入門指南

AWS 管理主控台

版本 1.0

AWS 管理主控台: 入門指南

Table of Contents

什麼是 AWS 管理主控台？

AWS 管理主控台 是以 Web 為基礎的應用程式，其中包含並提供所有個別 AWS 服務主控台的集中存取。您可以在 中使用統一導覽 AWS 管理主控台 來搜尋服務、檢視通知、Access AWS CloudShell、存取帳戶和帳單資訊，以及自訂一般主控台設定。首頁 AWS 管理主控台 稱為 AWS Console Home。您可以從 AWS Console Home中管理您的 AWS 應用程式，並存取所有其他個別服務主控台。您也可以使用小工具自訂 AWS Console Home 以顯示有關 AWS 和 資源的其他有用資訊。您可以新增、移除和重新排列小工具，例如最近造訪的小工具、AWS 運作狀態等。

主題

的功能 AWS 管理主控台

的重要功能 AWS 管理主控台 包括下列項目：

- 導覽至 AWS 服務主控台 – 您可以使用統一導覽來存取最近造訪的服務主控台、檢視服務並將其新增至我的最愛清單、存取您的主控台設定和存取 AWS 使用者通知。
- 搜尋 AWS 服務和其他 AWS 資訊 – 使用統一搜尋來搜尋 AWS 服務和功能，以及 AWS 市場產品。
- 自訂主控台 – 您可以使用統一設定來自訂 的各個層面 AWS 管理主控台。這包括語言、預設區域等。
- 執行 CLI 命令 – AWS CloudShell 可從主控台直接存取。您可以使用 CloudShell 針對您偏好的服務執行 AWS CLI 命令。
- 存取所有 AWS 事件通知 – 您可以使用 AWS 管理主控台 來存取來自 AWS 使用者通知 和 的通知 AWS Health。
- 自訂 AWS Console Home – 您可以使用小工具完全自訂您的 AWS Console Home 體驗。
- 建立和管理 AWS 應用程式 – 使用 myApplications 管理和監控應用程式的成本、運作狀態、安全狀態和效能 AWS Console Home。
- 與 Amazon Q 聊天 – 您可以直接從主控台取得生成式人工智慧 (AI) 助理支援 AWS 服務 的問題解答。您也可以與即時代理程式連線，以取得其他支援。

- 控制您網路中的 AWS 帳戶存取 – 當流量來自您的網路時，您可以使用 AWS 管理主控台 私有存取將對 的存取限制 AWS 管理主控台 在指定的一組已知 AWS 帳戶。

中的個別 AWS 服務主控台 AWS 管理主控台

每個 AWS 服務都有自己的個別服務主控台，您可以在 中存取 AWS 管理主控台。您在統一設定中選擇的設定 AWS 管理主控台，例如視覺化模式和預設語言，會套用至所有個別 AWS 主控台。 AWS 服務主控台提供各種雲端運算工具，以及您的帳戶和帳單的相關資訊。如果您想要進一步了解特定服務及其主控台，例如 Amazon Elastic Compute Cloud，請在導覽列中使用統一搜尋 AWS 管理主控台 導覽至其主控台，並從 AWS 文件網站存取 Amazon EC2 文件。

當您導覽至個別 AWS 服務的主控台時，您仍然可以使用主控台頂端的 AWS 管理主控台 統一導覽存取的功能。您可以透過導覽至該主控台並在頁面頁尾中選擇意見回饋，來保留個別服務主控台的意見回饋。

存取 AWS 管理主控台

您可以在 https AWS 管理主控台 ：//https://console.aws.amazon.com/ 存取 。

AWS 管理主控台 使用行動裝置存取

AWS 管理主控台 旨在處理平板電腦和其他類型的行動裝置：

- 水平和垂直空間設計最大化，讓您的畫面能顯示更多內容。
- 為了提供更好的使用觸感，按鈕與選擇器均已變大。

若要 AWS 管理主控台 在行動裝置上存取 ，您必須使用 AWS Console Mobile Application。此應用程式適用於 Android 和 iOS。主控台行動應用程式提供行動相關任務，是完整 Web 體驗的好夥伴。例如，您可以從手機輕鬆檢視及管理現有的 Amazon EC2 執行個體和 Amazon CloudWatch 警示。如需詳細資訊，請參閱AWS Console Mobile Application 《 使用者指南》中的什麼是 AWS Console Mobile Application？。

您可以從 Amazon Appstore、Google Play 和 iOS App Store 下載主控台行動應用程式。

中的服務入門 AWS 管理主控台

AWS 管理主控台提供前往各服務主控台的多種導覽方式。

開啟服務的主控台

執行以下任意一項：

- 在導覽列上的搜尋方塊中，輸入完整或部分服務名稱。在 Services (服務) 底下，從搜尋結果的清單中選擇您需要的服務。如需詳細資訊，請參閱在 中使用統一搜尋來搜尋產品、服務、功能等 AWS 管理主控台。
- 在 Recently visited services (最近用過的服務) 小工具中，選擇服務名稱。
- 在最近造訪的服務小工具中，選擇檢視所有 AWS 服務。然後，在所有 AWS 服務頁面上，選擇服務名稱。
- 在導覽列上選擇 Services (服務)，開啟完整的服務清單。接著，選擇 Recently visited (最近用過) 或 All Services (所有服務)。

透過統一 AWS 管理主控台 導覽使用導覽列

本主題說明如何使用統一導覽。統一導覽是指做為主控台標頭和頁尾的導覽列。您可以使用統一導覽來：

- 搜尋和存取 AWS 服務、功能、產品等。
- 啟動 AWS Cloudshell。
- 存取 AWS 通知和 AWS 運作狀態事件。
- 從各種 AWS 知識來源取得支援。
- AWS 管理主控台 選擇您的預設語言、視覺化模式、區域等來設定 。
- 存取帳戶、組織、服務配額和帳單資訊。

主題

在 中存取服務功能表 AWS 管理主控台

您可以使用搜尋列旁邊的服務選單來存取最近造訪的服務、檢視我的最愛清單，以及檢視所有 AWS 服務。您也可以選擇服務類型來依類型檢視服務，例如 Analytics 或 Application Integration。

下列程序說明如何存取 服務選單。

存取服務功能表

1. 登入 AWS 管理主控台。

2. 在導覽列中，選擇服務 (⁝⁝⁝)。
3. （選用）選擇最近造訪，以檢視您最近互動的服務和應用程式。
4. （選用）選擇我的最愛以檢視我的最愛清單。
5. （選用）選擇所有應用程式以檢視您的 myApplications 應用程式。
6. （選用）選擇所有服務以檢視所有 AWS 服務的字母清單。
7. （選用）選擇服務類型，依類型檢視 AWS 服務。

在 中使用統一搜尋來搜尋產品、服務、功能等 AWS 管理主控台

導覽列中的搜尋方塊提供統一的搜尋工具，可用來尋找 AWS 服務和功能、服務文件、 AWS Marketplace 產品等。只要輸入幾個字元或問題，即可開始從所有可用的內容類型產生結果。您輸入的每個單字都會進一步縮小結果範圍。可用的內容類型包括：

- 服務
- 功能
- 文件
- 部落格
- 知識文章
- 事件
- 教學
- 市集
- Resources

> **Note**
>
> 您可以篩選搜尋結果，透過執行聚焦搜尋來僅顯示資源。若要執行聚焦搜尋，`/Resources`請在搜尋列的查詢開頭輸入 ，然後從下拉式選單中選擇 /Resources。然後輸入查詢的其餘部分。

主題

- 在 中搜尋 AWS 產品 AWS 管理主控台
- 在 中精簡您的搜尋 AWS 管理主控台
- 在 中檢視服務的功能 AWS 管理主控台

在 中搜尋 AWS 產品 AWS 管理主控台

下列程序詳細說明如何使用搜尋工具搜尋 AWS 產品。

搜尋服務、功能、文件或 AWS Marketplace 產品

1. 在 導覽列的搜尋方塊中AWS 管理主控台，輸入您的查詢。
2. 選擇任何連結以導覽至預期的目的地。

> **Tip**
>
> 您也可以使用鍵盤快速導覽至最上方的搜尋結果。首先按下 Alt + s 鍵 (Windows) 或 Option + s 鍵 (macOS)，存取搜尋列。接著，開始輸入您的搜尋字詞。當清單最上方出現您需要的結果時，按下 Enter 鍵。例如，若要快速導覽至 Amazon EC2 主控台，請輸入 ec2 並按下Enter 鍵。

在 中精簡您的搜尋 AWS 管理主控台

您可以依內容類型縮小搜尋範圍，並檢視搜尋結果的其他資訊。

將搜尋精簡為特定內容類型

1. 在 導覽列的搜尋方塊中AWS 管理主控台，輸入您的查詢。
2. 選擇搜尋結果旁的其中一個內容類型。
3. （選用）若要查看特定類別的所有結果：
   - 選擇顯示更多。新的索引標籤隨即開啟，顯示結果。
4. （選用）若要檢視搜尋結果的其他資訊：
   a. 在搜尋結果中，將游標停留在搜尋結果上。
   b. 檢視可用的其他資訊。

在 中檢視服務的功能 AWS 管理主控台

您可以從搜尋結果中檢視服務的功能。

檢視 服務的功能

1. 在 導覽列的搜尋方塊中AWS 管理主控台，輸入您的查詢。
2. 在搜尋結果中，將游標暫留在服務中的服務上。
3. 在熱門功能中選擇其中一個連結。

AWS CloudShell 從 中的導覽列啟動 AWS 管理主控台

AWS CloudShell 是以瀏覽器為基礎的預先驗證 Shell，您可以直接從 AWS 管理主控台 導覽列啟動。您可以使用您偏好的 shell (Bash、PowerShell 或 Z shell) 對 服務執行 AWS CLI 命令。

您可以使用下列兩種方法 AWS 管理主控台 之一，從 啟動 CloudShell：

- 選擇 主控台頁尾中的 CloudShell 圖示。
- 從主控台的瀏覽列上選擇 CloudShell 圖示。

如需有關此服務的詳細資訊，請參閱 AWS CloudShell 使用者指南。

如需 AWS CloudShell 可用 AWS 區域 的詳細資訊，請參閱AWS 區域服務清單。主控台區域的選取項目會與 CloudShell 區域同步。如果選取的區域無法使用 CloudShell，則 CloudShell 將在最近的區域中運作。

存取 AWS 通知和運作狀態事件

您可以從導覽列存取一些 AWS 通知並檢視運作狀態事件。您也可以從導覽列存取 AWS 使用者通知 以檢視所有 AWS 通知和 AWS Health 儀表板。

如需詳細資訊，請參閱AWS 使用者通知 《 使用者指南》中的什麼是 AWS 使用者通知？和《 AWS Health 使用者指南》中的什麼是 AWS Health？

下列程序說明如何存取您的 AWS 事件資訊。

存取您的 AWS 事件資訊

1. 登入 AWS 管理主控台。
2. 在導覽列中，選擇鈴鐺圖示。
3. 檢視您的通知和運作狀態事件。
4. （選用）選擇查看所有通知以導覽至 使用者通知 主控台。

5. （選用）選擇查看所有運作狀態事件以導覽至 AWS Health 主控台。

取得支援

您可以在導覽列中選擇問號圖示來取得支援。從支援選單中，您可以選擇：

- 導覽至支援中心服務主控台
- 從 AWS IQ 取得專家協助
- 在 AWS re：Post 上檢視社群文章和知識中心的精選知識
- 前往 AWS 文件
- 導覽至 AWS 訓練
- 導覽至 AWS 入門資源中心
- 保留您目前存取之任何服務主控台的意見回饋

> **Note**
>
> 您也可以在主控台頁尾中選擇意見回饋來完成此操作。開啟的模態標題會顯示您目前留下意見回饋的主控台

您也可以隨時在主控台中取得協助、與即時客服人員連線，以及與 AWS Q AWS 聊天以詢問有關 的任何問題。如需詳細資訊，請參閱???。

AWS 管理主控台 使用統一設定來設定

本主題說明如何 AWS 管理主控台 使用統一設定頁面來設定 ，以設定適用於所有服務主控台的預設值。

主題

- 在 中設定統一設定 AWS 管理主控台
- 在 中設定可見的區域和服務 AWS 管理主控台
- 選擇您的區域
- 中的我的最愛 AWS 管理主控台
- 在 中變更您的密碼 AWS 管理主控台
- 變更 的語言 AWS 管理主控台

在 中設定統一設定 AWS 管理主控台

您可以從 AWS 管理主控台 統一設定頁面設定設定和預設值，例如顯示、語言和區域。您可以透過統一導覽中的導覽列存取統一設定。視覺模式和預設語言也可以直接從導覽列設定。這些變更會套用至所有服務主控台。

> **Important**
>
> 為了確保您的設定、我的最愛服務和最近造訪的服務在全球範圍內持續存在，這些資料會存放在所有 中 AWS 區域，包括預設為停用的區域。這些區域是非洲 (開普敦)、亞太區域 (香港)、亞太區域 (海德拉巴)、亞太區域 (雅加達)、歐洲 (米蘭)、歐洲 (西班牙)、歐洲 (蘇黎世)、中東 (巴林) 和中東 (阿拉伯聯合大公國)。如想存取特定區域，然後在該區域中建立和管理資源，您仍然必須手動啟用區域。如果您不想全部存放此資料 AWS 區域，請選擇全部重設以清除您的設定，然後在設定管理中選擇不記住最近存取的服務。

主題

在 中存取統一設定 AWS 管理主控台

下列程序說明如何存取統一設定。

如何存取統一設定

1. 登入 AWS 管理主控台。
2. 在導覽列中，選擇齒輪圖示 (#)。
3. 若要開啟統一設定頁面，請選擇查看所有使用者設定。

在 中重設統一設定 AWS 管理主控台

您可以刪除所有統一設定組態，並透過重設統一設定來還原預設設定。

> **Note**
>
> 這會影響 的多個區域 AWS，包括導覽和 服務選單中最愛的服務、主控台首頁小工具和 中最近造訪的服務 AWS Console Mobile Application，以及跨服務套用的所有設定，例如預設語言、預設區域和視覺化模式。

重設所有統一設定

1. 登入 AWS 管理主控台。
2. 在導覽列中，選擇齒輪圖示 (#)。
3. 選擇查看所有使用者設定，開啟統一設定頁面。
4. 選擇全部重設。

在 中編輯統一設定 AWS 管理主控台

下列程序說明如何編輯您偏好的設定。

編輯統一設定

1. 登入 AWS 管理主控台。
2. 在導覽列中，選擇齒輪圖示 (#)。
3. 選擇查看所有使用者設定，以開啟統一設定頁面。
4. 選擇位於偏好設定旁的 Edit (編輯)：

   - Localization and default Region: (本地化和預設區域：)
     - 語言讓您能選取主控台文字的預設語言。
     - Default Region (預設區域) 讓您能選取每次登入時套用的預設區域。您可以為帳戶選取任何可用區域，也能選取前一次使用的區域做為預設區域。

       若要進一步了解AWS 管理主控台中的區域路由，請參閱選擇區域。
   - Display: (顯示：)
     - Visual mode (視覺模式) 可讓您將主控台設定為淺色模式、深色模式或瀏覽器的預設顯示模式。

       深色模式是測試版功能，可能不適用於所有 AWS 服務主控台。

- 我的最愛列顯示模式：可選擇讓我的最愛列顯示完整服務名稱及圖示，或者僅顯示服務圖示。
- 我的最愛列圖示大小：可切換我的最愛列顯示的服務圖示大小，可選擇小 (16x16 像素) 和大 (24x24 像素)。

- Settings management (設定管理)：
  - 請記住，最近造訪的服務可讓您選擇 是否 AWS 管理主控台 記住您最近造訪的服務。關閉此功能也會刪除您最近造訪的服務歷史記錄，因此您將無法再在服務功能表 AWS Console Mobile Application或主控台首頁小工具中看到最近造訪的服務。

5. 選擇儲存變更。

變更 的視覺化模式 AWS 管理主控台

您的視覺化模式會將主控台設定為淺色模式、深色模式或瀏覽器的預設顯示模式。

從導覽列變更視覺模式

1. 登入 AWS 管理主控台。
2. 在導覽列中，選擇齒輪圖示 (#)。
3. 針對視覺模式，選擇淺色以使用淺色模式，選擇深色以使用深色模式，或選擇瀏覽器預設值，使用瀏覽器的預設顯示模式。

在 中設定可見的區域和服務 AWS 管理主控台

帳戶管理員可以控制哪些 AWS 區域 和 AWS 服務會顯示在 AWS 管理主控台 導覽中。這些帳戶層級設定可在統一設定頁面的帳戶設定索引標籤上取得。當您隱藏區域時，會從帳戶中所有使用者的區域選取器中移除該區域。當您隱藏服務時，該服務會在帳戶中所有使用者的服務功能表的個別區段中顯示為無法使用。隱藏的服務也會在統一搜尋結果和主控台首頁上最近造訪和我的最愛小工具中呈現灰色。

如果使用者透過 URL 直接導覽至隱藏的區域或服務，他們會看到一個浮水印，通知他們帳戶層級的區域或服務會隱藏。

> **Note**
>
> 統一設定頁面的導覽一律可用，因此管理員無法自行鎖定這些設定。如果使用者沒有所需的許可，或 AWS 使用者體驗自訂服務無法使用，則預設會顯示所有區域和服務。

主題

設定可見區域和服務的必要條件

若要檢視和變更可見的區域和服務設定，您需要特定的 IAM 許可。

- 若要檢視設定，您需要 `uxc:GetAccountCustomizations`許可。
- 若要變更設定，您需要 `uxc:UpdateAccountCustomizations`許可。

AWS 受管政策 `AWSManagementConsoleBasicUserAccess`和 `AWSManagementConsoleAdministratorAccess`包含這些許可。

如需詳細資訊，請參閱???。

在 中設定可見區域 AWS 管理主控台

您可以為您帳戶中的所有使用者選擇區域選取器中 AWS 區域 出現的 。

設定可見區域

1. 登入 AWS 管理主控台。
2. 在導覽列中，選擇齒輪圖示 (#)。
3. 選擇查看所有使用者設定以開啟統一設定頁面。
4. 選擇帳戶設定索引標籤。
5. 針對可見區域，選取您要顯示之區域的核取方塊，或清除您要隱藏之區域的核取方塊。
6. 選擇儲存變更。

儲存後，隱藏的區域會從帳戶中所有使用者的區域選取器中移除。

在 中設定可見的服務 AWS 管理主控台

您可以選擇哪些 AWS 服務出現在您帳戶中所有使用者的服務選單中。

設定可見的服務

1. 登入 AWS 管理主控台。

2. 在導覽列中，選擇齒輪圖示 (#)。
3. 選擇查看所有使用者設定以開啟統一設定頁面。
4. 選擇帳戶設定索引標籤。
5. 針對可見服務，選取您要顯示之服務的核取方塊，或清除您要隱藏之服務的核取方塊。
6. 選擇儲存變更。

儲存後，隱藏的服務會在帳戶中所有使用者的服務功能表的個別區段中顯示為無法使用。隱藏的服務也會在統一搜尋結果和主控台首頁上最近造訪和我的最愛小工具中呈現灰色。

選擇您的區域

對於許多 服務，您可以選擇指定資源管理位置 AWS 區域 的 。區域是位於相同地理區域的一組 AWS 資源。您不需要為 AWS 管理主控台或某些服務選擇區域，例如 AWS Identity and Access Management。若要進一步了解 AWS 區域，請參閱 AWS 一般參考 中的管理 AWS 區域。

> **Note**
>
> 如果您已建立 AWS 資源，但未在主控台中看到這些資源，則主控台可能會顯示來自不同區域的資源。有些資源 (例如 Amazon EC2 執行個體) 會專屬於一開始建立的區域，

主題

- 從 中的導覽列中選擇區域 AWS 管理主控台
- 在 中設定預設區域 AWS 管理主控台

從 中的導覽列中選擇區域 AWS 管理主控台

下列程序詳細說明如何從導覽列變更您的區域。

從導覽列選擇區域

1. 登入 AWS 管理主控台。
2. 在導覽列上選擇目前顯示區域的名稱，
3. 選擇要切換的區域。

在 中設定預設區域 AWS 管理主控台

下列程序詳細說明如何從統一設定頁面變更預設區域。

設定您的預設區域

1. 在導覽列中，選擇齒輪圖示 (#)。
2. 選擇查看所有使用者設定以導覽至統一設定頁面。
3. 選擇位於 Localization and default Region (本地化和預設區域) 旁的 Edit (編輯)。
4. 在預設區域中，選擇區域。

> **Note**
>
> 如未選擇預設區域，則您前一次存取的區域會成為您的預設區域。

5. 選擇儲存設定。
6. （選用）選擇移至新的預設區域，以立即移至新的預設區域。

中的我的最愛 AWS 管理主控台

若要更快速地存取常用服務和應用程式，您可以將其服務主控台儲存至我的最愛清單。您可以使用 新增和移除我的最愛 AWS 管理主控台。當您將服務或應用程式新增至我的最愛時，它會出現在我的最愛快速列上。

主題

- 在 中新增我的最愛 AWS 管理主控台
- 在 中存取我的最愛 AWS 管理主控台
- 在 中移除我的最愛 AWS 管理主控台

在 中新增我的最愛 AWS 管理主控台

您可以從服務功能表和最近造訪的功能表，將服務和應用程式新增至我的最愛。您也可以使用搜尋方塊中的搜尋結果頁面，將服務新增至我的最愛。您新增至我的最愛服務和應用程式會顯示在我的最愛快速列中。

主題

- 中的我的最愛快速列 AWS 管理主控台
- 在 中將服務新增至我的最愛 AWS 管理主控台
- 在 中將應用程式新增至我的最愛 AWS 管理主控台

中的我的最愛快速列 AWS 管理主控台

當您至少將一項 AWS 服務或應用程式新增至我的最愛時，會顯示我的最愛快速列。我的最愛快速列位於導覽列後面，並可見於所有 AWS 服務主控台，因此您可以快速存取您最愛的服務和應用程式。您可以透過將服務或應用程式拖曳至左側或右側，在我的最愛快速列中重新排列服務和應用程式的順序。

