor 主控台中檢視或重新整理檢查。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "support:DescribeTrustedAdvisorCheckRefreshStatuses",
                "support:DescribeTrustedAdvisorCheckResult",
                "support:DescribeTrustedAdvisorChecks",
                "support:DescribeTrustedAdvisorCheckSummaries",
                "support:RefreshTrustedAdvisorCheck",
                "trustedadvisor:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "support:AddAttachmentsToSet",
                "support:AddCommunicationToCase",
                "support:CreateCase",
                "support:DescribeAttachment",
                "support:DescribeCases",
                "support:DescribeCommunications",
                "support:DescribeServices",
                "support:DescribeSeverityLevels",
                "support:ResolveCase"
            ],
            "Resource": "*"
        }
    ]
}
```

如需 IAM 如何使用和的詳細資訊 AWS Support Trusted Advisor，請參閱動作。

針對 Trusted Advisor 優先權的 IAM 政策範例

您可以使用下列 AWS 受管理的策略來控制對 Trusted Advisor 優先順序的存取。如需詳細資訊，請參閱 AWS 受管理的政策 AWS Trusted Advisor 及 開始使用 AWS Trusted Advisor 優先權。

適用於 Trusted Advisor Engage 的 IAM 政策範例

> **Note**
>
> Trusted Advisor Engage 是預覽版本，目前沒有任何 AWS 受管理的政策。您可以在 IAM 主控台中使用下列其中一項政策來建立客戶受管政策。

在 Trusted Advisor Engage 中授予讀取和寫入存取權限的範例原則：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:CreateEngagement*",
                "trustedadvisor:DescribeAccount*",
                "trustedadvisor:GetEngagement*",
                "trustedadvisor:ListEngagement*",
                "trustedadvisor:UpdateEngagement*"
            ],
            "Resource": "*"
        }
    ]
}
```

在 Trusted Advisor Engage 中授予唯讀存取權限的範例原則：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:DescribeAccount*",
                "trustedadvisor:GetEngagement*",
                "trustedadvisor:ListEngagement*"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

在 Trusted Advisor Engage 中授予讀取和寫入存取權限的範例原則，以及啟用受信任存取權限的能力 Trusted Advisor：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAWSServiceAccessForOrganization",
                "trustedadvisor:CreateEngagement*",
                "trustedadvisor:DescribeAccount*",
                "trustedadvisor:DescribeOrganization",
                "trustedadvisor:GetEngagement*",
                "trustedadvisor:ListEngagement*",
                "trustedadvisor:SetOrganizationAccess",
                "trustedadvisor:UpdateEngagement*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": [
                        "reporting.trustedadvisor.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting",
```

```
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "reporting.trustedadvisor.amazonaws.com"
                }
            }
        }
    ]
}
```

另請參閱

如需有關 Trusted Advisor 權限的詳細資訊，請參閱下列資源：

- IAM 使用者指南中的 AWS Trusted Advisor定義的動作。
- 控制對 Trusted Advisor 主控台的存取權

適用於 AWS Trusted Advisor的服務控制政策範例

AWS Trusted Advisor 支援服務控制原則 (SCP)。SCP 是您附加至組織中元素的政策，藉此管理該組織內的許可。SCP 適用於您附加 SCP 之元素下的所有 AWS 帳戶。SCP 可集中控制組織中所有帳戶可用的許可上限。他們可協助您確保 AWS 帳戶符合組織的存取控制準則。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的服務控制政策。

主題

- 必要條件
- 服務控制政策的範例

必要條件

若要使用 SCP，您必須執行下列動作：

- 啟用您組織的所有功能。如需詳細資訊，請參閱 AWS Organizations 使用者指南中的啟用組織中的所有功能。
- 啟用 SCP 以便於您的組織內使用。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的啟用和停用政策類型。
- 建立您需要的 SCP。如需有關建立 SCP 的詳細資訊，請參閱《AWS Organizations 使用者指南》中的建立、更新和刪除服務控制政策。

服務控制政策的範例

下列範例展示您可以如何控制組織中資源共享的各個層面。

Example ：防止使用者在「參與」中建立或編輯參與 Trusted Advisor

下列 SCP 可防止使用者建立新的業務開發或編輯現有的業務開發。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "trustedadvisor:CreateEngagement",
        "trustedadvisor:UpdateEngagement*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Example ：拒絕 Trusted Advisor 參與和 Trusted Advisor 優先存取

下列 SCP 可防止使用者存取或執行「 Trusted Advisor 參與」和「 Trusted Advisor 優先順序」中的任何動作。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "trustedadvisor:ListEngagement*",
        "trustedadvisor:GetEngagement*",
        "trustedadvisor:CreateEngagement*",
        "trustedadvisor:UpdateEngagement*",
        "trustedadvisor:DescribeRisk*",
        "trustedadvisor:UpdateRisk*",
        "trustedadvisor:DownloadRisk"
      ],
```

```
      "Resource": [
        "*"
      ]
    }
  ]
}
```

疑難排解 AWS Support 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 Support 常見問題。

主題

- 我沒有授權執行 iam：PassRole
- 我想要檢視我的存取金鑰
- 我是系統管理員，想要允許其他人存取 AWS Support
- 我想允許 AWS 帳戶以外的人員存取我的 AWS Support 資源

我沒有授權執行 iam：PassRole

如果您收到錯誤，告知您未獲授權執行 `iam:PassRole` 動作，您的政策必須更新，允許您將角色傳遞給 AWS Support。

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

名為 `marymajor` 的 IAM 使用者嘗試使用主控台在 AWS Support中執行動作時，發生下列範例錯誤。但是，動作要求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

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

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

如果您需要協助，請聯絡您的 AWS 系統管理員。您的管理員提供您的登入憑證。

我想要檢視我的存取金鑰

在您建立 IAM 使用者存取金鑰後，您可以隨時檢視您的存取金鑰 ID。但是，您無法再次檢視您的私密存取金鑰。若您遺失了密碼金鑰，您必須建立新的存取金鑰對。

存取金鑰包含兩個部分：存取金鑰 ID (例如 AKIAIOSFODNN7EXAMPLE) 和私密存取金鑰 (例如 wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY)。如同使用者名稱和密碼，您必須一起使用存取金鑰 ID 和私密存取金鑰來驗證您的請求。就如對您的使用者名稱和密碼一樣，安全地管理您的存取金鑰。

> **Important**
>
> 請勿將您的存取金鑰提供給第三方，甚至是協助尋找您的標準使用者 ID。通過這樣做，您可能會讓某人永久訪問您的 AWS 帳戶.

建立存取金鑰對時，您會收到提示，要求您將存取金鑰 ID 和私密存取金鑰儲存在安全位置。私密存取金鑰只會在您建立它的時候顯示一次。若您遺失了私密存取金鑰，您必須將新的存取金鑰新增到您的 IAM 使用者。您最多可以擁有兩個存取金鑰。若您已有兩個存取金鑰，您必須先刪除其中一個金鑰對，才能建立新的金鑰對。若要檢視說明，請參閱《IAM 使用者指南》中的管理存取金鑰。

我是系統管理員，想要允許其他人存取 AWS Support

若要允許其他人存取 AWS Support，您必須為需要存取的人員或應用程式建立 IAM 實體 (使用者或角色)。他們將使用該實體的憑證來存取 AWS。您接著必須將政策連接到實體，在 AWS Support中授予他們正確的許可。

若要立即開始使用，請參閱《IAM 使用者指南》中的建立您的第一個 IAM 委派使用者及群組。

我想允許 AWS 帳戶以外的人員存取我的 AWS Support 資源

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

如需進一步了解，請參閱以下內容：

- 若要瞭解是否 AWS Support 支援這些功能，請參閱如何與 IAM AWS Support 搭配使用。
- 若要了解如何提供對您所擁有資源 AWS 帳戶 的存取權，請參閱《IAM 使用者指南》中您擁有的另一 AWS 帳戶 個 IAM 使用者提供存取權限。
- 若要了解如何向第三方提供對資源的存取權 AWS 帳戶，請參閱 IAM 使用者指南中的提供第三方 AWS 帳戶 擁有的存取權。
- 若要了解如何透過聯合身分提供存取權，請參閱《IAM 使用者指南》中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。

- 若要了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 角色與資源型政策的差異。

事件反應

的事件回應 AWS Support 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。如需詳細資訊，請參閱簡介 AWS 安全性事件回應白皮書。

使用下列選項自行取得關於操作問題的通知：

- 在 AWS Service Health Dashboard 上檢視具有廣泛影響的 AWS 作業問題。例如，會影響不專屬於您帳戶之服務或區域的事件。
- 檢視 AWS Health Dashboard 中個別帳戶的操作問題。例如，會影響您帳戶中服務或資源的事件。如需詳細資訊，請參閱 AWS Health 使用者指南中的 AWS Health Dashboard入門。

登錄和監控 AWS SupportAWS Trusted Advisor

監控是維持和其他 AWS 解決方案的可靠性、可用性和效能的 AWS Support 重要組成部分。 AWS Trusted Advisor AWS 提供以下監視工具來監視 AWS Support 和 AWS Trusted Advisor報告錯誤，並在適當時採取行動：

- Amazon 會即時 CloudWatch監控您的 AWS 資源和執行 AWS 的應用程式。您可以收集和追蹤指標、建立自訂儀板表，以及設定警示，在特定指標達到您指定的閾值時通知您或採取動作。例如，您可以 CloudWatch 追蹤 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 CPU 使用率或其他指標，並在需要時自動啟動新執行個體。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。
- Amazon EventBridge 提供近乎即時的系統事件串流，用於描述 AWS 資源變更。 EventBridge 啟用自動化事件驅動計算，因為您可以編寫規則來監視某些事件，並在這些事件發生時觸發其他 AWS 服務中的自動化操作。如需詳細資訊，請參閱 Amazon EventBridge 使用者指南。
- AWS CloudTrail擷取您帳戶或代表您的 AWS 帳戶發出的 API 呼叫和相關事件，並將日誌檔交付到您指定的 Amazon Simple Storage Service (Amazon S3) 儲存貯體。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。如需詳細資訊，請參閱 AWS CloudTrail 使用者指南。

如需更多詳細資訊，請參閱 AWS Support 的監控和日誌記錄 及 AWS Trusted Advisor 的監控和日誌記錄。

符合性驗證 AWS Support

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。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

韌性 AWS Support

AWS 全球基礎架構是圍繞區 AWS 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，您可以設計與操作的應

用程式和資料庫，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、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需區域和可用區域的詳 AWS 細資訊，請參閱AWS 全域基礎結構。

基礎結構安全 AWS Support

身為受管服務， AWS Support 受 Amazon Web Services：安 AWS 全程序概觀白皮書中所述的全球網路安全程序保護。

您可以使用 AWS 已發佈的 API 呼叫透 AWS Support 過網路進行存取。用戶端必須支援 Transport Layer Security (TLS) 1.0 或更新版本。建議使用 TLS 1.2 或更新版本。用戶端也必須支援具備完美轉送私密 (PFS) 的密碼套件，例如臨時 Diffie-Hellman (DHE) 或橢圓曲線臨時 Diffie-Hellman (ECDHE)。現代系統 (如 Java 7 和更新版本) 大多會支援這些模式。

此外，請求必須使用存取索引鍵 ID 和與 IAM 主體相關聯的私密存取索引鍵來簽署。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 Support

對於 AWS Trusted Advisor， AWS 處理基本安全性工作，例如客體作業系統 (OS) 和資料庫修補、防火牆組態和嚴重損壞修復。

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。

AWS Support 使用 AWS SDK 的程式碼範例

下列程式碼範例顯示如何搭 AWS Support 配 AWS 軟體開發套件 (SDK) 使用。

Actions 是大型程式的程式碼摘錄，必須在內容中執行。雖然動作會告訴您如何呼叫個別服務函數，但您可以在其相關情境和跨服務範例中查看內容中的動作。

案例是向您展示如何呼叫相同服務中的多個函數來完成特定任務的程式碼範例。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭配 AWS SDK 使用 AWS Support。此主題也包含入門相關資訊和舊版 SDK 的詳細資訊。

開始使用

你好 AWS Support

下列程式碼範例示範如何開始使用 AWS Support。

.NET

AWS SDK for .NET

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
using Amazon.AWSSupport;
using Microsoft.Extensions.DependencyInjection;
using Microsoft.Extensions.Hosting;

public static class HelloSupport
{
    static async Task Main(string[] args)
    {
        // Use the AWS .NET Core Setup package to set up dependency injection for
 the AWS Support service.
        // Use your AWS profile name, or leave it blank to use the default
 profile.
```

```
        // You must have one of the following AWS Support plans: Business,
 Enterprise On-Ramp, or Enterprise. Otherwise, an exception will be thrown.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonAWSSupport>()
            ).Build();

        // Now the client is available for injection.
        var supportClient =
 host.Services.GetRequiredService<IAmazonAWSSupport>();

        // You can use await and any of the async methods to get a response.
        var response = await supportClient.DescribeServicesAsync();
        Console.WriteLine($"\tHello AWS Support! There are
 {response.Services.Count} services available.");
    }
}
```

- 如需 API 詳細資訊，請參閱 AWS SDK for .NET API 參考DescribeServices中的。

Java

適用於 Java 2.x 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.support.SupportClient;
import software.amazon.awssdk.services.support.model.Category;
import software.amazon.awssdk.services.support.model.DescribeServicesRequest;
import software.amazon.awssdk.services.support.model.DescribeServicesResponse;
import software.amazon.awssdk.services.support.model.Service;
import software.amazon.awssdk.services.support.model.SupportException;
import java.util.ArrayList;
import java.util.List;

/**
```

```
 * Before running this Java (v2) code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * In addition, you must have the AWS Business Support Plan to use the AWS
 * Support Java API. For more information, see:
 *
 * https://aws.amazon.com/premiumsupport/plans/
 *
 * This Java example performs the following task:
 *
 * 1. Gets and displays available services.
 *
 *
 * NOTE: To see multiple operations, see SupportScenario.
 */

public class HelloSupport {
    public static void main(String[] args) {
        Region region = Region.US_WEST_2;
        SupportClient supportClient = SupportClient.builder()
                .region(region)
                .build();

        System.out.println("***** Step 1. Get and display available services.");
        displayServices(supportClient);
    }

    // Return a List that contains a Service name and Category name.
    public static void displayServices(SupportClient supportClient) {
        try {
            DescribeServicesRequest servicesRequest =
 DescribeServicesRequest.builder()
                    .language("en")
                    .build();

            DescribeServicesResponse response =
 supportClient.describeServices(servicesRequest);
            List<Service> services = response.services();
```

```
            System.out.println("Get the first 10 services");
            int index = 1;
            for (Service service : services) {
                if (index == 11)
                    break;

                System.out.println("The Service name is: " + service.name());

                // Display the Categories for this service.
                List<Category> categories = service.categories();
                for (Category cat : categories) {
                    System.out.println("The category name is: " + cat.name());
                }
                index++;
            }

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
}
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考DescribeServices中的。

JavaScript

適用於 JavaScript (v3) 的開發套件

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

呼叫 `main()` 來執行這個範例。

```
import {
  DescribeServicesCommand,
  SupportClient,
} from "@aws-sdk/client-support";
```

```
// Change the value of 'region' to your preferred AWS Region.
const client = new SupportClient({ region: "us-east-1" });

const getServiceCount = async () => {
  try {
    const { services } = await client.send(new DescribeServicesCommand({}));
    return services.length;
  } catch (err) {
    if (err.name === "SubscriptionRequiredException") {
      throw new Error(
        "You must be subscribed to the AWS Support plan to use this feature.",
      );
    } else {
      throw err;
    }
  }
};

export const main = async () => {
  try {
    const count = await getServiceCount();
    console.log(`Hello, AWS Support! There are ${count} services available.`);
  } catch (err) {
    console.error("Failed to get service count: ", err.message);
  }
};
```

- 如需 API 詳細資訊，請參閱 AWS SDK for JavaScript API 參考DescribeServices中的。

Kotlin

適用於 Kotlin 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
/**
```

```
Before running this Kotlin code example, set up your development environment,
including your credentials.

For more information, see the following documentation topic:
https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html

In addition, you must have the AWS Business Support Plan to use the AWS Support
 Java API. For more information, see:

https://aws.amazon.com/premiumsupport/plans/

This Kotlin example performs the following task:

1. Gets and displays available services.
 */

suspend fun main() {
    displaySomeServices()
}

// Return a List that contains a Service name and Category name.
suspend fun displaySomeServices() {
    val servicesRequest = DescribeServicesRequest {
        language = "en"
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeServices(servicesRequest)
        println("Get the first 10 services")
        var index = 1

        response.services?.forEach { service ->
            if (index == 11) {
                return@forEach
            }

            println("The Service name is: " + service.name)

            // Get the categories for this service.
            service.categories?.forEach { cat ->
                println("The category name is ${cat.name}")
                index++
            }
        }
```

```
    }
}
```

- 有關 API 的詳細信息，請參閱 AWS SDK DescribeServices中的 Kotlin API 參考。

Python

適用於 Python (Boto3) 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
import logging
import boto3
from botocore.exceptions import ClientError

logger = logging.getLogger(__name__)


def hello_support(support_client):
    """
    Use the AWS SDK for Python (Boto3) to create an AWS Support client and count
    the available services in your account.
    This example uses the default settings specified in your shared credentials
    and config files.

    :param support_client: A Boto3 Support Client object.
    """
    try:
        print("Hello, AWS Support! Let's count the available Support services:")
        response = support_client.describe_services()
        print(f"There are {len(response['services'])} services available.")
    except ClientError as err:
        if err.response["Error"]["Code"] == "SubscriptionRequiredException":
            logger.info(
                "You must have a Business, Enterprise On-Ramp, or Enterprise
 Support "
```

```
                "plan to use the AWS Support API. \n\tPlease upgrade your
 subscription to run these "
                "examples."
            )
        else:
            logger.error(
                "Couldn't count services. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise


if __name__ == "__main__":
    hello_support(boto3.client("support"))
```

- 如需 API 的詳細資訊，請參閱AWS 開發套件DescribeServices中的 Python (博托 3) API 參考。

程式碼範例

- AWS Support 使用 AWS SDK 的動作
  - 使用 AWS SDK 將 AWS Support 通訊新增至案例
  - 使用 AWS SDK 將 AWS Support 附件新增至集
  - 使用 AWS SDK 建立 AWS Support 案例
  - 使用 AWS SDK 描述 AWS Support 案例的附件
  - 使用 AWS SDK 描述 AWS Support 案例
  - 使用 AWS SDK 描述案例的 AWS Support 通訊
  - 使用 AWS SDK 描述支 AWS 援案例的可用服務
  - 使用 AWS SDK 描述 AWS Support 嚴重性層級
  - 使用 AWS SDK 解決 AWS Support 案例
- AWS Support 使用 AWS 軟體開發套件的案例
  - 使用 AWS SDK 開始使用 AWS Support 案例

AWS Support 使用 AWS SDK 的動作

下列程式碼範例示範如何使用 AWS SDK 執 AWS Support 行個別動作。這些摘錄會呼叫 AWS Support API，是來自必須在內容中執行的大型程式碼摘錄。每個範例都包含一個連結 GitHub，您可以在其中找到設定和執行程式碼的指示。

下列範例僅包含最常使用的動作。如需完整清單，請參閱《AWS Support API 參考》。

範例

- 使用 AWS SDK 將 AWS Support 通訊新增至案例
- 使用 AWS SDK 將 AWS Support 附件新增至集
- 使用 AWS SDK 建立 AWS Support 案例
- 使用 AWS SDK 描述 AWS Support 案例的附件
- 使用 AWS SDK 描述 AWS Support 案例
- 使用 AWS SDK 描述案例的 AWS Support 通訊
- 使用 AWS SDK 描述支 AWS 援案例的可用服務
- 使用 AWS SDK 描述 AWS Support 嚴重性層級
- 使用 AWS SDK 解決 AWS Support 案例

使用 AWS SDK 將 AWS Support 通訊新增至案例

下列程式碼範例說明如何將含有附件的 AWS Support 通訊新增至支援案例。

動作範例是大型程式的程式碼摘錄，必須在內容中執行。您可以在下列程式碼範例的內容中看到此動作：

- 開始使用案例

.NET

AWS SDK for .NET

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
    /// <summary>
    /// Add communication to a case, including optional attachment set ID and CC
 email addresses.
    /// </summary>
    /// <param name="caseId">Id for the support case.</param>
    /// <param name="body">Body text of the communication.</param>
    /// <param name="attachmentSetId">Optional Id for an attachment set.</param>
    /// <param name="ccEmailAddresses">Optional list of CC email addresses.</
param>
    /// <returns>True if successful.</returns>
    public async Task<bool> AddCommunicationToCase(string caseId, string body,
        string? attachmentSetId = null, List<string>? ccEmailAddresses = null)
    {
        var response = await _amazonSupport.AddCommunicationToCaseAsync(
            new AddCommunicationToCaseRequest()
            {
                CaseId = caseId,
                CommunicationBody = body,
                AttachmentSetId = attachmentSetId,
                CcEmailAddresses = ccEmailAddresses
            });
        return response.Result;
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for .NET API 參考AddCommunicationToCase中的。

Java

適用於 Java 2.x 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
    public static void addAttachSupportCase(SupportClient supportClient, String
 caseId, String attachmentSetId) {
```

```
        try {
            AddCommunicationToCaseRequest caseRequest =
AddCommunicationToCaseRequest.builder()
                    .caseId(caseId)
                    .attachmentSetId(attachmentSetId)
                    .communicationBody("Please refer to attachment for details.")
                    .build();

            AddCommunicationToCaseResponse response =
supportClient.addCommunicationToCase(caseRequest);
            if (response.result())
                System.out.println("You have successfully added a communication
to an AWS Support case");
            else
                System.out.println("There was an error adding the communication
to an AWS Support case");

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考AddCommunicationToCase中的。

JavaScript

適用於 JavaScript (v3) 的開發套件

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
import { AddCommunicationToCaseCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";
```

```
export const main = async () => {
  let attachmentSetId;

  try {
    // Add a communication to a case.
    const response = await client.send(
      new AddCommunicationToCaseCommand({
        communicationBody: "Adding an attachment.",
        // Set value to an existing support case id.
        caseId: "CASE_ID",
        // Optional. Set value to an existing attachment set id to add
 attachments to the case.
        attachmentSetId,
      }),
    );
    console.log(response);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- 如需 API 詳細資訊，請參閱 AWS SDK for JavaScript API 參考AddCommunicationToCase中的。

Kotlin

適用於 Kotlin 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
suspend fun addAttachSupportCase(caseIdVal: String?, attachmentSetIdVal: String?)
 {
    val caseRequest = AddCommunicationToCaseRequest {
        caseId = caseIdVal
        attachmentSetId = attachmentSetIdVal
```

```
        communicationBody = "Please refer to attachment for details."
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addCommunicationToCase(caseRequest)
        if (response.result) {
            println("You have successfully added a communication to an AWS
 Support case")
        } else {
            println("There was an error adding the communication to an AWS
 Support case")
        }
    }
}
```

- 有關 API 的詳細信息，請參閱 AWS SDK AddCommunicationToCase中的 Kotlin API 參考。

Python

適用於 Python (Boto3) 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
```

```
        support_client = boto3.client("support")
        return cls(support_client)


    def add_communication_to_case(self, attachment_set_id, case_id):
        """
        Add a communication and an attachment set to a case.

        :param attachment_set_id: The ID of an existing attachment set.
        :param case_id: The ID of the case.
        """
        try:
            self.support_client.add_communication_to_case(
                caseId=case_id,
                communicationBody="This is an example communication added to a
support case.",
                attachmentSetId=attachment_set_id,
            )
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add communication. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
```

- 如需 API 的詳細資訊，請參閱AWS 開發套件AddCommunicationToCase中的 Python (博托 3) API 參考。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭配 AWS SDK 使用 AWS Support。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

使用 AWS SDK 將 AWS Support 附件新增至集

下列程式碼範例顯示如何將 AWS Support 附件新增至附件集。

動作範例是大型程式的程式碼摘錄，必須在內容中執行。您可以在下列程式碼範例的內容中看到此動作：

- 開始使用案例

.NET

AWS SDK for .NET

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
   /// <summary>
   /// Add an attachment to a set, or create a new attachment set if one does
not exist.
   /// </summary>
   /// <param name="data">The data for the attachment.</param>
   /// <param name="fileName">The file name for the attachment.</param>
   /// <param name="attachmentSetId">Optional setId for the attachment. Creates
a new attachment set if empty.</param>
   /// <returns>The setId of the attachment.</returns>
   public async Task<string> AddAttachmentToSet(MemoryStream data, string
fileName, string? attachmentSetId = null)
   {
       var response = await _amazonSupport.AddAttachmentsToSetAsync(
           new AddAttachmentsToSetRequest
           {
               AttachmentSetId = attachmentSetId,
               Attachments = new List<Attachment>
               {
                   new Attachment
                   {
                       Data = data,
```

```
                        FileName = fileName
                    }
                }
            });
        return response.AttachmentSetId;
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for .NET API 參考AddAttachmentsToSet中的。

Java

適用於 Java 2.x 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
   public static String addAttachment(SupportClient supportClient, String
fileAttachment) {
       try {
           File myFile = new File(fileAttachment);
           InputStream sourceStream = new FileInputStream(myFile);
           SdkBytes sourceBytes = SdkBytes.fromInputStream(sourceStream);

           Attachment attachment = Attachment.builder()
                   .fileName(myFile.getName())
                   .data(sourceBytes)
                   .build();

           AddAttachmentsToSetRequest setRequest =
AddAttachmentsToSetRequest.builder()
                   .attachments(attachment)
                   .build();

           AddAttachmentsToSetResponse response =
supportClient.addAttachmentsToSet(setRequest);
           return response.attachmentSetId();
```

```
        } catch (SupportException | FileNotFoundException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考AddAttachmentsToSet中的。

JavaScript

適用於 JavaScript (v3) 的開發套件

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
import { AddAttachmentsToSetCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Create a new attachment set or add attachments to an existing set.
    // Provide an 'attachmentSetId' value to add attachments to an existing set.
    // Use AddCommunicationToCase or CreateCase to associate an attachment set
 with a support case.
    const response = await client.send(
      new AddAttachmentsToSetCommand({
        // You can add up to three attachments per set. The size limit is 5 MB
 per attachment.
        attachments: [
          {
            fileName: "example.txt",
            data: new TextEncoder().encode("some example text"),
          },
        ],
      }),
    );
```

```
    // Use this ID in AddCommunicationToCase or CreateCase.
    console.log(response.attachmentSetId);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- 如需 API 詳細資訊，請參閱 AWS SDK for JavaScript API 參考AddAttachmentsToSet中的。

Kotlin

適用於 Kotlin 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
suspend fun addAttachment(fileAttachment: String): String? {
    val myFile = File(fileAttachment)
    val sourceBytes = (File(fileAttachment).readBytes())
    val attachmentVal = Attachment {
        fileName = myFile.name
        data = sourceBytes
    }

    val setRequest = AddAttachmentsToSetRequest {
        attachments = listOf(attachmentVal)
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addAttachmentsToSet(setRequest)
        return response.attachmentSetId
    }
}
```

- 有關 API 的詳細信息，請參閱 AWS SDK AddAttachmentsToSet中的 Kotlin API 參考。

Python

適用於 Python (Boto3) 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def add_attachment_to_set(self):
        """
        Add an attachment to a set, or create a new attachment set if one does
 not exist.