在 中將服務新增至我的最愛 AWS 管理主控台

您可以從服務功能表將服務新增至我的最愛，或從搜尋方塊中新增搜尋結果頁面。

Services menu

從服務功能表新增我的最愛

1. 開啟 AWS 管理主控台。
2. 在導覽列中，選擇服務 (⁝⁝⁝)。
3. （選用）將最近造訪的服務新增至我的最愛：
   a. 在最近造訪的 中，將游標暫留在服務上。
   b. 選取服務名稱旁的星號。
4. 選擇所有 服務。
5. 將游標暫留在您選擇的服務上。
6. 選取服務名稱旁的星號。

Search box

從搜尋方塊中新增我的最愛

1. 開啟 AWS 管理主控台。
2. 在搜尋方塊中輸入服務的名稱。
3. 在搜尋結果頁面中，選取服務名稱旁的星號。

> **Note**
>
> 將服務新增至我的最愛後，該服務會新增至導覽列後面的我的最愛快速列。

在 中將應用程式新增至我的最愛 AWS 管理主控台

您可以從服務功能表將應用程式新增至我的最愛。

從服務功能表新增我的最愛

1. 開啟 AWS 管理主控台。
2. 在導覽列中，選擇服務 (⁝⁝⁝)。
3. （選用）將最近造訪的應用程式新增至我的最愛：
   a. 在最近造訪的 中，將游標暫留在應用程式上。
   b. 選取應用程式名稱旁的星號。
4. 選擇 Applications (應用程式)。
5. 將游標暫留在您選擇的應用程式上。
6. 選取應用程式名稱旁的星號。

> **Note**
>
> 將應用程式新增至我的最愛後，它會新增至導覽列後面的我的最愛快速列。

在 中存取我的最愛 AWS 管理主控台

您可以從服務功能表、我的最愛快速列和我的最愛小工具存取新增至我的最愛中的服務和應用程式。

Services menu

從服務功能表存取您的最愛

1. 開啟 AWS 管理主控台。
2. 在導覽列中，選擇服務 (⁝⁝⁝)。
3. 選擇我的最愛。

4. 檢視您新增至我的最愛之服務和應用程式。
5. （選用）檢視應用程式資源：
   a. 選取應用程式。
   b. （選用）選取檢視。
   c. 檢視您的 資源。
   d. （選用）選取篩選條件。您可以依屬性或標籤篩選資源。如需詳細資訊，請參閱《 AWS 資源總管 使用者指南》中的搜尋 Resource Explorer 的查詢語法參考。
   e. （選用）選取資源以在相關服務主控台中檢視。

> **Tip**
>
> 您可以選擇服務 (⁝⁝⁝) 繼續瀏覽您離開的資源。您套用的搜尋篩選條件也會保留。

Favorites quickbar

從我的最愛快速列存取我的最愛

1. 開啟 AWS 管理主控台。
2. 在我的最愛快速列中檢視服務和應用程式。

Favorites widget

從我的最愛小工具存取我的最愛

1. 開啟 AWS 管理主控台。
2. （選用）如果您沒有我的最愛小工具，請新增它：
   a. 選擇主控台首頁上的 + 新增小工具按鈕。
   b. 在新增小工具功能表中，使用 ⁝⁝ 圖示拖曳我的最愛小工具，並將其放在您的主控台首頁。
3. 在我的最愛小工具中檢視服務和應用程式。

如需小工具的詳細資訊，請參閱 the section called “使用 Widgets”。

在 中移除我的最愛 AWS 管理主控台

您可以使用服務功能表，從我的最愛中移除服務和應用程式。您也可以使用搜尋列中的搜尋結果頁面來移除服務。

Services menu

從服務功能表移除我的最愛

1. 開啟 AWS 管理主控台。
2. 在導覽列上選擇 Services (服務)。
3. 選擇我的最愛。
4. 取消選取服務或應用程式旁的星號。

Search box

> **Note**
>
> 目前，您只能使用搜尋結果頁面從搜尋列移除服務。

從搜尋方塊中移除我的最愛

1. 開啟 AWS 管理主控台。
2. 在搜尋方塊中輸入服務的名稱。
3. 在搜尋結果頁面中，取消選取服務名稱旁的星號。

在 中變更您的密碼 AWS 管理主控台

您可以AWS 管理主控台根據您的使用者類型和許可，從 變更密碼。下列主題說明如何變更每個使用者類型的密碼。

主題

- 中的根使用者 AWS 管理主控台
- 中的 IAM 使用者 AWS 管理主控台
- 中的 IAM Identity Center 使用者 AWS 管理主控台

- 中的聯合身分 AWS 管理主控台

中的根使用者 AWS 管理主控台

根使用者可以直接從 變更其密碼 AWS 管理主控台。根使用者是帳戶擁有者，可完整存取所有 AWS 服務和資源。如果您建立 AWS 帳戶並使用根使用者電子郵件和密碼登入，則您是根使用者。如需詳細資訊，請參閱AWS IAM Identity Center 《 使用者指南》中的根使用者。

以根使用者身分變更您的密碼

1. 登入 AWS 管理主控台。
2. 在導覽列上選擇您的帳戶名稱。
3. 選擇 Security credentials (安全登入資料)。
4. 顯示的選項會根據您的 AWS 帳戶 類型而有所不同。遵循主控台上顯示的指示來變更您的密碼。
5. 輸入一次您的目前密碼，然後輸入兩次您的新密碼。

   新密碼長度必須至少具有八個字元，並且必須包括以下內容：

   - 至少有一個符號
   - 至少有一個數字
   - 至少一個大寫字母
   - 至少一個小寫字母
6. 選擇 Change Password (變更密碼) 或者 Save changes (儲存變更)。

中的 IAM 使用者 AWS 管理主控台

IAM 使用者可以 AWS 管理主控台 根據其許可，從 變更其密碼。否則，他們必須使用 AWS 存取入口網站。IAM 使用者是您 AWS 帳戶中獲授予特定自訂許可的身分。如果您未建立 AWS 帳戶，且管理員或服務台員工提供您包含 AWS 帳戶 ID 或帳戶別名、IAM 使用者名稱和密碼的登入憑證，則您是 IAM 使用者。如需詳細資訊，請參閱《 AWS 登入 使用者指南》中的 IAM 使用者。

如果您有下列政策的許可：AWS：允許 IAM 使用者在安全登入資料頁面上變更自己的主控台密碼，您可以從主控台變更密碼。如需詳細資訊，請參閱《 使用者指南》中的 IAM 使用者如何變更自己的密碼。 AWS Identity and Access Management

如果您沒有變更密碼的必要許可， AWS 管理主控台 請參閱AWS IAM Identity Center 《 使用者指南》中的重設您的 AWS IAM Identity Center 使用者密碼。

中的 IAM Identity Center 使用者 AWS 管理主控台

AWS IAM Identity Center 使用者必須從 AWS 存取入口網站變更其密碼。如需詳細資訊，請參閱AWS IAM Identity Center 《使用者指南》中的重設您的 AWS IAM Identity Center 使用者密碼。

IAM Identity Center 使用者是 AWS 帳戶所屬的使用者，透過 AWS 存取入口網站使用唯一的 URL AWS Organizations 登入。這些使用者可以直接在 IAM Identity Center 的使用者或 Active Directory 或其他外部身分提供者中建立。如需詳細資訊，請參閱《使用者指南AWS IAM Identity Center》中的使用者。 AWS 登入

中的聯合身分 AWS 管理主控台

聯合身分使用者必須從 AWS 存取入口網站變更其密碼。如需詳細資訊，請參閱AWS IAM Identity Center 《使用者指南》中的重設您的 AWS IAM Identity Center 使用者密碼。

聯合身分使用者使用外部身分提供者 (IdP) 登入。如果您符合以下任一條件，則表示您是聯合身分：

- 使用 Login with Amazon、Facebook 或 Google 等第三方登入資料存取 AWS 您的帳戶或資源。
- 使用相同的登入資料登入公司系統和 AWS 服務，而您使用自訂公司入口網站登入 AWS。

如需詳細資訊，請參閱AWS 登入 《使用者指南》中的聯合身分。

變更 的語言 AWS 管理主控台

AWS Console Home 體驗包括統一設定頁面，您可以在其中變更 中 AWS 服務的預設語言 AWS 管理主控台。您也可以從導覽列的設定選單快速變更預設語言。

> **Note**
>
> 下列程序會變更所有 AWS 服務主控台的語言，但不會變更 AWS 文件的語言。若要變更文件的語言，請使用文件頁面右上方的語言選單選擇所需語言。

主題

- 支援的語言
- 從 中的導覽列變更預設語言 AWS 管理主控台
- 在 中透過統一設定變更預設語言 AWS 管理主控台

支援的語言

AWS 管理主控台 目前支援下列語言：

- 英文 (美國)
- 英文 (英國)
- 印度尼西亞語
- 德文
- 西班牙文
- 法文
- 日文
- 義大利文
- 葡萄牙文
- 韓文
- 簡體中文
- 繁體中文
- Turkish

從 中的導覽列變更預設語言 AWS 管理主控台

下列程序詳細說明如何直接從導覽列變更預設語言。

從導覽列變更預設語言

1. 登入 AWS 管理主控台。
2. 在導覽列中，選擇齒輪圖示 (#)。
3. 針對語言，從下拉式清單選擇瀏覽器預設值或是偏好的語言。

在 中透過統一設定變更預設語言 AWS 管理主控台

下列程序詳細說明如何從統一設定頁面變更預設語言。

在統一設定中變更預設語言

1. 登入 AWS 管理主控台。

2. 在導覽列中，選擇齒輪圖示 (#)。
3. 若要開啟統一設定頁面，請選擇查看所有使用者設定。
4. 在 Unified Settings (統一設定) 中，選擇位於 Localization and default Region (本地化和預設區域) 旁的 Edit (編輯)。
5. 若要選取您想要的主控台語言，請選擇下列其中一個選項：

   - 從下拉式清單中選擇瀏覽器預設值，然後選擇儲存設定。

     所有 AWS 服務的主控台文字會以您在瀏覽器設定中設定的偏好語言顯示。

     > **Note**
     >
     > 瀏覽器預設值僅支援 AWS 管理主控台所支援的語言。

   - 從下拉式清單選擇偏好的語言，然後選擇儲存設定。

     所有 AWS 服務的主控台文字會以您偏好的語言顯示。

在 中存取 AWS 您的帳戶、組織、服務配額和帳單資訊 AWS 管理主控台

如果您有必要的許可，您可以從 主控台存取 AWS 您的帳戶、服務配額、組織和帳單資訊。

> **Note**
>
> AWS 管理主控台 僅提供帳戶、組織、服務配額和帳單資訊的存取權。這些服務有自己的個別主控台。如需詳細資訊，請參閱下列內容：
>
> - 《 AWS 帳戶管理 參考指南》中的管理 AWS 您的帳戶。
> - AWS Organizations 《 使用者指南》中的什麼是 AWS Organizations？。
> - 《Service Quotas 使用者指南》中的什麼是 Service Quotas？。 Service Quotas
> - 使用 AWS 帳單使用者指南中的 AWS 帳單與成本管理 首頁。

> **Tip**
>
> 您也可以詢問 Amazon Q 以取得任何這些主題的詳細資訊。如需詳細資訊，請參閱與 Amazon Q 開發人員聊天。

主題

在 中存取帳戶資訊 AWS 管理主控台

如果您有必要的許可，您可以從 主控台存取 AWS 帳戶的相關資訊。

存取您的帳戶資訊

1. 登入 AWS 管理主控台。
2. 在導覽列上，選擇您的帳戶名稱。
3. 選擇帳戶。
4. 檢視您的帳戶資訊。

> **Note**
>
> 如果您想要關閉 AWS 帳戶，請參閱《 AWS 帳戶管理 參考指南》中的關閉 AWS 帳戶。

在 中存取組織資訊 AWS 管理主控台

如果您有必要的許可，您可以從 AWS 主控台存取組織的相關資訊。

存取組織資訊

1. 登入 AWS 管理主控台。

2. 在導覽列上，選擇您的帳戶名稱。
3. 選擇組織。
4. 檢視您的組織資訊。

在 中存取服務配額資訊 AWS 管理主控台

如果您有必要的許可，您可以從 主控台存取服務配額的相關資訊。

存取服務配額資訊

1. 登入 AWS 管理主控台。
2. 在導覽列上，選擇您的帳戶名稱。
3. 選擇服務配額。
4. 檢視並管理您的服務配額資訊。

在 中存取帳單資訊 AWS 管理主控台

如果您有必要的許可，您可以從 AWS 主控台存取費用的相關資訊。

存取您的帳單資訊

1. 登入 AWS 管理主控台。
2. 在導覽列上，選擇您的帳戶名稱。
3. 選擇帳單和成本管理。
4. 使用 AWS 帳單與成本管理 儀表板來尋找每月支出的摘要和明細。

登入多個帳戶

您可以在 的單一 Web 瀏覽器中同時登入最多五個不同的身分 AWS 管理主控台。這些可以是不同帳戶或相同帳戶中根、IAM 或聯合角色的任意組合。您登入的每個身分都會在新標籤 AWS 管理主控台 中開啟自己的 執行個體。

當您啟用多工作階段支援時，主控台 URL 會包含子網域（例如 `https://000000000000-aaaaaaaa.us-east-1.console.aws.amazon.com/console/home?region=us-east-1`）。請務必更新您的書籤和主控台連結。

> **Note**
>
> 您必須選擇在 的帳戶選單中開啟多工作階段，或選擇在 https：//https://console.aws.amazon.com/ 上啟用多工作階段 AWS 管理主控台，以選擇加入多工作階段支援。 您可以隨時選擇在 https://console.aws.amazon.com/ 上停用多工作階段，或清除瀏覽器 Cookie，以選擇退出多工作階段。選擇加入是瀏覽器特定的。

登入多個身分

1. 登入 AWS 管理主控台。
2. 在導覽列上選擇您的帳戶名稱。
3. 選擇新增工作階段，然後選擇登入。系統會開啟新標籤，供您登入。

   > **Note**
   >
   > 如需以根或 IAM 使用者身分登入的詳細資訊，請參閱《 AWS 管理主控台登入使用者指南》中的AWS 登入 。

4. 輸入您的 憑證。
5. 選擇登入。此索引標籤中的 AWS 管理主控台 負載會做為您選擇的 AWS 身分。
6. （選用）聯合到其他角色

   a. 在 AWS IAM Identity Center 存取入口網站或您的單一登入 (SSO) 入口網站中，登入其他角色。

   b. 在 AWS 管理主控台 中選擇您的帳戶名稱。

   c. 檢視您可以選擇的其他工作階段。

AWS 中的建議動作 AWS 管理主控台

AWS 建議的動作透過 AWS 管理主控台 提供完成任務和實作最佳實務的情境建議，協助您更有效率地在 中工作。當相關建議可用時，會出現動態按鈕，您可以用來根據這些建議快速採取動作。

> **Note**
>
> AWS 建議的動作會分析資源狀態以提供建議，但不會處理使用者資料。

主題

AWS 建議動作的功能

- 動作建議 — 根據資源狀態、最佳實務和常用模式取得相關建議
- 一鍵式動作 — 直接從成功訊息或資源檢視完成建議的動作
- 整合式右側面板 — 存取整合式側邊面板以實作建議，而不會中斷您的工作流程
- 多服務支援 — 取得跨多個 AWS 服務的建議

使用建議的動作

使用建議的動作

1. 登入 AWS 管理主控台
2. 尋找#建議的動作按鈕。

> **Note**
>
> 建議的動作按鈕可以出現在 的任何位置， AWS 管理主控台 而且只有在建議的動作可用時才能存取。

3. 選擇 按鈕以檢視可用的動作。
4. 直接或透過側邊面板執行建議。

使用 記錄 AWS 建議動作 API 呼叫 AWS CloudTrail

AWS 建議的動作已與 整合AWS CloudTrail，此服務提供使用者、角色或 所採取動作的記錄 AWS 服務。CloudTrail 會將 AWS 建議動作的所有 API 呼叫擷取為事件。擷取的呼叫包括來自 的 AWS 管理主控台 呼叫，以及對 AWS 建議動作 API 操作的程式碼呼叫。您可以使用 CloudTrail 所收集的資訊，判斷對 AWS 建議動作提出的請求、提出請求的 IP 地址、提出請求的時間，以及其他詳細資訊。

當您建立帳戶 AWS 帳戶 時CloudTrail 會在 中處於作用中狀態，而且您會自動存取 CloudTrail 事件歷史記錄。CloudTrail 事件歷史記錄為 AWS 區域中過去 90 天記錄的管理事件，提供可檢視、可搜尋、可下載且不可變的記錄。如需詳細資訊，請參閱「AWS CloudTrail 使用者指南」中的使用 CloudTrail 事件歷史記錄。檢視事件歷史記錄不會產生 CloudTrail 費用。

如需 AWS 帳戶 過去 90 天內持續記錄的事件，請建立線索或 CloudTrail Lake 事件資料存放區。

AWS CloudTrail 中的建議動作管理事件

管理事件提供有關在 資源上執行的管理操作的資訊 AWS 帳戶。這些也稱為控制平面操作。根據預設，CloudTrail 記錄管理事件。

AWS 建議動作 將所有 AWS 建議動作控制平面操作記錄為管理事件。

AWS 建議的動作事件範例

一個事件代表任何來源提出的單一請求，並包含請求 API 操作的相關資訊、操作的日期和時間、請求參數等。CloudTrail 日誌檔案不是公有 API 呼叫的已排序堆疊追蹤，因此事件不會以任何特定順序顯示。

以下範例顯示的 CloudTrail 事件會示範 操作。


```
{
  "awsRegion": "us-east-2",
  "eventCategory": "Management",
  "eventID": "3510a29e-8070-4cbc-b6a0-9e11f18e26ec",
  "eventName": "ListRecommendedActions",
  "eventSource": "action-recommendations.amazonaws.com",
  "eventTime": "2025-09-03T03:52:02Z",
  "eventType": "AwsApiCall",
  "eventVersion": "1.09",
  "managementEvent": true,
  "readOnly": true,
  "recipientAccountId": "123456789098",
  "requestID": "ec431c91-0315-413d-bdb6-d282fd4f6d83",
  "requestParameters": {
    "context": "*",
    "uxChannel": "EXAMPLE"
  },
  "responseElements": null,
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "EXAMPLE",
```

```
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROARZDBH75ZCUYWFSTUS:EXAMPLE",
    "arn": "arn:aws:sts::123456789098:assumed-role/EXAMPLE",
    "accountId": "12345678909",
    "accessKeyId": "ASIARZDBEXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
          "type": "Role",
          "principalId": "AROARZDBHEXAMPLE",
          "arn": "arn:aws:iam::12345678909:role/EXAMPLE",
          "accountId": "12345678909",
          "userName": "EXAMPLE"
        },
        "attributes": {
          "creationDate": "2025-09-03T03:52:00Z",
          "mfaAuthenticated": "false"
        }
      },
    "invokedBy": "action-recommendations.amazonaws.com"
  }
}
```


如需有關 CloudTrail 記錄內容的資訊，請參閱《AWS CloudTrail 使用者指南》中的 CloudTrail record contents。

在 AWS Console Home 中使用 AWS 管理主控台

本主題說明如何使用 AWS Console Home，包括如何自訂您的主控台首頁。主控台首頁是 的首頁 AWS 管理主控台。當您第一次登入 主控台時，您會登陸 主控台首頁。您可以使用小工具和應用程式自訂主控台首頁。小工具可讓您新增自訂元件，以追蹤 AWS 服務和資源的相關資訊。應用程式可讓您將 AWS 資源和中繼資料分組。您可以使用 myApplications 管理應用程式。您也可以使用主控台首頁來檢視所有 AWS 服務的清單，並與 Amazon Q 聊天。

主題

在 中檢視所有 AWS 服務 AWS Console Home

您可以檢視所有 AWS 服務的清單，並從主控台首頁存取其主控台。

存取 AWS 服務的完整清單

1. 登入 AWS 管理主控台。
2. 選擇漢堡圖示 (☰)，展開主控台首頁選單。
3. 選擇所有 服務。
4. 選取要導覽至其主控台的 AWS 服務。

在 中使用小工具 AWS Console Home

主控台首頁儀表板包含小工具，可顯示您 AWS 環境的重要資訊，並提供 服務的捷徑。您可以藉由新增和移除小工具、進行規模調整或變更其大小來自訂您的體驗。

管理小工具

您可以透過新增、移除、重新執行和調整小工具大小來管理小工具。預設小工具可以移除並再次新增。您也可以將主控台首頁重設為預設配置，並請求新的小工具。

若要新增小工具

1. 在「主控台首頁」儀表板右上角或右下角，選擇 +新增小工具按鈕。
2. 選擇拖曳指標，以小工具標題列左上角的六個垂直點 (⁞⁞) 表示，然後將其拖曳至主控台首頁儀表板。

若要移除小工具

1. 選擇省略符號，以小工具標題列右上角的三個垂直點 (⋮) 表示。
2. 選擇 Remove widget (移除 Widget)。

重新排列您的小工具

- 選擇拖曳指標，以小工具標題列左上角的六個垂直點 (⁞⁞) 表示，然後將小工具拖曳至主控台首頁儀表板上的新位置。

若要重新調整小工具

- 選擇小工具右下角的調整大小圖示，然後拖曳以調整小工具的大小。

如果您想重新開始組織和設定小工具，您可以將「主控台首頁」儀表板重設為預設配置。這會將您對「主控台首頁」儀表板配置的變更進行還原，並將所有小工具還原為其預設位置和大小。

若要將頁面重設為預設配置

1. 在頁面右上角，選擇重設為預設配置按鈕。
2. 若要確認，請選擇重設。

> **Note**
>
> 這將會還原您對「主控台首頁」儀表板配置的所有變更。

在「主控台首頁」儀表板中請求新的小工具

1. 在「主控台首頁」儀表板左下角，選擇要查看其他小工具？ 告訴我們！

說明您想要在「主控台首頁」儀表板中新增的小工具。

2. 選擇提交。

> **Note**
>
> 您的建議會定期審核，並且會透過日後的更新將小工具新增到 AWS 管理主控台。

什麼是 myApplications AWS Console Home？

MyApplications 是主控台首頁的延伸，可協助您管理和監控 AWS上應用程式的成本、健全狀況、安全狀態和效能。應用程式可讓您將資源和中繼資料分組。您可以從 中的單一檢視存取您帳戶中的所有應用程式、所有應用程式的關鍵指標，以及來自多個服務主控台的成本、安全性和操作指標和洞見的概觀 AWS 管理主控台。myApplications 包含下列項目：

- 主控台首頁上的應用程式小工具
- myApplications 可用來檢視應用程式資源成本與安全性調查結果
- myApplications 儀表板，提供重要應用程式指標的檢視，例如成本、效能和安全性調查結果

主題

myApplications 的功能

- 建立應用程式：建立新應用程式並組織其資源。您的應用程式會自動顯示在 myApplications 中，因此您可以在 AWS 管理主控台、 APIs、CLI 和 SDKs 中採取動作。基礎設施即程式碼 (IaC) 會在建

立應用程式時產生，並且您可以透過 myApplication 儀表板存取。IaC 可用於 IaC 工具，包括 AWS CloudFormation 和 Terraform。

- 存取應用程式：您可以透過選取 myApplications 小工具，快速存取任何應用程式。
- 存取您的資源 – 您可以選取應用程式，從服務選單快速檢視您的應用程式資源。選取資源時，您可以直接前往相關的服務主控台。您在資源資料表中的位置已儲存，因此您可以隨時從服務選單繼續瀏覽。
- 比較應用程式指標：使用 myApplications 來比較應用程式的關鍵指標，例如應用程式資源成本以及多個應用程式的重要安全性調查結果。
- 監控和管理應用程式 – 使用警示、Canary 和服務層級目標 Amazon CloudWatch、調查結果和成本趨勢來評估應用程式運作狀態 AWS Security Hub CSPM和效能 AWS Cost Explorer Service。您也可以找到運算指標摘要和最佳化，並從中管理資源合規和組態狀態 AWS Systems Manager。

相關服務

myApplications 會使用下列服務：

- AppRegistry
- AppManager
- Amazon CloudWatch
- Amazon EC2
- AWS Lambda
- AWS 資源總管
- AWS Security Hub CSPM
- Systems Manager
- AWS Service Catalog
- 標記

存取 myApplications

您可以在左側邊欄中選擇 myApplications，以從 AWS 管理主控台 中存取 myApplications。

定價

上的 myApplications AWS 免費提供。沒有安裝費或者預付款。MyApplication 儀表板摘要的基礎資源和服務的使用費用仍按這些資源的已發布費率計算。

myApplications 支援的 區域

myApplications 可在下列位置使用 AWS 區域：

- 美國東部 (俄亥俄)
- 美國東部 (維吉尼亞北部)
- 美國西部 (加利佛尼亞北部)
- 美國西部 (奧勒岡)
- 亞太地區 (孟買)
- 亞太區域 (大阪)
- 亞太區域 (首爾)
- 亞太區域 (新加坡)
- 亞太地區 (雪梨)
- 亞太區域 (東京)
- 加拿大 (中部)
- 歐洲 (法蘭克福)
- 歐洲 (愛爾蘭)
- 歐洲 (倫敦)
- 歐洲 (巴黎)
- 歐洲 (斯德哥爾摩)
- 南美洲 (聖保羅)

選擇加入區域

依預設未啟用選擇加入區域。您必須手動啟用這些區域，才能將其與 myApplications 搭配使用。如需的詳細資訊 AWS 區域，請參閱管理 AWS 區域。支援下列選擇加入的區域：

- 非洲 (開普敦)

- 亞太地區 (香港)
- 亞太區域 (海德拉巴)
- 亞太地區 (雅加達)
- 亞太地區 (墨爾本)
- 歐洲 (米蘭)
- 歐洲 (西班牙)
- 歐洲 (蘇黎世)
- Middle East (Bahrain)
- 中東 (阿拉伯聯合大公國)
- 以色列 (特拉維夫)

myApplications 中的應用程式

應用程式可讓您將資源和中繼資料分組。您可以透過建立、加入、檢視、編輯或刪除應用程式來管理您的應用程式。您也可以建立程式碼片段，以自動將新資源新增至應用程式。

> **Note**
>
> 您也可以將應用程式新增至我的最愛，以便更輕鬆地存取。如需詳細資訊，請參閱???。

主題

- 在 myApplications 中建立應用程式
- 在 myApplications 中加入現有的 AppRegistry 應用程式
- 在 myApplications 中檢視應用程式
- 在 myApplications 中編輯應用程式
- 刪除 myApplications 中的應用程式
- 在 myApplications 中建立程式碼片段

在 myApplications 中建立應用程式

您可以建立新的應用程式，或在 2023 年 11 月 8 日之前the section called “加入應用程式”建立以開始使用 myApplications。建立新應用程式時，您可以透過搜尋和選取資源或使用現有標籤來新增資源。

建立新的應用程式

1. 登入 AWS 管理主控台。
2. 展開左側邊欄，然後選擇 myApplications。
3. 選擇建立應用程式。
4. 輸入應用程式的名稱。
5. (選用) 輸入應用程式描述。
6. (選用) 新增標籤。標籤是可套用至資源的索引鍵/值組，可保存這些資源的相關中繼資料。

> **Note**
>
> AWS 應用程式標籤會自動套用至新建立的應用程式。如需詳細資訊，請參閱 AWS Service Catalog AppRegistry 管理員指南中的AWS 應用程式標籤。

7. (選用) 新增屬性群組。您可以使用屬性群組來儲存應用程式中繼資料。
8. 選擇下一步。
9. （選用）新增資源：

   Search and select resources

   > **Note**
   >
   > 若要搜尋並新增資源，您必須開啟 AWS 資源總管。如需詳細資訊，請參閱 入門 AWS 資源總管。
   > 所有新增的資源都會以 AWS 應用程式標籤標記。

   使用搜尋新增資源

   1. 選擇搜尋並選取資源。
   2. 選擇選取資源。
   3. (選用) 選擇檢視。
   4. 搜尋資源。您可以依關鍵字、名稱或類型進行搜尋，也可以選擇資源類型。

> **Note**
>
> 如果您找不到要尋找的資源，請針對 進行疑難排解 AWS 資源總管。如需詳細資訊，請參閱《Resource Explorer 使用者指南》中的疑難排解 Resource Explorer 搜尋問題。

5. 選取要新增之資源旁的核取方塊。
6. 選擇新增。
7. 選擇下一步。
8. 檢閱選擇。

Automatically add resources using tags

建立應用程式時，您可以透過指定現有的標籤鍵/值對來大量載入資源。透過此方法， AWS 會自動將`awsApplication`標籤套用至所有以指定鍵值對標記的資源，並依預設為應用程式的資源建立標籤同步。啟用 tag-sync 後，任何以指定標籤鍵值對標記的資源都會自動新增至應用程式。如需解決 tag-sync 錯誤的資訊，請參閱 the section called “解決 myApplications 中的標籤同步錯誤”。

> **Note**
>
> 使用標籤將資源新增至應用程式需要許可，才能建立 AppRegistry 應用程式、群組和取消群組資源，以及標記和取消標籤資源。您可以新增資源群組`ResourceGroupsTaggingAPITagUntagSupportedResources` AWS 受管政策，也可以建立和維護自己的自訂政策。下列許可必須新增至 IAM 中的使用者政策陳述式：
>
> - `servicecatalog:CreateApplication`
> - `resource-groups:GroupResources`
> - `resource-groups:UngroupResources`
> - `tag:TagResources`
> - `tag:UntagResources`

使用現有標籤新增資源

1. 選擇使用標籤自動新增資源。
2. 選取現有的標籤索引鍵和值：
   a. 選取用於標記資源的角色。如需詳細資訊，請參閱 AWS Service Catalog AppRegistry 管理員指南中的 Tag-sync 必要許可。
   b. 選取標籤金鑰。
   c. 選取標籤值。
   d. （選用）選擇預覽資源以預覽使用標籤鍵/值對標記的資源。
   e. 檢閱並接受我確認將啟用群組生命週期事件以建立標籤同步通知。GLE 允許 AWS 注意到使用索引鍵/值對標記之資源的變更。
3. 選擇下一步。
4. 檢閱您的應用程式詳細資訊、選取的標籤鍵/值對，以及將新增至應用程式的資源預覽。

> **Note**
>
> 根據預設，使用現有的標籤鍵值對建立應用程式會建立 tag-sync。設定後，tag-sync 也會持續管理應用程式的資源，新增或移除使用指定鍵值對標記或取消標記的資源。您可以從應用程式的管理資源頁面管理 tag-sync。

10. 如果關聯 CloudFormation 堆疊，請選取頁面底部的核取方塊。

> **Note**
>
> 將 CloudFormation 堆疊新增至應用程式需要更新堆疊，因為新增至應用程式的所有資源都會加上 AWS 應用程式標籤。在此更新之後，可能不會反映在最後一次更新堆疊之後執行的手動組態。這可能會導致停機或其他應用程式問題。如需詳細資訊，請參閱《CloudFormation 使用者指南》中的更新堆疊資源的行為。

11. 選擇建立應用程式。

在 myApplications 中加入現有的 AppRegistry 應用程式

您可以加入 2023 年 11 月 8 日之前建立的現有 AppRegistry 應用程式，以開始使用 myApplications。

加入現有的 AppRegistry 應用程式

1. 登入 AWS 管理主控台。
2. 在左側邊欄中，選擇 myApplications。
3. 使用搜尋列尋找應用程式。
4. 選取您的應用程式。
5. 選擇加入 ######。
6. 如果要與 CloudFormation 堆疊建立關聯，請選取提醒方塊中的核取方塊。
7. 選擇加入應用程式。

在 myApplications 中檢視應用程式

您可以從 myApplications 或服務選單檢視您的應用程式。如果從 myApplications 檢視您的應用程式，您可以在卡片或資料表檢視中檢視所有 AWS 區域 或特定 AWS 區域 及其相關資訊。

> **Note**
>
> 您也可以從我的最愛功能表檢視新增至我的最愛的應用程式。如需詳細資訊，請參閱中的我的最愛 AWS 管理主控台。

myApplications

在 myApplications 中檢視應用程式

1. 開啟 AWS 管理主控台。
2. 在左側邊欄中，選擇 myApplications。
3. 在地區中，選取目前地區或支援的區域。
4. 若要尋找特定應用程式，請在搜尋列中輸入其名稱、關鍵字或說明。
5. (選用) 預設檢視為卡片檢視。若要自訂應用程式頁面：
   a. 選取齒輪圖示。
   b. (選用) 選取頁面大小。
   c. (選用) 選擇卡片或資料表檢視。
   d. (選用) 選取頁面大小。

e. (選用) 如果使用資料表檢視，請選取資料表檢視的屬性。

f. (選用) 切換可見的應用程式屬性及其顯示順序。

g. 選擇確認。

Services menu

從服務功能表檢視應用程式

1. 開啟 AWS 管理主控台。
2. 在導覽列中，選擇服務 (⁝⁝⁝)。
3. 選擇所有應用程式。
4. 選取應用程式。
5. （選用）選取檢視。
6. （選用）選取篩選條件。您可以依屬性或標籤篩選資源。如需詳細資訊，請參閱《 AWS 資源總管 使用者指南》中的搜尋 Resource Explorer 的查詢語法參考。
7. （選用）選取資源以在相關服務主控台中檢視。

> **Tip**
>
> 您可以選擇服務 (⁝⁝⁝) 繼續瀏覽您離開的資源。您套用的搜尋篩選條件也會保留。

在 myApplications 中編輯應用程式

編輯應用程式會開啟 AppRegistry，以便您可以更新其說明。您也可以使用 AppRegistry 編輯應用程式的標籤和屬性群組。

編輯應用程式

1. 開啟 AWS 管理主控台。
2. 在主控台的左側邊欄中，選擇 myApplications。
3. 選取您要編輯的應用程式。
4. 在 myApplication 儀表板上，選擇動作，然後選擇編輯應用程式。
5. 在編輯應用程式中，對應用程式的描述、標籤和屬性群組進行所需的變更。

> **Note**
>
> 如需管理標籤和屬性群組的詳細資訊，請參閱 AWS Service Catalog AppRegistry 管理員指南中的管理標籤和編輯屬性群組。

6. 選擇更新。

刪除 myApplications 中的應用程式

如果已不再需要應用程式，則可將其刪除。刪除應用程式之前，請務必移除所有未由 AWS 服務建立的相關聯資源共用和屬性群組。

> **Note**
>
> 刪除應用程式不會影響您的資源。以 AWS 應用程式標籤標記的資源將保持標記。

刪除 應用程式

1. 開啟 AWS 管理主控台。
2. 在主控台的左側邊欄中，選擇 myApplications。
3. 選取您要刪除的應用程式。
4. 在 myApplication 儀表板上，選擇動作。
5. 選擇刪除應用程式。
6. 確認您的刪除，然後選擇刪除。

在 myApplications 中建立程式碼片段

myApplications 會為所有應用程式建立程式碼片段。您可以使用程式碼片段，自動將新建立的資源新增至使用基礎設施即程式碼 (IaC) 工具的應用程式。所有新增的資源都會加上 AWS 應用程式標籤，以將其與您的應用程式建立關聯。

建立應用程式的程式碼片段

1. 開啟 AWS 管理主控台。
2. 在主控台的左側邊欄中，選擇 myApplications。

3. 搜尋並選取應用程式。
4. 選擇動作。
5. 選擇取得程式碼片段。
6. 選取程式碼片段類型。
7. 選擇複製可將程式碼複製到剪貼簿。
8. 將程式碼貼入 IaC 工具中。

myApplications 中的資源

在 中 AWS，資源是您可以使用的實體。範例包括 Amazon EC2 執行個體、 AWS CloudFormation 堆疊或 Amazon S3 儲存貯體。您可以在 myApplications 中新增和移除資源，以管理這些資源。

主題

- 在 myApplications 中新增資源
- 移除 myApplications 中的資源
- 檢視 myApplications 中的資源

在 myApplications 中新增資源

將資源新增至應用程式可讓您將資源分組並管理其安全性、效能和合規性。您可以透過搜尋並選取現有應用程式，或使用現有標籤並執行標籤同步，將資源新增至現有應用程式。

Search and select resources

搜尋並選取資源

1. 開啟 AWS 管理主控台。
2. 在主控台的左側邊欄中，選擇 myApplications。
3. 搜尋並選取應用程式。
4. 選擇管理資源。
5. 選擇新增資源。
6. (選用) 選擇檢視。
7. 搜尋資源。您可以依關鍵字、名稱或類型進行搜尋，也可以選擇資源類型。

> **Note**
>
> 如果您找不到要尋找的資源，請針對 進行疑難排解 AWS 資源總管。如需詳細資訊，請參閱《Resource Explorer 使用者指南》中的疑難排解 Resource Explorer 搜尋問題。

8. 選取要新增之資源旁的核取方塊。
9. 選擇新增。

Automatically add resources using tags

建立應用程式時，您可以透過指定現有的標籤鍵/值對來大量載入資源。透過此方法， AWS 會自動將`awsApplication`標籤套用至所有資源，並依預設為應用程式的資源建立 tag-sync。啟用 tag-sync 後，任何以指定標籤鍵值對標記的資源都會自動新增至應用程式。

使用現有標籤新增資源

1. 開啟 AWS 管理主控台。
2. 在主控台的左側邊欄中，選擇 myApplications。
3. 選擇管理資源。
4. 選擇建立 tag-sync。
5. 選取現有的標籤索引鍵和值：
   a. 選取用於標記資源的角色。如需詳細資訊，請參閱 AWS Service Catalog AppRegistry 管理員指南中的標籤同步任務所需許可。
   b. 選取標籤金鑰。
   c. 選取標籤值。
   d. 檢閱並接受我確認將啟用群組生命週期事件以建立標籤同步通知。GLE 允許 AWS 注意到使用索引鍵/值對標記之資源的變更。
6. 選擇建立標籤同步。

解決 myApplications 中的標籤同步錯誤

本節說明常見的 tag-sync 錯誤，以及如何解決這些錯誤。嘗試解決錯誤之後，您可以重試失敗的 tag-sync 任務。

- 權限不足 — 您未具備啟動、更新或取消標籤同步所需的最低權限。如需詳細資訊，請檢閱 Tag-sync 所需的許可。確保您指定執行 tag-sync 的角色具有最低必要許可後，請重試失敗的 tag-sync 任務。
- 已存在 — 此應用程式已有具有此標籤鍵值對的任務。應用程式可以支援多個標籤同步，但每個標籤同步必須有不同的標籤鍵值對。請在指定不同的標籤鍵值對後，重試失敗的標籤同步任務。
- 達到上限 — 您已達到所有應用程式中每個帳戶 100 個標籤同步讓務的上限。

移除 myApplications 中的資源

您可以移除資源以取消資源與應用程式的關聯。

移除資源

1. 開啟 AWS 管理主控台。
2. 在主控台的左側邊欄中，選擇 myApplications。
3. 搜尋並選取應用程式。
4. 選擇管理資源。
5. (選用) 選擇檢視。
6. 搜尋資源。您可以依關鍵字、名稱或類型進行搜尋，也可以選擇資源類型。

> **Note**
>
> 如果您找不到要尋找的資源，請針對 進行疑難排解 AWS 資源總管。如需詳細資訊，請參閱《Resource Explorer 使用者指南》中的疑難排解 Resource Explorer 搜尋問題。

7. 選擇移除。
8. 選擇移除資源，確認您要移除資源。

檢視 myApplications 中的資源

您可以從 myApplications 和服務選單檢視應用程式資源。

myApplications

在 myApplications 中檢視您的資源

1. 開啟 AWS 管理主控台。
2. 展開左側邊欄，然後選擇 myApplications。

3. 選取應用程式。
4. 在資源小工具中，檢視您的資源。

Services menu

從服務功能表檢視應用程式

1. 開啟 AWS 管理主控台。
2. 在導覽列中，選擇服務 (⁝⁝⁝)。
3. 選擇所有應用程式。
4. 選取應用程式。
5. （選用）選取檢視。
6. （選用）選取篩選條件。您可以依屬性或標籤篩選資源。如需詳細資訊，請參閱《 AWS 資源總管 使用者指南》中的搜尋 Resource Explorer 的查詢語法參考。
7. （選用）選取資源以在相關服務主控台中檢視。

> **Tip**
>
> 您可以選擇服務 (⁝⁝⁝) 繼續瀏覽您離開的資源。您套用的搜尋篩選條件也會保留。

中的 myApplications 儀表板 AWS Console Home

您建立或加入的每個應用程式都有其自己的 myApplications 儀表板。myApplications 儀表板包含成本、安全性和操作小工具，可呈現來自多個 AWS 服務的洞見。您也可以將每個小工具加入最愛，重新排序，移除或調整大小。如需詳細資訊，請參閱在 中使用小工具 AWS Console Home。

主題

- 應用程式儀表板安裝小工具
- 應用程式摘要小工具
- 運算小工具
- 成本和用量小工具
- AWS 安全小工具
- AWS 彈性小工具

- 資源小工具
- DevOps 小工具
- 監控和操作小工具
- 標籤小工具

應用程式儀表板安裝小工具

此小工具包含建議的入門活動清單，可用來協助您設定 AWS 服務 來管理應用程式資源。

應用程式摘要小工具

此小工具會顯示應用程式的名稱、說明和 AWS 應用程式標籤。您可以存取和複製基礎設施即程式碼 (IaC) 中的應用程式標籤，以手動標記資源。

運算小工具

此小工具會顯示您新增至應用程式之運算資源的資訊和指標。其中包括警示總數和運算資源類型總數。此小工具也會顯示 Amazon CloudWatch Amazon EC2 執行個體 CPU 使用率和 Lambda 調用的資源效能指標趨勢圖。

設定運算小工具

若要在運算小工具中填入資料，請為應用程式設定至少一個 Amazon EC2 執行個體或 Lambda 函數。如需詳細資訊，請參閱《AWS Lambda 開發人員指南》中的 Amazon 彈性運算雲端文件和 Lambda 入門。

成本和用量小工具

此小工具會顯示應用程式資源 AWS 的成本和用量資料。您可以使用此資料來比較每月成本，並依據 AWS 服務檢視成本明細。此小工具只會摘要標示 AWS 應用程式標籤的資源成本，但不包括稅金、費用和其他未直接與資源關聯的共用成本。顯示的是非混合的成本，更新頻率為每 24 小時至少一次。如需詳細資訊，請參閱《AWS Cost Management 使用者指南》中的使用 AWS 資源總管分析成本。

設定成本和用量小工具

若要設定成本和用量小工具，請 AWS Cost Explorer Service 為您的應用程式和帳戶啟用 。這項服務不收取額外費用，而且沒有安裝費或預付款。如需詳細資訊，請參閱《AWS Cost Management 使用者指南》中的啟用 Cost Explorer。

AWS 安全小工具

此小工具會顯示 AWS 您應用程式安全性的安全性問題清單。 AWS 安全性提供應用程式安全性問題清單的完整檢視 AWS。您可以依嚴重性存取最近的優先順序調查結果、監控其安全狀態、存取最近的重大或非常嚴重的調查結果，以及取得後續步驟的深入洞見。如需詳細資訊，請參閱AWS Security Hub CSPM。

設定 AWS 安全性小工具

若要設定 AWS 安全性小工具， AWS Security Hub CSPM 請為您的應用程式和帳戶設定 。如需詳細資訊，請參閱AWS Security Hub CSPM 《 使用者指南》中的什麼是 AWS Security Hub CSPM？。如需定價資訊，請參閱《AWS Security Hub CSPM 使用者指南》中的 AWS Security Hub CSPM 免費試用、用量和定價。