        :return: The attachment set ID.
        """
        try:
            response = self.support_client.add_attachments_to_set(
                attachments=[
                    {
                        "fileName": "attachment_file.txt",
                        "data": b"This is a sample file for attachment to a
 support case.",
```

```
                    }
                ]
            )
            new_set_id = response["attachmentSetId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add attachment. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return new_set_id
```

- 如需 API 的詳細資訊，請參閱AWS 開發套件AddAttachmentsToSet中的 Python (博托 3) API 參考。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭配 AWS SDK 使用 AWS Support。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

使用 AWS SDK 建立 AWS Support 案例

下列程式碼範例會示範如何建立新 AWS Support 案例。

動作範例是大型程式的程式碼摘錄，必須在內容中執行。您可以在下列程式碼範例的內容中看到此動作：

- 開始使用案例

.NET

AWS SDK for .NET

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
    /// <summary>
    /// Create a new support case.
    /// </summary>
    /// <param name="serviceCode">Service code for the new case.</param>
    /// <param name="categoryCode">Category for the new case.</param>
    /// <param name="severityCode">Severity code for the new case.</param>
    /// <param name="subject">Subject of the new case.</param>
    /// <param name="body">Body text of the new case.</param>
    /// <param name="language">Optional language support for your case.
    /// Currently "en" (English) and "ja" (Japanese) are supported.</param>
    /// <param name="attachmentSetId">Optional Id for an attachment set for the
new case.</param>
    /// <param name="issueType">Optional issue type for the new case. Options are
"customer-service" or "technical".</param>
    /// <returns>The caseId of the new support case.</returns>
    public async Task<string> CreateCase(string serviceCode, string categoryCode,
string severityCode, string subject,
        string body, string language = "en", string? attachmentSetId = null,
string issueType = "customer-service")
    {
        var response = await _amazonSupport.CreateCaseAsync(
            new CreateCaseRequest()
            {
                ServiceCode = serviceCode,
                CategoryCode = categoryCode,
                SeverityCode = severityCode,
                Subject = subject,
                Language = language,
                AttachmentSetId = attachmentSetId,
                IssueType = issueType,
                CommunicationBody = body
```

```
            });
        return response.CaseId;
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for .NET API 參考CreateCase中的。

CLI

AWS CLI

若要建立案例

下列create-case範例會為您的 AWS 帳戶建立支援案例。

```
aws support create-case \
    --category-code "using-aws" \
    --cc-email-addresses "myemail@example.com" \
    --communication-body "I want to learn more about an AWS service." \
    --issue-type "technical" \
    --language "en" \
    --service-code "general-info" \
    --severity-code "low" \
    --subject "Question about my account"
```

輸出：

```
{
    "caseId": "case-12345678910-2013-c4c1d2bf33c5cf47"
}
```

如需詳細資訊，請參閱 Sup AWS port 使用者指南中的案例管理。

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考CreateCase中的。

Java

適用於 Java 2.x 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
   public static String createSupportCase(SupportClient supportClient,
List<String> sevCatList, String sevLevel) {
       try {
           String serviceCode = sevCatList.get(0);
           String caseCat = sevCatList.get(1);
           CreateCaseRequest caseRequest = CreateCaseRequest.builder()
                   .categoryCode(caseCat.toLowerCase())
                   .serviceCode(serviceCode.toLowerCase())
                   .severityCode(sevLevel.toLowerCase())
                   .communicationBody("Test issue with " +
serviceCode.toLowerCase())
                   .subject("Test case, please ignore")
                   .language("en")
                   .issueType("technical")
                   .build();

           CreateCaseResponse response = supportClient.createCase(caseRequest);
           return response.caseId();

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
       return "";
   }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考CreateCase中的。

JavaScript

適用於 JavaScript (v3) 的開發套件

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
import { CreateCaseCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Create a new case and log the case id.
    // Important: This creates a real support case in your account.
    const response = await client.send(
      new CreateCaseCommand({
        // The subject line of the case.
        subject: "IGNORE: Test case",
        // Use DescribeServices to find available service codes for each service.
        serviceCode: "service-quicksight-end-user",
        // Use DescribeSecurityLevels to find available severity codes for your
 support plan.
        severityCode: "low",
        // Use DescribeServices to find available category codes for each
 service.
        categoryCode: "end-user-support",
        // The main description of the support case.
        communicationBody: "This is a test. Please ignore.",
      }),
    );
    console.log(response.caseId);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- 如需 API 詳細資訊，請參閱 AWS SDK for JavaScript API 參考CreateCase中的。

Kotlin

適用於 Kotlin 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
suspend fun createSupportCase(sevCatListVal: List<String>, sevLevelVal: String):
 String? {
    val serCode = sevCatListVal[0]
    val caseCategory = sevCatListVal[1]
    val caseRequest = CreateCaseRequest {
        categoryCode = caseCategory.lowercase(Locale.getDefault())
        serviceCode = serCode.lowercase(Locale.getDefault())
        severityCode = sevLevelVal.lowercase(Locale.getDefault())
        communicationBody = "Test issue with
 ${serCode.lowercase(Locale.getDefault())}"
        subject = "Test case, please ignore"
        language = "en"
        issueType = "technical"
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.createCase(caseRequest)
        return response.caseId
    }
}
```

- 有關 API 的詳細信息，請參閱 AWS SDK CreateCase中的 Kotlin API 參考。

Python

適用於 Python (Boto3) 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def create_case(self, service, category, severity):
        """
        Create a new support case.

        :param service: The service to use for the new case.
        :param category: The category to use for the new case.
        :param severity: The severity to use for the new case.
        :return: The caseId of the new case.
        """
        try:
            response = self.support_client.create_case(
                subject="Example case for testing, ignore.",
                serviceCode=service["code"],
                severityCode=severity["code"],
```

```
                categoryCode=category["code"],
                communicationBody="Example support case body.",
                language="en",
                issueType="customer-service",
            )
            case_id = response["caseId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't create case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return case_id
```

- 如需 API 的詳細資訊，請參閱AWS 開發套件CreateCase中的 Python (博托 3) API 參考。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭配 AWS SDK 使用 AWS Support。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

使用 AWS SDK 描述 AWS Support 案例的附件

下列程式碼範例示範如何描述 AWS Support 案例的附件。

動作範例是大型程式的程式碼摘錄，必須在內容中執行。您可以在下列程式碼範例的內容中看到此動作：

- 開始使用案例

.NET

AWS SDK for .NET

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
    /// <summary>
    /// Get description of a specific attachment.
    /// </summary>
    /// <param name="attachmentId">Id of the attachment, usually fetched by
describing the communications of a case.</param>
    /// <returns>The attachment object.</returns>
    public async Task<Attachment> DescribeAttachment(string attachmentId)
    {
        var response = await _amazonSupport.DescribeAttachmentAsync(
            new DescribeAttachmentRequest()
            {
                AttachmentId = attachmentId
            });
        return response.Attachment;
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for .NET API 參考DescribeAttachment中的。

CLI

AWS CLI

描述附件

下列describe-attachment範例會傳回有關具有指定 ID 之附件的資訊。

```
aws support describe-attachment \
```

```
    --attachment-id "attachment-KBnjRNrePd9D6Jx0-Mm00xZuDEaL2JAj_0-
gJv9qqDooTipsz3V1Nb19rCfkZneeQeDPgp8X1iVJyHH7UuhZDdNeqGoduZsPrAhyMakqlc60-
iJjL5HqyYGiT1FG8EXAMPLE"
```

輸出：

```
{
    "attachment": {
        "fileName": "troubleshoot-screenshot.png",
        "data": "base64-blob"
    }
}
```

如需詳細資訊，請參閱 Sup AWS port 使用者指南中的案例管理。

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考DescribeAttachment中的。

Java

適用於 Java 2.x 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
   public static void describeAttachment(SupportClient supportClient, String
attachId) {
       try {
           DescribeAttachmentRequest attachmentRequest =
DescribeAttachmentRequest.builder()
                   .attachmentId(attachId)
                   .build();

           DescribeAttachmentResponse response =
supportClient.describeAttachment(attachmentRequest);
           System.out.println("The name of the file is " +
response.attachment().fileName());

       } catch (SupportException e) {
```

```
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考DescribeAttachment中的。

JavaScript

適用於 JavaScript (v3) 的開發套件

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
import { DescribeAttachmentCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get the metadata and content of an attachment.
    const response = await client.send(
      new DescribeAttachmentCommand({
        // Set value to an existing attachment id.
        // Use DescribeCommunications or DescribeCases to find an attachment id.
        attachmentId: "ATTACHMENT_ID",
      }),
    );
    console.log(response.attachment?.fileName);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- 如需 API 詳細資訊，請參閱 AWS SDK for JavaScript API 參考DescribeAttachment中的。

Kotlin

適用於 Kotlin 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
suspend fun describeAttachment(attachId: String?) {
    val attachmentRequest = DescribeAttachmentRequest {
        attachmentId = attachId
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeAttachment(attachmentRequest)
        println("The name of the file is ${response.attachment?.fileName}")
    }
}
```

- 有關 API 的詳細信息，請參閱 AWS SDK DescribeAttachment中的 Kotlin API 參考。

Python

適用於 Python (Boto3) 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
```

```
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_attachment(self, attachment_id):
        """
        Get information about an attachment by its attachmentID.

        :param attachment_id: The ID of the attachment.
        :return: The name of the attached file.
        """
        try:
            response = self.support_client.describe_attachment(
                attachmentId=attachment_id
            )
            attached_file = response["attachment"]["fileName"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get attachment description. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return attached_file
```

- 如需 API 的詳細資訊，請參閱AWS 開發套件DescribeAttachment中的 Python (博托 3) API 參考。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭配 AWS SDK 使用 AWS Support。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

使用 AWS SDK 描述 AWS Support 案例

下列程式碼範例會示範如何描述 AWS Support 案例。

動作範例是大型程式的程式碼摘錄，必須在內容中執行。您可以在下列程式碼範例的內容中看到此動作：

- 開始使用案例

.NET

AWS SDK for .NET

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
    /// <summary>
    /// Get case details for a list of case ids, optionally with date filters.
    /// </summary>
    /// <param name="caseIds">The list of case IDs.</param>
    /// <param name="displayId">Optional display ID.</param>
    /// <param name="includeCommunication">True to include communication.
 Defaults to true.</param>
    /// <param name="includeResolvedCases">True to include resolved cases.
 Defaults to false.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
```

```
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <param name="language">Optional language support for your case.
    /// Currently "en" (English) and "ja" (Japanese) are supported.</param>
    /// <returns>A list of CaseDetails.</returns>
    public async Task<List<CaseDetails>> DescribeCases(List<string> caseIds,
 string? displayId = null, bool includeCommunication = true,
        bool includeResolvedCases = false, DateTime? afterTime = null, DateTime?
 beforeTime = null,
        string language = "en")
    {
        var results = new List<CaseDetails>();
        var paginateCases = _amazonSupport.Paginators.DescribeCases(
            new DescribeCasesRequest()
            {
                CaseIdList = caseIds,
                DisplayId = displayId,
                IncludeCommunications = includeCommunication,
                IncludeResolvedCases = includeResolvedCases,
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s"),
                Language = language
            });
        // Get the entire list using the paginator.
        await foreach (var cases in paginateCases.Cases)
        {
            results.Add(cases);
        }
        return results;
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for .NET API 參考DescribeCases中的。

CLI

AWS CLI

描述案例

下列describe-cases範例會傳回您 AWS 帳戶中指定支援案例的相關資訊。

```
aws support describe-cases \
    --display-id "1234567890" \
    --after-time "2020-03-23T21:31:47.774Z" \
    --include-resolved-cases \
    --language "en" \
    --no-include-communications \
    --max-item 1
```

輸出：

```
{
    "cases": [
        {
            "status": "resolved",
            "ccEmailAddresses": [],
            "timeCreated": "2020-03-23T21:31:47.774Z",
            "caseId": "case-12345678910-2013-c4c1d2bf33c5cf47",
            "severityCode": "low",
            "language": "en",
            "categoryCode": "using-aws",
            "serviceCode": "general-info",
            "submittedBy": "myemail@example.com",
            "displayId": "1234567890",
            "subject": "Question about my account"
        }
    ]
}
```

如需詳細資訊，請參閱 Sup AWS port 使用者指南中的案例管理。

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考DescribeCases中的。

Java

適用於 Java 2.x 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
   public static void getOpenCase(SupportClient supportClient) {
       try {
           // Specify the start and end time.
           Instant now = Instant.now();
           java.time.LocalDate.now();
           Instant yesterday = now.minus(1, ChronoUnit.DAYS);

           DescribeCasesRequest describeCasesRequest =
DescribeCasesRequest.builder()
                   .maxResults(20)
                   .afterTime(yesterday.toString())
                   .beforeTime(now.toString())
                   .build();

           DescribeCasesResponse response =
supportClient.describeCases(describeCasesRequest);
           List<CaseDetails> cases = response.cases();
           for (CaseDetails sinCase : cases) {
               System.out.println("The case status is " + sinCase.status());
               System.out.println("The case Id is " + sinCase.caseId());
               System.out.println("The case subject is " + sinCase.subject());
           }

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
   }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考DescribeCases中的。

JavaScript

適用於 JavaScript (v3) 的開發套件

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
import { DescribeCasesCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get all of the unresolved cases in your account.
    // Filter or expand results by providing parameters to the
 DescribeCasesCommand. Refer
    // to the TypeScript definition and the API doc for more information on
 possible parameters.
    // https://docs.aws.amazon.com/AWSJavaScriptSDK/v3/latest/clients/client-
support/interfaces/describecasescommandinput.html
    const response = await client.send(new DescribeCasesCommand({}));
    const caseIds = response.cases.map((supportCase) => supportCase.caseId);
    console.log(caseIds);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- 如需 API 詳細資訊，請參閱 AWS SDK for JavaScript API 參考DescribeCases中的。

Kotlin

適用於 Kotlin 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
suspend fun getOpenCase() {
    // Specify the start and end time.
    val now = Instant.now()
    LocalDate.now()
    val yesterday = now.minus(1, ChronoUnit.DAYS)
    val describeCasesRequest = DescribeCasesRequest {
```

```
        maxResults = 20
        afterTime = yesterday.toString()
        beforeTime = now.toString()
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeCases(describeCasesRequest)
        response.cases?.forEach { sinCase ->
            println("The case status is ${sinCase.status}")
            println("The case Id is ${sinCase.caseId}")
            println("The case subject is ${sinCase.subject}")
        }
    }
}
```

- 有關 API 的詳細信息，請參閱 AWS SDK DescribeCases中的 Kotlin API 參考。

Python

適用於 Python (Boto3) 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
```

```
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_cases(self, after_time, before_time, resolved):
        """
        Describe support cases over a period of time, optionally filtering
        by status.

        :param after_time: The start time to include for cases.
        :param before_time: The end time to include for cases.
        :param resolved: True to include resolved cases in the results,
            otherwise results are open cases.
        :return: The final status of the case.
        """
        try:
            cases = []
            paginator = self.support_client.get_paginator("describe_cases")
            for page in paginator.paginate(
                afterTime=after_time,
                beforeTime=before_time,
                includeResolvedCases=resolved,
                language="en",
            ):
                cases += page["cases"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't describe cases. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            if resolved:
                cases = filter(lambda case: case["status"] == "resolved", cases)
```

```
            return cases
```

- 如需 API 的詳細資訊，請參閱AWS 開發套件DescribeCases中的 Python (博托 3) API 參考。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭配 AWS SDK 使用 AWS Support。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

使用 AWS SDK 描述案例的 AWS Support 通訊

下列程式碼範例說明如何描述案例的 AWS Support 通訊。

動作範例是大型程式的程式碼摘錄，必須在內容中執行。您可以在下列程式碼範例的內容中看到此動作：

- 開始使用案例

.NET

AWS SDK for .NET

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
    /// <summary>
    /// Describe the communications for a case, optionally with a date filter.
    /// </summary>
    /// <param name="caseId">The ID of the support case.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <returns>The list of communications for the case.</returns>
    public async Task<List<Communication>> DescribeCommunications(string caseId,
 DateTime? afterTime = null, DateTime? beforeTime = null)
```

```
    {
        var results = new List<Communication>();
        var paginateCommunications =
_amazonSupport.Paginators.DescribeCommunications(
            new DescribeCommunicationsRequest()
            {
                CaseId = caseId,
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s")
            });
        // Get the entire list using the paginator.
        await foreach (var communications in
paginateCommunications.Communications)
        {
            results.Add(communications);
        }
        return results;
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for .NET API 參考[DescribeCommunications](#)中的。

CLI

AWS CLI

描述案件的最新通訊

下列`describe-communications`範例會傳回您 AWS 帳戶中指定支援案例的最新通訊。

```
aws support describe-communications \
    --case-id "case-12345678910-2013-c4c1d2bf33c5cf47" \
    --after-time "2020-03-23T21:31:47.774Z" \
    --max-item 1
```

輸出：

```
{
    "communications": [
        {
            "body": "I want to learn more about an AWS service.",
```

```
            "attachmentSet": [],
            "caseId": "case-12345678910-2013-c4c1d2bf33c5cf47",
            "timeCreated": "2020-05-12T23:12:35.000Z",
            "submittedBy": "Amazon Web Services"
        }
    ],
    "NextToken":
 "eyJuZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQEXAMPLE=="
}
```

如需詳細資訊，請參閱 Sup AWS port 使用者指南中的案例管理。

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考DescribeCommunications中的。

Java

適用於 Java 2.x 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
   public static String listCommunications(SupportClient supportClient, String
caseId) {
       try {
           String attachId = null;
           DescribeCommunicationsRequest communicationsRequest =
DescribeCommunicationsRequest.builder()
                   .caseId(caseId)
                   .maxResults(10)
                   .build();

           DescribeCommunicationsResponse response =
supportClient.describeCommunications(communicationsRequest);
           List<Communication> communications = response.communications();
           for (Communication comm : communications) {
               System.out.println("the body is: " + comm.body());

               // Get the attachment id value.
               List<AttachmentDetails> attachments = comm.attachmentSet();
```

```
                for (AttachmentDetails detail : attachments) {
                    attachId = detail.attachmentId();
                }
            }
            return attachId;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考DescribeCommunications中的。

JavaScript

適用於 JavaScript (v3) 的開發套件

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
import { DescribeCommunicationsCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get all communications for the support case.
    // Filter results by providing parameters to the
 DescribeCommunicationsCommand. Refer
    // to the TypeScript definition and the API doc for more information on
 possible parameters.
    // https://docs.aws.amazon.com/AWSJavaScriptSDK/v3/latest/clients/client-
support/interfaces/describecommunicationscommandinput.html
    const response = await client.send(
```

```
      new DescribeCommunicationsCommand({
        // Set value to an existing case id.
        caseId: "CASE_ID",
      }),
    );
    const text = response.communications.map((item) => item.body).join("\n");
    console.log(text);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- 如需 API 詳細資訊，請參閱 AWS SDK for JavaScript API 參考DescribeCommunications中的。

Kotlin

適用於 Kotlin 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
suspend fun listCommunications(caseIdVal: String?): String? {
    val communicationsRequest = DescribeCommunicationsRequest {
        caseId = caseIdVal
        maxResults = 10
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeCommunications(communicationsRequest)
        response.communications?.forEach { comm ->
            println("the body is: " + comm.body)
            comm.attachmentSet?.forEach { detail ->
                return detail.attachmentId
            }
```

```
        }
    }
    return ""
}
```

- 有關 API 的詳細信息，請參閱 AWS SDK DescribeCommunications中的 Kotlin API 參考。

Python

適用於 Python (Boto3) 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_all_case_communications(self, case_id):
        """
        Describe all the communications for a case using a paginator.

        :param case_id: The ID of the case.
        :return: The communications for the case.
```

```
        """
        try:
            communications = []
            paginator =
self.support_client.get_paginator("describe_communications")
            for page in paginator.paginate(caseId=case_id):
                communications += page["communications"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't describe communications. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return communications
```

- 如需 API 的詳細資訊，請參閱AWS 開發套件DescribeCommunications中的 Python (博托 3) API 參考。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭配 AWS SDK 使用 AWS Support。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

使用 AWS SDK 描述支 AWS 援案例的可用服務

下列程式碼範例會示範如何描述 AWS 服務清單。

動作範例是大型程式的程式碼摘錄，必須在內容中執行。您可以在下列程式碼範例的內容中看到此動作：

- 開始使用案例

.NET

AWS SDK for .NET

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
/// <summary>
/// Get the descriptions of AWS services.
/// </summary>
/// <param name="name">Optional language for services.
/// Currently "en" (English) and "ja" (Japanese) are supported.</param>
/// <returns>The list of AWS service descriptions.</returns>
public async Task<List<Service>> DescribeServices(string language = "en")
{
    var response = await _amazonSupport.DescribeServicesAsync(
        new DescribeServicesRequest()
        {
            Language = language
        });
    return response.Services;
}
```

- 如需 API 詳細資訊，請參閱 AWS SDK for .NET API 參考DescribeServices中的。

CLI

AWS CLI

列出 AWS 服務和服務類別

下列`describe-services`範例會列出要求一般資訊的可用服務類別。

```
aws support describe-services \
    --service-code-list "general-info"
```

輸出：

```
{
    "services": [
        {
            "code": "general-info",
            "name": "General Info and Getting Started",
            "categories": [
                {
                    "code": "charges",
                    "name": "How Will I Be Charged?"
                },
                {
                    "code": "gdpr-queries",
                    "name": "Data Privacy Query"
                },
                {
                    "code": "reserved-instances",
                    "name": "Reserved Instances"
                },
                {
                    "code": "resource",
                    "name": "Where is my Resource?"
                },
                {
                    "code": "using-aws",
                    "name": "Using AWS & Services"
                },
                {
                    "code": "free-tier",
                    "name": "Free Tier"
                },
                {
                    "code": "security-and-compliance",
                    "name": "Security & Compliance"
                },
                {
                    "code": "account-structure",
                    "name": "Account Structure"
                }
            ]
        }
    ]
```

```
}
```

如需詳細資訊，請參閱 Sup AWS port 使用者指南中的案例管理。

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考DescribeServices中的。

Java

適用於 Java 2.x 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
   // Return a List that contains a Service name and Category name.
   public static List<String> displayServices(SupportClient supportClient) {
       try {
           DescribeServicesRequest servicesRequest =
DescribeServicesRequest.builder()
                   .language("en")
                   .build();

           DescribeServicesResponse response =
supportClient.describeServices(servicesRequest);
           String serviceCode = null;
           String catName = null;
           List<String> sevCatList = new ArrayList<>();
           List<Service> services = response.services();

           System.out.println("Get the first 10 services");
           int index = 1;
           for (Service service : services) {
               if (index == 11)
                   break;

               System.out.println("The Service name is: " + service.name());
               if (service.name().compareTo("Account") == 0)
                   serviceCode = service.code();

               // Get the Categories for this service.
```

```
                List<Category> categories = service.categories();
                for (Category cat : categories) {
                    System.out.println("The category name is: " + cat.name());
                    if (cat.name().compareTo("Security") == 0)
                        catName = cat.name();
                }
                index++;
            }

            // Push the two values to the list.
            sevCatList.add(serviceCode);
            sevCatList.add(catName);
            return sevCatList;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return null;
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考DescribeServices中的。

Kotlin

適用於 Kotlin 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
// Return a List that contains a Service name and Category name.
suspend fun displayServices(): List<String> {
    var serviceCode = ""
    var catName = ""
    val sevCatList = mutableListOf<String>()
    val servicesRequest = DescribeServicesRequest {
        language = "en"
    }
```

```
    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeServices(servicesRequest)
        println("Get the first 10 services")
        var index = 1

        response.services?.forEach { service ->
            if (index == 11) {
                return@forEach
            }

            println("The Service name is ${service.name}")
            if (service.name == "Account") {
                serviceCode = service.code.toString()
            }

            // Get the categories for this service.
            service.categories?.forEach { cat ->
                println("The category name is ${cat.name}")
                if (cat.name == "Security") {
                    catName = cat.name!!
                }
            }
            index++
        }
    }

    // Push the two values to the list.
    serviceCode.let { sevCatList.add(it) }
    catName.let { sevCatList.add(it) }
    return sevCatList
}
```

- 有關 API 的詳細信息，請參閱 AWS SDK DescribeServices中的 Kotlin API 參考。

Python

適用於 Python (Boto3) 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_services(self, language):
        """
        Get the descriptions of AWS services available for support for a
 language.

        :param language: The language for support services.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of AWS service descriptions.
        """
        try:
            response = self.support_client.describe_services(language=language)
            services = response["services"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
```

```
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get Support services for language %s. Here's why:
%s: %s",
                    language,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return services
```

- 如需 API 的詳細資訊，請參閱AWS 開發套件DescribeServices中的 Python (博托 3) API 參考。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭配 AWS SDK 使用 AWS Support。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

使用 AWS SDK 描述 AWS Support 嚴重性層級

下列程式碼範例說明如何描述 AWS Support 嚴重性層級。

動作範例是大型程式的程式碼摘錄，必須在內容中執行。您可以在下列程式碼範例的內容中看到此動作：

- 開始使用案例

.NET

AWS SDK for .NET

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
    /// <summary>
    /// Get the descriptions of support severity levels.
    /// </summary>
    /// <param name="name">Optional language for severity levels.
    /// Currently "en" (English) and "ja" (Japanese) are supported.</param>
    /// <returns>The list of support severity levels.</returns>
    public async Task<List<SeverityLevel>> DescribeSeverityLevels(string language
= "en")
    {
        var response = await _amazonSupport.DescribeSeverityLevelsAsync(
            new DescribeSeverityLevelsRequest()
            {
                Language = language
            });
        return response.SeverityLevels;
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for .NET API 參考DescribeSeverityLevels中的。

CLI

AWS CLI

列出可用的嚴重性層級

下列`describe-severity-levels`範例列出支援案例的可用嚴重性等級。

```
aws support describe-severity-levels
```

輸出：

```
{
    "severityLevels": [
        {
            "code": "low",
            "name": "Low"
        },
        {
            "code": "normal",
            "name": "Normal"
        },
        {
            "code": "high",
            "name": "High"
        },
        {
            "code": "urgent",
            "name": "Urgent"
        },
        {
            "code": "critical",
            "name": "Critical"
        }
    ]
}
```

如需詳細資訊，請參閱 Sup AWS port 使用指南中的選擇嚴重性。

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考DescribeSeverityLevels中的。

Java

適用於 Java 2.x 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
    public static String displaySevLevels(SupportClient supportClient) {
```

```
        try {
            DescribeSeverityLevelsRequest severityLevelsRequest =
DescribeSeverityLevelsRequest.builder()
                    .language("en")
                    .build();

            DescribeSeverityLevelsResponse response =
supportClient.describeSeverityLevels(severityLevelsRequest);
            List<SeverityLevel> severityLevels = response.severityLevels();
            String levelName = null;
            for (SeverityLevel sevLevel : severityLevels) {
                System.out.println("The severity level name is: " +
sevLevel.name());
                if (sevLevel.name().compareTo("High") == 0)
                    levelName = sevLevel.name();
            }
            return levelName;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考DescribeSeverityLevels中的。

JavaScript

適用於 JavaScript (v3) 的開發套件

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
import { DescribeSeverityLevelsCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";
```

```
export const main = async () => {
  try {
    // Get the list of severity levels.
    // The available values depend on the support plan for the account.
    const response = await client.send(new DescribeSeverityLevelsCommand({}));
    console.log(response.severityLevels);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- 如需 API 詳細資訊，請參閱 AWS SDK for JavaScript API 參考[DescribeSeverityLevels]中的。

Kotlin

適用於 Kotlin 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在[AWS 設定和執行程式碼範例儲存庫]。

```
suspend fun displaySevLevels(): String {
    var levelName = ""
    val severityLevelsRequest = DescribeSeverityLevelsRequest {
        language = "en"
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeSeverityLevels(severityLevelsRequest)
        response.severityLevels?.forEach { sevLevel ->
            println("The severity level name is: ${sevLevel.name}")
            if (sevLevel.name == "High") {
                levelName = sevLevel.name!!
            }
        }
```

```
        return levelName
    }
}
```

- 有關 API 的詳細信息，請參閱 AWS SDK DescribeSeverityLevels中的 Kotlin API 參考。

Python

適用於 Python (Boto3) 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_severity_levels(self, language):
        """
        Get the descriptions of available severity levels for support cases for a
 language.