AWS Security Hub CSPM 需要您設定 AWS Config 錄製。此服務提供與您 AWS 帳戶相關聯資源的詳細檢視。如需詳細資訊，請參閱《AWS Systems Manager 使用者指南》中的 AWS Systems Manager。

AWS 彈性小工具

此小工具會顯示來自 AWS Resilience Hub 的應用程式彈性詳細資訊。啟動評估後， AWS Resiliency Hub 會針對預先定義的彈性政策評估其資源，以分析應用程式的彈性狀態。您可以存取指標，例如彈性分數、政策違規、政策偏離、資源偏離，以及您的彈性分數歷史記錄。您的應用程式會每日評估以增強追蹤功能，但您可以隨時停用此功能。如需詳細資訊，請參閱AWS Resilience Hub。如需定價資訊，請參閱 AWS Resilience Hub 定價。

設定 AWS 彈性小工具

若要設定 AWS 彈性小工具，請新增應用程式。如需詳細資訊，請參閱AWS Resilience Hub 《 使用者指南》中的什麼是 AWS Resilience Hub？。

資源小工具

此小工具使用 AWS Resource Explorer 來顯示您在檢視中新增至應用程式的資源。您也可以使用此小工具，使用名稱、標籤和 IDs 等資源中繼資料來搜尋或篩選資源。如需詳細資訊，請參閱 AWS Resource Explorer。

設定資源小工具

若要設定資源小工具，請使用 Resource Explorer 加入。如需詳細資訊，請參閱《Resource Explorer 使用者指南》中的 Resource Explorer 入門。 AWS

DevOps 小工具

這個小工具會顯示操作洞見，以便您評估合規性並採取適合應用程式的行動。這些洞見包含：

- 機群管理
- 狀態管理
- 修補管理
- 組態與 OpsItems 管理

設定 DevOps 小工具

若要設定 DevOps 小工具，請為您的應用程式和帳戶啟用 AWS Systems Manager OpsCenter。若要詳細資訊，請參閱《AWS Systems Manager 使用者指南》中的 Systems Manager Explorer 和 OpsCenter 入門。啟用 OpsCenter AWS Systems Manager Explorer 可讓 設定 AWS Config 和 ，Amazon CloudWatch 使其事件根據常用的規則和事件自動建立 OpsItems。如需詳細資訊，請參閱《AWS Systems Manager 使用者指南》中的設定 OpsCenter。

您可以設定執行個體，讓 Systems Manager 代理程式執行，並套用許可以啟用修補程式掃描。如需詳細資訊，請參閱《AWS Systems Manager 使用者指南》中的 AWS Systems Manager 快速設定。

您也可以設定修補程式管理員，為您的應用程式設定 Amazon EC2 執行個體的自動 AWS Systems Manager 修補。如需詳細資訊，請參閱《AWS Systems Manager 使用者指南》中的使用快速設定修補程式政策。

如需定價資訊，請參閱 AWS Systems Manager 定價。

監控和操作小工具

這個小工具顯示：

- 與應用程式相關聯之資源的警示和提醒
- 應用程式服務層級目標 (SLO) 和指標
- 可用的 AWS Application Signals 指標

設定監控和操作小工具

若要設定監控和操作小工具，請在 AWS 您的帳戶中建立 CloudWatch 警示和 Canary。如需詳細資訊，請參閱《Amazon CloudWatch 使用者指南》中的使用 Amazon CloudWatch 警示和建立金絲雀。

如需 CloudWatch 警示和合成金絲雀定價，請分別參閱 Amazon CloudWatch 定價和 AWS 雲端操作和遷移部落格。

如需 CloudWatch Application Signals 的詳細資訊，請參閱《Amazon CloudWatch 使用者指南》中的啟用 Amazon CloudWatch Application Signals。 Amazon CloudWatch

標籤小工具

這個小工具顯示與應用程式相關的所有標籤。您可以使用此小工具來追蹤和管理應用程式中繼資料 (重要性、環境、成本中心)。如需詳細資訊，請參閱 標記 AWS 資源的最佳實務 AWS 白皮書中的什麼是標籤？。

在 中與 Amazon Q Developer 聊天 AWS Console Home

Amazon Q Developer 是生成式人工智慧 (AI) 支援的對話式助理，可協助您了解、建置、擴展和操作 AWS 應用程式。您可以向 Amazon Q 詢問任何有關 AWS 架構 AWS、 AWS 資源、最佳實務、文件等的問題。您也可以建立支援案例，並從即時客服人員取得協助。如需詳細資訊，請參閱《Amazon Q 開發人員使用者指南》中的什麼是 Amazon Q？。

開始使用 Amazon Q

您可以在 AWS 管理主控台、 AWS 文件網站、 AWS 網站或 AWS 主控台行動應用程式中選擇六邊形 Amazon Q 圖示，開始與 Amazon Q 聊天。如需詳細資訊，請參閱《Amazon Q 開發人員使用者指南》中的開始使用 Amazon Q 開發人員。

範例問題

以下是您可以詢問 Amazon Q 的一些範例問題：

- `How do I get billing support?`
- `How do I create an EC2 instance?`
- `How do I troubleshoot a "Failed to load" error?`
- `How do I close an AWS account?`
- `Can you connect me with a person?`

AWS 管理主控台 私有存取

AWS 管理主控台 Private Access 是一項進階安全功能，用於控制對 的存取 AWS 管理主控台。當您想要防止使用者 AWS 帳戶 從網路中意外登入 時，主控台私有存取非常有用。使用此功能時，您可以將的存取限制 AWS 管理主控台 為 AWS 帳戶 當流量來自您的網路時指定的一組已知 。當您想要確保來自 的所有呼叫都來自您的網路和允許的帳戶時 AWS 管理主控台 ， AWS 服務 主控台私有存取也很有用。

主題

Private Access 支援的 AWS 區域服務主控台和功能

AWS 管理主控台 Private Access 僅支援一部分的區域 AWS 和服務。 AWS 管理主控台中不受支援的服務主控台將處於非作用中。此外，使用 AWS 管理主控台 私有存取時，某些 AWS 管理主控台 功能可能會停用，例如，統一設定中的預設區域選擇。

支援下列區域和服務主控台。

支援的區域

- 美國東部 (俄亥俄)
- 美國東部 (維吉尼亞北部)
- 美國西部 (加利佛尼亞北部)
- 美國西部 (奧勒岡)
- 亞太地區 (海德拉巴)
- 亞太地區 (孟買)

- 亞太地區 (首爾)
- 亞太地區 (大阪)
- 亞太地區 (新加坡)
- 亞太地區 (雪梨)
- 亞太地區 (馬來西亞)
- 亞太區域 (泰國)
- 亞太地區 (東京)
- 加拿大 (中部)
- 歐洲 (法蘭克福)
- 歐洲 (愛爾蘭)
- 歐洲 (倫敦)
- 歐洲 (巴黎)
- 歐洲 (斯德哥爾摩)
- 南美洲 (聖保羅)
- 非洲 (開普敦)
- 亞太地區 (香港)
- 亞太地區 (雅加達)
- 亞太地區 (墨爾本)
- 加拿大西部 (卡加利)
- 墨西哥 (中部)
- 歐洲 (米蘭)
- 歐洲 (西班牙)
- 歐洲 (蘇黎世)
- Middle East (Bahrain)
- 中東 (阿拉伯聯合大公國)
- 以色列 (特拉維夫)

支援的服務主控台

- Amazon API Gateway

- AWS App Mesh
- AWS Application Migration Service
- AWS Artifact
- Amazon Athena
- AWS Audit Manager
- AWS Auto Scaling
- AWS Batch
- AWS Billing Conductor
- AWS 帳單與成本管理
- AWS Budgets
- AWS Certificate Manager
- AWS Cloud Map
- AWS CloudFormation
- Amazon CloudFront
- AWS CloudTrail
- Amazon CloudWatch
- AWS CodeArtifact
- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- Amazon CodeGuru
- AWS CodePipeline
- Amazon Comprehend
- Amazon Comprehend Medical
- AWS Compute Optimizer
- AWS Console Home
- AWS Control Tower
- Amazon DataZone

- AWS Database Migration Service
- AWS DataSync
- AWS DeepRacer
- AWS Direct Connect
- AWS Directory Service
- Amazon DocumentDB
- Amazon DynamoDB
- Amazon EC2
- Amazon EC2 全域檢視
- EC2 Image Builder
- Amazon EC2 Instance Connect
- Amazon Elastic Container Registry
- Amazon Elastic Container Service
- AWS Elastic Disaster Recovery
- Amazon Elastic File System
- Amazon Elastic Kubernetes Service
- Elastic Load Balancing
- Amazon ElastiCache
- Amazon EMR
- Amazon EventBridge
- AWS Firewall Manager
- Amazon GameLift Servers
- AWS Glue
- AWS Global Accelerator
- AWS Glue DataBrew
- AWS Ground Station
- Amazon GuardDuty
- AWS IAM Identity Center

- AWS Identity and Access Management
- AWS Identity and Access Management Access Analyzer
- Amazon Inspector
- Amazon Kendra
- AWS Key Management Service
- Amazon Kinesis
- Amazon Managed Service for Apache Flink
- Amazon Data Firehose
- Amazon Kinesis Data Streams
- Amazon Kinesis Video Streams
- AWS Lambda
- Amazon Lex
- AWS License Manager
- Amazon Managed Grafana
- Amazon Macie
- Amazon Managed Streaming for Apache Kafka
- Amazon Managed Workflows for Apache Airflow (MWAA)
- AWS Migration Hub 策略建議
- Amazon MQ
- 網路存取分析器
- AWS Network Firewall
- AWS Network Manager
- Amazon OpenSearch Service
- AWS Organizations
- AWS 私有憑證授權單位
- 公有運作狀態儀表板
- Amazon Rekognition
- Amazon Relational Database Service

- AWS Resource Access Manager
- AWS Resource Groups 和 標籤編輯器
- Amazon Route 53 Resolver
- Amazon Route 53 Resolver DNS 防火牆
- Amazon S3 on Outposts
- Amazon SageMaker
- Amazon SageMaker 執行期
- Amazon SageMaker AI 合成資料
- AWS Secrets Manager
- AWS Service Catalog
- AWS Security Hub CSPM
- Service Quotas
- AWS Signer
- Amazon Simple Email Service
- Amazon SNS
- Amazon Simple Queue Service
- Amazon Simple Storage Service (Amazon S3)
- AWS SQL Workbench
- AWS Step Functions
- AWS Storage Gateway
- 支援
- AWS Systems Manager
- Amazon Timestream
- AWS Transfer Family
- AWS Trusted Advisor
- 統一設定
- Amazon VPC IP 地址管理員
- Amazon Virtual Private Cloud
- Amazon WorkSpaces 精簡型用戶端

AWS 管理主控台 Private Access 安全控制概觀

AWS 管理主控台 來自您網路的 帳戶限制

AWS 管理主控台 當您只想將 AWS 管理主控台 網路對 的存取限制為 AWS 帳戶 組織中指定的一組已知時，私有存取非常有用。如此一來，您就可以防止使用者從您的網路中登入到意外 AWS 帳戶 狀態。您可以使用 AWS 管理主控台 VPC 端點政策來實作這些控制項。如需詳細資訊，請參閱實作服務控制政策和 VPC 端點政策。

從您的網路到網際網路的連線

存取 所使用的資產，例如靜態內容 (JavaScript、CSS、映像），以及 AWS 服務 未啟用的所有資產 AWS 管理主控台，仍需要來自您網路的網際網路連線AWS PrivateLink。如需 使用的頂層網域清單 AWS 管理主控台，請參閱 疑難排解。

> **Note**
>
> 目前， AWS 管理主控台 Private Access 不支援 `status.aws.amazon.com`、`health.aws.amazon.com`和 等端點`docs.aws.amazon.com`。您需要將這些網域路由到公有網際網路。

必要的 VPC 端點和 DNS 組態

AWS 管理主控台 私有存取需要每個區域以下兩個 VPC 端點。以您自己的區域資訊取代*##*。

1. 適用於 的 com.amazonaws.*region*.console AWS 管理主控台
2. 的 com.amazonaws.*region*.signin AWS 登入

> **Note**
>
> 一律將基礎設施和網路連線佈建至美國東部 (維吉尼亞北部)(us-east-1) 區域，無論您使用 AWS 管理主控台的其他區域如何。您可以使用 AWS Transit Gateway 來設定美國東部 (維吉尼亞北部) 與其他所有區域之間的連線。如需詳細資訊，請參閱《Amazon VPC 傳輸閘道指南》中的開始使用傳輸閘道。您也可以使用 Amazon VPC 對等互連。如需詳細資訊，請參閱《Amazon VPC 對等互連指南》中的什麼是 VPC 對等互連。若要比較這些選項，請參閱 Amazon Virtual Private Cloud 連線選項白皮書中的 Amazon VPC 對 Amazon VPC 連線選項。

主題

DNS AWS 管理主控台 和 的 組態 AWS 登入

如要將網路流量路由至個別的 VPC 端點，在您的使用者將存取 AWS 管理主控台的網路中設定 DNS 記錄。這些 DNS 記錄會將您的使用者瀏覽器流量導向您建立的 VPC 端點。

您可以建立單一託管區域。然而 `health.aws.amazon.com` 和 `docs.aws.amazon.com` 這類端點將無法存取，因為它們沒有 VPC 端點。您需要將這些網域路由到公有網際網路。我們建議您為每個區域建立兩個私有託管區域，一個用於 `signin.aws.amazon.com`，另一個用於包含下列 CNAME 記錄的 `console.aws.amazon.com`：

- 登入
  - *region*.signin.aws.amazon.com 指向登入區域中的 AWS 登入 VPC 端點，DNS其中 *region* 是所需區域
  - signin.aws.amazon.com 指向美國東部（維吉尼亞北部）的 AWS 登入 VPC 端點 (us-east-1)
- 主控台
  - *region*.console.aws.amazon.com 指向主控台區域中的 AWS 管理主控台 VPC 端點，DNS其中 *region* 是所需區域
  - *.*region*.console.aws.amazon.com 指向主控台區域中的 AWS 管理主控台 VPC 端點，DNS其中 *region* 是所需區域
  - *.*region*.console.aws.amazon.com 指向主控台區域中的 AWS 管理主控台 VPC 端點 DNS
  - 僅適用美國東部 (維吉尼亞北部) 區域的無區域 CNAME 記錄。您一律須設定美國東部 (維吉尼亞北部) 區域。
    - signin.aws.amazon.com 指向美國東部（維吉尼亞北部）(us-east-1) 的 AWS 登入 VPC 端點
    - *.console.aws.amazon.com 指向美國東部（維吉尼亞北部）(us-east-1) 的 AWS 管理主控台 VPC 端點

  如需有關建立 CNAME 記錄的說明，請參閱 Amazon Route 53 開發人員指南中的使用記錄。

  有些 AWS 主控台，包括 Amazon S3，會針對其DNS名稱使用不同的模式。以下是兩個範例：
  - support.console.aws.amazon.com
  - s3.console.aws.amazon.com

若要將此流量導向 AWS 管理主控台 VPC 端點，您需要個別新增這些名稱。建議您為所有端點設定路由，以提供完全私有的體驗。不過，這不需要使用 AWS 管理主控台 Private Access。

下列json檔案包含每個區域要設定的 AWS 服務和主控台端點完整清單。使用 `com.amazonaws.region.console` 端點下方的 `PrivateIpv4DnsNames` 欄位做為 DNS 名稱。

- https://configuration.private-access.console.amazonaws.com/us-east-1.config.json
- https://configuration.private-access.console.amazonaws.com/us-east-2.config.json
- https://configuration.private-access.console.amazonaws.com/us-west-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-northeast-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-northeast-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-southeast-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-southeast-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-south-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-south-2.config.json
- https://configuration.private-access.console.amazonaws.com/ca-central-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-central-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-west-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-west-2.config.json
- https://configuration.private-access.console.amazonaws.com/il-central-1.config.json

> **Note**
>
> 當我們在 AWS 管理主控台 私人存取範圍中新增其他端點時，此清單每個月都會更新。若要讓您的私人託管區域保持更新，請定期提取前述檔案清單。

如果您使用 Route 53 來設定您的 DNS，請前往 https://console.aws.amazon.com/route53/v2/hostedzones# 以驗證 DNS 設定。對於 Route 53 中的每個私人託管區域，請確認下列記錄集存在。

- console.aws.amazon.com
- signin.aws.amazon.com
- *.*region*.console.aws.amazon.com
- *region*.console.aws.amazon.com
- *.*region*.console.aws.amazon.com

- signin.aws.amazon.com
- *region*.signin.aws.amazon.com
- 之前列出的 JSON 檔案中存在的其他記錄

中的 AWS 服務的 VPC 端點和DNS組態 AWS 管理主控台

透過直接瀏覽器請求和 Web 伺服器代理之請求的 AWS 服務 組合進行 AWS 管理主控台 呼叫。若要將此流量導向您的 AWS 管理主控台 VPC 端點，您必須新增 VPC 端點，並DNS為每個相依 AWS 服務進行設定。

下列json檔案列出可供您使用的 AWS PrivateLink 支援 AWS 服務 。如果服務未與 整合 AWS PrivateLink，則不會包含在這些檔案中。

- https://configuration.private-access.console.amazonaws.com/us-east-1.config.json
- https://configuration.private-access.console.amazonaws.com/us-east-2.config.json
- https://configuration.private-access.console.amazonaws.com/us-west-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-northeast-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-northeast-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-southeast-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-southeast-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-south-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-south-2.config.json
- https://configuration.private-access.console.amazonaws.com/ca-central-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-central-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-west-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-west-2.config.json
- https://configuration.private-access.console.amazonaws.com/il-central-1.config.json

使用對應服務之 VPC 端點的 `ServiceName` 欄位，以新增至您的 VPC。

> **Note**
>
> 我們每個月都會更新此清單，因為我們將 AWS 管理主控台 私有存取支援新增至更多服務主控台。若要保持最新狀態，請定期提取上述檔案清單並更新您的 VPC 端點。

實作服務控制政策和 VPC 端點政策

您可以使用服務控制政策 (SCPs) 和 VPC 端點政策進行 AWS 管理主控台 私有存取，以限制允許 AWS 管理主控台 從您的 VPC 及其連線的內部部署網路使用 的一組帳戶。

主題

搭配 AWS Organizations 服務控制政策使用 AWS 管理主控台 私有存取

如果您的 AWS 組織使用允許特定服務的服務控制政策 (SCP)，您必須將 `signin:*`新增至允許的動作。需要此許可，因為 AWS 管理主控台 透過私有存取 VPC 端點登入 會執行 SCP 在沒有許可的情況下封鎖的 IAM 授權。例如，下列服務控制政策允許在組織中使用 Amazon EC2 和 CloudWatch 服務，包括何時使用 AWS 管理主控台 私有存取端點進行存取。

```
{
  "Effect": "Allow",
  "Action": [
    "signin:*",
    "ec2:*",
    "cloudwatch:*",
    ... Other services allowed
  },
  "Resource": "*"
}
```

如需 SCP 的詳細資訊，請參閱《AWS Organizations 使用者指南》中的服務控制政策 (SCP)。

僅允許將 AWS 管理主控台 用於預期的帳戶和組織（受信任的身分）

AWS 管理主控台 和 AWS 登入 支援專門控制登入帳戶身分的 VPC 端點政策。

與其他 VPC 端點政策不同，政策會在身分驗證之前進行評估。因此，它會特別控制已驗證工作階段的登入和使用，而不是工作階段採取的任何 AWS 服務特定動作。例如，當工作階段存取 AWS 服務主控台時，例如 Amazon EC2 主控台，這些 VPC 端點政策將不會針對顯示該頁面所採取的 Amazon EC2 動作進行評估。反之，您可以使用與登入 IAM 主體相關聯的 IAM 政策來控制其 AWS 服務動作的許可。

> **Note**
>
> AWS 管理主控台 和 SignIn VPC 端點的 VPC 端點政策僅支援有限的政策配方子集。每個 `Principal` 和 `Resource` 都應設定為 `*`，而 `Action` 應設定為 `*` 或 `signin:*`。您可以使用 `aws:PrincipalOrgId` 和 `aws:PrincipalAccount` 條件金鑰控制對 VPC 端點的存取。

建議主控台和 SignIn VPC 端點使用下列政策。

此 VPC 端點政策允許在指定的 AWS 組織中登入 AWS 帳戶 ，並封鎖任何其他帳戶的登入。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgId": "o-xxxxxxxxxxx"
        }
      }
    }
  ]
}
```

此 VPC 端點政策會將登入限制為特定 清單， AWS 帳戶 並封鎖任何其他帳戶的登入。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalAccount": [ "111122223333", "222233334444" ]
        }
      }
    }
  ]
}
```

限制 AWS 帳戶 和 AWS 管理主控台 登入 VPC 端點上組織的政策會在登入時進行評估，並定期重新評估現有工作階段。

實作以身分為基礎的政策以及其他政策類型

您可以透過 AWS 建立政策並將其連接到 IAM 身分 （使用者、使用者群組或角色） 或 AWS 資源來管理 中的存取。此頁面說明 政策與 AWS 管理主控台 Private Access 搭配使用時的運作方式。

支援的 AWS 全域條件內容索引鍵

AWS 管理主控台 Private Access 不支援 `aws:SourceVpce`和 `aws:VpcSourceIp` AWS 全域條件內容金鑰。使用 AWS 管理主控台 私有存取時，您可以改為在政策中使用 `aws:SourceVpc` IAM 條件。

AWS 管理主控台 私有存取如何與 aws：SourceVpc 搭配使用

本節說明 產生的請求 AWS 管理主控台 可採取的各種網路路徑 AWS 服務。一般而言， AWS 服務主控台會與 AWS 管理主控台 Web 伺服器代理的直接瀏覽器請求和請求混合實作 AWS 服務。這些實作可能會有所變更，且不會另行通知。如果您的安全需求包括 AWS 服務 使用 VPC 端點的存取權，我們建議您為打算從 VPC 使用的所有服務設定 VPC 端點，無論是直接或透過 AWS 管理主控台 私有存

取。此外，您必須在政策中使用 aws:SourceVpc IAM 條件，而不是具有 AWS 管理主控台 私有存取功能的特定aws:SourceVpce值。本節提供不同網路路徑如何運作的詳細資訊。

使用者登入 後 AWS 管理主控台，他們會 AWS 服務 透過直接瀏覽器請求和 AWS 管理主控台 Web 伺服器代理到 AWS 伺服器的請求組合向 提出請求。例如，CloudWatch 圖形資料請求會直接從瀏覽器發出。而某些 AWS 服務主控台請求，例如 Amazon S3，是由 Web 伺服器代理至 Amazon S3。

對於直接瀏覽器請求，使用 AWS 管理主控台 Private Access 不會進行任何變更。和以前一樣，請求會透過 VPC 設定為到達 monitoring.region.amazonaws.com 的任何網路路徑來到達服務。如果 VPC 為 com.amazonaws.region.monitoring 設定了 VPC 端點，則該請求將透過 CloudWatch VPC 端點到達 CloudWatch。如果 CloudWatch 沒有適用的 VPC 端點，則該請求將透過 VPC 上的網際網路閘道到達其公用端點的 CloudWatch。透過 CloudWatch VPC 端點到達 CloudWatch 的請求將具有 IAM 條件，aws:SourceVpc 與 aws:SourceVpce 會設定為各自的值。那些透過其公有端點到達 CloudWatch 的使用者會將 aws:SourceIp 設為請求的來源 IP 地址。如需有關這些條件金鑰的詳細資訊，請參閱 IAM 使用者指南中的全域條件金鑰。

對於 AWS 管理主控台 Web 伺服器代理的請求，例如 Amazon S3 主控台在您造訪 Amazon S3 主控台時用來列出儲存貯體的請求，網路路徑會不同。這些請求不是從您的 VPC 啟動的，因此不會使用您可能在 VPC 上為該服務設定的 VPC 端點。即使您在這種情況下擁有適用於 Amazon S3 的 VPC 端點，對 Amazon S3 列出儲存貯體的工作階段請求也不會使用 Amazon S3 VPC 端點。不過，當您搭配支援的 服務使用 AWS 管理主控台 Private Access 時，這些請求 （ 例如 Amazon S3) 會在其請求內容中包含 aws:SourceVpc 條件金鑰。aws:SourceVpc 條件金鑰將設定為 VPC ID，其中部署了用於登入和主控台的 AWS 管理主控台 私有存取端點。因此，如果您在以身分識別為基礎的政策中使用 aws:SourceVpc 限制，則必須新增託管 AWS 管理主控台 私人存取登入和主控台端點的 VPC 的 VPC ID。aws:SourceVpce 條件將設為各自的登入或主控台 VPC 端點 ID。

> **Note**
>
> 如果您的使用者要求存取 AWS 管理主控台 私有存取不支援的服務主控台，您必須在使用者的身分式政策中使用 aws:SourceIP 條件金鑰來包含您預期的公有網路地址清單 (例如您的內部部署網路範圍)。

不同的網路路徑如何反映在 CloudTrail 中

您產生的請求所使用的不同網路路徑 AWS 管理主控台 會反映在您的 CloudTrail 事件歷史記錄中。

對於直接瀏覽器請求，使用 AWS 管理主控台 Private Access 不會有任何變更。CloudTrail 事件將包含有關連線的詳細資料，例如用來進行服務 API 呼叫的 VPC 端點 ID。

對於 Web AWS 管理主控台 伺服器代理的請求，CloudTrail 事件不會包含任何 VPC 相關詳細資訊。不過，建立瀏覽器工作階段 AWS 登入 所需的初始請求，例如`AwsConsoleSignIn`事件類型，會在事件詳細資訊中包含 AWS 登入 VPC 端點 ID。

嘗試 AWS 管理主控台 私有存取

本節說明如何在新帳戶中設定和測試 AWS 管理主控台 私有存取。

AWS 管理主控台 Private Access 是一種進階安全功能，需要事先具備聯網和設定 VPCs的相關知識。本主題說明如何在沒有完整規模基礎設施的情況下嘗試 AWS 管理主控台 私有存取。

主題

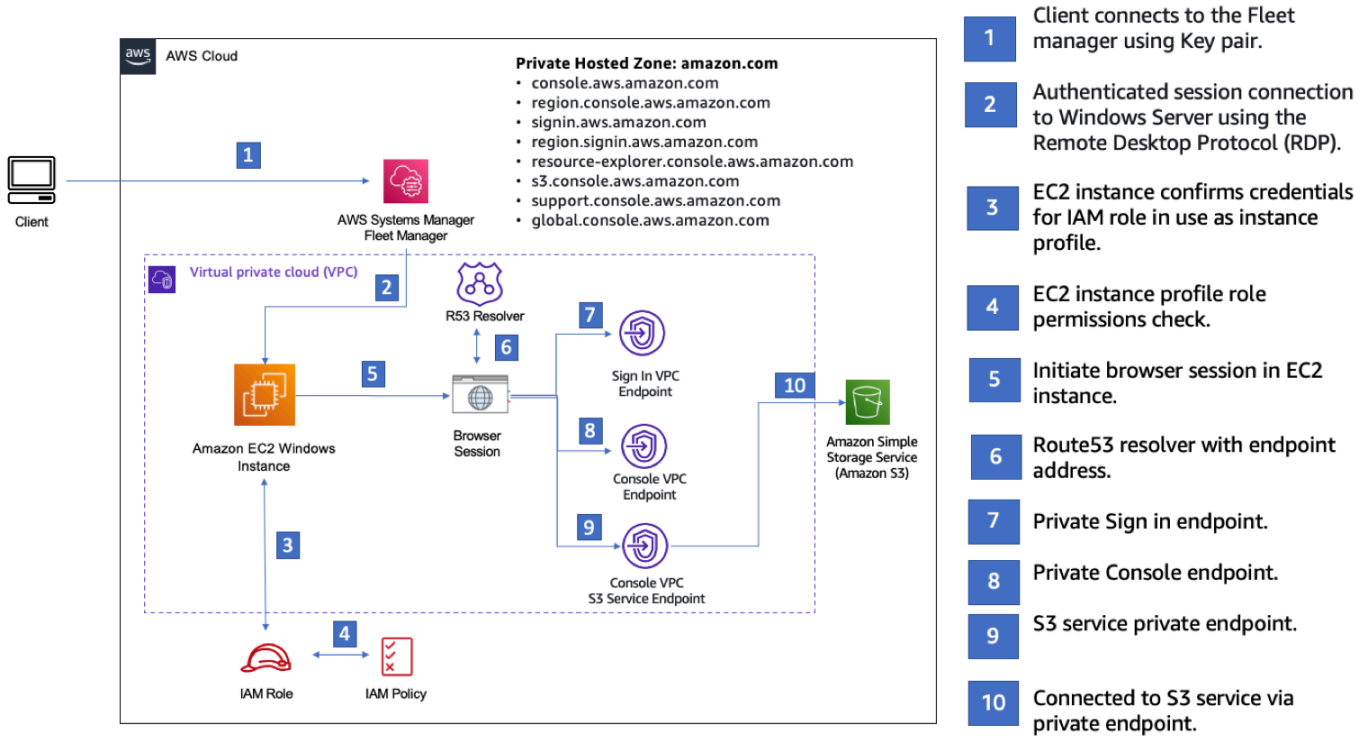
- 使用 Amazon EC2 進行測試設定
- 使用 Amazon WorkSpaces 測試設定
- 以 IAM 政策測試 VPC 設定

使用 Amazon EC2 進行測試設定

Amazon Elastic Compute Cloud (Amazon EC2) 在 Amazon Web Services Cloud 中提供了可擴展的運算容量。您可使用 Amazon EC2 按需要啟動任意數量的虛擬伺服器，設定安全性和聯網功能以及管理儲存。在此設定中，我們使用 Fleet Manager (AWS Systems Manager的一項功能) 透過遠端桌面協定 (RDP) 連接到 Amazon EC2 Windows 執行個體。

本指南示範測試環境，以設定和體驗從 Amazon EC2 執行個體到 Amazon Simple Storage Service 的 AWS 管理主控台 私有存取連線。本教學課程使用 CloudFormation 來建立和設定 Amazon EC2 用來視覺化此功能的網路設定。

下圖說明使用 Amazon EC2 存取 AWS 管理主控台 私有存取設定的工作流程。它顯示使用者如何使用私有端點連接到 Amazon S3。



複製下列 CloudFormation 範本，並將其儲存到您在設定網路程序的步驟三中使用的檔案。

> **Note**
>
> 此 CloudFormation 範本使用以色列（特拉維夫）區域目前不支援的組態。

AWS 管理主控台 私有存取環境 Amazon EC2 CloudFormation template

```
Description: |
  AWS Management Console Private Access.
Parameters:
  VpcCIDR:
    Type: String
    Default: 172.16.0.0/16
    Description: CIDR range for VPC

  Ec2KeyPair:
    Type: AWS::EC2::KeyPair::KeyName
    Description: The EC2 KeyPair to use to connect to the Windows instance
```

```
  PublicSubnet1CIDR:
    Type: String
    Default: 172.16.1.0/24
    Description: CIDR range for Public Subnet A

  PublicSubnet2CIDR:
    Type: String
    Default: 172.16.0.0/24
    Description: CIDR range for Public Subnet B

  PublicSubnet3CIDR:
    Type: String
    Default: 172.16.2.0/24
    Description: CIDR range for Public Subnet C

  PrivateSubnet1CIDR:
    Type: String
    Default: 172.16.4.0/24
    Description: CIDR range for Private Subnet A

  PrivateSubnet2CIDR:
    Type: String
    Default: 172.16.5.0/24
    Description: CIDR range for Private Subnet B

  PrivateSubnet3CIDR:
    Type: String
    Default: 172.16.3.0/24
    Description: CIDR range for Private Subnet C

  LatestWindowsAmiId:
    Type: 'AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>'
    Default: '/aws/service/ami-windows-latest/Windows_Server-2022-English-Full-Base'

  InstanceTypeParameter:
    Type: String
    Default: 't3.medium'


Resources:

##########################
# VPC AND SUBNETS
##########################
```

```
AppVPC:
  Type: 'AWS::EC2::VPC'
  Properties:
    CidrBlock: !Ref VpcCIDR
    InstanceTenancy: default
    EnableDnsSupport: true
    EnableDnsHostnames: true

PublicSubnetA:
  Type: 'AWS::EC2::Subnet'
  Properties:
    VpcId: !Ref AppVPC
    CidrBlock: !Ref PublicSubnet1CIDR
    MapPublicIpOnLaunch: true
    AvailabilityZone:
      Fn::Select:
        - 0
        - Fn::GetAZs: ""

PublicSubnetB:
  Type: 'AWS::EC2::Subnet'
  Properties:
    VpcId: !Ref AppVPC
    CidrBlock: !Ref PublicSubnet2CIDR
    MapPublicIpOnLaunch: true
    AvailabilityZone:
      Fn::Select:
        - 1
        - Fn::GetAZs: ""

PublicSubnetC:
  Type: 'AWS::EC2::Subnet'
  Properties:
    VpcId: !Ref AppVPC
    CidrBlock: !Ref PublicSubnet3CIDR
    MapPublicIpOnLaunch: true
    AvailabilityZone:
      Fn::Select:
        - 2
        - Fn::GetAZs: ""

PrivateSubnetA:
  Type: 'AWS::EC2::Subnet'
```

```
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet1CIDR
      AvailabilityZone:
        Fn::Select:
          - 0
          - Fn::GetAZs: ""

  PrivateSubnetB:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet2CIDR
      AvailabilityZone:
        Fn::Select:
          - 1
          - Fn::GetAZs: ""

  PrivateSubnetC:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet3CIDR
      AvailabilityZone:
        Fn::Select:
          - 2
          - Fn::GetAZs: ""

  InternetGateway:
    Type: AWS::EC2::InternetGateway

  InternetGatewayAttachment:
    Type: AWS::EC2::VPCGatewayAttachment
    Properties:
      InternetGatewayId: !Ref InternetGateway
      VpcId: !Ref AppVPC

  NatGatewayEIP:
    Type: AWS::EC2::EIP
    DependsOn: InternetGatewayAttachment

  NatGateway:
    Type: AWS::EC2::NatGateway
    Properties:
```

```
      AllocationId: !GetAtt NatGatewayEIP.AllocationId
      SubnetId: !Ref PublicSubnetA

#########################
# Route Tables
#########################

  PrivateRouteTable:
    Type: 'AWS::EC2::RouteTable'
    Properties:
      VpcId: !Ref AppVPC

  DefaultPrivateRoute:
    Type: AWS::EC2::Route
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      NatGatewayId: !Ref NatGateway

  PrivateSubnetRouteTableAssociation1:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetA

  PrivateSubnetRouteTableAssociation2:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetB

  PrivateSubnetRouteTableAssociation3:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetC

  PublicRouteTable:
    Type: AWS::EC2::RouteTable
    Properties:
      VpcId: !Ref AppVPC

  DefaultPublicRoute:
    Type: AWS::EC2::Route
```

```
    DependsOn: InternetGatewayAttachment
    Properties:
      RouteTableId: !Ref PublicRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      GatewayId: !Ref InternetGateway

  PublicSubnetARouteTableAssociation1:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetA

  PublicSubnetBRouteTableAssociation2:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetB

  PublicSubnetBRouteTableAssociation3:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetC


##########################
# SECURITY GROUPS
##########################

  VPCEndpointSecurityGroup:
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
      GroupDescription: Allow TLS for VPC Endpoint
      VpcId: !Ref AppVPC
      SecurityGroupIngress:
        - IpProtocol: tcp
          FromPort: 443
          ToPort: 443
          CidrIp: !GetAtt AppVPC.CidrBlock

  EC2SecurityGroup:
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
      GroupDescription: Default EC2 Instance SG
```

```
      VpcId: !Ref AppVPC

#########################
# VPC ENDPOINTS
#########################

  VPCEndpointGatewayS3:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.s3'
      VpcEndpointType: Gateway
      VpcId: !Ref AppVPC
      RouteTableIds:
        - !Ref PrivateRouteTable

  VPCEndpointInterfaceSSM:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.ssm'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceEc2messages:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
        - !Ref PrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.ec2messages'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceSsmmessages:
    Type: 'AWS::EC2::VPCEndpoint'
```

```
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
        - !Ref PrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.ssmmessages'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceSignin:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
        - !Ref PrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.signin'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceConsole:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
        - !Ref PrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.console'
      VpcId: !Ref AppVPC

##########################
# ROUTE53 RESOURCES
##########################
```

```
  ConsoleHostedZone:
    Type: "AWS::Route53::HostedZone"
    Properties:
      HostedZoneConfig:
        Comment: 'Console VPC Endpoint Hosted Zone'
      Name: 'console.aws.amazon.com'
      VPCs:
        -
          VPCId: !Ref AppVPC
          VPCRegion: !Ref "AWS::Region"

  ConsoleRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 'console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  GlobalConsoleRecord:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 'global.console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ConsoleS3ProxyRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 's3.console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
```

```
       HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
     Type: A

 ConsoleSupportProxyRecordGlobal:
   Type: AWS::Route53::RecordSet
   Properties:
     HostedZoneId: !Ref 'ConsoleHostedZone'
     Name: "support.console.aws.amazon.com"
     AliasTarget:
       DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
       HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
     Type: A

 ExplorerProxyRecordGlobal:
   Type: AWS::Route53::RecordSet
   Properties:
     HostedZoneId: !Ref 'ConsoleHostedZone'
     Name: "resource-explorer.console.aws.amazon.com"
     AliasTarget:
       DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
       HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
     Type: A

 WidgetProxyRecord:
   Type: AWS::Route53::RecordSet
   Properties:
     HostedZoneId: !Ref 'ConsoleHostedZone'
     Name: "*.widget.console.aws.amazon.com"
     AliasTarget:
       DNSName: !Select ["1", !Split [":", !Select ["0", !GetAtt
VPCEndpointInterfaceConsole.DnsEntries],],]
       HostedZoneId: !Select ["0", !Split [":", !Select ["0", !GetAtt
VPCEndpointInterfaceConsole.DnsEntries],],]
     Type: A

 ConsoleRecordRegional:
   Type: AWS::Route53::RecordSet
   Properties:
     HostedZoneId: !Ref 'ConsoleHostedZone'
```

```
      Name: !Sub "${AWS::Region}.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ConsoleRecordRegionalMultiSession:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: !Sub "*.${AWS::Region}.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  SigninHostedZone:
    Type: "AWS::Route53::HostedZone"
    Properties:
      HostedZoneConfig:
        Comment: 'Signin VPC Endpoint Hosted Zone'
      Name: 'signin.aws.amazon.com'
      VPCs:
        -
          VPCId: !Ref AppVPC
          VPCRegion: !Ref "AWS::Region"

  SigninRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: 'signin.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A

  SigninRecordRegional:
```

```
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: !Sub "${AWS::Region}.signin.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A

#########################
# EC2 INSTANCE
#########################

  Ec2InstanceRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          -
            Effect: Allow
            Principal:
              Service:
                - ec2.amazonaws.com
            Action:
              - sts:AssumeRole
      Path: /
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore

  Ec2InstanceProfile:
    Type: AWS::IAM::InstanceProfile
    Properties:
      Path: /
      Roles:
       - !Ref Ec2InstanceRole

  EC2WinInstance:
    Type: 'AWS::EC2::Instance'
    Properties:
      ImageId: !Ref LatestWindowsAmiId
      IamInstanceProfile: !Ref Ec2InstanceProfile
```

```
      KeyName: !Ref Ec2KeyPair
      InstanceType:
        Ref: InstanceTypeParameter
      SubnetId: !Ref PrivateSubnetA
      SecurityGroupIds:
        - Ref: EC2SecurityGroup
      BlockDeviceMappings:
        - DeviceName: /dev/sda1
          Ebs:
            VolumeSize: 50
      Tags:
      - Key: "Name"
        Value: "Console VPCE test instance"
```

若要設定網路

1. 登入您組織的管理帳戶，並開啟 CloudFormation 主控台。
2. 選擇建立堆疊。
3. 選擇 With new resources (standard) (使用新資源 (標準))。上傳您先前建立的 CloudFormation 範本檔案，然後選擇下一步。
4. 輸入堆疊名稱，例如 **PrivateConsoleNetworkForS3**，然後選擇 下一步。
5. 對於 VPC 和子網路，請輸入您偏好的 IP CIDR 範圍，或使用提供的預設值。如果您使用預設值，請確認它們未與 中的現有 VPC 資源重疊 AWS 帳戶。
6. 對於 EC2KeyPair 參數，請從帳戶中現有的 Amazon EC2 金鑰對中選取一個金鑰。如果沒有現有的 Amazon EC2 金鑰對，您必須先建立一個，然後再進行下一個步驟。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的使用 Amazon EC2 建立金鑰對。 Amazon EC2
7. 選擇建立堆疊。
8. 建立堆疊後，選擇 資源 索引標籤以檢視已建立的資源。

如要連線到 Amazon EC2 執行個體

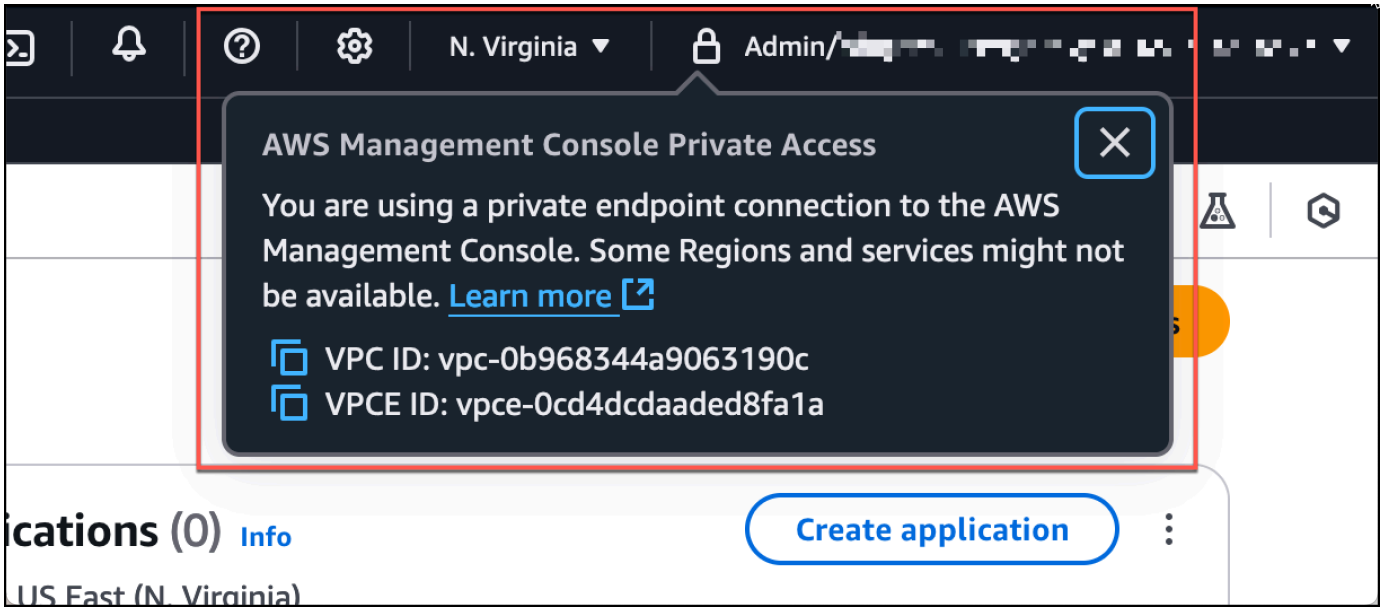
1. 登入您組織的管理帳戶，並開啟 Amazon EC2 主控台。
2. 在導覽窗格中，選擇執行個體。
3. 在執行個體頁面上，選取 CloudFormation 範本建立的主控台 VPCE 測試執行個體。然後選擇 連線。