        :param language: The language for support severity levels.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
```

```
        :return: The list of severity levels.
        """
        try:
            response =
self.support_client.describe_severity_levels(language=language)
            severity_levels = response["severityLevels"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get severity levels for language %s. Here's why:
%s: %s",
                    language,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return severity_levels
```

- 如需 API 的詳細資訊，請參閱AWS 開發套件DescribeSeverityLevels中的 Python (博托 3) API 參考。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭配 AWS SDK 使用 AWS Support。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

使用 AWS SDK 解決 AWS Support 案例

下列程式碼範例會示範如何解決 AWS Support 案例。

動作範例是大型程式的程式碼摘錄，必須在內容中執行。您可以在下列程式碼範例的內容中看到此動作：

- 開始使用案例

.NET

AWS SDK for .NET

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
/// <summary>
/// Resolve a support case by caseId.
/// </summary>
/// <param name="caseId">Id for the support case.</param>
/// <returns>The final status of the case after resolving.</returns>
public async Task<string> ResolveCase(string caseId)
{
    var response = await _amazonSupport.ResolveCaseAsync(
        new ResolveCaseRequest()
        {
            CaseId = caseId
        });
    return response.FinalCaseStatus;
}
```

- 如需 API 詳細資訊，請參閱 AWS SDK for .NET API 參考ResolveCase中的。

CLI

AWS CLI

若要解決支援案例

下列`resolve-case`範例會解決您 AWS 帳戶中的支援案例。

```
aws support resolve-case \
```

```
    --case-id "case-12345678910-2013-c4c1d2bf33c5cf47"
```

輸出：

```
{
    "finalCaseStatus": "resolved",
    "initialCaseStatus": "work-in-progress"
}
```

如需詳細資訊，請參閱 Sup AWS port 使用者指南中的案例管理。

- 如需 API 詳細資訊，請參閱AWS CLI 命令參考ResolveCase中的。

Java

適用於 Java 2.x 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
   public static void resolveSupportCase(SupportClient supportClient, String
caseId) {
       try {
           ResolveCaseRequest caseRequest = ResolveCaseRequest.builder()
                   .caseId(caseId)
                   .build();

           ResolveCaseResponse response =
supportClient.resolveCase(caseRequest);
           System.out.println("The status of case " + caseId + " is " +
response.finalCaseStatus());

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
   }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考ResolveCase中的。

JavaScript

適用於 JavaScript (v3) 的開發套件

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
import { ResolveCaseCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

const main = async () => {
  try {
    const response = await client.send(
      new ResolveCaseCommand({
        caseId: "CASE_ID",
      }),
    );

    console.log(response.finalCaseStatus);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- 如需 API 詳細資訊，請參閱 AWS SDK for JavaScript API 參考ResolveCase中的。

Kotlin

適用於 Kotlin 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
suspend fun resolveSupportCase(caseIdVal: String) {
    val caseRequest = ResolveCaseRequest {
        caseId = caseIdVal
    }
    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.resolveCase(caseRequest)
        println("The status of case $caseIdVal is ${response.finalCaseStatus}")
    }
}
```

- 有關 API 的詳細信息，請參閱 AWS SDK ResolveCase中的 Kotlin API 參考。

Python

適用於 Python (Boto3) 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
```

```
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def resolve_case(self, case_id):
        """
        Resolve a support case by its caseId.

        :param case_id: The ID of the case to resolve.
        :return: The final status of the case.
        """
        try:
            response = self.support_client.resolve_case(caseId=case_id)
            final_status = response["finalCaseStatus"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't resolve case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return final_status
```

- 如需 API 的詳細資訊，請參閱AWS 開發套件ResolveCase中的 Python (博托 3) API 參考。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭配 AWS SDK 使用 AWS Support。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

AWS Support 使用 AWS 軟體開發套件的案例

下列程式碼範例說明如何在 AWS SDK 中 AWS Support 實作常見案例。這些案例會示範如何透過在其中呼叫多個函式來完成特定工作 AWS Support。每個案例都包含一個連結 GitHub，您可以在其中找到如何設定和執行程式碼的指示。

範例

- 使用 AWS SDK 開始使用 AWS Support 案例

使用 AWS SDK 開始使用 AWS Support 案例

下列程式碼範例示範如何：

- 取得並顯示案例可用的服務和嚴重性層級。
- 根據選取的服務、類別和嚴重性層級建立支援案例。
- 取得並顯示當天開啟的案例清單。
- 將附件集和通訊新增至新案例。
- 描述案例的新附件和通訊。
- 解決案例。
- 取得並顯示當天已解決的案例清單。

.NET

AWS SDK for .NET

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

在命令提示中執行互動式案例。

```
/// <summary>
/// Hello AWS Support example.
/// </summary>
public static class SupportCaseScenario
{
    /*
    Before running this .NET code example, set up your development environment,
 including your credentials.
    To use the AWS Support API, you must have one of the following AWS Support
 plans: Business, Enterprise On-Ramp, or Enterprise.

    This .NET example performs the following tasks:
    1.  Get and display services. Select a service from the list.
    2.  Select a category from the selected service.
    3.  Get and display severity levels and select a severity level from the
 list.
    4.  Create a support case using the selected service, category, and severity
 level.
    5.  Get and display a list of open support cases for the current day.
    6.  Create an attachment set with a sample text file to add to the case.
    7.  Add a communication with the attachment to the support case.
    8.  List the communications of the support case.
    9.  Describe the attachment set.
    10. Resolve the support case.
    11. Get a list of resolved cases for the current day.
   */

    private static SupportWrapper _supportWrapper = null!;

    static async Task Main(string[] args)
    {
        // Set up dependency injection for the AWS Support service.
        // Use your AWS profile name, or leave it blank to use the default
 profile.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureLogging(logging =>
                logging.AddFilter("System", LogLevel.Debug)
                    .AddFilter<DebugLoggerProvider>("Microsoft",
 LogLevel.Information)
                    .AddFilter<ConsoleLoggerProvider>("Microsoft",
 LogLevel.Trace))
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonAWSSupport>(new AWSOptions()
 { Profile = "default" })
```

```
                    .AddTransient<SupportWrapper>()
            )
            .Build();

        var logger = LoggerFactory.Create(builder =>
        {
            builder.AddConsole();
        }).CreateLogger(typeof(SupportCaseScenario));

        _supportWrapper = host.Services.GetRequiredService<SupportWrapper>();

        Console.WriteLine(new string('-', 80));
        Console.WriteLine("Welcome to the AWS Support case example scenario.");
        Console.WriteLine(new string('-', 80));

        try
        {
            var apiSupported = await _supportWrapper.VerifySubscription();
            if (!apiSupported)
            {
                logger.LogError("You must have a Business, Enterprise On-Ramp, or
Enterprise Support " +
                                "plan to use the AWS Support API. \n\tPlease
upgrade your subscription to run these examples.");
                return;
            }

            var service = await DisplayAndSelectServices();

            var category = DisplayAndSelectCategories(service);

            var severityLevel = await DisplayAndSelectSeverity();

            var caseId = await CreateSupportCase(service, category,
severityLevel);

            await DescribeTodayOpenCases();

            var attachmentSetId = await CreateAttachmentSet();

            await AddCommunicationToCase(attachmentSetId, caseId);

            var attachmentId = await ListCommunicationsForCase(caseId);
```

```
            await DescribeCaseAttachment(attachmentId);

            await ResolveCase(caseId);

            await DescribeTodayResolvedCases();

            Console.WriteLine(new string('-', 80));
            Console.WriteLine("AWS Support case example scenario complete.");
            Console.WriteLine(new string('-', 80));
        }
        catch (Exception ex)
        {
            logger.LogError(ex, "There was a problem executing the scenario.");
        }
    }

    /// <summary>
    /// List some available services from AWS Support, and select a service for
the example.
    /// </summary>
    /// <returns>The selected service.</returns>
    private static async Task<Service> DisplayAndSelectServices()
    {
        Console.WriteLine(new string('-', 80));
        var services = await _supportWrapper.DescribeServices();
        Console.WriteLine($"AWS Support client returned {services.Count}
services.");

        Console.WriteLine($"1. Displaying first 10 services:");
        for (int i = 0; i < 10 && i < services.Count; i++)
        {
            Console.WriteLine($"\t{i + 1}. {services[i].Name}");
        }

        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > services.Count)
        {
            Console.WriteLine(
                "Select an example support service by entering a number from the
preceding list:");
            var choice = Console.ReadLine();
            Int32.TryParse(choice, out choiceNumber);
        }
        Console.WriteLine(new string('-', 80));
```

```
        return services[choiceNumber - 1];
    }

    /// <summary>
    /// List the available categories for a service and select a category for the
example.
    /// </summary>
    /// <param name="service">Service to use for displaying categories.</param>
    /// <returns>The selected category.</returns>
    private static Category DisplayAndSelectCategories(Service service)
    {
        Console.WriteLine(new string('-', 80));

        Console.WriteLine($"2. Available support categories for Service
\"{service.Name}\":");
        for (int i = 0; i < service.Categories.Count; i++)
        {
            Console.WriteLine($"\t{i + 1}. {service.Categories[i].Name}");
        }

        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > service.Categories.Count)
        {
            Console.WriteLine(
                "Select an example support category by entering a number from the
preceding list:");
            var choice = Console.ReadLine();
            Int32.TryParse(choice, out choiceNumber);
        }

        Console.WriteLine(new string('-', 80));

        return service.Categories[choiceNumber - 1];
    }

    /// <summary>
    /// List available severity levels from AWS Support, and select a level for
the example.
    /// </summary>
    /// <returns>The selected severity level.</returns>
    private static async Task<SeverityLevel> DisplayAndSelectSeverity()
    {
        Console.WriteLine(new string('-', 80));
```

```
        var severityLevels = await _supportWrapper.DescribeSeverityLevels();

        Console.WriteLine($"3. Get and display available severity levels:");
        for (int i = 0; i < 10 && i < severityLevels.Count; i++)
        {
            Console.WriteLine($"\t{i + 1}. {severityLevels[i].Name}");
        }

        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > severityLevels.Count)
        {
            Console.WriteLine(
                "Select an example severity level by entering a number from the
preceding list:");
            var choice = Console.ReadLine();
            Int32.TryParse(choice, out choiceNumber);
        }
        Console.WriteLine(new string('-', 80));

        return severityLevels[choiceNumber - 1];
    }

    /// <summary>
    /// Create an example support case.
    /// </summary>
    /// <param name="service">Service to use for the new case.</param>
    /// <param name="category">Category to use for the new case.</param>
    /// <param name="severity">Severity to use for the new case.</param>
    /// <returns>The caseId of the new support case.</returns>
    private static async Task<string> CreateSupportCase(Service service,
        Category category, SeverityLevel severity)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"4. Create an example support case" +
                          $" with the following settings:" +
                          $" \n\tService: {service.Name}, Category:
{category.Name} " +
                          $"and Severity Level: {severity.Name}.");
        var caseId = await _supportWrapper.CreateCase(service.Code,
category.Code, severity.Code,
            "Example case for testing, ignore.", "This is my example support
case.");

        Console.WriteLine($"\tNew case created with ID {caseId}");
```

```
        Console.WriteLine(new string('-', 80));

        return caseId;
    }

    /// <summary>
    /// List open cases for the current day.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task DescribeTodayOpenCases()
    {
        Console.WriteLine($"5. List the open support cases for the current
day.");
        // Describe the cases. If it is empty, try again and allow time for the
new case to appear.
        List<CaseDetails> currentOpenCases = null!;
        while (currentOpenCases == null || currentOpenCases.Count == 0)
        {
            Thread.Sleep(1000);
            currentOpenCases = await _supportWrapper.DescribeCases(
                new List<string>(),
                null,
                false,
                false,
                DateTime.UtcNow.Date,
                DateTime.UtcNow);
        }

        foreach (var openCase in currentOpenCases)
        {
            Console.WriteLine($"\tCase: {openCase.CaseId} created
{openCase.TimeCreated}");
        }

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Create an attachment set for a support case.
    /// </summary>
    /// <returns>The attachment set id.</returns>
    private static async Task<string> CreateAttachmentSet()
    {
```

```
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"6. Create an attachment set for a support case.");
        var fileName = "example_attachment.txt";

        // Create the file if it does not already exist.
        if (!File.Exists(fileName))
        {
            await using StreamWriter sw = File.CreateText(fileName);
            await sw.WriteLineAsync(
                "This is a sample file for attachment to a support case.");
        }

        await using var ms = new MemoryStream(await
 File.ReadAllBytesAsync(fileName));

        var attachmentSetId = await _supportWrapper.AddAttachmentToSet(
            ms,
            fileName);

        Console.WriteLine($"\tNew attachment set created with id: \n
\t{attachmentSetId.Substring(0, 65)}...");

        Console.WriteLine(new string('-', 80));

        return attachmentSetId;
    }

    /// <summary>
    /// Add an attachment set and communication to a case.
    /// </summary>
    /// <param name="attachmentSetId">Id of the attachment set.</param>
    /// <param name="caseId">Id of the case to receive the attachment set.</
param>
    /// <returns>Async task.</returns>
    private static async Task AddCommunicationToCase(string attachmentSetId,
 string caseId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"7. Add attachment set and communication to
 {caseId}.");

        await _supportWrapper.AddCommunicationToCase(
            caseId,
            "This is an example communication added to a support case.",
```

```
            attachmentSetId);

        Console.WriteLine($"\tNew attachment set and communication added to
{caseId}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List the communications for a case.
    /// </summary>
    /// <param name="caseId">Id of the case to describe.</param>
    /// <returns>An attachment id.</returns>
    private static async Task<string> ListCommunicationsForCase(string caseId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"8. List communications for case {caseId}.");

        var communications = await
_supportWrapper.DescribeCommunications(caseId);
        var attachmentId = "";
        foreach (var communication in communications)
        {
            Console.WriteLine(
                $"\tCommunication created on: {communication.TimeCreated} has
{communication.AttachmentSet.Count} attachments.");
            if (communication.AttachmentSet.Any())
            {
                attachmentId = communication.AttachmentSet.First().AttachmentId;
            }
        }

        Console.WriteLine(new string('-', 80));
        return attachmentId;
    }

    /// <summary>
    /// Describe an attachment by id.
    /// </summary>
    /// <param name="attachmentId">Id of the attachment to describe.</param>
    /// <returns>Async task.</returns>
    private static async Task DescribeCaseAttachment(string attachmentId)
    {
        Console.WriteLine(new string('-', 80));
```

```
        Console.WriteLine($"9. Describe the attachment set.");

        var attachment = await _supportWrapper.DescribeAttachment(attachmentId);
        var data = Encoding.ASCII.GetString(attachment.Data.ToArray());
        Console.WriteLine($"\tAttachment includes {attachment.FileName} with
data: \n\t{data}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Resolve the support case.
    /// </summary>
    /// <param name="caseId">Id of the case to resolve.</param>
    /// <returns>Async task.</returns>
    private static async Task ResolveCase(string caseId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"10. Resolve case {caseId}.");

        var status = await _supportWrapper.ResolveCase(caseId);
        Console.WriteLine($"\tCase {caseId} has final status {status}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List resolved cases for the current day.
    /// </summary>
    /// <returns>Async Task.</returns>
    private static async Task DescribeTodayResolvedCases()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"11. List the resolved support cases for the current
day.");
        var currentCases = await _supportWrapper.DescribeCases(
            new List<string>(),
            null,
            false,
            true,
            DateTime.UtcNow.Date,
            DateTime.UtcNow);

        foreach (var currentCase in currentCases)
```

```
        {
            if (currentCase.Status == "resolved")
            {
                Console.WriteLine(
                    $"\tCase: {currentCase.CaseId}: status
 {currentCase.Status}");
            }
        }

        Console.WriteLine(new string('-', 80));
    }
}
```

案例用於 AWS Support 動作的包裝函式方法。

```
/// <summary>
/// Wrapper methods to use AWS Support for working with support cases.
/// </summary>
public class SupportWrapper
{
    private readonly IAmazonAWSSupport _amazonSupport;
    public SupportWrapper(IAmazonAWSSupport amazonSupport)
    {
        _amazonSupport = amazonSupport;
    }


    /// <summary>
    /// Get the descriptions of AWS services.
    /// </summary>
    /// <param name="name">Optional language for services.
    /// Currently "en" (English) and "ja" (Japanese) are supported.</param>
    /// <returns>The list of AWS service descriptions.</returns>
    public async Task<List<Service>> DescribeServices(string language = "en")
    {
        var response = await _amazonSupport.DescribeServicesAsync(
            new DescribeServicesRequest()
            {
                Language = language
            });
        return response.Services;
```

```
    }



    /// <summary>
    /// Get the descriptions of support severity levels.
    /// </summary>
    /// <param name="name">Optional language for severity levels.
    /// Currently "en" (English) and "ja" (Japanese) are supported.</param>
    /// <returns>The list of support severity levels.</returns>
    public async Task<List<SeverityLevel>> DescribeSeverityLevels(string language
= "en")
    {
        var response = await _amazonSupport.DescribeSeverityLevelsAsync(
            new DescribeSeverityLevelsRequest()
            {
                Language = language
            });
        return response.SeverityLevels;
    }



    /// <summary>
    /// Create a new support case.
    /// </summary>
    /// <param name="serviceCode">Service code for the new case.</param>
    /// <param name="categoryCode">Category for the new case.</param>
    /// <param name="severityCode">Severity code for the new case.</param>
    /// <param name="subject">Subject of the new case.</param>
    /// <param name="body">Body text of the new case.</param>
    /// <param name="language">Optional language support for your case.
    /// Currently "en" (English) and "ja" (Japanese) are supported.</param>
    /// <param name="attachmentSetId">Optional Id for an attachment set for the
new case.</param>
    /// <param name="issueType">Optional issue type for the new case. Options are
"customer-service" or "technical".</param>
    /// <returns>The caseId of the new support case.</returns>
    public async Task<string> CreateCase(string serviceCode, string categoryCode,
string severityCode, string subject,
        string body, string language = "en", string? attachmentSetId = null,
string issueType = "customer-service")
    {
        var response = await _amazonSupport.CreateCaseAsync(
```

```
            new CreateCaseRequest()
            {
                ServiceCode = serviceCode,
                CategoryCode = categoryCode,
                SeverityCode = severityCode,
                Subject = subject,
                Language = language,
                AttachmentSetId = attachmentSetId,
                IssueType = issueType,
                CommunicationBody = body
            });
        return response.CaseId;
    }



    /// <summary>
    /// Add an attachment to a set, or create a new attachment set if one does
not exist.
    /// </summary>
    /// <param name="data">The data for the attachment.</param>
    /// <param name="fileName">The file name for the attachment.</param>
    /// <param name="attachmentSetId">Optional setId for the attachment. Creates
a new attachment set if empty.</param>
    /// <returns>The setId of the attachment.</returns>
    public async Task<string> AddAttachmentToSet(MemoryStream data, string
fileName, string? attachmentSetId = null)
    {
        var response = await _amazonSupport.AddAttachmentsToSetAsync(
            new AddAttachmentsToSetRequest
            {
                AttachmentSetId = attachmentSetId,
                Attachments = new List<Attachment>
                {
                    new Attachment
                    {
                        Data = data,
                        FileName = fileName
                    }
                }
            });
        return response.AttachmentSetId;
    }
```

```
    /// <summary>
    /// Get description of a specific attachment.
    /// </summary>
    /// <param name="attachmentId">Id of the attachment, usually fetched by
 describing the communications of a case.</param>
    /// <returns>The attachment object.</returns>
    public async Task<Attachment> DescribeAttachment(string attachmentId)
    {
        var response = await _amazonSupport.DescribeAttachmentAsync(
            new DescribeAttachmentRequest()
            {
                AttachmentId = attachmentId
            });
        return response.Attachment;
    }



    /// <summary>
    /// Add communication to a case, including optional attachment set ID and CC
 email addresses.
    /// </summary>
    /// <param name="caseId">Id for the support case.</param>
    /// <param name="body">Body text of the communication.</param>
    /// <param name="attachmentSetId">Optional Id for an attachment set.</param>
    /// <param name="ccEmailAddresses">Optional list of CC email addresses.</
param>
    /// <returns>True if successful.</returns>
    public async Task<bool> AddCommunicationToCase(string caseId, string body,
        string? attachmentSetId = null, List<string>? ccEmailAddresses = null)
    {
        var response = await _amazonSupport.AddCommunicationToCaseAsync(
            new AddCommunicationToCaseRequest()
            {
                CaseId = caseId,
                CommunicationBody = body,
                AttachmentSetId = attachmentSetId,
                CcEmailAddresses = ccEmailAddresses
            });
        return response.Result;
    }
```

```
    /// <summary>
    /// Describe the communications for a case, optionally with a date filter.
    /// </summary>
    /// <param name="caseId">The ID of the support case.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <returns>The list of communications for the case.</returns>
    public async Task<List<Communication>> DescribeCommunications(string caseId,
 DateTime? afterTime = null, DateTime? beforeTime = null)
    {
        var results = new List<Communication>();
        var paginateCommunications =
 _amazonSupport.Paginators.DescribeCommunications(
            new DescribeCommunicationsRequest()
            {
                CaseId = caseId,
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s")
            });
        // Get the entire list using the paginator.
        await foreach (var communications in
 paginateCommunications.Communications)
        {
            results.Add(communications);
        }
        return results;
    }



    /// <summary>
    /// Get case details for a list of case ids, optionally with date filters.
    /// </summary>
    /// <param name="caseIds">The list of case IDs.</param>
    /// <param name="displayId">Optional display ID.</param>
    /// <param name="includeCommunication">True to include communication.
 Defaults to true.</param>
    /// <param name="includeResolvedCases">True to include resolved cases.
 Defaults to false.</param>
```

```
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <param name="language">Optional language support for your case.
    /// Currently "en" (English) and "ja" (Japanese) are supported.</param>
    /// <returns>A list of CaseDetails.</returns>
    public async Task<List<CaseDetails>> DescribeCases(List<string> caseIds,
 string? displayId = null, bool includeCommunication = true,
        bool includeResolvedCases = false, DateTime? afterTime = null, DateTime?
 beforeTime = null,
        string language = "en")
    {
        var results = new List<CaseDetails>();
        var paginateCases = _amazonSupport.Paginators.DescribeCases(
            new DescribeCasesRequest()
            {
                CaseIdList = caseIds,
                DisplayId = displayId,
                IncludeCommunications = includeCommunication,
                IncludeResolvedCases = includeResolvedCases,
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s"),
                Language = language
            });
        // Get the entire list using the paginator.
        await foreach (var cases in paginateCases.Cases)
        {
            results.Add(cases);
        }
        return results;
    }



    /// <summary>
    /// Resolve a support case by caseId.
    /// </summary>
    /// <param name="caseId">Id for the support case.</param>
    /// <returns>The final status of the case after resolving.</returns>
    public async Task<string> ResolveCase(string caseId)
    {
        var response = await _amazonSupport.ResolveCaseAsync(
            new ResolveCaseRequest()
```

```
            {
                CaseId = caseId
            });
        return response.FinalCaseStatus;
    }


    /// <summary>
    /// Verify the support level for AWS Support API access.
    /// </summary>
    /// <returns>True if the subscription level supports API access.</returns>
    public async Task<bool> VerifySubscription()
    {
        try
        {
            var response = await _amazonSupport.DescribeServicesAsync(
                new DescribeServicesRequest()
                {
                    Language = "en"
                });
            return response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (Amazon.AWSSupport.AmazonAWSSupportException ex)
        {
            if (ex.ErrorCode == "SubscriptionRequiredException")
            {
                return false;
            }
            else throw;
        }
    }
}
```

- 如需 API 詳細資訊，請參閱《AWS SDK for .NET API 參考》中的下列主題。
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications

- DescribeServices
- DescribeSeverityLevels
- ResolveCase

Java

適用於 Java 2.x 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

運行各種 AWS Support 操作。

```
import software.amazon.awssdk.core.SdkBytes;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.support.SupportClient;
import software.amazon.awssdk.services.support.model.AddAttachmentsToSetResponse;
import
 software.amazon.awssdk.services.support.model.AddCommunicationToCaseRequest;
import
 software.amazon.awssdk.services.support.model.AddCommunicationToCaseResponse;
import software.amazon.awssdk.services.support.model.Attachment;
import software.amazon.awssdk.services.support.model.AttachmentDetails;
import software.amazon.awssdk.services.support.model.CaseDetails;
import software.amazon.awssdk.services.support.model.Category;
import software.amazon.awssdk.services.support.model.Communication;
import software.amazon.awssdk.services.support.model.CreateCaseRequest;
import software.amazon.awssdk.services.support.model.CreateCaseResponse;
import software.amazon.awssdk.services.support.model.DescribeAttachmentRequest;
import software.amazon.awssdk.services.support.model.DescribeAttachmentResponse;
import software.amazon.awssdk.services.support.model.DescribeCasesRequest;
import software.amazon.awssdk.services.support.model.DescribeCasesResponse;
import
 software.amazon.awssdk.services.support.model.DescribeCommunicationsRequest;
import
 software.amazon.awssdk.services.support.model.DescribeCommunicationsResponse;
import software.amazon.awssdk.services.support.model.DescribeServicesRequest;
import software.amazon.awssdk.services.support.model.DescribeServicesResponse;
```

```
import
 software.amazon.awssdk.services.support.model.DescribeSeverityLevelsRequest;
import
 software.amazon.awssdk.services.support.model.DescribeSeverityLevelsResponse;
import software.amazon.awssdk.services.support.model.ResolveCaseRequest;
import software.amazon.awssdk.services.support.model.ResolveCaseResponse;
import software.amazon.awssdk.services.support.model.Service;
import software.amazon.awssdk.services.support.model.SeverityLevel;
import software.amazon.awssdk.services.support.model.SupportException;
import software.amazon.awssdk.services.support.model.AddAttachmentsToSetRequest;
import java.io.File;
import java.io.FileInputStream;
import java.io.FileNotFoundException;
import java.io.InputStream;
import java.time.Instant;
import java.time.temporal.ChronoUnit;
import java.util.ArrayList;
import java.util.List;

/**
 * Before running this Java (v2) code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * In addition, you must have the AWS Business Support Plan to use the AWS
 * Support Java API. For more information, see:
 *
 * https://aws.amazon.com/premiumsupport/plans/
 *
 * This Java example performs the following tasks:
 *
 * 1. Gets and displays available services.
 * 2. Gets and displays severity levels.
 * 3. Creates a support case by using the selected service, category, and
 * severity level.
 * 4. Gets a list of open cases for the current day.
 * 5. Creates an attachment set with a generated file.
 * 6. Adds a communication with the attachment to the support case.
 * 7. Lists the communications of the support case.
 * 8. Describes the attachment set included with the communication.
```

```
 * 9. Resolves the support case.
 * 10. Gets a list of resolved cases for the current day.
 */
public class SupportScenario {

   public static final String DASHES = new String(new char[80]).replace("\0",
 "-");

   public static void main(String[] args) {
       final String usage = """

               Usage:
                   <fileAttachment>Where:
                   fileAttachment - The file can be a simple saved .txt file to
 use as an email attachment.\s
               """;

       if (args.length != 1) {
           System.out.println(usage);
           System.exit(1);
       }

       String fileAttachment = args[0];
       Region region = Region.US_WEST_2;
       SupportClient supportClient = SupportClient.builder()
               .region(region)
               .build();

       System.out.println(DASHES);
       System.out.println("***** Welcome to the AWS Support case example
 scenario.");
       System.out.println(DASHES);

       System.out.println(DASHES);
       System.out.println("1. Get and display available services.");
       List<String> sevCatList = displayServices(supportClient);
       System.out.println(DASHES);

       System.out.println(DASHES);
       System.out.println("2. Get and display Support severity levels.");
       String sevLevel = displaySevLevels(supportClient);
       System.out.println(DASHES);

       System.out.println(DASHES);
```

```
        System.out.println("3. Create a support case using the selected service,
category, and severity level.");
        String caseId = createSupportCase(supportClient, sevCatList, sevLevel);
        if (caseId.compareTo("") == 0) {
            System.out.println("A support case was not successfully created!");
            System.exit(1);
        } else
            System.out.println("Support case " + caseId + " was successfully
created!");
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("4. Get open support cases.");
        getOpenCase(supportClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("5. Create an attachment set with a generated file to
add to the case.");
        String attachmentSetId = addAttachment(supportClient, fileAttachment);
        System.out.println("The Attachment Set id value is" + attachmentSetId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("6. Add communication with the attachment to the
support case.");
        addAttachSupportCase(supportClient, caseId, attachmentSetId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("7. List the communications of the support case.");
        String attachId = listCommunications(supportClient, caseId);
        System.out.println("The Attachment id value is" + attachId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("8. Describe the attachment set included with the
communication.");
        describeAttachment(supportClient, attachId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("9. Resolve the support case.");
        resolveSupportCase(supportClient, caseId);
```

```
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("10. Get a list of resolved cases for the current
day.");
        getResolvedCase(supportClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("***** This Scenario has successfully completed");
        System.out.println(DASHES);
    }

    public static void getResolvedCase(SupportClient supportClient) {
        try {
            // Specify the start and end time.
            Instant now = Instant.now();
            java.time.LocalDate.now();
            Instant yesterday = now.minus(1, ChronoUnit.DAYS);

            DescribeCasesRequest describeCasesRequest =
DescribeCasesRequest.builder()
                    .maxResults(30)
                    .afterTime(yesterday.toString())
                    .beforeTime(now.toString())
                    .includeResolvedCases(true)
                    .build();

            DescribeCasesResponse response =
supportClient.describeCases(describeCasesRequest);
            List<CaseDetails> cases = response.cases();
            for (CaseDetails sinCase : cases) {
                if (sinCase.status().compareTo("resolved") == 0)
                    System.out.println("The case status is " + sinCase.status());
            }

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static void resolveSupportCase(SupportClient supportClient, String
caseId) {
```

```
        try {
            ResolveCaseRequest caseRequest = ResolveCaseRequest.builder()
                    .caseId(caseId)
                    .build();

            ResolveCaseResponse response =
supportClient.resolveCase(caseRequest);
            System.out.println("The status of case " + caseId + " is " +
response.finalCaseStatus());

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static void describeAttachment(SupportClient supportClient, String
attachId) {
        try {
            DescribeAttachmentRequest attachmentRequest =
DescribeAttachmentRequest.builder()
                    .attachmentId(attachId)
                    .build();

            DescribeAttachmentResponse response =
supportClient.describeAttachment(attachmentRequest);
            System.out.println("The name of the file is " +
response.attachment().fileName());

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static String listCommunications(SupportClient supportClient, String
caseId) {
        try {
            String attachId = null;
            DescribeCommunicationsRequest communicationsRequest =
DescribeCommunicationsRequest.builder()
                    .caseId(caseId)
                    .maxResults(10)
                    .build();
```

```
            DescribeCommunicationsResponse response =
supportClient.describeCommunications(communicationsRequest);
            List<Communication> communications = response.communications();
            for (Communication comm : communications) {
                System.out.println("the body is: " + comm.body());

                // Get the attachment id value.
                List<AttachmentDetails> attachments = comm.attachmentSet();
                for (AttachmentDetails detail : attachments) {
                    attachId = detail.attachmentId();
                }
            }
            return attachId;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    public static void addAttachSupportCase(SupportClient supportClient, String
caseId, String attachmentSetId) {
        try {
            AddCommunicationToCaseRequest caseRequest =
AddCommunicationToCaseRequest.builder()
                    .caseId(caseId)
                    .attachmentSetId(attachmentSetId)
                    .communicationBody("Please refer to attachment for details.")
                    .build();

            AddCommunicationToCaseResponse response =
supportClient.addCommunicationToCase(caseRequest);
            if (response.result())
                System.out.println("You have successfully added a communication
to an AWS Support case");
            else
                System.out.println("There was an error adding the communication
to an AWS Support case");

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
```

```
        }
    }

    public static String addAttachment(SupportClient supportClient, String
fileAttachment) {
        try {
            File myFile = new File(fileAttachment);
            InputStream sourceStream = new FileInputStream(myFile);
            SdkBytes sourceBytes = SdkBytes.fromInputStream(sourceStream);

            Attachment attachment = Attachment.builder()
                    .fileName(myFile.getName())
                    .data(sourceBytes)
                    .build();

            AddAttachmentsToSetRequest setRequest =
AddAttachmentsToSetRequest.builder()
                    .attachments(attachment)
                    .build();

            AddAttachmentsToSetResponse response =
supportClient.addAttachmentsToSet(setRequest);
            return response.attachmentSetId();

        } catch (SupportException | FileNotFoundException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    public static void getOpenCase(SupportClient supportClient) {
        try {
            // Specify the start and end time.
            Instant now = Instant.now();
            java.time.LocalDate.now();
            Instant yesterday = now.minus(1, ChronoUnit.DAYS);

            DescribeCasesRequest describeCasesRequest =
DescribeCasesRequest.builder()
                    .maxResults(20)
                    .afterTime(yesterday.toString())
                    .beforeTime(now.toString())
                    .build();
```

```
            DescribeCasesResponse response =
supportClient.describeCases(describeCasesRequest);
            List<CaseDetails> cases = response.cases();
            for (CaseDetails sinCase : cases) {
                System.out.println("The case status is " + sinCase.status());
                System.out.println("The case Id is " + sinCase.caseId());
                System.out.println("The case subject is " + sinCase.subject());
            }

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static String createSupportCase(SupportClient supportClient,
List<String> sevCatList, String sevLevel) {
        try {
            String serviceCode = sevCatList.get(0);
            String caseCat = sevCatList.get(1);
            CreateCaseRequest caseRequest = CreateCaseRequest.builder()
                    .categoryCode(caseCat.toLowerCase())
                    .serviceCode(serviceCode.toLowerCase())
                    .severityCode(sevLevel.toLowerCase())
                    .communicationBody("Test issue with " +
serviceCode.toLowerCase())
                    .subject("Test case, please ignore")
                    .language("en")
                    .issueType("technical")
                    .build();

            CreateCaseResponse response = supportClient.createCase(caseRequest);
            return response.caseId();

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    public static String displaySevLevels(SupportClient supportClient) {
        try {
```

```
            DescribeSeverityLevelsRequest severityLevelsRequest =
DescribeSeverityLevelsRequest.builder()
                    .language("en")
                    .build();

            DescribeSeverityLevelsResponse response =
supportClient.describeSeverityLevels(severityLevelsRequest);
            List<SeverityLevel> severityLevels = response.severityLevels();
            String levelName = null;
            for (SeverityLevel sevLevel : severityLevels) {
                System.out.println("The severity level name is: " +
sevLevel.name());
                if (sevLevel.name().compareTo("High") == 0)
                    levelName = sevLevel.name();
            }
            return levelName;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    // Return a List that contains a Service name and Category name.
    public static List<String> displayServices(SupportClient supportClient) {
        try {
            DescribeServicesRequest servicesRequest =
DescribeServicesRequest.builder()
                    .language("en")
                    .build();

            DescribeServicesResponse response =
supportClient.describeServices(servicesRequest);
            String serviceCode = null;
            String catName = null;
            List<String> sevCatList = new ArrayList<>();
            List<Service> services = response.services();

            System.out.println("Get the first 10 services");
            int index = 1;
            for (Service service : services) {
                if (index == 11)
                    break;
```

```
                System.out.println("The Service name is: " + service.name());
                if (service.name().compareTo("Account") == 0)
                    serviceCode = service.code();

                // Get the Categories for this service.
                List<Category> categories = service.categories();
                for (Category cat : categories) {
                    System.out.println("The category name is: " + cat.name());
                    if (cat.name().compareTo("Security") == 0)
                        catName = cat.name();
                }
                index++;
            }

            // Push the two values to the list.
            sevCatList.add(serviceCode);
            sevCatList.add(catName);
            return sevCatList;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return null;
    }
}
```

- 如需 API 詳細資訊，請參閱《AWS SDK for Java 2.x API 參考》中的下列主題。
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityLevels
  - ResolveCase

JavaScript

適用於 JavaScript (v3) 的開發套件

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

在終端中執行互動式案例。

```
import {
  AddAttachmentsToSetCommand,
  AddCommunicationToCaseCommand,
  CreateCaseCommand,
  DescribeAttachmentCommand,
  DescribeCasesCommand,
  DescribeCommunicationsCommand,
  DescribeServicesCommand,
  DescribeSeverityLevelsCommand,
  ResolveCaseCommand,
  SupportClient,
} from "@aws-sdk/client-support";
import inquirer from "inquirer";

// Retry an asynchronous function on failure.
const retry = async ({ intervalInMs = 500, maxRetries = 10 }, fn) => {
  try {
    return await fn();
  } catch (err) {
    console.log(`Function call failed. Retrying.`);
    console.error(err.message);
    if (maxRetries === 0) throw err;
    await new Promise((resolve) => setTimeout(resolve, intervalInMs));
    return retry({ intervalInMs, maxRetries: maxRetries - 1 }, fn);
  }
};

const wrapText = (text, char = "=") => {
  const rule = char.repeat(80);
  return `${rule}\n    ${text}\n${rule}\n`;
};
```

```
const client = new SupportClient({ region: "us-east-1" });

// Verify that the account has a Support plan.
export const verifyAccount = async () => {
  const command = new DescribeServicesCommand({});

  try {
    await client.send(command);
  } catch (err) {
    if (err.name === "SubscriptionRequiredException") {
      throw new Error(
        "You must be subscribed to the AWS Support plan to use this feature."
      );
    } else {
      throw err;
    }
  }
};

// Get the list of available services.
export const getService = async () => {
  const { services } = await client.send(new DescribeServicesCommand({}));
  const { selectedService } = await inquirer.prompt({
    name: "selectedService",
    type: "list",
    message:
      "Select a service. Your support case will be created for this service. The
 list of services is truncated for readability.",
    choices: services.slice(0, 10).map((s) => ({ name: s.name, value: s })),
  });
  return selectedService;
};

// Get the list of available support case categories for a service.
export const getCategory = async (service) => {
  const { selectedCategory } = await inquirer.prompt({
    name: "selectedCategory",
    type: "list",
    message: "Select a category.",
    choices: service.categories.map((c) => ({ name: c.name, value: c })),
  });
  return selectedCategory;
};
```

```
// Get the available severity levels for the account.
export const getSeverityLevel = async () => {
  const command = new DescribeSeverityLevelsCommand({});
  const { severityLevels } = await client.send(command);
  const { selectedSeverityLevel } = await inquirer.prompt({
    name: "selectedSeverityLevel",
    type: "list",
    message: "Select a severity level.",
    choices: severityLevels.map((s) => ({ name: s.name, value: s })),
  });
  return selectedSeverityLevel;
};

// Create a new support case and return the caseId.
export const createCase = async ({
  selectedService,
  selectedCategory,
  selectedSeverityLevel,
}) => {
  const command = new CreateCaseCommand({
    subject: "IGNORE: Test case",
    communicationBody: "This is a test. Please ignore.",
    serviceCode: selectedService.code,
    categoryCode: selectedCategory.code,
    severityCode: selectedSeverityLevel.code,
  });
  const { caseId } = await client.send(command);
  return caseId;
};

// Get a list of open support cases created today.
export const getTodaysOpenCases = async () => {
  const d = new Date();
  const startOfToday = new Date(d.getFullYear(), d.getMonth(), d.getDate());
  const command = new DescribeCasesCommand({
    includeCommunications: false,
    afterTime: startOfToday.toISOString(),
  });

  const { cases } = await client.send(command);

  if (cases.length === 0) {
    throw new Error(
```

```
      "Unexpected number of cases. Expected more than 0 open cases."
    );
  }
  return cases;
};

// Create an attachment set.
export const createAttachmentSet = async () => {
  const command = new AddAttachmentsToSetCommand({
    attachments: [
      {
        fileName: "example.txt",
        data: new TextEncoder().encode("some example text"),
      },
    ],
  });
  const { attachmentSetId } = await client.send(command);
  return attachmentSetId;
};

export const linkAttachmentSetToCase = async (attachmentSetId, caseId) => {
  const command = new AddCommunicationToCaseCommand({
    attachmentSetId,
    caseId,
    communicationBody: "Adding attachment set to case.",
  });
  await client.send(command);
};

// Get all communications for a support case.
export const getCommunications = async (caseId) => {
  const command = new DescribeCommunicationsCommand({
    caseId,
  });
  const { communications } = await client.send(command);
  return communications;
};

// Get an attachment set.
export const getFirstAttachment = (communications) => {
  const firstCommWithAttachment = communications.find(
    (c) => c.attachmentSet.length > 0
  );
  return firstCommWithAttachment?.attachmentSet[0].attachmentId;
```

```
};

// Get an attachment.
export const getAttachment = async (attachmentId) => {
  const command = new DescribeAttachmentCommand({
    attachmentId,
  });
  const { attachment } = await client.send(command);
  return attachment;
};

// Resolve the case matching the given case ID.
export const resolveCase = async (caseId) => {
  const { shouldResolve } = await inquirer.prompt({
    name: "shouldResolve",
    type: "confirm",
    message: `Do you want to resolve ${caseId}?`,
  });

  if (shouldResolve) {
    const command = new ResolveCaseCommand({
      caseId: caseId,
    });

    await client.send(command);
    return true;
  }
  return false;
};

// Find a specific case in the list of provided cases by case ID.
// If the case is not found, and the results are paginated, continue
// paging through the results.
export const findCase = async ({ caseId, cases, nextToken }) => {
  const foundCase = cases.find((c) => c.caseId === caseId);

  if (foundCase) {
    return foundCase;
  }

  if (nextToken) {
    const response = await client.send(
      new DescribeCasesCommand({
        nextToken,
```

```
        includeResolvedCases: true,
      })
    );
    return findCase({
      caseId,
      cases: response.cases,
      nextToken: response.nextToken,
    });
  }

  throw new Error(`${caseId} not found.`);
};

// Get all cases created today.
export const getTodaysResolvedCases = async (caseIdToWaitFor) => {
  const d = new Date("2023-01-18");
  const startOfToday = new Date(d.getFullYear(), d.getMonth(), d.getDate());
  const command = new DescribeCasesCommand({
    includeCommunications: false,
    afterTime: startOfToday.toISOString(),
    includeResolvedCases: true,
  });
  const { cases, nextToken } = await client.send(command);
  await findCase({ cases, caseId: caseIdToWaitFor, nextToken });
  return cases.filter((c) => c.status === "resolved");
};

const main = async () => {
  let caseId;
  try {
    console.log(wrapText("Welcome to the AWS Support basic usage scenario."));

    // Verify that the account is subscribed to support.
    await verifyAccount();

    // Provided a truncated list of services and prompt the user to select one.
    const selectedService = await getService();

    // Provided the categories for the selected service and prompt the user to
 select one.
    const selectedCategory = await getCategory(selectedService);

    // Provide the severity available severity levels for the account and prompt
 the user to select one.
```

```
    const selectedSeverityLevel = await getSeverityLevel();

    // Create a support case.
    console.log("\nCreating a support case.");
    caseId = await createCase({
      selectedService,
      selectedCategory,
      selectedSeverityLevel,
    });
    console.log(`Support case created: ${caseId}`);

    // Display a list of open support cases created today.
    const todaysOpenCases = await retry(
      { intervalInMs: 1000, maxRetries: 15 },
      getTodaysOpenCases
    );
    console.log(
      `\nOpen support cases created today: ${todaysOpenCases.length}`
    );
    console.log(todaysOpenCases.map((c) => `${c.caseId}`).join("\n"));

    // Create an attachment set.
    console.log("\nCreating an attachment set.");
    const attachmentSetId = await createAttachmentSet();
    console.log(`Attachment set created: ${attachmentSetId}`);

    // Add the attachment set to the support case.
    console.log(`\nAdding attachment set to ${caseId}`);
    await linkAttachmentSetToCase(attachmentSetId, caseId);
    console.log(`Attachment set added to ${caseId}`);

    // List the communications for a support case.
    console.log(`\nListing communications for ${caseId}`);
    const communications = await getCommunications(caseId);
    console.log(
      communications
        .map(
          (c) =>
            `Communication created on ${c.timeCreated}. Has
${c.attachmentSet.length} attachments.`
        )
        .join("\n")
    );
```

```
    // Describe the first attachment.
    console.log(`\nDescribing attachment ${attachmentSetId}`);
    const attachmentId = getFirstAttachment(communications);
    const attachment = await getAttachment(attachmentId);
    console.log(
      `Attachment is the file '${
        attachment.fileName
      }' with data: \n${new TextDecoder().decode(attachment.data)}`
    );

    // Confirm that the support case should be resolved.
    const isResolved = await resolveCase(caseId);
    if (isResolved) {
      // List the resolved cases and include the one previously created.
      // Resolved cases can take a while to appear.
      console.log(
        "\nWaiting for case status to be marked as resolved. This can take some
 time."
      );
      const resolvedCases = await retry(
        { intervalInMs: 20000, maxRetries: 15 },
        () => getTodaysResolvedCases(caseId)
      );
      console.log("Resolved cases:");
      console.log(resolvedCases.map((c) => c.caseId).join("\n"));
    }
  } catch (err) {
    console.error(err);
  }
};
```

- 如需 API 詳細資訊，請參閱《AWS SDK for JavaScript API 參考》中的下列主題。
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices

- DescribeSeverityLevels
- ResolveCase

Kotlin

適用於 Kotlin 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
/**
Before running this Kotlin code example, set up your development environment,
including your credentials.

For more information, see the following documentation topic:

https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html
In addition, you must have the AWS Business Support Plan to use the AWS Support
 Java API. For more information, see:

https://aws.amazon.com/premiumsupport/plans/

This Kotlin example performs the following tasks:
1. Gets and displays available services.
2. Gets and displays severity levels.
3. Creates a support case by using the selected service, category, and severity
 level.
4. Gets a list of open cases for the current day.
5. Creates an attachment set with a generated file.
6. Adds a communication with the attachment to the support case.
7. Lists the communications of the support case.
8. Describes the attachment set included with the communication.
9. Resolves the support case.
10. Gets a list of resolved cases for the current day.
*/

suspend fun main(args: Array<String>) {
    val usage = """
```

```
   Usage:
       <fileAttachment>
   Where:
        fileAttachment - The file can be a simple saved .txt file to use as an
email attachment.
   """

   if (args.size != 1) {
       println(usage)
       exitProcess(0)
   }

   val fileAttachment = args[0]
   println("***** Welcome to the AWS Support case example scenario.")
   println("***** Step 1. Get and display available services.")
   val sevCatList = displayServices()

   println("***** Step 2. Get and display Support severity levels.")
   val sevLevel = displaySevLevels()

   println("***** Step 3. Create a support case using the selected service,
category, and severity level.")
   val caseIdVal = createSupportCase(sevCatList, sevLevel)
   if (caseIdVal != null) {
       println("Support case $caseIdVal was successfully created!")
   } else {
       println("A support case was not successfully created!")
       exitProcess(1)
   }

   println("***** Step 4. Get open support cases.")
   getOpenCase()

   println("***** Step 5. Create an attachment set with a generated file to add
to the case.")
   val attachmentSetId = addAttachment(fileAttachment)
   println("The Attachment Set id value is $attachmentSetId")

   println("***** Step 6. Add communication with the attachment to the support
case.")
   addAttachSupportCase(caseIdVal, attachmentSetId)

   println("***** Step 7. List the communications of the support case.")
   val attachId = listCommunications(caseIdVal)
```

```
    println("The Attachment id value is $attachId")

    println("***** Step 8. Describe the attachment set included with the
 communication.")
    describeAttachment(attachId)

    println("***** Step 9. Resolve the support case.")
    resolveSupportCase(caseIdVal)

    println("***** Step 10. Get a list of resolved cases for the current day.")
    getResolvedCase()
    println("***** This Scenario has successfully completed")
}

suspend fun getResolvedCase() {
    // Specify the start and end time.
    val now = Instant.now()
    LocalDate.now()
    val yesterday = now.minus(1, ChronoUnit.DAYS)
    val describeCasesRequest = DescribeCasesRequest {
        maxResults = 30
        afterTime = yesterday.toString()
        beforeTime = now.toString()
        includeResolvedCases = true
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeCases(describeCasesRequest)
        response.cases?.forEach { sinCase ->
            println("The case status is ${sinCase.status}")
            println("The case Id is ${sinCase.caseId}")
            println("The case subject is ${sinCase.subject}")
        }
    }
}

suspend fun resolveSupportCase(caseIdVal: String) {
    val caseRequest = ResolveCaseRequest {
        caseId = caseIdVal
    }
    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.resolveCase(caseRequest)
        println("The status of case $caseIdVal is ${response.finalCaseStatus}")
    }
```

```
}

suspend fun describeAttachment(attachId: String?) {
    val attachmentRequest = DescribeAttachmentRequest {
        attachmentId = attachId
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeAttachment(attachmentRequest)
        println("The name of the file is ${response.attachment?.fileName}")
    }
}

suspend fun listCommunications(caseIdVal: String?): String? {
    val communicationsRequest = DescribeCommunicationsRequest {
        caseId = caseIdVal
        maxResults = 10
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeCommunications(communicationsRequest)
        response.communications?.forEach { comm ->
            println("the body is: " + comm.body)
            comm.attachmentSet?.forEach { detail ->
                return detail.attachmentId
            }
        }
    }
    return ""
}

suspend fun addAttachSupportCase(caseIdVal: String?, attachmentSetIdVal: String?)
 {
    val caseRequest = AddCommunicationToCaseRequest {
        caseId = caseIdVal
        attachmentSetId = attachmentSetIdVal
        communicationBody = "Please refer to attachment for details."
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addCommunicationToCase(caseRequest)
        if (response.result) {
```

```
            println("You have successfully added a communication to an AWS
 Support case")
        } else {
            println("There was an error adding the communication to an AWS
 Support case")
        }
    }
}

suspend fun addAttachment(fileAttachment: String): String? {
    val myFile = File(fileAttachment)
    val sourceBytes = (File(fileAttachment).readBytes())
    val attachmentVal = Attachment {
        fileName = myFile.name
        data = sourceBytes
    }

    val setRequest = AddAttachmentsToSetRequest {
        attachments = listOf(attachmentVal)
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addAttachmentsToSet(setRequest)
        return response.attachmentSetId
    }
}

suspend fun getOpenCase() {
    // Specify the start and end time.
    val now = Instant.now()
    LocalDate.now()
    val yesterday = now.minus(1, ChronoUnit.DAYS)
    val describeCasesRequest = DescribeCasesRequest {
        maxResults = 20
        afterTime = yesterday.toString()
        beforeTime = now.toString()
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeCases(describeCasesRequest)
        response.cases?.forEach { sinCase ->
            println("The case status is ${sinCase.status}")
            println("The case Id is ${sinCase.caseId}")
            println("The case subject is ${sinCase.subject}")
```

```
        }
    }
}

suspend fun createSupportCase(sevCatListVal: List<String>, sevLevelVal: String):
 String? {
    val serCode = sevCatListVal[0]
    val caseCategory = sevCatListVal[1]
    val caseRequest = CreateCaseRequest {
        categoryCode = caseCategory.lowercase(Locale.getDefault())
        serviceCode = serCode.lowercase(Locale.getDefault())
        severityCode = sevLevelVal.lowercase(Locale.getDefault())
        communicationBody = "Test issue with
 ${serCode.lowercase(Locale.getDefault())}"
        subject = "Test case, please ignore"
        language = "en"
        issueType = "technical"
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.createCase(caseRequest)
        return response.caseId
    }
}

suspend fun displaySevLevels(): String {
    var levelName = ""
    val severityLevelsRequest = DescribeSeverityLevelsRequest {
        language = "en"
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeSeverityLevels(severityLevelsRequest)
        response.severityLevels?.forEach { sevLevel ->
            println("The severity level name is: ${sevLevel.name}")
            if (sevLevel.name == "High") {
                levelName = sevLevel.name!!
            }
        }
        return levelName
    }
}
```

```
// Return a List that contains a Service name and Category name.
suspend fun displayServices(): List<String> {
    var serviceCode = ""
    var catName = ""
    val sevCatList = mutableListOf<String>()
    val servicesRequest = DescribeServicesRequest {
        language = "en"
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeServices(servicesRequest)
        println("Get the first 10 services")
        var index = 1

        response.services?.forEach { service ->
            if (index == 11) {
                return@forEach
            }

            println("The Service name is ${service.name}")
            if (service.name == "Account") {
                serviceCode = service.code.toString()
            }

            // Get the categories for this service.
            service.categories?.forEach { cat ->
                println("The category name is ${cat.name}")
                if (cat.name == "Security") {
                    catName = cat.name!!
                }
            }
            index++
        }
    }

    // Push the two values to the list.
    serviceCode.let { sevCatList.add(it) }
    catName.let { sevCatList.add(it) }
    return sevCatList
}
```

- 如需 API 詳細資訊，請參閱 AWS 適用於 Kotlin 的 SDK API 參考中的下列主題。

- AddAttachmentsToSet
- AddCommunicationToCase
- CreateCase
- DescribeAttachment
- DescribeCases
- DescribeCommunications
- DescribeServices
- DescribeSeverityLevels
- ResolveCase

Python

適用於 Python (Boto3) 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

在命令提示中執行互動式案例。

```
class SupportCasesScenario:
    """Runs an interactive scenario that shows how to get started using AWS
 Support."""

    def __init__(self, support_wrapper):
        """
        :param support_wrapper: An object that wraps AWS Support actions.
        """
        self.support_wrapper = support_wrapper

    def display_and_select_service(self):
        """
        Lists support services and prompts the user to select one.