> **Note**
>
> 此範例使用 Fleet Manager 來連線至您的 Windows Server AWS Systems Manager Explorer。可能需要幾分鐘才會開始連接。

4. 在 連線至執行個體 頁面上，選擇 RDP 用戶端，然後選擇 使用 Fleet Manager 連線。
5. 選擇 Fleet Manager 遠端桌面。
6. 若要取得 Amazon EC2 執行個體的管理密碼並使用 Web 界面存取 Windows 桌面，請使用與您在建立 CloudFormation 範本 時使用的 Amazon EC2 金鑰對相關聯的私有金鑰。
7. 從 Amazon EC2 Windows 執行個體，在瀏覽器 AWS 管理主控台 中開啟 。
8. 使用 AWS 登入資料登入後，請開啟 Amazon S3 主控台，並驗證您使用 Private Access 連線 AWS 管理主控台 。

測試 AWS 管理主控台 私有存取設定

1. 登入您組織的管理帳戶，並開啟 Amazon S3 主控台。
2. 選擇導覽列中的鎖定私有圖示，以檢視使用中的 VPC 端點。下列螢幕擷取畫面顯示鎖定私有圖示的位置和 VPC 資訊。



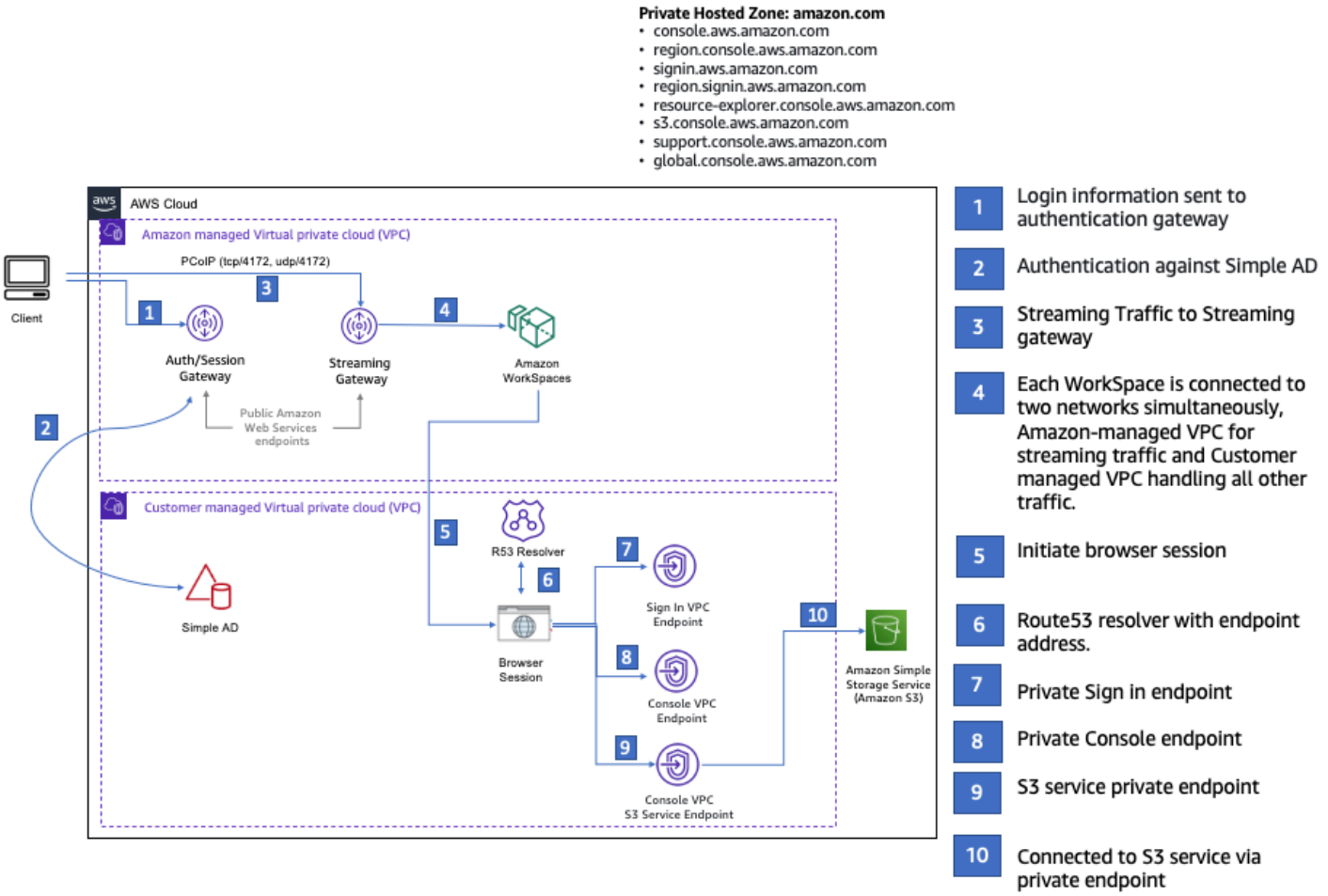
使用 Amazon WorkSpaces 測試設定

Amazon WorkSpaces 可讓您為使用者佈建虛擬、雲端式 Windows、Amazon Linux 或 Ubuntu Linux 桌面，也稱為 WorkSpaces。您可以在需求變更時快速新增或移除使用者。使用者可以從多個裝置或 Web 瀏覽器存取其虛擬桌面。若要進一步了解 WorkSpaces，請參閱 Amazon WorkSpaces 管理指南。

本節中的範例說明測試環境，其中使用者環境使用在 WorkSpace 上執行的 Web 瀏覽器來登入 AWS 管理主控台 Private Access。然後，使用者會造訪 Amazon Simple Storage Service 主控台。此 WorkSpace 旨在模擬企業使用者在 VPC 連線網路上使用筆記型電腦的體驗， AWS 管理主控台 並從瀏覽器存取 。

本教學課程使用 AWS CloudFormation 來建立和設定網路設定，以及由 WorkSpaces 使用的 Simple Active Directory，以及使用 設定 WorkSpace 的逐步說明 AWS 管理主控台。

下圖說明使用 WorkSpace 測試 AWS 管理主控台 私有存取設定的工作流程。它顯示了用戶端 WorkSpace、Amazon 受管 VPC 和客戶受管 VPC 之間的關係。



複製下列 CloudFormation 範本，並將其儲存到您在設定網路的程序步驟 3 中使用的檔案。

AWS 管理主控台 私有存取環境 CloudFormation 範本

```
Description: |
  AWS Management Console Private Access.
Parameters:

  VpcCIDR:
    Type: String
    Default: 172.16.0.0/16
    Description: CIDR range for VPC

  PublicSubnet1CIDR:
    Type: String
    Default: 172.16.1.0/24
    Description: CIDR range for Public Subnet A
```

```
  PublicSubnet2CIDR:
    Type: String
    Default: 172.16.0.0/24
    Description: CIDR range for Public Subnet B

  PrivateSubnet1CIDR:
    Type: String
    Default: 172.16.4.0/24
    Description: CIDR range for Private Subnet A

  PrivateSubnet2CIDR:
    Type: String
    Default: 172.16.5.0/24
    Description: CIDR range for Private Subnet B

  DSAdminPasswordResourceName:
    Type: String
    Default: ADAdminSecret
    Description: Password for directory services admin

# Amazon WorkSpaces is available in a subset of the Availability Zones for each
 supported Region.
# https://docs.aws.amazon.com/workspaces/latest/adminguide/azs-workspaces.html
Mappings:
  RegionMap:
    us-east-1:
      az1: use1-az2
      az2: use1-az4
      az3: use1-az6
    us-west-2:
      az1: usw2-az1
      az2: usw2-az2
      az3: usw2-az3
    ap-south-1:
      az1: aps1-az1
      az2: aps1-az2
      az3: aps1-az3
    ap-northeast-2:
      az1: apne2-az1
      az2: apne2-az3
    ap-southeast-1:
      az1: apse1-az1
      az2: apse1-az2
```

```
    ap-southeast-2:
      az1: apse2-az1
      az2: apse2-az3
    ap-northeast-1:
      az1: apne1-az1
      az2: apne1-az4
    ca-central-1:
      az1: cac1-az1
      az2: cac1-az2
    eu-central-1:
      az1: euc1-az2
      az2: euc1-az3
    eu-west-1:
      az1: euw1-az1
      az2: euw1-az2
    eu-west-2:
      az1: euw2-az2
      az2: euw2-az3
    sa-east-1:
      az1: sae1-az1
      az2: sae1-az3

Resources:

  iamLambdaExecutionRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service:
              - lambda.amazonaws.com
            Action:
              - 'sts:AssumeRole'
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole
      Policies:
        - PolicyName: describe-ec2-az
          PolicyDocument:
            Version: "2012-10-17"
            Statement:
              - Effect: Allow
```

```
                Action:
                  - 'ec2:DescribeAvailabilityZones'
                Resource: '*'
      MaxSessionDuration: 3600
      Path: /service-role/

  fnZoneIdtoZoneName:
    Type: AWS::Lambda::Function
    Properties:
      Runtime: python3.8
      Handler: index.lambda_handler
      Code:
        ZipFile: |
          import boto3
          import cfnresponse

          def zoneId_to_zoneName(event, context):
              responseData = {}
              ec2 = boto3.client('ec2')
              describe_az = ec2.describe_availability_zones()
              for az in describe_az['AvailabilityZones']:
                  if event['ResourceProperties']['ZoneId'] == az['ZoneId']:
                      responseData['ZoneName'] = az['ZoneName']
                      cfnresponse.send(event, context, cfnresponse.SUCCESS,
responseData, str(az['ZoneId']))

          def no_op(event, context):
              print(event)
              responseData = {}
              cfnresponse.send(event, context, cfnresponse.SUCCESS, responseData,
str(event['RequestId']))

          def lambda_handler(event, context):
              if event['RequestType'] == ('Create' or 'Update'):
                  zoneId_to_zoneName(event, context)
              else:
                  no_op(event,context)
      Role: !GetAtt iamLambdaExecutionRole.Arn

  getAZ1:
    Type: "Custom::zone-id-zone-name"
    Properties:
      ServiceToken: !GetAtt fnZoneIdtoZoneName.Arn
      ZoneId: !FindInMap [ RegionMap, !Ref 'AWS::Region', az1 ]
```

```
  getAZ2:
    Type: "Custom::zone-id-zone-name"
    Properties:
      ServiceToken: !GetAtt fnZoneIdtoZoneName.Arn
      ZoneId: !FindInMap [ RegionMap, !Ref 'AWS::Region', az2 ]

#########################
# VPC AND SUBNETS
#########################

  AppVPC:
    Type: 'AWS::EC2::VPC'
    Properties:
      CidrBlock: !Ref VpcCIDR
      InstanceTenancy: default
      EnableDnsSupport: true
      EnableDnsHostnames: true

  PublicSubnetA:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet1CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone: !GetAtt getAZ1.ZoneName

  PublicSubnetB:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet2CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone: !GetAtt getAZ2.ZoneName

  PrivateSubnetA:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet1CIDR
      AvailabilityZone: !GetAtt getAZ1.ZoneName

  PrivateSubnetB:
    Type: 'AWS::EC2::Subnet'
    Properties:
```

```
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet2CIDR
      AvailabilityZone: !GetAtt getAZ2.ZoneName

  InternetGateway:
    Type: AWS::EC2::InternetGateway

  InternetGatewayAttachment:
    Type: AWS::EC2::VPCGatewayAttachment
    Properties:
      InternetGatewayId: !Ref InternetGateway
      VpcId: !Ref AppVPC

  NatGatewayEIP:
    Type: AWS::EC2::EIP
    DependsOn: InternetGatewayAttachment

  NatGateway:
    Type: AWS::EC2::NatGateway
    Properties:
      AllocationId: !GetAtt NatGatewayEIP.AllocationId
      SubnetId: !Ref PublicSubnetA

##########################
# Route Tables
##########################

  PrivateRouteTable:
    Type: 'AWS::EC2::RouteTable'
    Properties:
      VpcId: !Ref AppVPC

  DefaultPrivateRoute:
    Type: AWS::EC2::Route
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      NatGatewayId: !Ref NatGateway

  PrivateSubnetRouteTableAssociation1:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetA
```

```
  PrivateSubnetRouteTableAssociation2:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetB

  PublicRouteTable:
    Type: AWS::EC2::RouteTable
    Properties:
      VpcId: !Ref AppVPC

  DefaultPublicRoute:
    Type: AWS::EC2::Route
    DependsOn: InternetGatewayAttachment
    Properties:
      RouteTableId: !Ref PublicRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      GatewayId: !Ref InternetGateway

  PublicSubnetARouteTableAssociation1:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetA

  PublicSubnetBRouteTableAssociation2:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetB


##########################
# SECURITY GROUPS
##########################

  VPCEndpointSecurityGroup:
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
      GroupDescription: Allow TLS for VPC Endpoint
      VpcId: !Ref AppVPC
      SecurityGroupIngress:
        - IpProtocol: tcp
```

```
          FromPort: 443
          ToPort: 443
          CidrIp: !GetAtt AppVPC.CidrBlock

#########################
# VPC ENDPOINTS
#########################

  VPCEndpointGatewayS3:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.s3'
      VpcEndpointType: Gateway
      VpcId: !Ref AppVPC
      RouteTableIds:
        - !Ref PrivateRouteTable

  VPCEndpointInterfaceSignin:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.signin'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceConsole:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.console'
      VpcId: !Ref AppVPC

#########################
```

```
# ROUTE53 RESOURCES
#########################

  ConsoleHostedZone:
    Type: "AWS::Route53::HostedZone"
    Properties:
      HostedZoneConfig:
        Comment: 'Console VPC Endpoint Hosted Zone'
      Name: 'console.aws.amazon.com'
      VPCs:
        -
          VPCId: !Ref AppVPC
          VPCRegion: !Ref "AWS::Region"

  ConsoleRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 'console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  GlobalConsoleRecord:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 'global.console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ConsoleS3ProxyRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 's3.console.aws.amazon.com'
      AliasTarget:
```

```
       DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
       HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
     Type: A

 ConsoleSupportProxyRecordGlobal:
   Type: AWS::Route53::RecordSet
   Properties:
     HostedZoneId: !Ref 'ConsoleHostedZone'
     Name: "support.console.aws.amazon.com"
     AliasTarget:
       DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
       HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
     Type: A

 ExplorerProxyRecordGlobal:
   Type: AWS::Route53::RecordSet
   Properties:
     HostedZoneId: !Ref 'ConsoleHostedZone'
     Name: "resource-explorer.console.aws.amazon.com"
     AliasTarget:
       DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
       HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
     Type: A

 WidgetProxyRecord:
   Type: AWS::Route53::RecordSet
   Properties:
     HostedZoneId: !Ref "ConsoleHostedZone"
     Name: "*.widget.console.aws.amazon.com"
     AliasTarget:
       DNSName: !Select ["1", !Split [":", !Select ["0", !GetAtt
VPCEndpointInterfaceConsole.DnsEntries],],]
       HostedZoneId: !Select ["0", !Split [":", !Select ["0", !GetAtt
VPCEndpointInterfaceConsole.DnsEntries],],]
     Type: A

 ConsoleRecordRegional:
   Type: AWS::Route53::RecordSet
```

```
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: !Sub "${AWS::Region}.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ConsoleRecordRegionalMultiSession:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: !Sub "*.${AWS::Region}.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  SigninHostedZone:
    Type: "AWS::Route53::HostedZone"
    Properties:
      HostedZoneConfig:
        Comment: 'Signin VPC Endpoint Hosted Zone'
      Name: 'signin.aws.amazon.com'
      VPCs:
        -
          VPCId: !Ref AppVPC
          VPCRegion: !Ref "AWS::Region"

  SigninRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: 'signin.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A
```

```
  SigninRecordRegional:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: !Sub "${AWS::Region}.signin.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A

#########################
# WORKSPACE RESOURCES
#########################
  ADAdminSecret:
    Type: AWS::SecretsManager::Secret
    Properties:
      Name: !Ref DSAdminPasswordResourceName
      Description: "Password for directory services admin"
      GenerateSecretString:
        SecretStringTemplate: '{"username": "Admin"}'
        GenerateStringKey: password
        PasswordLength: 30
        ExcludeCharacters: '"@/\'

  WorkspaceSimpleDirectory:
    Type: AWS::DirectoryService::SimpleAD
    DependsOn: AppVPC
    Properties:
      Name: "corp.awsconsole.com"
      Password: '{{resolve:secretsmanager:ADAdminSecret:SecretString:password}}'
      Size: "Small"
      VpcSettings:
        SubnetIds:
          - Ref: PrivateSubnetA
          - Ref: PrivateSubnetB

        VpcId:
          Ref: AppVPC


Outputs:
```

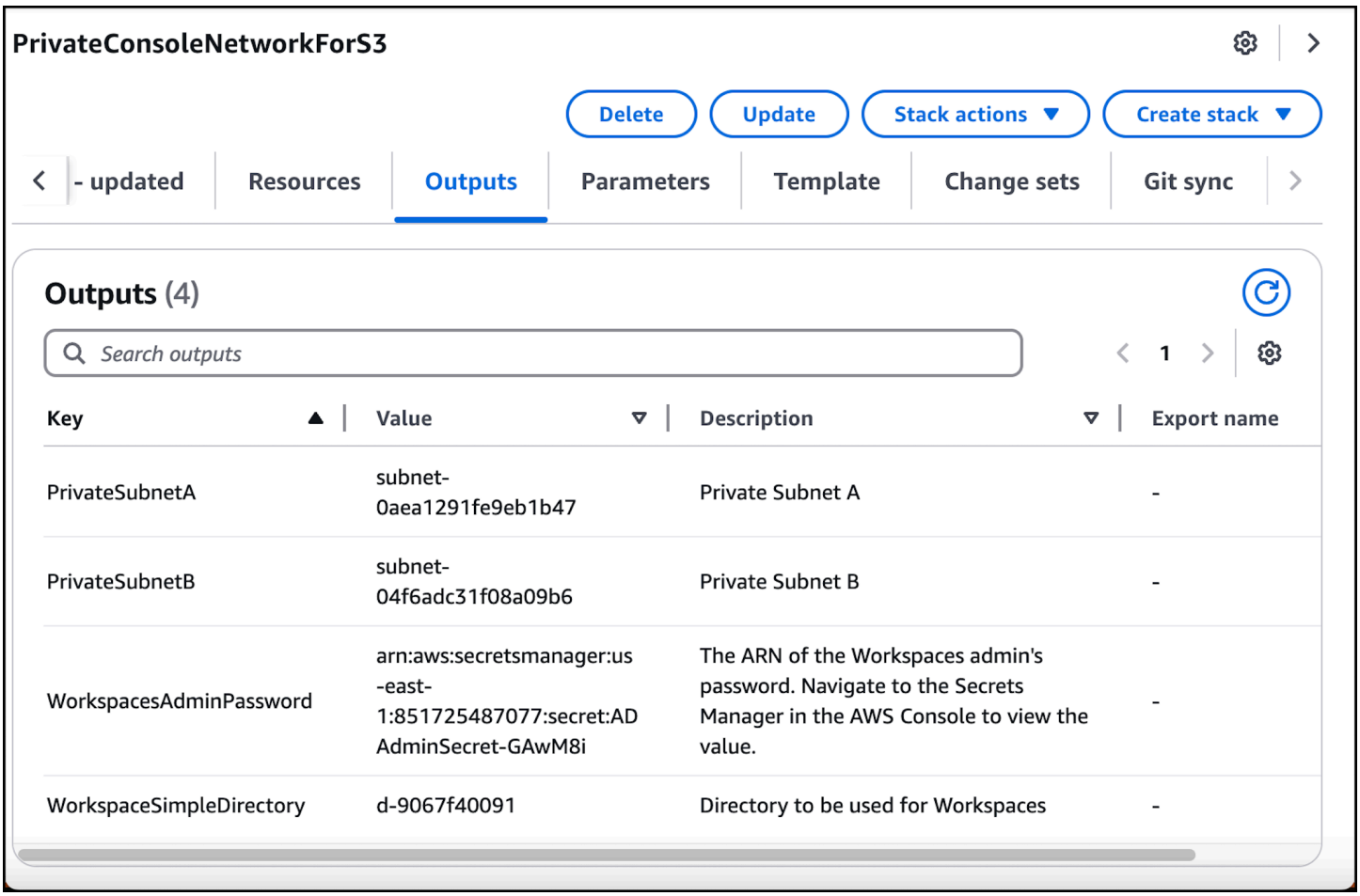
```
  PrivateSubnetA:
    Description: Private Subnet A
    Value: !Ref PrivateSubnetA

  PrivateSubnetB:
    Description: Private Subnet B
    Value: !Ref PrivateSubnetB

  WorkspaceSimpleDirectory:
    Description: Directory to be used for Workspaces
    Value: !Ref WorkspaceSimpleDirectory

  WorkspacesAdminPassword:
    Description : "The ARN of the Workspaces admin's password.  Navigate to the Secrets
Manager in the AWS Console to view the value."
    Value: !Ref ADAdminSecret
```

> **Note**
>
> 本測試設定會在美國東部 (維吉尼亞北部) 區域中執行。

若要設定網路

1. 登入您組織的管理帳戶，並開啟 CloudFormation 主控台。
2. 選擇建立堆疊。
3. 選擇 With new resources (standard) (使用新資源 (標準))。上傳您先前建立的 CloudFormation 範本檔案，然後選擇下一步。
4. 輸入堆疊名稱，例如 **PrivateConsoleNetworkForS3**，然後選擇 下一步。
5. 對於 VPC 和子網路，請輸入您偏好的 IP CIDR 範圍，或使用提供的預設值。如果您使用預設值，請確認它們未與 中的現有 VPC 資源重疊 AWS 帳戶。
6. 選擇建立堆疊。
7. 建立堆疊後，選擇 資源 索引標籤以檢視已建立的資源。
8. 選擇 輸出 索引標籤，以檢視私有子網路和 Workspace Simple Directory 的值。請記下這些值，因為您將在下一個建立和設定 WorkSpace 的步驟四中使用這些值。