        :return: The support service selected by the user.
        """
```

```
        print("-" * 88)
        services_list = self.support_wrapper.describe_services("en")
        print(f"AWS Support client returned {len(services_list)} services.")
        print("Displaying first 10 services:")

        service_choices = [svc["name"] for svc in services_list[:10]]
        selected_index = q.choose(
            "Select an example support service by entering a number from the
preceding list:",
            service_choices,
        )
        selected_service = services_list[selected_index]
        print("-" * 88)
        return selected_service

    def display_and_select_category(self, service):
        """
        Lists categories for a support service and prompts the user to select
one.

        :param service: The service of the categories.
        :return: The selected category.
        """
        print("-" * 88)
        print(
            f"Available support categories for Service {service['name']}
{len(service['categories'])}:"
        )
        categories_choices = [category["name"] for category in
service["categories"]]
        selected_index = q.choose(
            "Select an example support category by entering a number from the
preceding list:",
            categories_choices,
        )
        selected_category = service["categories"][selected_index]
        print("-" * 88)
        return selected_category

    def display_and_select_severity(self):
        """
        Lists available severity levels and prompts the user to select one.

        :return: The selected severity level.
```

```
        """
        print("-" * 88)
        severity_levels_list =
self.support_wrapper.describe_severity_levels("en")
        print(f"Available severity levels:")
        severity_choices = [level["name"] for level in severity_levels_list]
        selected_index = q.choose(
            "Select an example severity level by entering a number from the
preceding list:",
            severity_choices,
        )
        selected_severity = severity_levels_list[selected_index]
        print("-" * 88)
        return selected_severity

    def create_example_case(self, service, category, severity_level):
        """
        Creates an example support case with the user's selections.

        :param service: The service for the new case.
        :param category: The category for the new case.
        :param severity_level: The severity level for the new case.
        :return: The caseId of the new support case.
        """
        print("-" * 88)
        print(f"Creating new case for service {service['name']}.")
        case_id = self.support_wrapper.create_case(service, category,
severity_level)
        print(f"\tNew case created with ID {case_id}.")
        print("-" * 88)
        return case_id

    def list_open_cases(self):
        """
        List the open cases for the current day.
        """
        print("-" * 88)
        print("Let's list the open cases for the current day.")
        start_time = str(datetime.utcnow().date())
        end_time = str(datetime.utcnow().date() + timedelta(days=1))
        open_cases = self.support_wrapper.describe_cases(start_time, end_time,
False)
        for case in open_cases:
            print(f"\tCase: {case['caseId']}: status {case['status']}.")
```

```
        print("-" * 88)

    def create_attachment_set(self):
        """
        Create an attachment set with a sample file.

        :return: The attachment set ID of the new attachment set.
        """
        print("-" * 88)
        print("Creating attachment set with a sample file.")
        attachment_set_id = self.support_wrapper.add_attachment_to_set()
        print(f"\tNew attachment set created with ID {attachment_set_id}.")
        print("-" * 88)
        return attachment_set_id

    def add_communication(self, case_id, attachment_set_id):
        """
        Add a communication with an attachment set to the case.

        :param case_id: The ID of the case for the communication.
        :param attachment_set_id: The ID of the attachment set to
        add to the communication.
        """
        print("-" * 88)
        print(f"Adding a communication and attachment set to the case.")
        self.support_wrapper.add_communication_to_case(attachment_set_id,
case_id)
        print(
            f"Added a communication and attachment set {attachment_set_id} to the
case {case_id}."
        )
        print("-" * 88)

    def list_communications(self, case_id):
        """
        List the communications associated with a case.

        :param case_id: The ID of the case.
        :return: The attachment ID of an attachment.
        """
        print("-" * 88)
        print("Let's list the communications for our case.")
        attachment_id = ""
```

```
        communications =
self.support_wrapper.describe_all_case_communications(case_id)
        for communication in communications:
            print(
                f"\tCommunication created on {communication['timeCreated']} "
                f"has {len(communication['attachmentSet'])} attachments."
            )
            if len(communication["attachmentSet"]) > 0:
                attachment_id = communication["attachmentSet"][0]["attachmentId"]
        print("-" * 88)
        return attachment_id

    def describe_case_attachment(self, attachment_id):
        """
        Describe an attachment associated with a case.

        :param attachment_id: The ID of the attachment.
        """
        print("-" * 88)
        print("Let's list the communications for our case.")
        attached_file = self.support_wrapper.describe_attachment(attachment_id)
        print(f"\tAttachment includes file {attached_file}.")
        print("-" * 88)

    def resolve_case(self, case_id):
        """
        Shows how to resolve an AWS Support case by its ID.

        :param case_id: The ID of the case to resolve.
        """
        print("-" * 88)
        print(f"Resolving case with ID {case_id}.")
        case_status = self.support_wrapper.resolve_case(case_id)
        print(f"\tFinal case status is {case_status}.")
        print("-" * 88)

    def list_resolved_cases(self):
        """
        List the resolved cases for the current day.
        """
        print("-" * 88)
        print("Let's list the resolved cases for the current day.")
        start_time = str(datetime.utcnow().date())
        end_time = str(datetime.utcnow().date() + timedelta(days=1))
```

```
        resolved_cases = self.support_wrapper.describe_cases(start_time,
 end_time, True)
        for case in resolved_cases:
            print(f"\tCase: {case['caseId']}: status {case['status']}.")
        print("-" * 88)

    def run_scenario(self):
        logging.basicConfig(level=logging.INFO, format="%(levelname)s:
 %(message)s")

        print("-" * 88)
        print("Welcome to the AWS Support get started with support cases demo.")
        print("-" * 88)

        selected_service = self.display_and_select_service()
        selected_category = self.display_and_select_category(selected_service)
        selected_severity = self.display_and_select_severity()
        new_case_id = self.create_example_case(
            selected_service, selected_category, selected_severity
        )
        wait(10)
        self.list_open_cases()
        new_attachment_set_id = self.create_attachment_set()
        self.add_communication(new_case_id, new_attachment_set_id)
        new_attachment_id = self.list_communications(new_case_id)
        self.describe_case_attachment(new_attachment_id)
        self.resolve_case(new_case_id)
        wait(10)
        self.list_resolved_cases()

        print("\nThanks for watching!")
        print("-" * 88)


if __name__ == "__main__":
    try:
        scenario = SupportCasesScenario(SupportWrapper.from_client())
        scenario.run_scenario()
    except Exception:
        logging.exception("Something went wrong with the demo.")
```

定義包裝支援用戶端動作的類別。

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_services(self, language):
        """
        Get the descriptions of AWS services available for support for a
 language.

        :param language: The language for support services.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of AWS service descriptions.
        """
        try:
            response = self.support_client.describe_services(language=language)
            services = response["services"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
 Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
 subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get Support services for language %s. Here's why:
 %s: %s",
```

```
                    language,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return services


    def describe_severity_levels(self, language):
        """
        Get the descriptions of available severity levels for support cases for a
language.

        :param language: The language for support severity levels.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of severity levels.
        """
        try:
            response =
self.support_client.describe_severity_levels(language=language)
            severity_levels = response["severityLevels"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get severity levels for language %s. Here's why:
%s: %s",
                    language,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return severity_levels
```

```
    def create_case(self, service, category, severity):
        """
        Create a new support case.

        :param service: The service to use for the new case.
        :param category: The category to use for the new case.
        :param severity: The severity to use for the new case.
        :return: The caseId of the new case.
        """
        try:
            response = self.support_client.create_case(
                subject="Example case for testing, ignore.",
                serviceCode=service["code"],
                severityCode=severity["code"],
                categoryCode=category["code"],
                communicationBody="Example support case body.",
                language="en",
                issueType="customer-service",
            )
            case_id = response["caseId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't create case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return case_id


    def add_attachment_to_set(self):
        """
        Add an attachment to a set, or create a new attachment set if one does
not exist.
```

```
        :return: The attachment set ID.
        """
        try:
            response = self.support_client.add_attachments_to_set(
                attachments=[
                    {
                        "fileName": "attachment_file.txt",
                        "data": b"This is a sample file for attachment to a
support case.",
                    }
                ]
            )
            new_set_id = response["attachmentSetId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add attachment. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return new_set_id


    def add_communication_to_case(self, attachment_set_id, case_id):
        """
        Add a communication and an attachment set to a case.

        :param attachment_set_id: The ID of an existing attachment set.
        :param case_id: The ID of the case.
        """
        try:
            self.support_client.add_communication_to_case(
                caseId=case_id,
```

```
                communicationBody="This is an example communication added to a
support case.",
                attachmentSetId=attachment_set_id,
            )
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add communication. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise


    def describe_all_case_communications(self, case_id):
        """
        Describe all the communications for a case using a paginator.

        :param case_id: The ID of the case.
        :return: The communications for the case.
        """
        try:
            communications = []
            paginator =
self.support_client.get_paginator("describe_communications")
            for page in paginator.paginate(caseId=case_id):
                communications += page["communications"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
```

```
            else:
                logger.error(
                    "Couldn't describe communications. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return communications


    def describe_attachment(self, attachment_id):
        """
        Get information about an attachment by its attachmentID.

        :param attachment_id: The ID of the attachment.
        :return: The name of the attached file.
        """
        try:
            response = self.support_client.describe_attachment(
                attachmentId=attachment_id
            )
            attached_file = response["attachment"]["fileName"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get attachment description. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return attached_file


    def resolve_case(self, case_id):
```

```
        """
        Resolve a support case by its caseId.

        :param case_id: The ID of the case to resolve.
        :return: The final status of the case.
        """
        try:
            response = self.support_client.resolve_case(caseId=case_id)
            final_status = response["finalCaseStatus"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't resolve case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return final_status


    def describe_cases(self, after_time, before_time, resolved):
        """
        Describe support cases over a period of time, optionally filtering
        by status.

        :param after_time: The start time to include for cases.
        :param before_time: The end time to include for cases.
        :param resolved: True to include resolved cases in the results,
            otherwise results are open cases.
        :return: The final status of the case.
        """
        try:
            cases = []
            paginator = self.support_client.get_paginator("describe_cases")
            for page in paginator.paginate(
```

```
                afterTime=after_time,
                beforeTime=before_time,
                includeResolvedCases=resolved,
                language="en",
            ):
                cases += page["cases"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't describe cases. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            if resolved:
                cases = filter(lambda case: case["status"] == "resolved", cases)
            return cases
```

- 如需 API 的詳細資訊，請參閱《適用於 Python (Boto3) 的AWS SDK API 參考資料》中的下列主題。
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices

- DescribeSeverityLevels
- ResolveCase

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭配 AWS SDK 使用 AWS Support。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

AWS Support 的監控和日誌記錄

監控是維護 AWS Support 及其他 AWS 解決方案的可靠性、可用性和效能的重要部分。AWS 提供以下監控工具，可讓您監看 AWS Support、在發現錯誤時回報，並適時採取自動動作。

- Amazon EventBridge 可傳送近乎即時的系統事件串流，以說明 AWS 資源發生的變動。EventBridge 啟用自動的事件驅動運算，因為您可以在這些事件發生時，編寫監看特定事件與在其他 AWS 服務內觸發自動化動作的規則。如需詳細資訊，請參閱《Amazon EventBridge 使用者指南》。
- AWS CloudTrail 擷取您 AWS 帳戶發出或代表發出的 API 呼叫和相關事件，並傳送記錄檔案至您指定的 Simple Storage Service (Amazon S3) 儲存貯體。您可以找出哪些使用者和帳戶呼叫 AWS、發出呼叫的來源 IP 地址，以及呼叫的發生時間。如需詳細資訊，請參閱《AWS CloudTrail 使用者指南》。

主題

使用 Amazon 監控AWS Support案例 EventBridge

您可以使 EventBridge 用 Amazon 偵測AWS Support案例的變更並做出回應。然後，根據您建立的規則，當事件符合您在規則中指定的值時， EventBridge 叫用一或多個目標動作。

您可以根據事件傳送通知、擷取事件資訊、採取修正動作、啟動事件，或採取其他動作。例如，每當您的帳戶中發生下列動作時，您可以收到通知：

- 建立支援案例
- 將案例通訊新增至現有支援案例
- 解決支援案例
- 重新開啟支援案例

> **Note**
>
> AWS Support 會全力傳遞事件。並未始終保證將事件傳遞至 EventBridge。

為 AWS Support 案例建立 EventBridge 規則

您可以建立 EventBridge 規則以接收AWS Support案例事件的通知。該規則將會監控您帳戶中支援案例的更新，包括您、您的 IAM 使用者或支援代理執行的動作。在您為 AWS Support 案例事件建立規則之前，請執行下列動作：

- 熟悉中的事件、規則和目標。 EventBridge如需詳細資訊，請參閱什麼是 Amazon EventBridge？ 在 Amazon 用 EventBridge戶指南。
- 建立要在事件規則中使用的目標。例如，您可建立 Amazon Simple Notification Service (Amazon SNS) 主題，以便每當更新支援案例時，您都會收到簡訊或電子郵件。如需詳細資訊，請參閱 EventBridge 目標。

> **Note**
>
> AWS Support 是全球服務。若要接收支援案例的更新，您可以使用下列其中一個區域：美國東部 (維吉尼亞北部) 區域、美國西部 (奧勒岡) 區域或歐洲 (愛爾蘭) 區域。

若要建立AWS Support案例事件的 EventBridge 規則

1. 在以下位置打開 Amazon EventBridge 控制台 https://console.aws.amazon.com/events/。
2. 若尚未就緒，請使用頁面右上角的區域選擇器，然後選擇美國東部 (維吉尼亞北部)。
3. 在導覽窗格中，選擇 Rules(規則)。
4. 選擇 Create rule (建立規則)。
5. 在 Define rule detail (定義規則詳細資訊) 頁面中，輸入規則名稱和描述。
6. 請保留 Event bus (事件匯流排) 和 Rule type (規則類型) 的預設值，然後選擇 Next (下一步)。
7. 在 [建立事件模式] 頁面上，針對 [事件來源] 選擇AWS事件或 EventBridge 合作夥伴事件。
8. 在 Event pattern (事件模式) 下，保留 AWS 服務 的預設值。
9. 對於 AWS 服務，選擇 Support (支援)。
10. 對於 Event type，請選擇 Support Case Update (支援案例更新)。
11. 選擇 下一步。
12. 在 Select target(s) (選取目標) 區段中，請選擇您為此規則建立的目標類型，然後設定該類型所需的任何其他選項。例如，如果您選擇 Amazon SNS，請確認您的 SNS 主題設定正確，以便透過電子郵件或簡訊通知您。

13. 選擇 下一步。
14. (選用) 在 設定標籤頁面，新增任何標籤，然後選擇下一步。
15. 在 Review and create (檢閱並建立) 頁面上，檢閱您的規則設定，並確定其符合您的事件監控要求。
16. 選擇 Create rule (建立規則)。您的規則現在將監控 AWS Support 案例事件，然後將這些事件傳送至您指定的目標。

> **備註**
>
> - 當您收到事件時，您可以使用 `origin` 參數來確定您還是 AWS Support 客服人員向支援案例新增案例通訊。`origin` 的值可以是 `CUSTOMER` 或 `AWS`。
>
> 目前僅 `AddCommunicationToCase` 動作的事件具有此值。
> - 如需有關建立事件模式的詳細資訊，請參閱 Amazon EventBridge 使用者指南中的事件模式。
> - 您也可以透過 CloudTrail事件類型為 AWS API 呼叫建立另一個規則。此規則將監控您帳戶中 AWS Support API 呼叫的 AWS CloudTrail 日誌。

範例 AWS Support 事件

您的帳戶中發生支援動作時，將會建立以下事件。

Example ：建立支援案例

建立支援案例時，將會建立以下事件。

```
{
    "version": "0",
    "id": "3433df007-9285-55a3-f6d1-536944be45d7",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:51:19Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
```

```
        "case-id": "case-111122223333-muen-2022-7118885805350839",
        "display-id": "1234563851",
        "communication-id": "",
        "event-name": "CreateCase",
        "origin": ""
    }
}
```

Example ：更新支援案例

AWS Support 回覆支援案例時，將會建立以下事件。

```
{
    "version": "0",
    "id": "f90cb8cb-32be-1c91-c0ba-d50b4ca5e51b",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:51:31Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2022-7118885805350839",
        "display-id": "1234563851",
        "communication-id": "ekko:us-east-1:12345678-268a-424b-be08-54613cab84d2",
        "event-name": "AddCommunicationToCase",
        "origin": "AWS"
    }
}
```

Example ：解決支援案例

解決支援案例時，將會建立以下事件。

```
{
    "version": "0",
    "id": "1aa4458d-556f-732e-ddc1-4a5b2fbd14a5",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:51:31Z",
    "region": "us-east-1",
```

```
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2022-7118885805350839",
        "display-id": "1234563851",
        "communication-id": "",
        "event-name": "ResolveCase",
        "origin": ""
    }
}
```

Example ：重新開啟支援案例

重新開啟支援案例時，將會建立以下事件。

```
{
    "version": "0",
    "id": "3bb9d8fe-6089-ad27-9508-804209b233ad",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:47:19Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2021-27f40618fe0303ea",
        "display-id": "1234563851",
        "communication-id": "",
        "event-name": "ReopenCase",
        "origin": ""
    }
}
```

另請參閱

如需如何搭 EventBridge 配使用的詳細資訊AWS Support，請參閱下列資源：

- 如何使用 Amazon 自動化 AWS Support API EventBridge
- AWS Support案例活動通知 GitHub

使用 AWS CloudTrail 記錄 AWS Support API 呼叫

AWS Support 已與 AWS CloudTrail 整合，這項服務可提供由使用者、角色或 AWS Support 中的 AWS 服務所採取之動作的記錄。CloudTrail 會擷取 AWS Support 的 API 呼叫當作事件。擷取的呼叫包括從 AWS Support 主控台進行的呼叫，以及針對 AWS Support API 操作的程式碼呼叫。

如果您建立追蹤記錄，就可以將 CloudTrail 事件持續提供給 Amazon Simple Storage Service (Amazon S3) 儲存貯體，包括 AWS Support 的事件。即使您未設定追蹤，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。

您可以利用 CloudTrail 所收集的資訊來判斷向 AWS Support 發出的請求，以及發出請求的 IP 地址、人員、時間和其他詳細資訊。

若要進一步了解 CloudTrail，包括如何設定及啟用，請參閱《AWS CloudTrail 使用者指南》。

CloudTrail 中的 AWS Support 資訊

當您建立帳戶時，系統即會在 AWS 帳戶中啟用 CloudTrail。當 AWS Support 發生支援的事件活動時，系統便會將該活動記錄至 CloudTrail 事件，並將其他 AWS 服務事件記錄到 Event history (事件歷史記錄) 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 帳戶中正在進行事件的記錄 (包含 AWS Support 的事件)，請建立線索。追蹤能讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。根據預設，當您在主控台建立線索時，線索會套用到所有 AWS 區域。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務和整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 接收多個區域的 CloudTrail 日誌檔案及接收多個帳戶的 CloudTrail 日誌檔案

所有 AWS Support API 作業均由 CloudTrail 記錄，並記載於 AWS Support API 參考中。

例如，對 `CreateCase`、`DescribeCases` 和 `ResolveCase` 作業的呼叫都會在 CloudTrail 日誌檔案中產生項目。

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：

- 該請求是否透過根或 AWS Identity and Access Management (IAM) 使用者憑證來提出。
- 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 userIdentity 元素。

您也可以將來自多個 AWS 區域和多個 AWS 帳戶的 AWS Support 日誌檔案，彙總至單一 Amazon S3 儲存貯體。

CloudTrail 記錄中的 AWS Trusted Advisor 資訊

Trusted Advisor 是一項 AWS Support 服務，可讓您用來查看 AWS 帳戶，了解如何節省成本、改善安全性以及最佳化帳戶。

所有 Trusted Advisor API 作業均由 CloudTrail 記錄，並記載於 AWS Support API 參考中。

例如，對 `DescribeTrustedAdvisorCheckRefreshStatuses`、`DescribeTrustedAdvisorCheckResult` 和 `RefreshTrustedAdvisorCheck` 作業的呼叫都會在 CloudTrail 日誌檔案中產生項目。

> **Note**
>
> CloudTrail 也會記錄 Trusted Advisor 主控台動作。請參閱 使用 AWS CloudTrail 記錄 AWS Trusted Advisor 主控台動作。

了解 AWS Support 日誌檔案項目

追蹤是一種組態，可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。事件代表來自任何來源的單一請求。其中包含請求的作業、作業日期和時間、請求參數等相關資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

Example ：CreateCase 的日誌項目

以下範例顯示 CreateCase 作業的 CloudTrail 日誌項目。

```
{
   "Records": [
      {
```

```
         "eventVersion": "1.04",
         "userIdentity": {
            "type": "IAMUser",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/janedoe",
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "userName": "janedoe",
            "sessionContext": {
               "attributes": {
                  "mfaAuthenticated": "false",
                  "creationDate": "2016-04-13T17:51:37Z"
               }
            },
            "invokedBy": "signin.amazonaws.com"
         },
         "eventTime": "2016-04-13T18:05:53Z",
         "eventSource": "support.amazonaws.com",
         "eventName": "CreateCase",
         "awsRegion": "us-east-1",
         "sourceIPAddress": "198.51.100.15",
         "userAgent": "signin.amazonaws.com",
         "requestParameters": {
            "severityCode": "low",
            "categoryCode": "other",
            "language": "en",
            "serviceCode": "support-api",
            "issueType": "technical"
         },
         "responseElements": {
            "caseId": "case-111122223333-muen-2016-c3f2077e504940f2"
         },
         "requestID": "58c257ef-01a2-11e6-be2a-01c031063738",
         "eventID": "5aa34bfc-ad5b-4fb1-8a55-2277c86e746a",
         "eventType": "AwsApiCall",
         "recipientAccountId": "111122223333"
      }
   ],
   ...
}
```

Example ：RefreshTrustedAdvisorCheck 的日誌項目

以下範例顯示 RefreshTrustedAdvisorCheck 作業的 CloudTrail 日誌項目。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/Admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Admin"
    },
    "eventTime": "2020-10-21T16:34:13Z",
    "eventSource": "support.amazonaws.com",
    "eventName": "RefreshTrustedAdvisorCheck",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.198.67",
    "userAgent": "signin.amazonaws.com",
    "requestParameters": {
        "checkId": "Pfx0RwqBli"
    },
    "responseElements": null,
    "requestID": "4c4d5fc8-c403-4f82-9544-41f820e0fa01",
    "eventID": "2f4630ac-5c27-4f0d-b93f-63742d6fc85e",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```


使用 AWS CloudTrail 在 Slack API 呼叫中記錄 AWS Support 應用程式

Slack 中的 AWS Support 應用程式已與 AWS CloudTrail 整合。CloudTrail 會提供由使用者、角色或 AWS 服務 在 AWS Support 應用程式中採取之動作的記錄。為了建立此記錄，CloudTrail 會將 AWS Support 應用程式的所有公有 API 呼叫擷取為事件。這些擷取的呼叫包括來自 AWS Support 應用程式主控台的呼叫，以及針對 AWS Support 應用程式公有 API 操作進行的程式碼呼叫。若您建立追蹤，便可將 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 的事件。這包括 AWS Support 應用程式的事件。即使您未設定追蹤，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 CloudTrail 收集的資訊來確定向 AWS Support 應用程式發出的請求。您還可以瞭解發起呼叫的 IP 地址、提出請求的人員和時間以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱《AWS CloudTrail 使用者指南》。

CloudTrail 中的 AWS Support 應用程式資訊

當您建立 AWS 帳戶 時，系統即會在帳戶中啟用 CloudTrail。當 AWS Support 應用程式中發生公有 API 活動時，該活動會記錄在 CloudTrail 事件中，其他 AWS 服務事件則記錄於 Event history (事件歷史記錄) 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 AWS 帳戶 中正在進行事件的記錄 (包含 AWS Support 應用程式的事件)，請建立追蹤。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，您可以設定其他 AWS 服務，以進一步分析 CloudTrail 日誌中收集的事件資料，並對這些資料採取操作。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務和整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 接收多個區域的 CloudTrail 日誌檔案和接收多個帳戶的 CloudTrail 日誌檔案

CloudTrail 會記錄所有公有 AWS Support 應用程式動作。這些動作也記錄在 Slack API 參考的 AWS Support 應用程式中。例如，對 `CreateSlackChannelConfiguration`、`GetAccountAlias` 和 `UpdateSlackChannelConfiguration` 動作發出的呼叫會在 CloudTrail 記錄檔案中產生項目。

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：

- 該請求是否透過根或 AWS Identity and Access Management (IAM) 使用者憑證來提出。
- 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 服務提出。

如需詳細資訊，請參閱 CloudTrail userIdentity 元素。

了解 AWS Support 應用程式日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌項目。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 日誌檔案並不是公有 API 呼叫的有序堆疊追蹤。這意味著日誌不會以任何特定順序顯示。

Example ：**CreateSlackChannelConfiguration** 的日誌範例

以下範例顯示 CreateSlackChannelConfiguration 操作的 CloudTrail 日誌項目。


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:JaneDoe",
        "arn": "arn:aws:sts::111122223333:assumed-role/Administrator/JaneDoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Administrator",
                "accountId": "111122223333",
                "userName": "Administrator"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-02-26T01:37:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-02-26T01:48:20Z",
    "eventSource": "supportapp.amazonaws.com",
    "eventName": "CreateSlackChannelConfiguration",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5",
    "requestParameters": {
        "notifyOnCreateOrReopenCase": true,
        "teamId": "T012ABCDEFG",
        "notifyOnAddCorrespondenceToCase": true,
        "notifyOnCaseSeverity": "all",
        "channelName": "troubleshooting-channel",
        "notifyOnResolveCase": true,
        "channelId": "C01234A5BCD",
        "channelRoleArn": "arn:aws:iam::111122223333:role/AWSSupportAppRole"
    },
    "responseElements": null,
```

```
    "requestID": "d06df6ca-c233-4ffb-bbff-63470c5dc255",
    "eventID": "0898ce29-a396-444a-899d-b068f390c361",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example ：**ListSlackChannelConfigurations** 的日誌範例

以下範例顯示 ListSlackChannelConfigurations 操作的 CloudTrail 日誌項目。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:AWSSupportAppRole",
        "arn": "arn:aws:sts::111122223333:assumed-role/AWSSupportAppRole",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/AWSSupportAppRole",
                "accountId": "111122223333",
                "userName": "AWSSupportAppRole"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-03-01T20:06:32Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-03-01T20:06:46Z",
    "eventSource": "supportapp.amazonaws.com",
    "eventName": "ListSlackChannelConfigurations",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.217.131",
    "userAgent": "aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5",
    "requestParameters": null,
    "responseElements": null,
```