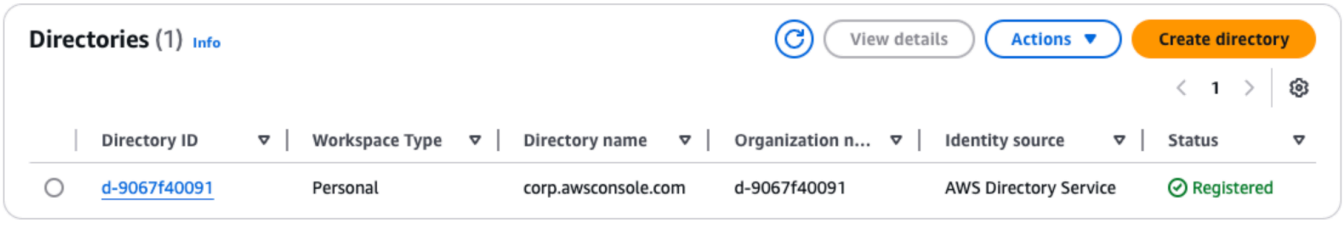
下列螢幕擷取畫面顯示 輸出 索引標籤的檢視，其中顯示私有子網路和 Workspace Simple Directory 的值。



現在您已經建立網路，請使用下列程序來建立並存取 WorkSpace。

如要建立 WorkSpace

1. 開啟 WorkSpaces 主控台。
2. 在導覽窗格中，選擇目錄。
3. 在 目錄 頁面上，確認目錄狀態為 作用中。以下螢幕擷取畫面顯示了作用中目錄的 目錄 頁面。



4. 如要在 WorkSpaces 中使用目錄，您必須註冊該目錄。在導覽窗格中，選擇 WorkSpaces，然後選擇 建立 WorkSpaces。

5. 在 選取目錄 中，請選擇上述程序中由 CloudFormation 建立的目錄。在 動作 功能表上，選擇 註冊。
6. 對於子網路選擇，請選取上述程序步驟九中所述的兩個私有子網路。
7. 選取 啟用自助服務許可，然後選擇 註冊。
8. 註冊目錄之後，請繼續建立 WorkSpace。選取已註冊的目錄，然後選擇 下一步。
9. 在 建立使用者 頁面上選擇 建立其他使用者。輸入您的姓名和電子郵件，以便您使用 WorkSpace。驗證電子郵件地址是否有效，因為 WorkSpace 登入資訊已傳送至此電子郵件地址。
10. 選擇下一步。
11. 在 識別使用者 頁面上，選取您在步驟九中建立的使用者，然後選擇 下一步。
12. 在 選取套件 頁面上，選擇 Standard with Amazon Linux 2，然後選擇 下一步。
13. 使用執行模式和使用者自訂的預設設定，檢閱並選擇建立工作區。WorkSpace 會以 `Pending` 狀態開始，並在 20 分鐘內轉換為 `Available`。
14. 在 WorkSpace 可用時，您將收到一封電子郵件，包含有關如何透過第九步驟中提供之電子郵件地址以進行存取的說明。

登入 WorkSpace 之後，您可以測試您是否正在使用 AWS 管理主控台 私有存取許可進行存取。

如要存取 WorkSpace

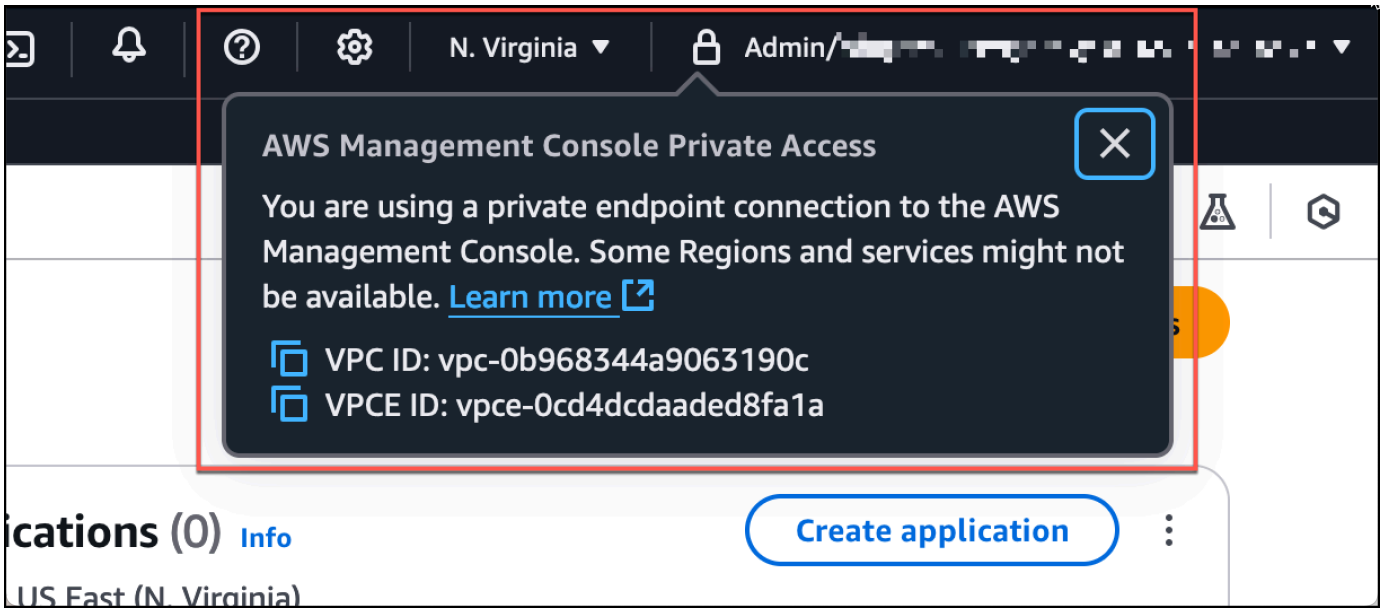
1. 開啟您在上述程序中的步驟 14 收到的電子郵件。
2. 在該電子郵件中，選擇提供的唯一連結來設定您的設定檔，並下載 WorkSpaces 用戶端。
3. 設定您的密碼。
4. 下載您選擇的客戶。
5. 安裝並啟動用戶端。輸入電子郵件中提供的註冊碼，然後選擇 註冊。
6. 使用您在步驟三中建立的憑證來登入 Amazon WorkSpaces。

測試 AWS 管理主控台 私有存取設定

1. 在 WorkSpace 中，開啟瀏覽器。然後，導覽至 AWS 管理主控台 並使用您的憑據登入。

> **Note**
>
> 如果您使用 Firefox 作為您的瀏覽器，請確認您的瀏覽器設定中的透過 HTTPS 啟用 DNS 選項已關閉。

2. 開啟 Amazon S3 主控台，您可以在其中驗證您使用 AWS 管理主控台 Private Access 連線。
3. 選擇導覽列上的鎖定私有圖示，以檢視 VPC 與使用中的 VPC 端點。下列螢幕擷取畫面顯示鎖定私有圖示的位置和 VPC 資訊。



以 IAM 政策測試 VPC 設定

您可以部署限制存取權的 IAM 政策，以進一步測試使用 Amazon EC2 或 WorkSpaces 設定的 VPC。

下列政策會拒絕存取 Amazon S3，除非它使用您指定的 VPC。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "S3:*",
            "Resource": "*",
            "Condition": {
                "StringNotEqualsIfExists": {
                    "aws:SourceVpc": "vpc-12345678"
                },
                "Bool": {
                    "aws:ViaAwsService": "false"
                }
```

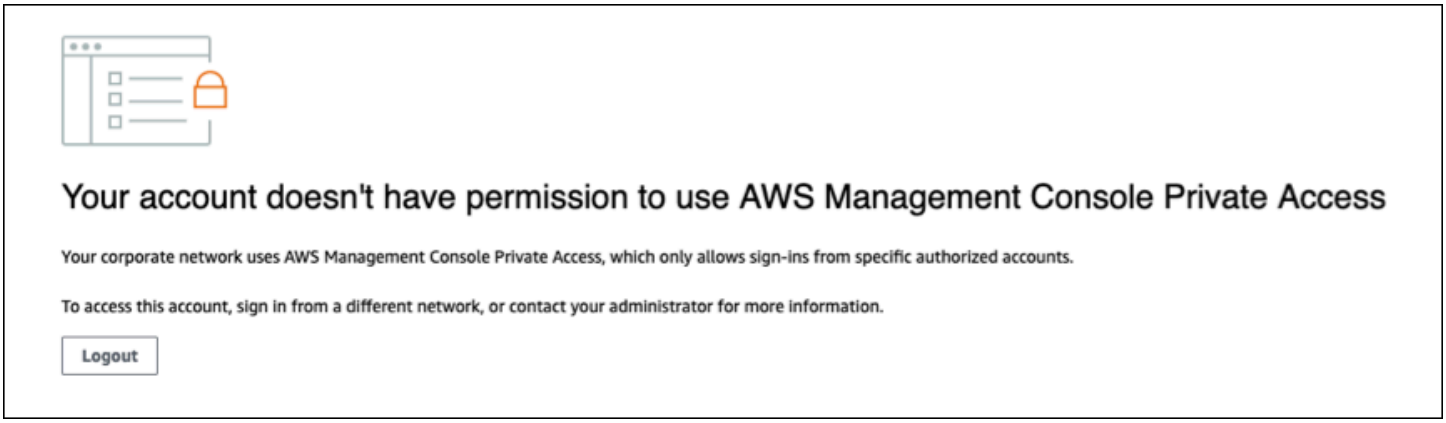
```
            }
        }
    ]
}
```

下列政策限制使用 AWS 管理主控台 登入端點的私有存取政策登入 AWS 帳戶 IDs。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalAccount": [
                        "AWSAccountID"
                    ]
                }
            }
        }
    ]
}
```

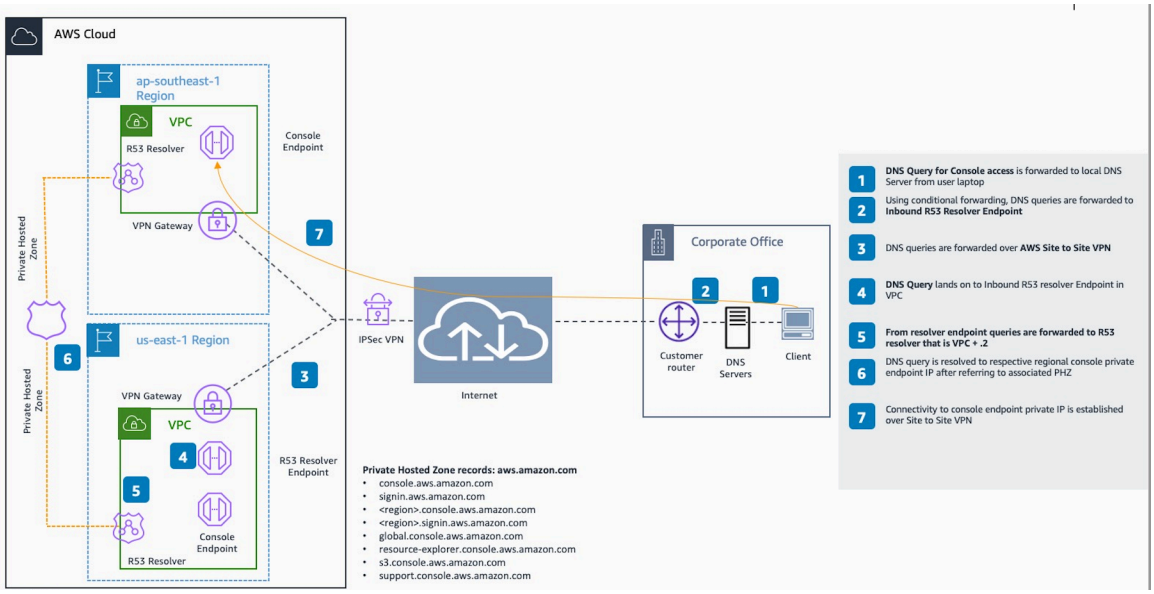
如果您連線的身分不屬於您的帳戶，則會顯示以下錯誤頁面。



參考架構

若要從內部部署網路私下連線至 AWS 管理主控台 私有存取，您可以利用 AWS Site-to-Site VPN 至 AWS 虛擬私有閘道 (VGW) 連線選項。 AWS Site-to-Site VPN 透過建立連線，以及設定路由以透過連線傳遞流量，啟用從 VPC 存取遠端網路。如需詳細資訊，請參閱AWS Site-to-Site使用者指南》中的什麼是AWS Site-to-Site VPN。 AWS 虛擬私有閘道 (VGW) 是一種高可用性的區域服務，可做為 VPC 與內部部署網路之間的閘道。

AWS Site-to-Site VPN 至 AWS 虛擬私有閘道 (VGW)



此參考架構設計中的基本元件是 Amazon Route 53 Resolver，特別是傳入解析程式。當您在建立 AWS 管理主控台 私有存取端點的 VPC 中設定它時，解析程式端點 （網路介面） 會在指定的子網路中建立。然後便可以在內部部署 DNS 伺服器上的條件式轉寄站中參照其 IP 地址，以便查詢私有託管區域中的記錄。當內部部署用戶端連線到 時 AWS 管理主控台，它們會路由到 AWS 管理主控台 私有存取端點的私有 IPs。

在設定與 AWS 管理主控台 私有存取端點的連線之前，請先完成先決條件步驟：在您要存取 的所有區域中設定 AWS 管理主控台 私有存取端點 AWS 管理主控台，以及在美國東部 （維吉尼亞北部） 區域中設定私有託管區域。

AWS 使用者體驗自訂 (UXC)

AWS 使用者體驗自訂 (UXC) 是一種公用程式，可讓帳戶管理員自訂 的視覺效果， AWS 管理主控台並在帳戶層級管理這些設定。

使用 UXC，您可以自訂下列設定：

- 帳戶顏色 – 您可以為帳戶設定顏色，以視覺化方式區分它們。例如，您可以將綠色用於開發帳戶、將黃色用於測試帳戶，以及將紅色用於生產帳戶。
- 服務可見性 – 您可以控制哪些 AWS 服務出現在主控台導覽中。服務可見性可簡化 AWS 管理主控台 ，僅顯示與您帳戶相關的 AWS 服務。
- 區域可見性 – 您可以控制 AWS 區域選擇器中顯示的區域。區域可見性可簡化 AWS 管理主控台 ，以僅顯示與您帳戶相關的區域。

如果您尚未設定設定，則會套用預設行為：所有服務和區域都會顯示，而且不會設定帳戶顏色。您可以將 值設定為 ，將帳戶顏色重設為其預設值"none"。您可以將可見服務和區域的值設定為 ，將其重設為預設值null。

> **Note**
>
> `visibleServices` 和 `visibleRegions`設定只會控制 中服務和區域的外觀 AWS 管理主控台。它們不會限制透過 AWS Command Line Interface、 SDKs 或其他 APIs存取。

主題

- AWS 使用者體驗自訂入門
- 使用 記錄 AWS 使用者體驗自訂 API 呼叫 AWS CloudTrail
- AWS 使用者體驗自訂的安全性

AWS 使用者體驗自訂入門

透過 UXC，帳戶管理員可以設定 的帳戶自訂 AWS 管理主控台。

先決條件

開始之前，您必須準備好以下事項：

- AWS 帳戶
- UXC 的適當 AWS Identity and Access Management (IAM) 許可。如需詳細資訊，請參閱 AWS 的使用者體驗自訂如何搭配 IAM 和 AWS 受管政策 AWS 管理主控台運作。

在 中存取 UXC 設定 AWS 管理主控台

若要在 中存取帳戶顏色 AWS 管理主控台，請參閱在 中存取帳戶資訊 AWS 管理主控台。若要存取 中的服務可見性和區域可見性 AWS 管理主控台，請參閱AWS 管理主控台 使用統一設定設定 。

在 主控台中設定帳戶顏色

1. 登入 AWS 管理主控台。
2. 在導覽列上，選擇您的帳戶名稱。
3. 選擇帳戶。
4. 在帳戶顯示設定中，選擇顏色。
5. 選擇更新。

在主控台中設定可見區域

1. 登入 AWS 管理主控台。
2. 開啟統一設定。
3. 在可見區域區段中選擇編輯。
4. 將您的可見區域設定為所有可用區域或選取區域，並設定您的清單。
5. 選擇儲存變更。

在主控台中設定可見的服務

1. 登入 AWS 管理主控台。
2. 開啟統一設定。
3. 在可見服務區段中選擇編輯。
4. 將可見的服務設定為所有服務或選取服務，並設定您的清單。
5. 選擇儲存變更。

以程式設計方式存取 UXC 設定

您也可以以程式設計方式或做為基礎設施做為程式碼來管理帳戶自訂設定。如需詳細資訊，請參閱AWS 使用者體驗自訂 API 參考和 AWS::UXC::AccountCustomization CloudFormation 範本參考。

使用 記錄 AWS 使用者體驗自訂 API 呼叫 AWS CloudTrail

AWS 使用者體驗自訂已與 整合AWS CloudTrail，此服務可提供使用者、角色或 所採取動作的記錄 AWS 服務。CloudTrail 會將 UXC 的所有 API 呼叫擷取為事件。擷取的呼叫包括來自 UXC 主控台的呼叫，以及對 UXC API 操作的程式碼呼叫。使用 CloudTrail 收集的資訊，您可以判斷對 UXC 提出的請求、提出請求的 IP 地址、提出請求的時間，以及其他詳細資訊。

當您建立帳戶 AWS 帳戶 時CloudTrail 會在 中處於作用中狀態，而且您會自動存取 CloudTrail 事件歷史記錄。CloudTrail 事件歷史記錄為 AWS 區域中過去 90 天記錄的管理事件，提供可檢視、可搜尋、可下載且不可變的記錄。如需詳細資訊，請參閱「AWS CloudTrail 使用者指南」中的使用 CloudTrail 事件歷史記錄。檢視事件歷史記錄不會產生 CloudTrail 費用。

如需 AWS 帳戶 過去 90 天內持續記錄的事件，請建立線索或 CloudTrail Lake 事件資料存放區。

CloudTrail 中的 UXC 管理事件

管理事件提供有關在 資源上執行的管理操作的資訊 AWS 帳戶。這些也稱為控制平面操作。根據預設，CloudTrail 記錄管理事件。

AWS 使用者體驗自訂會將所有 UXC 控制平面操作記錄為管理事件。如需 UXC 記錄到 CloudTrail 的 AWS 使用者體驗自訂控制平面操作清單，請參閱AWS 使用者體驗自訂 API 參考。

UXC 事件範例

一個事件代表任何來源提出的單一請求，並包含請求 API 操作的相關資訊、操作的日期和時間、請求參數等。CloudTrail 日誌檔案不是公有 API 呼叫的已排序堆疊追蹤，因此事件不會以任何特定順序顯示。

以下範例顯示的 CloudTrail 事件會示範 操作。

```
{
  "eventVersion" : "1.09",
  "userIdentity" : {
    "type" : "AssumedRole",
    "principalId" : "AIDACKCEVSQ6C2EXAMPLE:jdoe",
    "arn" : "arn:aws:sts::111122223333:assumed-role/user/jdoe",
```

```
    "accountId" : "111122223333",
    "accessKeyId" : "AKIAIOSFODNN7EXAMPLE",
    "sessionContext" : {
      "sessionIssuer" : {
        "type" : "Role",
        "principalId" : "AIDACKCEVSQ6C2EXAMPLE",
        "arn" : "arn:aws:iam::111122223333:role/user",
        "accountId" : "111122223333",
        "userName" : "jdoe"
      },
      "webIdFederationData" : { },
      "attributes" : {
        "creationDate" : "2022-12-09T23:48:51Z",
        "mfaAuthenticated" : "false"
      }
    }
  },
  "eventTime" : "2022-12-09T23:50:03Z",
  "eventSource" : "uxc.amazonaws.com",
  "eventName" : "GetAccountColor",
  "awsRegion" : "us-east-2",
  "sourceIPAddress" : "10.24.34.3",
  "userAgent" : "PostmanRuntime/7.43.4",
  "requestParameters" : null,
  "responseElements" : null,
  "requestID" : "543db7ab-b4b2-11e9-8925-d139e92a1fe8",
  "eventID" : "5b2805a5-3e06-4437-a7a2-b5fdb5cbb4e2",
  "readOnly" : true,
  "eventType" : "AwsApiCall",
  "managementEvent" : true,
  "recipientAccountId" : "111122223333",
  "eventCategory" : "Management"
}
```


如需有關 CloudTrail 記錄內容的資訊，請參閱《AWS CloudTrail 使用者指南》中的 CloudTrail record contents。

AWS 使用者體驗自訂的安全性

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

安全性是 AWS 與您之間的共同責任。共同責任模式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 中執行 AWS 服務的基礎設施 AWS 雲端。 AWS 也為您提供可安全使用的服務。在AWS 合規計畫中，第三方稽核人員會定期測試和驗證我們安全的有效性。若要了解適用於 AWS 使用者體驗自訂的合規計劃，請參閱AWS 合規計劃的 服務範圍。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

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

主題

- AWS 使用者體驗自訂的 Identity and Access Management

AWS 使用者體驗自訂的 Identity and Access Management

AWS 使用者體驗自訂 (UXC) 使用 IAM 政策來管理對 UXC API 操作的存取。

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

主題

- 目標對象
- 使用身分驗證
- 使用政策管理存取權
- AWS 使用者體驗自訂如何與 IAM 搭配使用
- AWS 使用者體驗自訂的身分型政策範例

目標對象

使用方式 AWS Identity and Access Management (IAM) 會根據您的角色而有所不同：

- 服務使用者 — 若無法存取某些功能，請向管理員申請所需許可 (請參閱 疑難排解 AWS 使用者體驗自訂身分和存取)
- 服務管理員 — 負責設定使用者存取權並提交相關許可請求 (請參閱 AWS 使用者體驗自訂如何與 IAM 搭配使用)
- IAM 管理員 — 撰寫政策以管理存取控制 (請參閱 AWS 使用者體驗自訂的身分型政策範例)