```
    "requestID": "20f81d63-31c5-4351-bd02-9eda7f76e7b8",
    "eventID": "70acb7fe-3f84-47cd-8c28-cc148ad06d21",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example ：**GetAccountAlias** 的日誌範例

以下範例顯示 GetAccountAlias 操作的 CloudTrail 日誌項目。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:devdsk",
        "arn": "arn:aws:sts::111122223333:assumed-role/AWSSupportAppRole/devdsk",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/AWSSupportAppRole",
                "accountId": "111122223333",
                "userName": "AWSSupportAppRole"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-03-01T20:31:27Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-03-01T20:31:47Z",
    "eventSource": "supportapp.amazonaws.com",
    "eventName": "GetAccountAlias",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.217.142",
    "userAgent": "aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5",
    "requestParameters": null,
    "responseElements": null,
```

```
    "requestID": "a225966c-0906-408b-b8dd-f246665e6758",
    "eventID": "79ebba8d-3285-4023-831a-64af7de8d4ad",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

監控和記錄 AWS Support Plans

監控是維護 Support Plans 及其他 AWS 解決方案的可靠性、可用性和效能的重要部分。AWS 提供以下監控工具，可讓您監看 Support Plans，在發現錯誤時報告，並適時採取自動動作：

- AWS CloudTrail 擷取您 AWS 帳戶發出或代表發出的 API 呼叫和相關事件，並傳送記錄檔案至您指定的 Simple Storage Service (Amazon S3) 儲存貯體。您可以找出哪些使用者和帳戶呼叫 AWS、發出呼叫的來源 IP 地址，以及呼叫的發生時間。如需詳細資訊，請參閱《AWS CloudTrail 使用者指南》。

主題

使用 AWS CloudTrail 記錄 AWS Support Plans API 呼叫

AWS Support Plans 整合了 AWS CloudTrail，這是一種提供使用者、角色或 AWS 服務 所採取之動作記錄的服務。CloudTrail 會擷取 AWS Support Plans 的 API 呼叫當作事件。擷取的呼叫包括從 AWS Support Plans 主控台進行的呼叫，以及針對 AWS Support Plans API 操作的程式碼呼叫。

如果您建立追蹤，就可以將 CloudTrail 事件持續提供給 Amazon Simple Storage Service (Amazon S3) 儲存貯體，包括 AWS Support Plans 的事件。即使您未設定追蹤，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。

您可以利用 CloudTrail 所收集的資訊來判斷向 AWS Support Plans 發出的請求，以及發出請求的 IP 地址、人員、時間和其他詳細資訊。

若要進一步了解 CloudTrail，包括如何設定及啟用，請參閱《AWS CloudTrail 使用者指南》。

CloudTrail 中的 AWS Support Plans 資訊

當您建立帳戶時，系統即會在 AWS 帳戶 中啟用 CloudTrail。當 AWS Support Plans 發生支援的事件活動時，系統便會將該活動記錄至 CloudTrail 事件，並將其他 AWS 服務 事件記錄到 Event history (事件歷史記錄) 中。您可以檢視、搜尋和下載 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。

如需帳戶中正在進行事件的記錄 (包含 AWS Support Plans 的事件)，請建立追蹤。追蹤能讓 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，您可以設定其他 AWS 服務 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務和整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 接收多個區域的 CloudTrail 日誌檔案及接收多個帳戶的 CloudTrail 日誌檔案

CloudTrail 會記錄全部 AWS Support Plans API 操作。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：

- 該請求是否透過根或 AWS Identity and Access Management (IAM) 使用者憑證來提出。
- 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 服務提出。

如需詳細資訊，請參閱 CloudTrail userIdentity 元素。

您也可以將來自多個 AWS 區域 和多個帳戶的 AWS Support Plans 日誌檔案彙總至單一 Amazon S3 儲存貯體。

了解 AWS Support Plans 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到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一個或多個日誌項目。事件代表來自任何來源的單一請求。其中包含請求的作業、作業日期和時間、請求參數等相關資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

Example ：**`GetSupportPlan`** 的日誌項目

以下範例顯示 `GetSupportPlan` 操作的 CloudTrail 日誌項目。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
```

```
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-06-29T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-06-29T16:39:11Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "GetSupportPlan",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "7665c39a-d6bf-4d0d-8010-2f59740b8ecb",
    "eventID": "b711bc30-16a5-4579-8f0d-9ada8fe6d1ce",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example ：**GetSupportPlanUpdateStatus** 的日誌項目

以下範例顯示 GetSupportPlanUpdateStatus 操作的 CloudTrail 日誌項目。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
```

```
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-06-29T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-06-29T16:39:02Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "GetSupportPlanUpdateStatus",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": {
        "supportPlanUpdateArn":
 "arn:aws:supportplans::111122223333:supportplanupdate/7f03b7a233a0e87ebc79e56d4d2bcaf19e976c37
    },
    "responseElements": null,
    "requestID": "75e5c767-8703-4ed3-b01e-4dda28020322",
    "eventID": "28d1c0e3-ccb6-4fd1-8793-65be010114cc",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Example ：**StartSupportPlanUpdate** 的日誌項目

以下範例顯示 StartSupportPlanUpdate 操作的 CloudTrail 日誌項目。


```
{
    "eventVersion": "1.08",
    "userIdentity": {
```

```
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-06-29T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-06-29T16:38:55Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "StartSupportPlanUpdate",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": {
        "clientToken": "98add111-dcc9-464d-8722-438d697fe242",
        "update": {
            "supportLevel": "BASIC"
        }
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-RequestId,x-amzn-ErrorType,x-amzn-
ErrorMessage,Date",
        "supportPlanUpdateArn":
 "arn:aws:supportplans::111122223333:supportplanupdate/7f03b7a233a0e87ebc79e56d4d2bcaf19e976c37
    },
    "requestID": "e5ff9382-5fb8-4764-9993-0f33fb0b1e17",
    "eventID": "5dba89f8-2e5b-42b9-9b8f-395580c52962",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
```

```
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example ：**CreateSupportPlanSchedule** 的日誌項目

以下範例顯示 CreateSupportPlanSchedule 操作的 CloudTrail 日誌項目。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-05-09T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-05-09T16:30:04Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "CreateSupportPlanSchedule",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": {
        "clientToken": "b998de5e-ad1c-4448-90db-2bf86d6d9e9a",
        "scheduleCreationDetails": {
            "startLevel": "BUSINESS",
            "startOffer": "TrialPlan7FB93B",
            "startTimestamp": "2023-06-03T17:23:56.109Z",
```

```
            "endLevel": "BUSINESS",
            "endOffer": "StandardPlan2074BB",
            "endTimestamp": "2023-09-03T17:23:55.109Z"
        }
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-RequestId,x-amzn-ErrorType,x-amzn-
ErrorMessage,Date",
        "supportPlanUpdateArn":
 "arn:aws:supportplans::111122223333:supportplanschedule/
b9a9a4336a3974950a6e670f7dab79b77a4b104db548a0d57050ce4544721d4b"
    },
    "requestID": "150450b8-e61a-4b15-93a8-c3b557a1ca48",
    "eventID": "a2a1ba44-610d-4dc8-bf16-29f1635b57a9",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


記錄 AWS Support 計劃的變更

> **Important**
>
> 自 2022 年 8 月 3 日起，下列操作已停用，且不會出現在您的新 CloudTrail 日誌中。如需支援的操作清單，請參閱 了解 AWS Support Plans 日誌檔案項目。

- `DescribeSupportLevelSummary` - 您開啟 Support plans (支援計劃) 頁面時，此動作會出現在您的日誌中。
- `UpdateProbationAutoCancellation` - 您註冊開發人員支援或企業支援計劃後，若嘗試在 30 天內取消，您的計劃將在這段期間結束時自動取消。您在 Support plans (支援計劃) 頁面上顯示的橫幅中選擇 Opt-out of automatic cancellation (退出自動取消) 時，此動作會出現在日誌中。您將繼續使用您的開發人員支援或企業支援計劃。
- `UpdateSupportLevel` - 您變更支援計劃時，此動作會出現在您的日誌中。

> **Note**
>
> eventSource 欄位具有用於這些動作的 support-subscription.amazonaws.com 命名空間。

Example ：DescribeSupportLevelSummary 的日誌項目

以下範例顯示 DescribeSupportLevelSummary 動作的 CloudTrail 日誌項目。


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-01-07T22:08:05Z"
      }
    }
  },
  "eventTime": "2021-01-07T22:08:07Z",
  "eventSource": "support-subscription.amazonaws.com",
  "eventName": "DescribeSupportLevelSummary",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "100.127.8.67",
  "userAgent": "AWS-SupportPlansConsole, aws-internal/3",
  "requestParameters": {
    "lang": "en"
  },
  "responseElements": null,
  "requestID": "b423b84d-829b-4090-a239-2b639b123abc",
  "eventID": "e1eeda0e-d77c-487b-a7e5-4014f7123abc",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
```

```
  "recipientAccountId": "111122223333"
}
```

Example ：UpdateProbationAutoCancellation 的日誌項目

以下範例顯示 UpdateProbationAutoCancellation 動作的 CloudTrail 日誌項目。

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE"
  },
  "eventTime": "2021-01-07T23:28:43Z",
  "eventSource": "support-subscription.amazonaws.com",
  "eventName": "UpdateProbationAutoCancellation",
  "awsRegion": "us-east-1", "sourceIPAddress": "100.127.8.67",
  "userAgent": "AWS-SupportPlansConsole, aws-internal/3",
  "requestParameters": {
    "lang": "en"
  },
  "responseElements": null,
  "requestID": "5492206a-e200-4c33-9fcf-4162d4123abc",
  "eventID": "f4a58c09-0bb0-4ba2-a8d3-df6909123abc",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```

Example ：UpdateSupportLevel 的日誌項目

以下範例顯示用於變更為開發人員支援的 UpdateSupportLevel 動作之 CloudTrail 日誌項目。

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
```

```
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-01-07T22:08:05Z"
      }
    }
  },
  "eventTime": "2021-01-07T22:08:43Z",
  "eventSource": "support-subscription.amazonaws.com",
  "eventName": "UpdateSupportLevel",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "100.127.8.247",
  "userAgent": "AWS-SupportPlansConsole, aws-internal/3",
  "requestParameters": {
    "supportLevel": "new_developer"
  },
  "responseElements": {
    "aispl": false,
    "supportLevel": "new_developer"
  },
  "requestID": "5df3da3a-61cd-4a3c-8f41-e5276b123abc",
  "eventID": "c69fb149-c206-47ce-8766-8df6ec123abc",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```

AWS Trusted Advisor 的監控和日誌記錄

監控是維護 Trusted Advisor 及其他 AWS 解決方案的可靠性、可用性和效能的重要部分。AWS 提供以下監控工具，可讓您監看 Trusted Advisor、在發現錯誤時回報，並適時採取自動動作。

- Amazon EventBridge 可傳送近乎即時的系統事件串流，以說明 AWS 資源發生的變動。EventBridge 啟用自動的事件驅動運算，因為您可以在這些事件發生時，編寫監看特定事件與在其他 AWS 服務內觸發自動化動作的規則。

  例如，Trusted Advisor 提供 Simple Storage Service (Amazon S3) 儲存貯體許可檢查。此檢查會識別您是否具有儲存貯體，其帶有開放存取權許可，或允許存取任何已驗證的 AWS 使用者。如果儲存貯體許可有所變化，Trusted Advisor 檢查的狀態就會變更。EventBridge 會偵測到此事件，然後傳送通知給您，方便您採取動作。如需詳細資訊，請參閱《Amazon EventBridge 使用者指南》。
- AWS Trusted Advisor 檢查會為您找出方法以降低成本、提升效能，並改善 AWS 帳戶的安全性。您可以使用 EventBridge 來監控 Trusted Advisor 檢查的狀態。接著您可以使用 Amazon CloudWatch，對 Trusted Advisor 指標建立警示。這些警示會在 Trusted Advisor 檢查的狀態變更時通知您，例如已更新資源或已達到服務配額。
- AWS CloudTrail 擷取您 AWS 帳戶發出或代表發出的 API 呼叫和相關事件，並傳送記錄檔案至您指定的 Simple Storage Service (Amazon S3) 儲存貯體。您可以找出哪些使用者和帳戶呼叫 AWS、發出呼叫的來源 IP 地址，以及呼叫的發生時間。如需詳細資訊，請參閱《AWS CloudTrail 使用者指南》。

主題

使用 Amazon 監控AWS Trusted Advisor檢查結果 EventBridge

您可以使用 EventBridge 來偵測何時檢查Trusted Advisor變更狀態。然後，根據您建立的規則，當狀態變更為您在規則中指定的值時， EventBridge 叫用一或多個目標動作。

根據狀態變更，您可以傳送通知、擷取狀態資訊，採取修正動作、啟動事件，或採取其他動作。例如，如果檢查狀態從未偵測到問題 (綠色) 變更為推薦的動作 (紅色)，則可指定以下目標類型。

- 使用 AWS Lambda 函數將通知傳送到 Slack 通道。

- 將有關檢查的資料推送到 Amazon Kinesis 串流，以支援完整且即時的狀態監控。
- 向您的電子郵件傳送 Amazon Simple Notification Service 主題。
- 通過 Amazon CloudWatch 警報操作獲得通知。

如需有關如何使用 EventBridge Lambda 函數來自動化回應的詳細資訊Trusted Advisor，請參閱 Trusted Advisor GitHub.

> **備註**
>
> - Trusted Advisor 會全力傳遞事件。並未始終保證將事件傳遞至 EventBridge。
> - 您必須具備 Business、Enterprise On-Ramp 或 Enterprise AWS Support 計畫才能建立 Trusted Advisor 檢查的規則。如需詳細資訊，請參閱變更 AWS Support 計劃。
> - Trusted Advisor就像全球服務一樣，所有事件都會 EventBridge 在美國東部 (維吉尼亞北部) 區域發出。

遵循此程序來建立的 EventBridge 規則Trusted Advisor。在您建立事件規則之前，請執行下列動作：

- 熟悉中的事件、規則和目標。 EventBridge如需詳細資訊，請參閱什麼是 Amazon EventBridge？ 在 Amazon 用 EventBridge 戶指南。
- 建立您將在事件規則中使用的目標。

若要建立 EventBridge 規則 Trusted Advisor

1. 在以下位置打開 Amazon EventBridge 控制台 https://console.aws.amazon.com/events/。
2. 若要變更區域，請使用頁面右上角的區域選擇器，然後選擇美國東部 (維吉尼亞北部)。
3. 在導覽窗格中，選擇 Rules(規則)。
4. 選擇 Create rule (建立規則)。
5. 在 Define rule detail (定義規則詳細資訊) 頁面中，輸入規則名稱和描述。
6. 請保留 Event bus (事件匯流排) 和 Rule type (規則類型) 的預設值，然後選擇 Next (下一步)。
7. 在 [建立事件模式] 頁面上，針對 [事件來源] 選擇AWS事件或 EventBridge 合作夥伴事件。
8. 在 Event pattern (事件模式) 下，保留 AWS 服務 的預設值。
9. 針對 AWS 服務，選擇 Trusted Advisor。

10. 對於 Event type (事件類型)，選擇 Check Item Refresh Status (檢查項目重新整理狀態)。
11. 針對檢查狀態，請選擇下列其中一個選項：
    - 選擇 Any status (任何狀態)，以建立監控任何狀態變更的規則。
    - 選擇 Specific status(es) (具體狀態)，然後選擇您希望要監控規則的值。
      - ERROR (錯誤) – Trusted Advisor 建議針對檢查執行的動作。
      - INFO (資訊) – Trusted Advisor 無法判斷檢查的狀態。
      - OK (正常) – Trusted Advisor 沒有偵測到檢查有問題。
      - WARN (警告)– Trusted Advisor 針對到可能的檢查問題，並建議調查。
12. 針對檢查，請選擇下列其中一個選項：
    - 選擇 Any check (任何檢查)。
    - 選擇 Specific check(s) (特定檢查)，然後從清單中選擇一個或多個檢查名稱。
13. 針對 AWS 資源，請選擇下列其中一個選項：
    - 選擇 Any resource ID (任何資源 ID)，以建立監控所有資源的規則。
    - 選擇 Specific resource ID(s) by ARN (依 ARN 列出的特定資源 ID)，然後輸入您需要的 Amazon 資源名稱 (ARN)。
14. 選擇 下一步。
15. 在 Select target(s) (選取目標) 區段中，選擇您為此規則建立的目標類型，然後設定該類型所需的任何其他選項。例如，您可能會將事件匯流排傳送至 Amazon SQS 佇列或 Amazon SNS 主題。
16. 選擇 下一步。
17. (選用) 在 設定標籤頁面，新增任何標籤，然後選擇下一步。
18. 在檢閱並建立頁面上，檢閱您的規則設定，並確定其符合您的事件監控要求。
19. 選擇 Create rule (建立規則)。您的規則現在將監控 Trusted Advisor 檢查，然後將事件傳送至您指定的目標。

建立 Amazon CloudWatch 警示來監控 AWS Trusted Advisor 指標

AWS Trusted Advisor 重新整理檢查時，Trusted Advisor 會將有關檢查結果的指標發佈至 CloudWatch。您可以在 CloudWatch 中檢視這些指標。您也可以建立警示，偵測資源和服務配額使用量 (先前稱為限額) 的 Trusted Advisor 檢查和狀態變更。例如，您可以建立警示，追蹤 Service Limits (服務配額) 類別中檢查的狀態變更。您達到或超過 AWS 帳戶的服務配額時，警示就會通知您。

依照此程序操作，針對特定 Trusted Advisor 指標建立 CloudWatch 警示。

主題

先決條件

為 Trusted Advisor 指標建立 CloudWatch 警示之前，請先檢閱下列資訊：

- 瞭解 CloudWatch 如何使用指標和警示。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的 CloudWatch 的運作方式。
- 使用 Trusted Advisor 主控台或 AWS Support API 來重新整理檢查並取得最新的檢查結果。如需詳細資訊，請參閱 重新整理檢查結果。

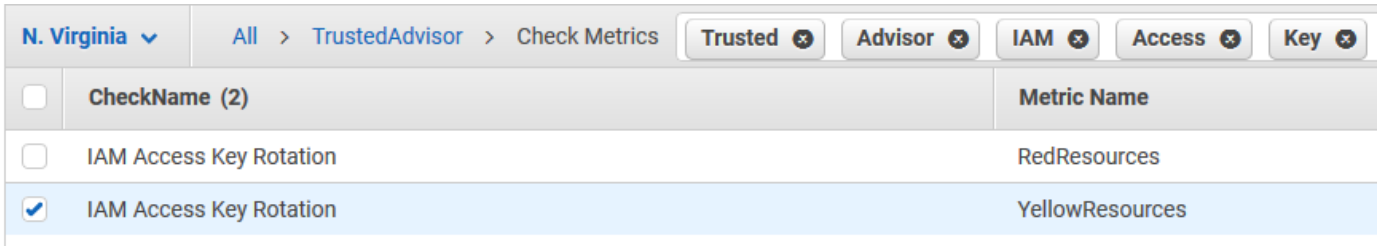
為 Trusted Advisor 指標建立 CloudWatch 警示

1. 在 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
2. 使用 Region selector (區域選擇器)，選擇 US East (N. Virginia)美國東部 (維吉尼亞北部)) AWS 區域。
3. 在導覽窗格中，選擇 Alarms (警示)。
4. 選擇建立警示。
5. 選擇 Select metric (選取指標)。
6. 針對 Metrics (指標)，輸入一或多個維度值來篩選指標清單。例如，您可以輸入指標名稱 ServiceLimitUsage，也可輸入維度，例如 Trusted Advisor 檢查名稱。

   > **Tip**
   >
   > - 您可以搜尋 **`Trusted Advisor`** 以列出服務的所有指標。
   > - 如需指標及維度的清單，請參閱「Trusted Advisor 指標與維度」。

7. 在結果表格中，選取該指標的核取方塊。

   在下列範例中，檢查名稱為 IAM 存取金鑰輪換，而指標名稱為 YellowResources。

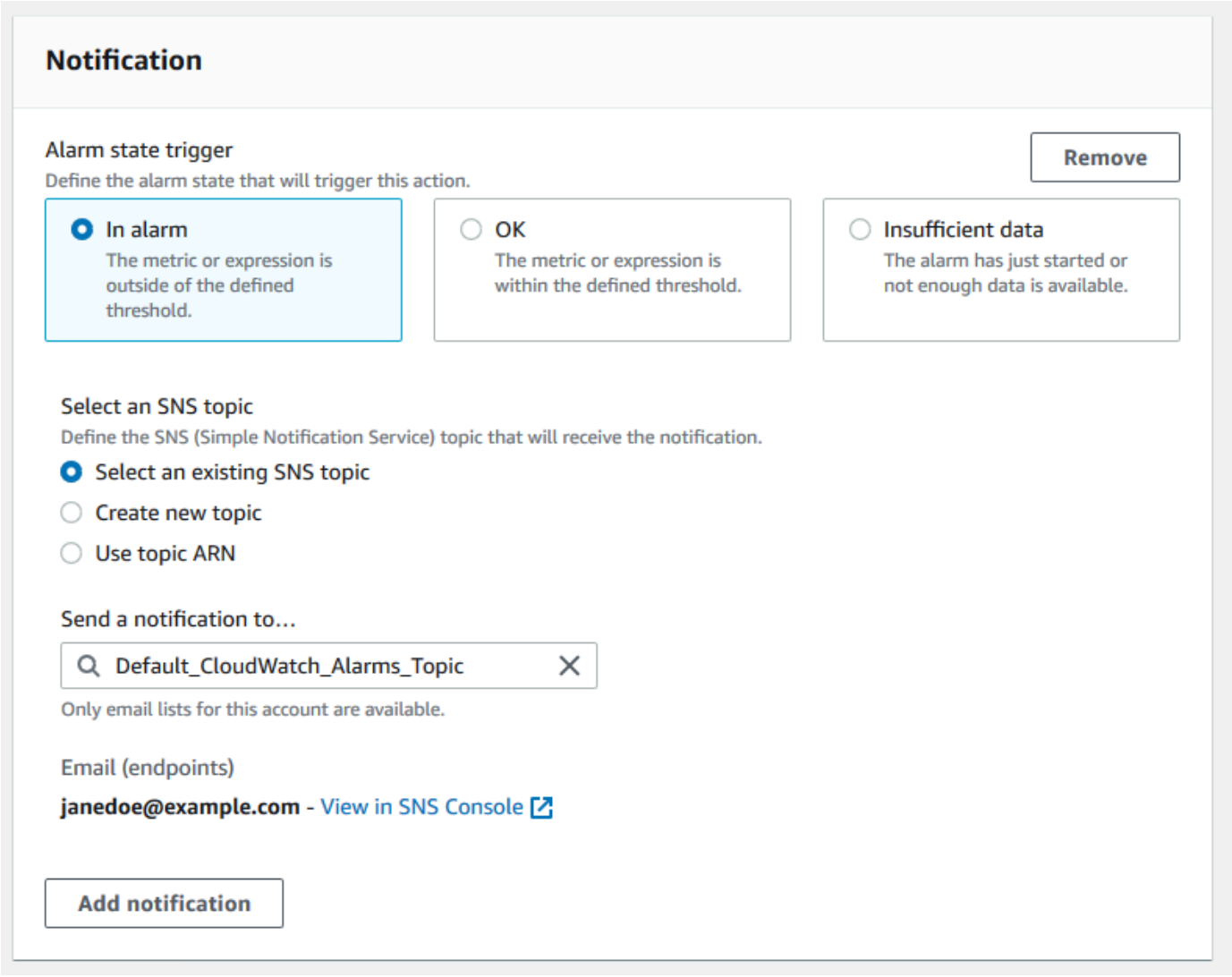


8. 選擇 Select metric (選取指標)。
9. 在 Specify metric and conditions (指定指標和條件) 頁面上，確認 Metric name (指標名稱) 和 CheckName 有顯示在頁面上。
10. 針對 Period (期間)，您可以指定檢查狀態變更時要啟動警示的期間，例如 5 分鐘。
11. 在 Conditions (條件) 底下，選擇 Static (靜態)，然後指定應啟動警示的警示條件。

    例如，如果您選擇 Greater/Equal >=threshold (大於/等於 >= 閾值)，然後輸入 **1** 閾值，就表示 Trusted Advisor 偵測到至少一個 IAM 存取金鑰在過去 90 天內未輪換時，警示就會啟動。

    > **備註**
    >
    > - 對於 GreenChecks、RedChecks、YellowChecks、RedResources 和 YellowResources 指標，您指定的閾值可以是大於或等於零的任何整數。
    > - Trusted Advisor 不會傳送 GreenResources 的指標，這些是 Trusted Advisor 未偵測到任何問題的資源。

12. 選擇 Next (下一步)。
13. 在 Configure actions (設定動作) 頁面上，為 Alarm state trigger (警示狀態觸發) 選擇 In alarm (警示中)。
14. 在 Select an SNS topic (選取 SNS 主題) 中，選擇現有的 Amazon Simple Notification Service (Amazon SNS) 主題，或建立一個主題。



15. 選擇 Next (下一步)。
16. 在 Name and description (名稱和描述) 中，輸入警示的名稱和描述。
17. 選擇 Next (下一步)。
18. 在 Preview and create (預覽並建立) 頁面上，檢閱您的警示詳細資訊，然後選擇 Create alarm (建立警示)。

    當 IAM 存取金鑰輪換檢查的狀態變為紅色 5 分鐘，警示會傳送通知至您的 SNS 主題。

Example ：CloudWatch 警示的電子郵件通知

下列電子郵件訊息顯示警示偵測到 IAM 存取金鑰輪換檢查有所變化。

```
You are receiving this email because your Amazon CloudWatch Alarm
 "IAMAcessKeyRotationCheckAlarm" in the US East (N. Virginia) region has entered the
 ALARM state,
because "Threshold Crossed: 1 out of the last 1 datapoints [9.0 (26/03/21 22:44:00)]
 was greater than or equal to the threshold (1.0) (minimum 1 datapoint for OK -> ALARM
 transition)." at "Friday 26 March, 2021 22:49:42 UTC".

View this alarm in the AWS Management Console:
https://us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-
east-1#s=Alarms&alarm=IAMAcessKeyRotationCheckAlarm

Alarm Details:
- Name:                       IAMAcessKeyRotationCheckAlarm
- Description:                This alarm starts when one or more AWS access keys in my
 AWS account have not been rotated in the last 90 days.
- State Change:               INSUFFICIENT_DATA -> ALARM
- Reason for State Change:    Threshold Crossed: 1 out of the last 1 datapoints [9.0
 (26/03/21 22:44:00)] was greater than or equal to the threshold (1.0) (minimum 1
 datapoint for OK -> ALARM transition).
- Timestamp:                  Friday 26 March, 2021 22:49:42 UTC
- AWS Account:                123456789012
- Alarm Arn:                  arn:aws:cloudwatch:us-
east-1:123456789012:alarm:IAMAcessKeyRotationCheckAlarm

Threshold:
- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 1.0
 for 300 seconds.

Monitored Metric:
- MetricNamespace:                    AWS/TrustedAdvisor
- MetricName:                         RedResources
- Dimensions:                         [CheckName = IAM Access Key Rotation]
- Period:                             300 seconds
- Statistic:                          Average
- Unit:                               not specified
- TreatMissingData:                   missing


State Change Actions:
- OK:
- ALARM: [arn:aws:sns:us-east-1:123456789012:Default_CloudWatch_Alarms_Topic]
- INSUFFICIENT_DATA:
```

Trusted Advisor 的 CloudWatch 指標

您可以使用 CloudWatch 主控台或 AWS Command Line Interface(AWS CLI) 尋找 Trusted Advisor 可用的指標。

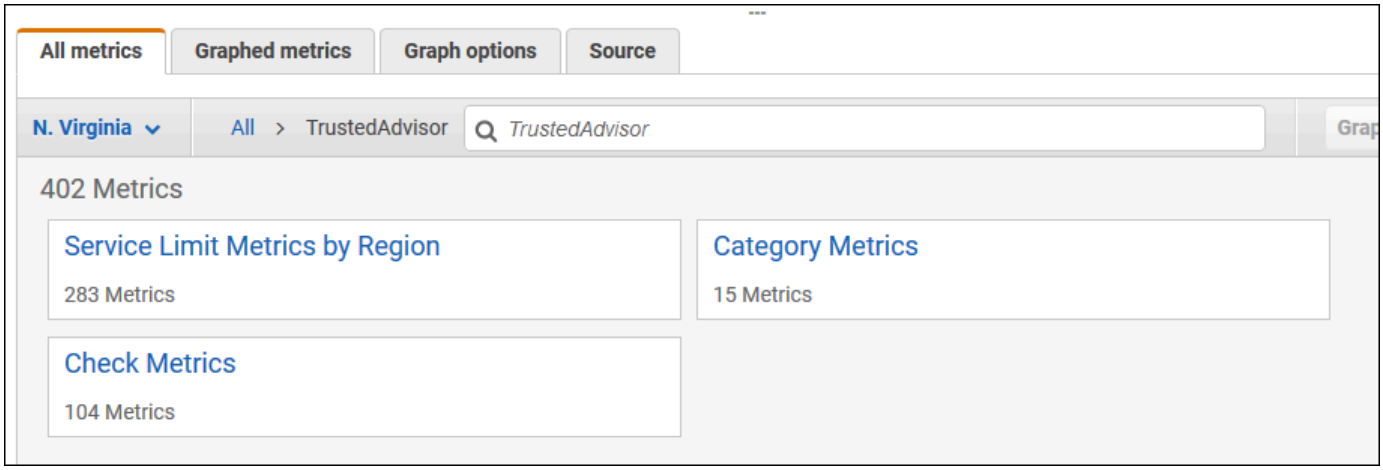
如需發佈指標的所有服務之命名空間、指標和維度清單，請參閱 Amazon CloudWatch 使用者指南中的發佈 CloudWatch 指標的 AWS 服務。

檢視 Trusted Advisor 指標 (主控台)

您可以登入 CloudWatch 主控台並檢視 Trusted Advisor 可用的指標。

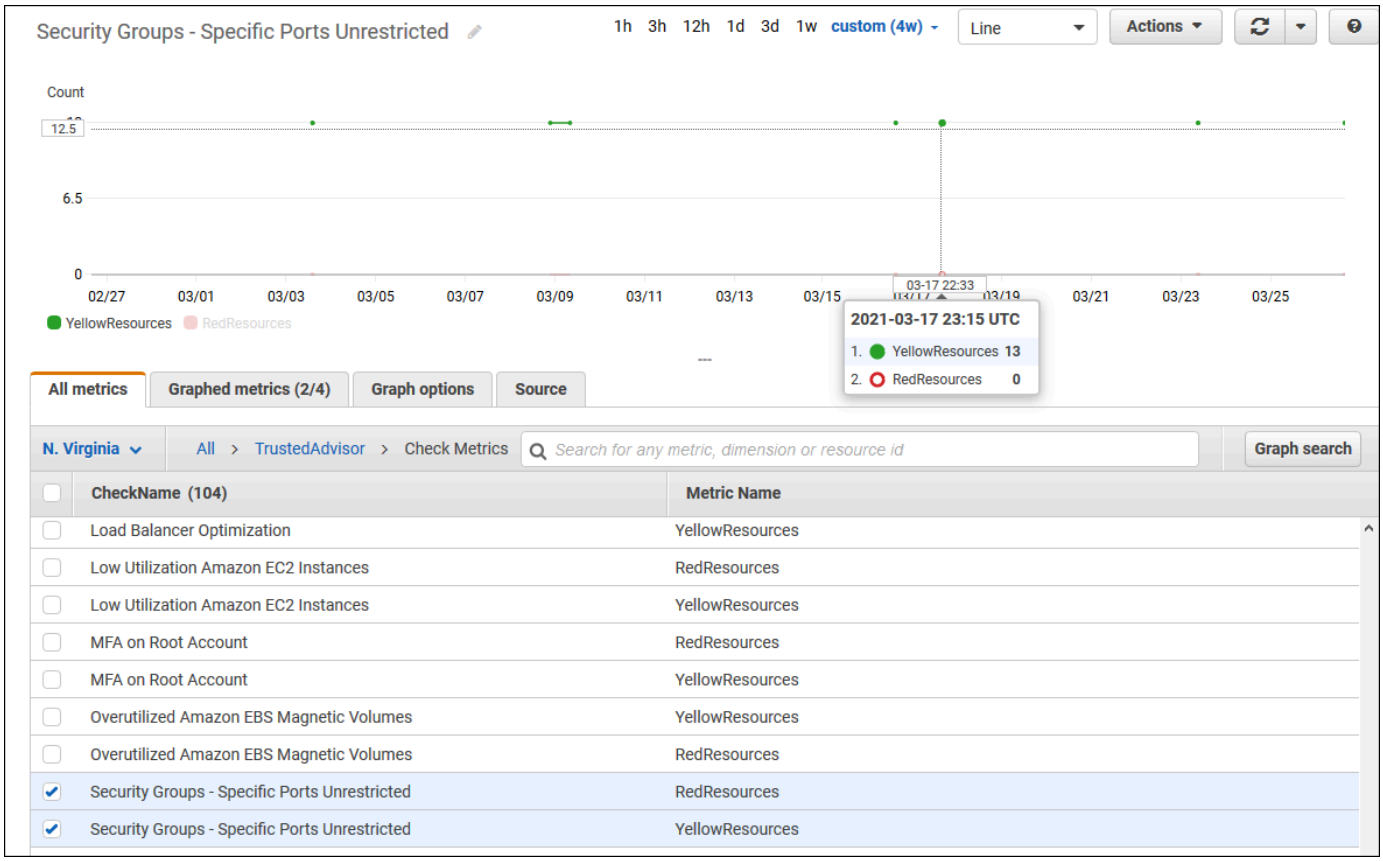
檢視可用的 Trusted Advisor 指標 (主控台)

1. 在 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
2. 使用 Region selector (區域選擇器)，選擇 US East (N. Virginia)美國東部 (維吉尼亞北部)) AWS 區域。
3. 在導覽窗格中，選擇 Metrics (指標)。
4. 輸入指標命名空間，例如 **`TrustedAdvisor`**。
5. 選擇指標維度，例如 Check Metrics (檢查指標)。



6. All metrics (所有指標) 索引標籤會顯示命名空間中該維度的指標。您可以執行下列作業：
   a. 若要將表格排序，請選擇直欄標題。
   b. 若要將指標圖形化，請勾選指標旁的核取方塊。若要選擇所有指標，請勾選表格標題列中的核取方塊。
   c. 若要依指標篩選，請選擇指標名稱，然後選擇 Add to search (新增至搜尋)。

下列範例顯示安全性群組 - 不受限制的特定連接埠檢查的結果。這項檢查識別出 13 個黃色的資源。Trusted Advisor 建議您對黃色的檢查進行調查。



7. (選用) 若要將此圖表新增至 CloudWatch 儀表板，請選擇 Actions (動作)，然後選擇 Add to dashboard (新增至儀表板)。

   如需建立圖表以檢視指標的詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的建立指標圖表。

檢視 Trusted Advisor 指標 (CLI)

您可以使用 list-metrics AWS CLI 命令來檢視 Trusted Advisor 可用的指標。

Example ：列出 Trusted Advisor 的所有指標

以下範例指定 `AWS/TrustedAdvisor` 命名空間，用於檢視 Trusted Advisor 的所有指標。

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor
```

輸出看起來應該類似以下內容。

```
{
    "Metrics": [
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "EBS"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Magnetic (standard) volume storage (TiB)"
                },
                {
                    "Name": "Region",
                    "Value": "ap-northeast-2"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Overutilized Amazon EBS Magnetic Volumes"
                }
            ],
            "MetricName": "YellowResources"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "EBS"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Provisioned IOPS"
                },
                {
```

```
                    "Name": "Region",
                    "Value": "eu-west-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "EBS"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Provisioned IOPS"
                },
                {
                    "Name": "Region",
                    "Value": "ap-south-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
    ...
  ]
}
```

Example ：列出一個維度的所有指標

以下範例指定 AWS/TrustedAdvisor 命名空間和 Region 維度，用於檢視指定 AWS 區域可用的指標。

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor --dimensions
 Name=Region,Value=us-east-1
```

輸出看起來應該類似以下內容。

```
{
    "Metrics": [
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
```

```
                {
                    "Name": "ServiceName",
                    "Value": "SES"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Daily sending quota"
                },
                {
                    "Name": "Region",
                    "Value": "us-east-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "AutoScaling"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Launch configurations"
                },
                {
                    "Name": "Region",
                    "Value": "us-east-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "CloudFormation"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Stacks"
                },
```

```
                {
                    "Name": "Region",
                    "Value": "us-east-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
    ...
  ]
}
```

Example ：列出特定指標名稱的指標

以下範例指定 AWS/TrustedAdvisor 命名空間和 RedResources 指標名稱，用於僅檢視此指定指標的結果。

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor --metric-name RedResources
```

輸出看起來應該類似以下內容。

```
{
    "Metrics": [
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Amazon RDS Security Group Access Risk"
                }
            ],
            "MetricName": "RedResources"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Exposed Access Keys"
                }
            ],
            "MetricName": "RedResources"
        },
```

```
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Large Number of Rules in an EC2 Security Group"
                }
            ],
            "MetricName": "RedResources"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Auto Scaling Group Health Check"
                }
            ],
            "MetricName": "RedResources"
        },
    ...
  ]
}
```

Trusted Advisor 指標與維度

請參閱下表，查看可用於 CloudWatch 警示和圖表的 Trusted Advisor 指標和維度。

Trusted Advisor 檢查層級指標

您可以為 Trusted Advisor 檢查使用下列指標。

指標	描述
RedResources	處於紅色狀態的資源數目 (建議採取動作)。
YellowResources	處於黃色狀態的資源數目 (建議進行調查)。

Trusted Advisor 類別層級指標

您可以為 Trusted Advisor 類別使用下列指標。

指標	描述
GreenChecks	處於綠色狀態的 Trusted Advisor 檢查數量 (未偵測到任何問題)。
RedChecks	處於紅色狀態的 Trusted Advisor 檢查數量 (建議採取動作)。
YellowChecks	處於黃色狀態的 Trusted Advisor 檢查數量 (建議進行調查)。

Trusted Advisor 服務配額層級指標

您可以為 AWS 服務 quotas 使用下列指標。

指標	描述
ServiceLimitUsage	針對服務配額 (先前稱為限額) 的資源使用量百分比。

檢查層級指標的維度

您可以為 Trusted Advisor 檢查使用下列維度。

維度	描述
CheckName	Trusted Advisor 檢查的名稱。 您可以在 Trusted Advisor主控台或 AWS Trusted Advisor 檢查參考中查看所有檢查名稱。

類別層級指標的維度

您可以為 Trusted Advisor 檢查類別使用下列維度。

維度	描述
Category	Trusted Advisor 檢查類別的名稱。

維度	描述
	您可以在 Trusted Advisor主控台或 檢視檢查類別 頁面上查看所有檢查類別。

服務配額指標的維度

您可以為 Trusted Advisor 服務配額指標使用下列維度。

維度	描述
`Region`	Service quotas 的 AWS 區域。
`ServiceName`	AWS 服務 的名稱。
`ServiceLimit`	服務配額的名稱。 如需有關服務配額的詳細資訊，請參閱《AWS 一般參考》中的 AWS 服務 配額。

使用 AWS CloudTrail 記錄 AWS Trusted Advisor 主控台動作

Trusted Advisor與 (提供中的使用者AWS CloudTrail、角色或服務所採取的動作記錄) 的AWS服務整合Trusted Advisor。 CloudTrail 擷取作Trusted Advisor為事件的動作。擷取的呼叫包括來自 Trusted Advisor 主控台的呼叫。如果您建立追蹤，您可以啟用持續交付 CloudTrail 事件到 Amazon Simple Storage Service (Amazon S3) 儲存貯體，包括Trusted Advisor. 如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。使用收集的資訊 CloudTrail，您可以判斷提出的要求Trusted Advisor、提出要求的 IP 位址、提出要求的人員、提出要求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，包括如何設定和啟用它，請參閱AWS CloudTrail使用者指南。

Trusted Advisor中的資訊 CloudTrail

CloudTrail 在您創建AWS帳戶時，您的帳戶已啟用。當Trusted Advisor主控台中發生受支援的事件活動時，該活動會與 CloudTrail 事件歷史記錄中的其他AWS服務事件一起記錄在事件中。您可以檢視、搜尋和下載 AWS 帳戶的最新事件。如需詳細資訊，請參閱檢視具有事 CloudTrail 件記錄的事件。

如需您 AWS 帳戶中正在進行事件的記錄 (包含 Trusted Advisor 的事件)，請建立線索。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。根據預設，當您在主控台建立線索時，線索會套用到所有 AWS 區域。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 Amazon S3 儲存貯體。此外，您還可以設定其他AWS服務，以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱下列內容：

- 建立系統線概述
- CloudTrail 支援的服務與整合
- 設定的 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 記錄檔並從多個帳戶接收 CloudTrail記錄檔

Trusted Advisor支援將Trusted Advisor主控台動作的子集記錄為記 CloudTrail 錄檔中的事件。CloudTrail 會記錄下列動作：

- `CreateEngagement`
- `CreateEngagementAttachment`
- `CreateEngagementCommunication`
- `CreateExcelReport`
- `DescribeAccount`
- `DescribeAccountAccess`
- `DescribeCheckItems`
- `DescribeCheckRefreshStatuses`
- `DescribeCheckSummaries`
- `DescribeChecks`
- `DescribeNotificationPreferences`
- `DescribeOrganization`
- `DescribeOrganizationAccounts`
- `DescribeReports`
- `DescribeServiceMetadata`
- `ExcludeCheckItems`
- `GenerateReport`

- GetEngagement
- GetEngagementAttachment
- GetEngagementType
- GetExcelReport
- GetOrganizationRecommendation
- GetRecommendation
- IncludeCheckItems
- ListAccountsForParent
- ListChecks
- ListEngagementCommunications
- ListEngagementTypes
- ListEngagements
- ListOrganizationRecommendationAccounts
- ListOrganizationRecommendationResources
- ListOrganizationRecommendations
- ListOrganizationalUnitsForParent
- ListRecommendationResources
- ListRecommendations
- ListRoots
- RefreshCheck
- SetAccountAccess
- SetOrganizationAccess
- UpdateEngagement
- UpdateEngagementStatus
- UpdateNotificationPreferences
- UpdateOrganizationRecommendationLifecycle
- UpdateRecommendationLifecycle

如需完整的 Trusted Advisor 主控台動作清單，請參閱「Trusted Advisor 動作」。

> **Note**
>
> CloudTrail 還將 Trusted Advisor API 操作記錄在 AWS SupportAPI 參考中。如需詳細資訊，請參閱 使用 AWS CloudTrail 記錄 AWS Support API 呼叫。

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：

- 該請求是否透過根或 AWS Identity and Access Management (IAM) 使用者憑證來提出。
- 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 userIdentity 元素。

範例：Trusted Advisor 日誌檔案項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。事件代表來自任何來源的單一請求，包括有關請求的操作，動作的日期和時間，請求參數等信息。 CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

Example ：的記錄項目 RefreshCheck

下列範例顯示示範 Amazon S3 儲存貯體版本控制檢查 (IDR365s2Qddf) `RefreshCheck` 動作的 CloudTrail 日誌項目。

```
{
        "eventVersion":"1.04",
        "userIdentity":{
        "type":"IAMUser",
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/janedoe",
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "userName":"janedoe",
        "sessionContext":{
        "attributes":{
        "mfaAuthenticated":"false",
        "creationDate":"2020-10-21T22:06:18Z"
        }
```

```
        }
        },
        "eventTime":"2020-10-21T22:06:33Z",
        "eventSource":"trustedadvisor.amazonaws.com",
        "eventName":"RefreshCheck",
        "awsRegion":"us-east-1",
        "sourceIPAddress":"100.127.34.136",
        "userAgent":"signin.amazonaws.com",
        "requestParameters":{
        "checkId":"R365s2Qddf"
        },
        "responseElements":{
        "status":{
        "checkId":"R365s2Qddf",
        "status":"enqueued",
        "millisUntilNextRefreshable":3599993
        }
        },
        "requestID":"d23ec729-8995-494c-8054-dedeaEXAMPLE",
        "eventID":"a49d5202-560f-4a4e-b38a-02f1cEXAMPLE",
        "eventType":"AwsApiCall",
        "recipientAccountId":"123456789012"
        }
```

Example ：的記錄項目 UpdateNotificationPreferences

下列範例顯示示範UpdateNotificationPreferences動作的 CloudTrail 記錄項目。

```
{
        "eventVersion":"1.04",
        "userIdentity":{
        "type":"IAMUser",
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/janedoe",
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "userName":"janedoe",
        "sessionContext":{
        "attributes":{
        "mfaAuthenticated":"false",
        "creationDate":"2020-10-21T22:06:18Z"
        }
        }
```

```
        },
        "eventTime":"2020-10-21T22:09:49Z",
        "eventSource":"trustedadvisor.amazonaws.com",
        "eventName":"UpdateNotificationPreferences",
        "awsRegion":"us-east-1",
        "sourceIPAddress":"100.127.34.167",
        "userAgent":"signin.amazonaws.com",
        "requestParameters":{
        "contacts":[
        {
        "id":"billing",
        "type":"email",
        "active":false
        },
        {
        "id":"operational",
        "type":"email",
        "active":false
        },
        {
        "id":"security",
        "type":"email",
        "active":false
        }
        ],
        "language":"en"
        },
        "responseElements":null,
        "requestID":"695295f3-c81c-486e-9404-fa148EXAMPLE",
        "eventID":"5f923d8c-d210-4037-bd32-997c6EXAMPLE",
        "eventType":"AwsApiCall",
        "recipientAccountId":"123456789012"
        }
```

Example ：的記錄項目 GenerateReport

下列範例顯示示範`GenerateReport`動作的 CloudTrail 記錄項目。此動作會為您的 AWS 組織建立報告。

```
{
        "eventVersion":"1.04",
        "userIdentity":{
```

```
        "type":"IAMUser",
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/janedoe",
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "userName":"janedoe",
        "sessionContext":{
        "attributes":{
        "mfaAuthenticated":"false",
        "creationDate":"2020-11-03T13:03:10Z"
        }
        }
        },
        "eventTime":"2020-11-03T13:04:29Z",
        "eventSource":"trustedadvisor.amazonaws.com",
        "eventName":"GenerateReport",
        "awsRegion":"us-east-1",
        "sourceIPAddress":"100.127.36.171",
        "userAgent":"signin.amazonaws.com",
        "requestParameters":{
        "refresh":false,
        "includeSuppressedResources":false,
        "language":"en",
        "format":"JSON",
        "name":"organizational-view-report",
        "preference":{
        "accounts":[

        ],
        "organizationalUnitIds":[
        "r-j134"
        ],
        "preferenceName":"organizational-view-report",
        "format":"json",
        "language":"en"
        }
        },
        "responseElements":{
        "status":"ENQUEUED"
        },
        "requestID":"bb866dc1-60af-47fd-a660-21498EXAMPLE",
        "eventID":"2606c89d-c107-47bd-a7c6-ec92fEXAMPLE",
        "eventType":"AwsApiCall",
        "recipientAccountId":"123456789012"
```

```
        }
```

疑難排解資源

如需常見疑難排解問題的答案，請參閱 AWS Support 知識中心。

對於 Windows，Amazon EC2 提供 EC2Rescue，客戶可以使用它們來檢查其 Windows 執行個體，以協助識別常見問題、收集記錄檔，並協助您 AWS Support 解決問題。您也可以使用 EC2Rescue 來分析無法運作之執行個體的啟動磁碟區。如需詳細資訊，請參閱「如何使用 EC2Rescue 進行疑難排解及修正 EC2 Windows 執行個體的常見問題？」

服務特定疑難排解

大多數 AWS 服務 文檔包含疑難排解主題，可以幫助您在聯繫之前開始 AWS Support。下表提供疑難排解主題連結 (以服務分類)。

> **Note**
>
> 下表列出最常見的服務。若要搜尋其他疑難排解主題，請使用 AWS 文件登陸頁面上的搜尋文字方塊。

服務	連結
Amazon Web Services	疑難排解 AWS 簽章版本 4 錯誤
Amazon API Gateway	疑難排解 HTTP API 問題
Amazon AppStream	Amazon 疑難 AppStream
Amazon Athena	疑難排解 Athena
Amazon Aurora MySQL	疑難排解 Amazon Aurora
Amazon Aurora PostgreSQL	疑難排解 Amazon Aurora
Amazon EC2 Auto Scaling	疑難排解 Auto Scaling
AWS Certificate Manager (ACM)	疑難排解

服務	連結
AWS CloudFormation	疑難排解 AWS CloudFormation
Amazon CloudFront	疑難排解 | RTMP 分佈的疑難排解
AWS CloudHSM	疑難排解
Amazon CloudSearch	Amazon 故障 CloudSearch
AWS CodeDeploy	疑難排解 AWS CodeDeploy
Amazon CloudWatch	疑難排解
AWS Database Migration Service	疑難排解移轉工作 AWS Database Migration Service
AWS Data Pipeline	疑難排解
AWS Direct Connect	疑難排解 AWS Direct Connect
AWS Directory Service	排解 AWS Directory Service 管理問題
Amazon DynamoDB	疑難排解 | 疑難排解 SSL/TLS 連線建立問題
AWS Elastic Beanstalk	疑難排解
Amazon Elastic Compute Cloud (Amazon EC2)	疑難排解執行個體 | 疑難排解 Windows 執行個體 | 疑難排解 VM Import/Export | 疑難排解 API 請求錯誤 | 疑難排解 AWS Management Pack | 針對 Microsoft SCVMM 疑難排解 AWS Systems Manager | 適用於 Microsoft Windows Server 的AWS 診斷
Amazon Elastic Container Service (Amazon ECS)	Amazon ECS 疑難排解
Amazon Elastic Kubernetes Service (Amazon EKS)	疑難排解 Amazon EKS
Elastic Load Balancing	疑難排解您的 Application Load Balancer | 疑難排解您的 Classic Load Balancer

服務	連結
Amazon ElastiCache	對應用程式進行疑難排解
Amazon ElastiCache 的雷迪斯	對應用程式進行疑難排解
Amazon EMR	對叢集進行疑難排解
AWS Flow Framework	疑難排解和偵錯秘訣
AWS Glue	疑難排解 AWS Glue
AWS Glue DataBrew	在 AWS Glue DataBrew中對身分與存取進行疑難排解
AWS GovCloud (US)	疑難排解
AWS Identity and Access Management (IAM)	疑難排解 IAM
Amazon Keyspaces (適用於 Apache Cassandra)	疑難排解 Amazon Keyspaces (適用於 Apache Cassandra)
Amazon Kinesis Data Streams	疑難排解 Amazon Kinesis Data Streams 產生者 | 疑難排解 Amazon Kinesis Data Streams 取用者
Amazon Managed Service for Apache Flink	疑難排解效能 | 疑難排解適用於 SQL 應用程式的 Amazon Managed Service for Apache Flink
Amazon 數據 Firehose	Amazon 數據 Firehose 故障
AWS Lambda	故障排除和監控 AWS Lambda 功能 CloudWatch
Amazon OpenSearch 服務	Amazon OpenSearch 服務故障
AWS OpsWorks	偵錯和疑難排解指南
Amazon Personalize	疑難排解
Amazon QLDB	疑難排解 Amazon QLDB
Amazon QuickSight	疑難排解 Amazon QuickSight | 疑難排解略過的列錯

服務	連結
AWS Resource Access Manager (AWS RAM)	使用 AWS RAM來疑難排解問題
Amazon Redshift	疑難排解查詢 | 疑難排解資料載入 | 疑難排解 Amazon Redshift 中的連線問題 | 疑難排解 Amazon Redshift 稽核日誌 | 疑難排解 Amazon Redshift Spectrum 中的查詢
Amazon Relational Database Service (Amazon RDS)	疑難排解 | 疑難排解 Amazon RDS 上的應用程式 | 疑難排解 Amazon RDS Custom 資料庫問題
Amazon Route 53	疑難排解 Amazon Route 53
Amazon SageMaker	疑難排解錯誤 | 疑 Amazon 排 SageMaker 解
Amazon Silk	疑難排解
Amazon Simple Email Service (Amazon SES)	疑難排解 Amazon SES
Amazon Simple Storage Service (Amazon S3)	疑難排解
Amazon Simple Workflow Service (Amazon SWF)	AWS Java 的流程架構：疑難排解和偵錯秘訣 | Ruby 的AWS 流程架構：工作流程疑難排解和偵錯
AWS Storage Gateway	為您的閘道進行疑難排解
AWS Systems Manager	疑難排解 SSM Agent
Amazon Virtual Private Cloud (Amazon VPC)	疑難排解
AWS Virtual Private Network (AWS VPN)	疑難排解客戶閘道裝置
AWS WAF	測試和調整您的 AWS WAF 保護
Amazon WorkMail	疑難排解 Amazon WorkMail 網路應用

服務	連結
Amazon WorkSpaces	Amazon WorkSpaces 問題疑難排解 | 疑難排解 Amazon WorkSpaces 客戶

文件歷史紀錄

下表說明自上次發行 AWS Support 服務以來，文件的重要變更。

- AWS Support API 版本：2013-04-15
- AWS Support 應用程序接口版本：

下表說明自 2021 年 5 月 10 日起對 AWS Support 和說明 AWS Trusted Advisor 文件的重要更新。您現在可以訂閱 RSS 摘要，接收有關更新的通知。

變更	描述	日期
更新 AWSSupportServiceRolePolicy 的說明文件	新增了許可以針對服務連結角色提供計費、管理和支援服務。如需詳細資訊，請參閱AWS 受管政策：AWSSupportServiceRolePolicy。	2024年3月22日
更新的 AWS Support 計劃文件	AWS Support 計劃功能的更新。如需詳細資訊，請參閱 AWS Support 計劃。	2024年3月11日
更新的文檔 Trusted Advisor	新增 1 個容錯檢查。如需詳細資訊，請參閱變更 AWS Trusted Advisor 檢查記錄。	2024 年 2 月 29 日
更新的文檔 Trusted Advisor	新增 1 個容錯檢查。如需詳細資訊，請參閱變更 AWS Trusted Advisor 檢查記錄。	2024 年 1 月 31 日
更新 AWSTrustedAdvisorServiceRolePolicy 的說明文件	新增了新的 IAM 動作cloudtrail:GetTrail cloudtrail:ListTrails cloudtrail:GetEventSelectors 、outposts:GetOutpost 、outposts:ListAsset	2024年1月18日

	s 和加outposts: ListOutposts 入新的檢查。如需詳細資訊，請參閱AWS 受管政策：AWSTrustedAdvisorServiceRolePolicy。	
更新 AWSSupportServiceRolePolicy 的說明文件	新增了許可以針對服務連結角色提供計費、管理和支援服務。如需詳細資訊，請參閱AWS 受管政策：AWSSupportServiceRolePolicy。	2024年1月17日
更新的文檔 Trusted Advisor	更新了 1 個容錯檢查以修改標題和說明。如需詳細資訊，請參閱變更 AWS Trusted Advisor 檢查記錄。	2024 年 1 月 8 日
更新的文檔 Trusted Advisor	更新了 1 個安全檢查以反映棄用期的變化。如需詳細資訊，請參閱變更 AWS Trusted Advisor 檢查記錄。	2023 年 12 月 21 日
更新的文檔 Trusted Advisor	添加了 2 個安全檢查和 2 個性能檢查。如需詳細資訊，請參閱變更 AWS Trusted Advisor 檢查記錄。	2023 年 12 月 20 日
更新的文檔 Trusted Advisor	添加了 1 個安全檢查。如需詳細資訊，請參閱變更 AWS Trusted Advisor 檢查記錄。	2023 年 12 月 15 日
對於 Trusted Advisor 搞更新文檔	更新Trusted Advisor 搞文檔與電子郵件通知選項的變化。	2023 年 12 月 14 日
對於 Trusted Advisor 搞更新文檔	已更新 Trusted Advisor Engage 文件，其中包含排程參與的變更。	2023 年 12 月 11 日

更新的文檔 Trusted Advisor	增加了 2 個新的容錯檢查和 1 個成本優化檢查。如需詳細資訊，請參閱變更 AWS Trusted Advisor 檢查記錄。	2023 年 12 月 7 日
更新 AWSSupportServiceRolePolicy 的說明文件	新增了許可以針對服務連結角色提供計費、管理和支援服務。如需詳細資訊，請參閱AWS 受管政策：AWSSupportServiceRolePolicy。	2023 年 12 月 6 日
已更新的 AWS 受管政策 Trusted Advisor	更新AWSTrustedAdvisorPriorityFullAccess 和受AWSTrustedAdvisorPriorityReadOnlyAccess AWS 管理的政策以包含陳述式 ID。如需詳細資訊，請參閱 AWS Trusted Advisor的AWS 受管政策。	2023 年 12 月 6 日
更新的文檔 Trusted Advisor	增加了 3 個新的容錯檢查。如需詳細資訊，請參閱變更 AWS Trusted Advisor 檢查記錄。	2023 年 11 月 17 日
更新的文檔 Trusted Advisor	為 Amazon RDS 添加了 37 個新的檢查。如需詳細資訊，請參閱變更 AWS Trusted Advisor 檢查記錄。	2023 年 11 月 15 日

更新 AWSTrustedAdvisorServiceRolePolicy 的說明文件	添加了新的 IAM 操作 ec2:DescribeRegions s3:GetLifecycleConfiguration ，ecs:DescribeTaskDefinition 並加ecs:ListTaskDefinitions 入了新的檢查。如需詳細資訊，請參閱AWS 受管政策：AWSTrustedAdvisorServiceRolePolicy。	2023 年 11 月 9 日
更新 AWSSupportServiceRolePolicy 的說明文件	新增了許可以針對服務連結角色提供計費、管理和支援服務。如需詳細資訊，請參閱AWS 受管政策：AWSSupportServiceRolePolicy。	2023 年 10 月 27 日
更新的文檔 Trusted Advisor	增加了 64 個集成的新檢查 AWS Config。如需詳細資訊，請參閱變更 AWS Trusted Advisor 檢查記錄。	2023 年 10 月 26 日
更新的文檔 Trusted Advisor	增加了六個新的容錯檢查 Trusted Advisor。如需詳細資訊，請參閱變更記錄以取得 AWS Trusted Advisor 檢查。	2023 年 10 月 12 日

更新 AWSTrustedAdvisorServiceRolePolicy 的說明文件	新增了全新的 IAM 動作 route53resolver:ListResolverEndpoints 、route53resolver:ListResolverEndpointIpAddresses 、ec2:DescribeSubnets 、kafka:ListClustersV2 以及 kafka:ListNodes 來加入全新彈性檢查。如需詳細資訊，請參閱AWS 受管政策：AWSTrustedAdvisorServiceRolePolicy。	2023 年 9 月 14 日
更新 AWSSupportServiceRolePolicy 的說明文件	新增了許可以針對服務連結角色提供計費、管理和支援服務。如需詳細資訊，請參閱AWS 受管政策：AWSSupportServiceRolePolicy。	2023 年 8 月 28 日
更新的文檔 Trusted Advisor	新增了 1 項針對 Lambda 的新服務限制檢查。如需詳細資訊，請參閱變更記錄以取得 AWS Trusted Advisor 檢查。	2023 年 8 月 17 日
更新的文檔 Trusted Advisor	為 Lambda 新增了 1 個新的容錯能力檢查。如需詳細資訊，請參閱變更記錄以取得 AWS Trusted Advisor 檢查。	2023 年 8 月 3 日
對於 Trusted Advisor 搞更新文檔	更新了 Trusted Advisor Engage 文件，包含對建立和編輯業務開發的表單所進行的變更。已新增包含範例服務控制政策的頁面 AWS Trusted Advisor。	2023 年 7 月 27 日

更新 AWSSupportServiceRolePolicy 的說明文件	新增了許可以針對服務連結角色提供計費、管理和支援服務。如需詳細資訊，請參閱AWS 受管政策：AWSSupportServiceRolePolicy。	2023 年 6 月 26 日
更新的文檔 Trusted Advisor	為 Amazon MQ 新增了兩個新的容錯能力檢查。新增了 Amazon Elastic File System 的一項全新容錯檢查和一項全新效能檢查。如需詳細資訊，請參閱變更記錄以取得 AWS Trusted Advisor 檢查。	2023 年 6 月 1 日
更新的文檔 Trusted Advisor	為 NAT Gateway 新增了兩個新的容錯能力檢查。如需詳細資訊，請參閱變更記錄以取得 AWS Trusted Advisor 檢查。	2023 年 5 月 16 日
AWS Support 計劃的更新文件	已新增建立支援計劃排程的新權限和 CloudTrail 文件。如需詳細資訊，請參閱使用管理方 AWS Support 案的存取權限、AWS Support 方案的 AWS 受管理原則和記錄 AWS Support 計劃 API 呼叫 AWS CloudTrail。	2023 年 5 月 8 日
更新 AWSSupportServiceRolePolicy 的說明文件	新增了許可以針對服務連結角色提供計費、管理和支援服務。如需詳細資訊，請參閱AWS 受管政策：AWSSupportServiceRolePolicy。	2023 年 5 月 2 日

更新的文檔參 Trusted Advisor 與和 Trusted Advisor 優先級	釐清了 Trusted Advisor 參與和 Trusted Advisor 優先順序的先決條件。加入了 IAM 政策範例，此範例能使用 Trusted Advisor Engage 並啟用受信任的 Trusted Advisor存取權。	2023 年 4 月 28 日
更新的文檔 Trusted Advisor	為 AWS Resilience Hub 和事件管理器添加了兩個新的容錯檢查。如需詳細資訊，請參閱變更記錄以取得 AWS Trusted Advisor 檢查。	2023 年 4 月 27 日
對於 Trusted Advisor 搞添加文檔	您可以使用 AWS Trusted Advisor Engage 充分利用您的 AWS Support 計劃，方法是讓您輕鬆查看、請求和追蹤所有主動參與，並與您的 AWS 帳戶 團隊溝通有關正在進行的活動。如需詳細資訊，請參閱 AWS Trusted Advisor Engage 入門。	2023 年 4 月 6 日
更新的文檔 Trusted Advisor	為 Amazon ECS 新增了兩個新的容錯能力檢查。如需詳細資訊，請參閱變更記錄以取得 AWS Trusted Advisor 檢查。	2023 年 3 月 30 日
更新 AWSSupportServiceRolePolicy 的說明文件	新增了許可以針對服務連結角色提供計費、管理和支援服務。如需詳細資訊，請參閱AWS 受管政策：AWSSupportServiceRolePolicy。	2023 年 3 月 16 日

對於 Trusted Advisor 優先添加文檔	更新了 Trusted Advisor 優先級控制台： • 確認和關閉按鈕已取代接受和拒絕按鈕。 • 您無需輸入職稱或姓名即可確認、解決、關閉或重新開啟建議。 如需詳細資訊，請參閱 Trusted Advisor 優先順序入門。	2023 年 2 月 16 日
更新的代碼示例 AWS Support	已新增 .NET、Java 和 Kotlin 程式碼範例，顯示如何 AWS Support 搭配 AWS 軟體開發套件 (SDK) 使用。如需詳細資訊，請參閱AWS Support 使用 AWS SDK 的程式碼範例。	2023 年 1 月 16 日
更新 AWSSupportServiceRolePolicy 的說明文件	新增了許可以針對服務連結角色提供計費、管理和支援服務。如需詳細資訊，請參閱AWS 受管政策：AWSSupportServiceRolePolicy。	2023 年 1 月 10 日
更新的 AWS Support 應用程序文檔	您可以使用篩選選項或依案例 ID 搜尋來在 Slack 中搜尋支援案例。如需詳細資訊，請參閱在 Slack 中搜尋支援案例。	2022 年 12 月 29 日
更新的 AWS Support 應用程序文檔	您還可以使用 Terraform 為應用程序創建資源。 AWS Support 如需詳細資訊，請參閱使用 Terraform 建立 AWS Support 應用程式資源。	2022 年 12 月 22 日

更新的文檔 Trusted Advisor	為 Amazon MemoryDB、Amazon ElastiCache 和. AWS CloudHSM如需詳細資訊，請參閱變更記錄以取得 AWS Trusted Advisor 檢查。	2022 年 12 月 15 日
Slack 中 AWS Support 應用程式的更新文件	您現在可以為下列選項請求即時聊天支援： • 帳戶和帳單支援案例。 • 技術支援案例的日文語言支援 • 如需詳細資訊，請參閱在 Slack 頻道中建立支援案例。	2022 年 12 月 14 日
更新的文檔 AWS Support	已新增 AWS Support API 新端點的相關文件。如需詳細資訊，請參閱關於 AWS Support API。	2022 年 12 月 14 日
已新增可在 Slack 中用於應用 AWS Support 程式的 AWS CloudFormation 範本說明文件	您可以使用 CloudFormation 範本建立 AWS 帳戶 中 AWS Organizations的 Slack 設定工作區和頻道。如需詳細資訊，請參閱使 AWS Support 用 AWS CloudFormation.	2022 年 12 月 5 日
更新的文檔 Trusted Advisor	增加了兩個新的容錯檢查 AWS Resilience Hub。如需詳細資訊，請參閱變更記錄以取得 AWS Trusted Advisor 檢查。	2022 年 11 月 17 日
為您的 AWS Security Hub 發現添加了文檔 Trusted Advisor	安全中心控制項中的發現項目會從 Trusted Advisor 更快的速度移除。如需詳細資訊，請參閱變更記錄以取得 AWS Trusted Advisor 檢查。	2022 年 11 月 17 日

更新的文檔 AWS Trusted Advisor	已新增 Trusted Advisor 建議文件。如需詳細資訊，請參閱變更記錄以取得 AWS Trusted Advisor 檢查。	2022 年 11 月 16 日
Slack 中 AWS Support 應用程式的更新文件	新增了日文語言支援的文件。如需詳細資訊，請參閱在 Slack 頻道中建立支援案例。	2022 年 11 月 11 日
AWS Support 計劃的更新文件	新增了疑難排解資訊，以允許在組織中存取 Support Plans。如需詳細資訊，請參閱疑難排解。	2022 年 11 月 9 日
Slack 中 AWS Support 應用程式的更新文件	已新增 `supportapp` 許可的文件。如需詳細資訊，請參閱AWS Support 應用程式連線至 Slack 所需的權限。	2022 年 11 月 1 日
Slack 中 AWS Support 應用程式的更新文件	您可以使用 `RegisterSlackWorkspaceForOrganization` API 操作為您的 AWS 帳戶註冊一個 Slack 工作空間。若要呼叫此 API，您的帳戶必須是 AWS Organizations中組織的一部分。如需詳細資訊，請參閱《Slack API 參考中的AWS Support 應用程式》。	2022 年 10 月 19 日
更新 `AWSSupportServiceRolePolicy` 的說明文件	新增了許可以針對服務連結角色提供計費、管理和支援服務。如需詳細資訊，請參閱AWS 受管政策：AWSSupportServiceRolePolicy。	2022 年 10 月 4 日

更新 Support Plans 的說明文件	您現在可以使用 AWS Identity and Access Management (IAM) 管理許可，以變更您的 AWS 帳戶. 如需詳細資訊，請參閱下列主題： • 管理 AWS Support 計劃的存取權 • AWS 受管理的 AWS Support 計劃原則 • 變更 AWS Support 計劃 • 記錄 AWS Support 計劃 API 呼叫 AWS CloudTrail	2022 年 9 月 29 日
Slack 中 AWS Support 應用程式的更新文件	已新增關於如何設定與應用 AWS Support 程式搭配使用的公開或私人頻道的文件。如需詳細資訊，請參閱設定 Slack 頻道。	2022 年 9 月 22 日
更新的文檔 AWS Support	新增了有關支援案例安全性的章節。如需詳細資訊，請參閱您 AWS Support 案例的安全性。	2022 年 9 月 9 日
更新的文檔 Trusted Advisor	新增了 Amazon EC2 的安全性檢查。如需詳細資訊，請參閱變更記錄以取得 AWS Trusted Advisor 檢查。	2022 年 9 月 1 日

Slack 中 AWS Support 應用程式的更新文件	請參閱下列主題： 您可以使用 AWS Support 應用程式來管理您的支援案例、要求增加服務配額，以及直接在 Slack 頻道中與支援專員聊天。如需詳細資訊，請參閱 Slack 文件中的AWS Support 應用程式。 您可以將 AWS 受管政策附加到 IAM 角色以使用該 AWS Support 應用程式。如需詳細資訊，請參閱 Slack 中 AWS Support 應用程式的AWS 受管理原則。 該 AWS Support 應用程序的新 API 參考。請參閱《AWS Support 應用程式 API 參考》。	2022 年 8 月 24 日
更新 AWSSupportServiceRolePolicy 的說明文件	新增了許可以針對服務連結角色提供計費、管理和支援服務。如需詳細資訊，請參閱AWS 受管政策：AWSSupportServiceRolePolicy。	2022 年 8 月 17 日

對於 Trusted Advisor 優先添加文檔	Trusted Advisor 優先級添加了對以下功能的支持： • 委派的管理員 • 建議摘要的每日和每週電子郵件通知 • 重新開啟已解決或已拒絕的建議 • AWS 受管理政策 如需詳細資訊，請參閱 Trusted Advisor 優先順序入門。	2022 年 8 月 17 日
更新的文檔 Trusted Advisor	Trusted Advisor 主控台中的「偏好設定」 頁面已更新。如需詳細資訊，請參閱開始使用 AWS Trusted Advisor。	2022 年 7 月 15 日
更新的文檔 Trusted Advisor	已更新檢查，包含下列資訊： • 警示條件 • 建議的動作 • 其他資源 • 報告欄位 如需詳細資訊，請參閱 AWS Trusted Advisor 檢查參考。	2022 年 7 月 7 日
更新的文檔 AWS Support	新增了文件，說明如何管理您的支援案例。 • 更新現有的支援案例 • 疑難排解	2022 年 6 月 28 日

更新 AWSSupportServiceRolePolicy 的說明文件	已更新許可，以針對服務連結角色提供計費、管理和支援服務。如需詳細資訊，請參閱AWS 受管政策：AWSSupportServiceRolePolicy。	2022 年 6 月 23 日
更新的文檔 Trusted Advisor	Trusted Advisor 支援來源於其他 AWS 基礎安全性最佳做法安全性標準控制項。 AWS Security Hub如需詳細資訊，請參閱變更記錄以取得 AWS Trusted Advisor 檢查。	2022 年 6 月 23 日
更新的文檔 Trusted Advisor	新增了有關如何請求增加服務配額的資訊。如需詳細資訊，請參閱服務限額。	2022 年 6 月 21 日
更新的文檔 AWS Support	建立案例體驗已在支援中心主控台中更新。如需詳細資訊，請參閱「建立支援案例和案例管理」。	2022 年 5 月 18 日
更新的文檔 Trusted Advisor	為 Amazon EBS 和 AWS Lambda新增了四項檢查。如需詳細資訊，請參閱選擇加入 AWS Compute Optimizer 以新增 Trusted Advisor 檢查。	2022 年 5 月 4 日
更新 AWSSupportServiceRolePolicy 的說明文件	新增了許可以針對服務連結角色提供計費、管理和支援服務。如需詳細資訊，請參閱AWS 受管政策：AWSSupportServiceRolePolicy。	2022 年 4 月 27 日
更新存取金鑰已暴露檢查的說明文件	此檢查現在會自動為您重新整理。如需詳細資訊，請參閱變更 AWS Trusted Advisor 檢查記錄。	2022 年 4 月 25 日

更新的文檔 Trusted Advisor	容錯性類別中的 AWS Direct Connect 檢查已更新。如需詳細資訊，請參閱變更 AWS Trusted Advisor 檢查記錄。	2022 年 3 月 29 日
更新 AWSSupportServiceRolePolicy 的說明文件	新增了許可以針對服務連結角色提供計費、管理和支援服務。如需詳細資訊，請參閱AWS 受管政策：AWSSupportServiceRolePolicy。	2022 年 3 月 14 日
對於 Trusted Advisor 優先添加文檔	您可以使用「 Trusted Advisor 優先順序」來檢視技術客戶經理 (TAM) 提供的優先順序建議清單。如需詳細資訊，請參閱Trusted Advisor 優先順序入門。	2022 年 2 月 28 日
對於使用 Amazon 更新 EventBridge 的文檔 Trusted Advisor	您可以建立 EventBridge 規則來監視 Trusted Advisor 檢查的變更。如需詳細資訊，請參閱使用監視 AWS Trusted Advisor 檢查結果 EventBridge。	2022 年 2 月 21 日
使用 Amazon EventBridge 監控 AWS Support 案例的新文件	您可以建立 EventBridge 規則來監控和接收有關支援案例的通知。如需詳細資訊，請參閱使 AWS Support 用 EventBridge.	2022 年 2 月 21 日
更新 AWSSupportServiceRolePolicy 的說明文件	新增了許可以針對服務連結角色提供計費、管理和支援服務。如需詳細資訊，請參閱AWS 受管政策：AWSSupportServiceRolePolicy。	2022 年 2 月 17 日

添加了文檔與集成 AWS Security Hub	在主控 Trusted Advisor 台中，您現在可以檢視屬於 AWS 基礎安全性最佳做法安全性標準一部分的 Security Hub 控制項的發現項目。如需詳細資訊，請參閱在AWS Trusted Advisor 主 AWS Security Hub 控台中檢視控制項。	2022 年 1 月 18 日
更新的文檔 Trusted Advisor	為正在執行 Microsoft SQL 伺服器的 Amazon EC2 執行個體新增了三項檢查。 • Microsoft SQL 伺服器的 Amazon EC2 執行個體合併 • Microsoft SQL 伺服器過度佈建的 Amazon EC2 執行個體 • Microsoft SQL 伺服器終止支援的 Amazon EC2 執行個體 如需詳細資訊，請參閱 AWS Trusted Advisor 檢查參考。	2021 年 12 月 20 日

更新的文檔 Trusted Advisor	Trusted Advisor 增加了四個新的檢查 AWS Well-Architected • AWS Well-Architected 成本最佳化的高風險問題 • AWS Well-Architected 效能的高風險問題 • AWS Well-Architected 安全性的高風險問題 • AWS Well-Architected 可靠性的高風險問題 如需詳細資訊，請參閱 AWS Trusted Advisor 檢查參考。	2021 年 12 月 20 日
已更新的文件	如果您有企業版支 Sup port 計劃，則可以存取所有 Trusted Advisor 檢查和 AWS Support API。	2021 年 11 月 24 日
更新的文檔 Trusted Advisor	Trusted Advisor 增加了兩個新的檢查 Amazon Comprehend。如需詳細資訊，請參閱 AWS Trusted Advisor 檢查參考。	2021 年 9 月 29 日
更新的文檔 Trusted Advisor	Amazon OpenSearch Service Reserved Instance Optimization 的檢查名稱已更新。如需詳細資訊，請參閱變更 AWS Trusted Advisor 檢查記錄。	2021 年 9 月 8 日
更新的文檔 Trusted Advisor 檢查	已新增所有 Trusted Advisor 檢查的參考主題。如需詳細資訊，請參閱 AWS Trusted Advisor 檢查參考。	2021 年 9 月 1 日

Trusted Advisor 受管理策略的更新文件	已更新 Trusted Advisor 受管理策略的說明文件。如需詳細資訊，請參閱AWS Support 和的AWS 受管理原則 AWS Trusted Advisor。	2021 年 8 月 10 日
更新的文檔 Trusted Advisor	已更新 Trusted Advisor 主控台的說明文件。如需詳細資訊，請參閱開始使用 AWS Trusted Advisor。	2021 年 7 月 16 日
用於創建 AWS Support 案例的更新文檔	新增有關如何為永久關閉的案例建立相關支援案例的說明文件。如需詳細資訊，請參閱重新開啟已關閉的案例和建立相關案例。	2021 年 6 月 8 日
更新的文檔 Trusted Advisor	Trusted Advisor 為 Amazon Elastic Block Store (Amazon EBS) 批量存儲添加了兩個新的檢查。如需詳細資訊，請參閱變更 AWS Trusted Advisor 檢查記錄。	2021 年 6 月 8 日
已更新的文件	下列主題更新： • 更新程序並新增內容至建立 Amazon CloudWatch 警示以監控 AWS Trusted Advisor 指標主題 • 已新增 AWS Support API 的服務配額區段	2021 年 5 月 12 日

舊版更新

變更	描述	日期
更新的文檔 Trusted Advisor	新增篩選、重新整理和下載檢查結果的說明文件。如需詳細資訊，請參閱下列章節： • 篩選檢查 • 重新整理檢查結果 • 下載檢查結果	2021 年 3 月 16 日
有關 AWS 受管理策略的更新文	已新增`AWSSupportServiceRolePolicy` AWS 受管理原則的相關資訊。如需詳細資訊，請參閱 使用 AWS Support的服務連結角色。	2021 年 3 月 16 日
添加了檢查 AWS Lambda	在中新增四個對 Lambda 的 AWS Trusted Advisor 檢查變更的記錄 AWS Trusted Advisor。	2021 年 3 月 8 日
更新適用於 Amazon Elastic Block Store 的服務配額檢查	更新了五個 AWS Trusted Advisor 檢查 Amazon EBS 在變更的記錄 AWS Trusted Advisor.	2021 年 3 月 5 日
CloudTrail 日誌記錄更新文檔	CloudTrail 支援在您變更 AWS Support 方案時記錄主控台動作。如需詳細資訊，請參閱 記錄 AWS Support 計劃的變更。	2021 年 2 月 9 日
更新的文檔 Trusted Advisor	更新 開始使用 Trusted Advisor Recommendations 主題。	2021 年 1 月 29 日
Trusted Advisor 報告的更新文件	已新增將 Trusted Advisor 報表與其他 AWS 服務搭配使用的疑難排解區段。	2020 年 12 月 4 日
增加了 AWS CloudTrail 日誌記錄 AWS Trusted Advisor 支持	CloudTrail 支援記錄 Trusted Advisor 主控台動作的子集。如需詳細資訊，請參閱 使用 AWS CloudTrail 記錄 AWS Trusted Advisor 主控台動作。	2020 年 11 月 23 日

變更	描述	日期
新增變更日誌主題	檢視對中 AWS Trusted Advisor 檢查和品類的變更變更的記錄 AWS Trusted Advisor。	2020 年 11 月 18 日
新增對組織單位的支援	您現在可以為組織單位 (OU) 的 Trusted Advisor 檢查建立報告。如需詳細資訊，請參閱 建立組織檢視報告。	2020 年 11 月 17 日
使用 AWS CloudTrail 主題更新了日誌記錄	新增 Trusted Advisor API 作業的範例記錄項目。請參閱 CloudTrail 記錄中的 AWS Trusted Advisor 資訊。	2020 年 10 月 22 日
新增 AWS Support 配額	新增有關 AWS Support目前配額和限制的資訊。請參閱《AWS 一般參考》中的 AWS Support 端點和配額。	2020 年 8 月 4 日
的組織檢視 AWS Trusted Advisor	您現在可以針對屬於其中的帳戶建立 Trusted Advisor 檢查報告 AWS Organizations。請參閱 AWS Trusted Advisor 的組織檢視。	2020 年 7 月 17 日
安全性和 AWS Support	新增了關於使用 AWS Support 及 Trusted Advisor時，安全性考量的資訊。請參閱 中的安全性 AWS Support	2020 年 5 月 5 日
安全性和 AWS Support	新增了關於使用 AWS Support時，安全性考量的資訊。	2020 年 1 月 10 日
用 Trusted Advisor 作網絡服務	已新增更新指示，以在取得 Trusted Advisor 檢查清單後重新整理 Trusted Advisor 資料。	2018 年 11 月 1 日
使用服務連結角色	新增章節。	2018 年 7 月 11 日
入門指南：疑難排解	新增 Route 53 和 AWS Certificate Manager的疑難排解連結。	2017 年 9 月 1 日
案例管理範例：建立案例	為基本支援計劃的使用者提供有關 CC 方塊中的新增注意事項。	2017 年 8 月 1 日

變更	描述	日期
使用 CloudWatch 事件監視 Trusted Advisor 檢查結果	新增章節。	2016 年 11 月 18 日
案例管理	更新案例嚴重性等級的名稱。	2016 年 10 月 27 日
記錄 AWS Support 呼叫 AWS CloudTrail	新增章節。	2016 年 4 月 21 日
入門指南：疑難排解	新增更多疑難排解連結。	2015 年 5 月 19 日
入門指南：疑難排解	新增更多疑難排解連結。	2014 年 11 月 18 日
入門：案例管理	已更新以反映 AWS Management Console中的 Service Catalog。	2014 年 10 月 30 日
編程案 AWS Support 例的生命週期	新增資訊，內容是有關用於將附件新增到案例以及在擷取案例歷史記錄時省略案例通訊的新 API 元素。	2014 年 7 月 16 日
存取 AWS Support	移除做為存取方法的指名支援聯絡人。	2014 年 5 月 28 日
開始	新增入門章節	2013 年 13 月 12 日
初次出版	新 AWS Support 服務發布。	2013 年 30 月 4 日

AWS 詞彙表

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

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。