使用身分驗證

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

您可以使用身分來源的登入資料，例如 AWS IAM Identity Center (IAM Identity Center)、單一登入身分驗證或 Google/Facebook 登入資料，以聯合身分的形式登入。如需有關登入的詳細資訊，請參閱《AWS 登入 使用者指南》中的如何登入您的 AWS 帳戶。

對於程式設計存取， AWS 提供 SDK 和 CLI 以密碼編譯方式簽署請求。如需詳細資訊，請參閱《IAM 使用者指南》中的 API 請求的AWS 第 4 版簽署程序。

AWS 帳戶 根使用者

當您建立 時 AWS 帳戶，您會從一個名為 AWS 帳戶 theroot 使用者的登入身分開始，該身分具有對所有 AWS 服務 和 資源的完整存取權。強烈建議不要使用根使用者來執行日常任務。有關需要根使用者憑證的任務，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https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html是一種身分具備單人或應用程式的特定許可權。建議以臨時憑證取代具備長期憑證的 IAM 使用者。如需詳細資訊，請參閱《IAM 使用者指南》中的要求人類使用者使用聯合身分提供者來 AWS 使用臨時憑證存取 。

IAM 群組會指定 IAM 使用者集合，使管理大量使用者的許可權更加輕鬆。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 使用者的使用案例。

IAM 角色

IAM 角色https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html的身分具有特定許可權，其可以提供臨時憑證。您可以透過從使用者切換到 IAM 角色 （主控台） 或呼叫 AWS CLI 或 AWS API 操作來擔任角色。如需詳細資訊，請參閱《IAM 使用者指南》中的擔任角色的方法。

IAM 角色適用於聯合身分使用者存取、臨時 IAM 使用者許可、跨帳戶存取權與跨服務存取，以及在 Amazon EC2 執行的應用程式。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的快帳戶資源存取。

使用政策管理存取權

您可以透過建立政策並將其連接到身分或資源 AWS 來控制 AWS 中的存取。政策定義與身分或資源相關聯的許可。當委託人提出請求時 AWS ， 會評估這些政策。大多數政策會以 JSON 文件 AWS 的形式存放在 中。如需進一步了解 JSON 政策文件，請參閱《IAM 使用者指南》中的 JSON 政策概觀。

管理員會使用政策，透過定義哪些主體可在哪些條件下對哪些資源執行動作，以指定可存取的範圍。

預設情況下，使用者和角色沒有許可。IAM 管理員會建立 IAM 政策並將其新增至角色，供使用者後續擔任。IAM 政策定義動作的許可，無論採用何種方式執行。

身分型政策

身分型政策是附加至身分 (使用者、使用者群組或角色) 的 JSON 許可政策文件。這類政策控制身分可對哪些資源執行哪些動作，以及適用的條件。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

身分型政策可分為內嵌政策 (直接內嵌於單一身分) 與受管政策 (可附加至多個身分的獨立政策)。如需了解如何在受管政策及內嵌政策之間做選擇，請參閱《IAM 使用者指南》中的在受管政策與內嵌政策之間選擇。

資源型政策

資源型政策是附加到資源的 JSON 政策文件。範例包括 IAM 角色信任政策與 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。您必須在資源型政策中指定主體。

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

其他政策類型

AWS 支援其他政策類型，可設定更多常見政策類型授予的最大許可：

- 許可界限 — 設定身分型政策可授與 IAM 實體的最大許可。如需詳細資訊，請參閱《 IAM 使用者指南》中的 IAM 實體許可界限。
- 服務控制政策 (SCP) — 為 AWS Organizations中的組織或組織單位指定最大許可。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的服務控制政策。
- 資源控制政策 (RCP) — 設定您帳戶中資源可用許可的上限。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的資源控制政策 (RCP)。
- 工作階段政策 — 在以程式設計方式為角色或聯合身分使用者建立臨時工作階段時，以參數形式傳遞的進階政策。如需詳細資訊，請參《IAM 使用者指南》中的工作階段政策。

多種政策類型

當多種類型的政策適用於請求時，產生的許可會更複雜而無法理解。若要了解如何 AWS 在涉及多種政策類型時決定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

AWS 使用者體驗自訂如何與 IAM 搭配使用

AWS 使用者體驗自訂 (UXC) 與 IAM 政策搭配使用，以管理對 UXC API 操作的存取。

在您使用 IAM 管理 AWS 使用者體驗自訂 （使用者體驗自訂） 的存取權之前，請先了解哪些 IAM 功能可與使用者體驗自訂搭配使用。我們建議您透過 AWS 受管政策與使用者體驗自訂整合，如需詳細資訊，請參閱 AWS 的 受管政策 AWS 管理主控台。

在您使用 IAM 管理使用者體驗自訂的存取權之前，請先了解哪些 IAM 功能可與使用者體驗自訂搭配使用。

IAM 功能	使用者體驗自訂支援
身分型政策	是
資源型政策	否
政策動作	是
政策資源	否
政策條件索引鍵	否
臨時憑證	是
跨服務主體許可	否
服務連結角色	否
服務角色	否

若要全面了解使用者體驗自訂和其他 AWS 服務如何與大多數 IAM 功能搭配使用，請參閱《IAM 使用者指南》中的AWS 與 IAM 搭配使用的 服務。

使用者體驗自訂的身分型政策

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素參考。

若要檢視使用者體驗自訂身分型政策的範例，請參閱AWS 使用者體驗自訂的身分型政策範例。

使用者體驗自訂的政策動作

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

JSON 政策的 `Action` 元素描述您可以用來允許或拒絕政策中存取的動作。政策會使用動作來授予執行相關聯動作的許可。

若要查看所有使用者體驗自訂動作，請參閱 API 參考。

使用者體驗自訂中的政策動作會在動作之前使用 `uxc:`字首 （ 例如 `uxc:GetAccountCustomizations`)。

若要在單一陳述式中指定多個動作，請用逗號分隔：

```
"Action": [
      "uxc:GetAccountCustomizations",
      "uxc:ListServices"
         ]
```

若要檢視使用者體驗自訂身分型政策的範例，請參閱AWS 使用者體驗自訂的身分型政策範例。

使用者體驗自訂的政策資源

使用者體驗自訂不支援政策資源。

將臨時登入資料與使用者體驗自訂搭配使用

臨時登入資料提供對 AWS 資源的短期存取，並在您使用聯合或切換角色時自動建立。 AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的臨時安全憑證與可與 IAM 搭配運作的AWS 服務。

疑難排解 AWS 使用者體驗自訂身分和存取

使用以下資訊來協助您診斷和修正使用 使用者體驗自訂和 IAM 時可能遇到的常見問題。

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

下列範例錯誤會在mateojackson IAM 使用者嘗試使用主控台檢視一個虛構 *my-example-widget* 資源的詳細資訊，但卻無虛構 uxc:*GetWidget* 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 uxc:GetWidget on resource: my-example-widget because no identity-based policy allows
 the GetWidget action
```

在此情況下，必須更新 mateojackson 使用者的政策，允許使用 uxc:*GetWidget* 動作存取 *my-example-widget* 資源。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

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。透過這樣做，您可以讓某人永久存取您的 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。

若要允許其他人存取使用者體驗自訂，您必須將許可授予需要存取的人員或應用程式。如果您使用 AWS IAM Identity Center 管理人員和應用程式，您可以將許可集指派給使用者或群組，以定義其存取層級。許可集會自動建立 IAM 政策，並將其指派給與該人員或應用程式相關聯的 IAM 角色。如需詳細資訊，請參閱AWS IAM Identity Center 《 使用者指南》中的許可集。

如果您不是使用 IAM Identity Center，則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）。然後，您必須將政策連接到實體，在使用者體驗自訂中授予他們正確的許可。授予許可後，請將登入資料提供給使用者或應用程式開發人員。他們將使用這些登入資料來存取 AWS。若要進一步

了解如何建立 IAM 使用者、群組、政策和許可，請參閱《IAM 使用者指南》中的 IAM 身分和政策和許可。

AWS 使用者體驗自訂的身分型政策範例

根據預設，使用者和角色沒有取得或修改 UXC 資源的許可。若要授予使用者對資源執行動作的許可，IAM 管理員可以建立 IAM 政策。如需了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策 (主控台)。

主題

- 政策最佳實務
- UXC 帳戶自訂的唯讀存取權
- 完整存取 UXC 帳戶自訂

政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除使用者體驗自訂資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

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

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

UXC 帳戶自訂的唯讀存取權

下列範例示範如何建立允許唯讀存取 UXC 帳戶自訂的政策：

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

完整存取 UXC 帳戶自訂

下列範例示範如何建立允許完整存取 UXC 帳戶自訂的政策：

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

AWS 的 受管政策 AWS 管理主控台

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

請記住， AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為這些許可可供所有 AWS 客戶使用。我們建議您定義特定於使用案例的客戶管理政策，以便進一步減少許可。

您無法變更 AWS 受管政策中定義的許可。如果 AWS 更新受 AWS 管政策中定義的許可，則更新會影響政策連接的所有委託人身分（使用者、群組和角色）。當新的 AWS 服務 啟動或新的 API 操作可用於現有服務時， AWS 最有可能更新 AWS 受管政策。

如需詳細資訊，請參閱 IAM 使用者指南中的 AWS 受管政策。

AWS 受管政策：AWSManagementConsoleBasicUserAccess

您可以將 AWSManagementConsoleBasicUserAccess 連接至使用者、群組與角色。

此政策會授予 非管理使用者所需的許可 AWS 管理主控台。這包括資源探索、通知、瀏覽器型 shell 存取和自訂導覽等功能。

許可詳細資訊

這AWSManagementConsoleBasicUserAccess會分組到下列一組許可：

- cloudshell – 允許主體完整存取 AWS CloudShell 功能，包括環境建立、工作階段管理和命令執行。
- ec2 – 允許主體描述統一導覽中為帳戶啟用的區域。
- notifications – 允許主體從中取得事件 AWS 使用者通知。

- q – 允許主體與 Amazon Q Developer 聊天。
- resource-explorer-2 – 允許主體使用統一搜尋來搜尋和探索 AWS 資源。
- uxc – 允許主體讀取 AWS 使用者體驗自訂設定。
- action-recommendations – 允許主體接收情境動作建議。
- account – 允許主體擷取指定帳戶的相關資訊，包括其帳戶名稱、帳戶 ID 和帳戶建立日期和時間。

若要檢視此政策的許可，請參閱《 受管政策參考》中的
AWSManagementConsoleBasicUserAccess。 AWS

AWS 受管政策：AWSManagementConsoleAdministratorAccess

您可以將 AWSManagementConsoleAdministratorAccess 連接至使用者、群組與角色。

此政策授予設定和自訂 的完整存取權 AWS 管理主控台。它可讓管理員設定帳戶顏色、啟用使用者通知，以及設定資源探索。它還包含 AWSManagementConsoleBasicUserAccess 受管政策的許可，這對 的非管理使用者至關重要 AWS 管理主控台。

許可詳細資訊

這AWSManagementConsoleAdministratorAccess會分組為下列一組許可：

- cloudshell – 允許主體完整存取 AWS CloudShell 功能，包括環境建立、工作階段管理和命令執行。
- ec2 – 允許主體描述統一導覽中為帳戶啟用的區域。
- notifications – 允許主體存取和更新通知組態、事件和功能選擇加入狀態。
- q – 允許主體與 Amazon Q Developer 聊天，以取得 AI 輔助支援。
- resource-explorer-2 – 允許主體使用統一搜尋來搜尋和探索 AWS 資源。
- uxc – 允許主體完整存取 AWS 使用者體驗自訂設定。
- action-recommendations – 允許主體接收情境動作建議。

- account – 允許主體擷取指定帳戶的相關資訊，包括其帳戶名稱、帳戶 ID 和帳戶建立日期和時間。

若要檢視此政策的許可，請參閱《 受管政策參考》中的 AWSManagementConsoleAdministratorAccess。 AWS

AWS 管理主控台 AWS 受管政策的更新

檢視自此服務開始追蹤這些變更 AWS 管理主控台 以來 AWS 受管政策更新的詳細資訊。如需此頁面變更的自動提醒，請訂閱 AWS 管理主控台 文件歷史記錄頁面上的 RSS 摘要。

變更	描述	Date
AWSManagementConsoleBasicUserAccess – 更新的政策	新增 `uxc:GetAccountCustomizations` 和 `uxc:ListServices` 許可。	2026 年 3 月 26 日
AWSManagementConsoleAdministratorAccess – 已更新政策	新增 `uxc:GetAccountCustomizations` 、 `uxc:UpdateAccountCustomizations` 和 `uxc:ListServices` 許可。	2026 年 3 月 26 日
AWSManagementConsoleBasicUserAccess – 更新的政策	更新政策以新增許可，允許使用者在導覽 時查看帳戶資訊並接收動作建議 AWS 管理主控台。	2025 年 12 月 9 日
AWSManagementConsoleAdministratorAccess – 更新的政策	更新政策以新增許可，允許使用者在導覽 時查看帳戶資訊並接收動作建議 AWS 管理主控台。	2025 年 12 月 9 日
AWSManagementConsoleBasicUserAccess – 新政策	新增了新的 AWS 受管政策，授予基本 AWS 管理主控台 導覽、帳戶色彩檢視和資源探索所需的許可。	2025 年 8 月 14 日

變更	描述	Date
AWSManagementConsoleAdministratorAccess – 新政策	新增了新的 AWS 受管政策，提供設定和自訂 的完整存取權 AWS 管理主控台。	2025 年 8 月 14 日
AWS 管理主控台 開始追蹤變更	AWS 管理主控台 已開始追蹤其 AWS 受管政策的變更。	2025 年 8 月 14 日

在主控台中使用 Markdown

中的某些服務 AWS 管理主控台，例如 Amazon CloudWatch，支援在特定欄位中使用 Markdown。此主題說明主控台中支援的 Markdown 格式類型。

目錄

段落、行距和水平線

段落是以空白行分隔。若要確保轉換為 HTML 後段落之間的空白行能順利呈現，請先加入含有非中斷空格的新行 ( )，再加上空白行。重複加入這兩行即可連續插入多個空白行，如以下範例所示：

```
 

 
```

若要建立用於分隔段落的水平線，請加入包含連續三個連字號的新行：`---`

```
Previous paragraph.
---
Next paragraph.
```

若要建立等寬類型的文字區塊，請在一行內輸入連續三個反引號 (`)，接著輸入要以等寬類型顯示的文字，再加入包含三個反引號的新行。下方為以等寬類型格式顯示文字的範例：

````
```
This appears in a text box with a background shading.
The text is in monospace.
```
````

標題

如要建立標題，請使用井字號 (#)。單一井字號加上空格代表頂層標題，使用兩個井字號可建立第二層標題，使用三個井字號則可建立第三層標題。以下範例分別顯示如何建立頂層、第二層、第三層標題：

```
# Top-level heading
```

```
## Second-level heading
```

```
### Third-level heading
```

文字格式

若要將文字格式設為斜體，請在文字兩側分別輸入一個底線 (_) 或星號 (*)。

```
*This text appears in italics.*
```

若要將文字格式設為粗體，請在文字兩側輸入兩個底線或兩個星號。

```
**This text appears in bold.**
```

若要為文字加上刪除線，請在文字兩側分別輸入兩個波狀符號 (~)。

```
~~This text appears in strikethrough.~~
```

連結

若要加入文字超連結，請用方括號 ([ ]) 括住連結文字，後面再加上用括號 (( )) 括住的完整 URL，如以下範例所示：

```
Choose [link_text](http://my.example.com).
```

清單

若要將數行的格式設定為項目符號清單，請在各行的開頭輸入單一星號 (*)，再加上一個空格，如以下範例所示：

```
Here is a bulleted list:
* Ant
* Bug
* Caterpillar
```

若要將數行的格式設定為編號清單，請在各行的開頭輸入數字，再加上一個空格和一個半型句號 (.)，如以下範例所示：

```
Here is a numbered list:
1. Do the first step
2. Do the next step
3. Do the final step
```

表格和按鈕 (CloudWatch 儀表板)

CloudWatch 儀表板文字小工具支援 Markdown 資料表和按鈕。

若要建立資料表，請使用垂直線 (|) 區隔資料欄，並使用新行加入資料列。若要將第一行設為標題行，請在標題行和第一行的值之間插入一行，然後為資料表中每個資料欄輸入至少三個連字號 (-)，並使用垂直線分隔各個資料欄。以下範例示範如何使用 Markdown 建立包含兩個資料欄、一個標題行及兩個資料行的資料表：

```
Table | Header
----|-----
Amazon Web Services | AWS
1 | 2
```

使用上方範例提到的 Markdown 文字，可建立下方資料表：

資料表	標頭
Amazon Web Services	AWS
1	2

在 CloudWatch 儀表板文字小工具中，您也可以將超連結設為按鈕格式。若要建立按鈕，請使用 `[button:Button text]`，其後再加上用括號 (( )) 括住的完整 URL，如以下範例所示：

```
[button:Go to AWS](http://my.example.com)
[button:primary:This button stands out even more](http://my.example.com)
```

疑難排解

請參閱本節以尋找 常見問題的解決方案 AWS 管理主控台。

您也可以使用 Amazon Q Developer 診斷和疑難排解某些 AWS 服務的常見錯誤。如需詳細資訊，請參閱《Amazon Q 開發人員使用者指南》中的使用 Amazon Q 開發人員診斷主控台中的常見錯誤。

主題

頁面未正確載入

- 如果這個問題只是偶爾發生，請檢查您的網際網路連線。嘗試透過不同的網路連線，或使用或不使用 VPN，或嘗試使用不同的 Web 瀏覽器。
- 如果所有受影響的使用者都來自同一個團隊，則可能是隱私權瀏覽器延伸或安全防火牆問題。隱私權瀏覽器擴充功能和安全防火牆可以封鎖對 所用網域的存取 AWS 管理主控台。請嘗試關閉這些擴充功能或調整防火牆設定。如果要確認連線問題，請開啟瀏覽器開發人員工具 (Chrome、Firefox) 並檢查 Console (主控台) 索引標籤的錯誤。 AWS 管理主控台 使用網域的字尾，包括下列清單。此清單並不詳盡。這些網域的尾碼並非專門由 AWS。
  - .a2z.com
  - .amazon.com
  - .amazonaws.com
  - .aws
  - .aws.com
  - .aws.dev
  - .awscloud.com
  - .awsplayer.com
  - .awsstatic.com
  - .cloudfront.net
  - .live-video.net

> **Warning**
>
> 自 2022 年 7 月 31 日起， AWS 不再支援 Internet Explorer 11。我們建議您 AWS 管理主控台搭配其他支援的瀏覽器使用 。如需詳細資訊，請參閱 AWS 新聞部落格。

我的瀏覽器在連線至 時顯示「存取遭拒」錯誤 AWS 管理主控台

如果符合下列所有條件，最近對主控台所做的變更可能會影響您的存取：

- 您可以從設定為透過 VPC 端點到達 AWS 服務端點 AWS 管理主控台 的網路存取 。
- 您可以在 IAM 政策中使用 `aws:SourceIp`或 `aws:SourceVpc`全域條件金鑰來限制對 AWS 服務的存取。

我們建議您檢閱包含 `aws:SourceIp`或 `aws:SourceVpc`全域條件金鑰的 IAM 政策。適用`aws:SourceVpc`時同時套用 `aws:SourceIp`和 。

有些 AWS 管理主控台 功能使用同時支援 IPv4 和 IPv6 連線的雙堆疊網域。如果您的 IAM 政策限制使用 `aws:SourceIp` 搭配 IPv4 CIDR 區塊的存取，則當您的作業系統偏好 IPv6 連線時，請求可能會失敗 （反之亦然）。若要避免這種情況，請在您的 `aws:SourceIp` 條件中同時包含 IPv4 和 IPv6 CIDR 區塊。如需詳細資訊，請參閱AWS Identity and Access Management 《 使用者指南》中的 aws：SourceIp。

您也可以加入 AWS 管理主控台 私有存取功能， AWS 管理主控台 透過 VPC 端點存取 ，並在政策中使用`aws:SourceVpc`條件。如需詳細資訊，請參閱下列內容：

- AWS 管理主控台 私有存取
- the section called “AWS 管理主控台 私有存取如何與 aws：SourceVpc 搭配使用”
- the section called “支援的 AWS 全域條件內容索引鍵”

我的瀏覽器在連線至 時顯示逾時錯誤 AWS 管理主控台

如果您的預設發生服務中斷 AWS 區域，您的瀏覽器可能會在嘗試連線至 時顯示 504 Gateway Timeout 錯誤 AWS 管理主控台。若要 AWS 管理主控台 從不同區域登入 ，請在 URL 中指定替代區域端點。例如，如果 `us-west-1` (加州北部) 區域發生中斷，可使用以下範本存取 `us-west-2` (奧勒岡州) 區域：

```
https://region.console.aws.amazon.com
```

如需詳細資訊，請參閱 AWS 一般參考 中的 AWS 管理主控台 服務端點。

若要檢視所有 的狀態 AWS 服務，包括 AWS 管理主控台，請參閱 AWS Health 儀板表。

我想要變更 的語言， AWS 管理主控台 但找不到頁面底部的語言選擇選單

語言選擇選單已移至新的「統一設定」頁面。若要變更 的語言 AWS 管理主控台，請導覽至統一設定頁面，然後選擇主控台的語言。

如需詳細資訊，請參閱變更 AWS 管理主控台的語言。

文件歷史紀錄

下表說明 AWS 管理主控台 入門指南 自 2021 年 3 月開始生效的重要變更。

變更	描述	Date
更新 AWS 受管政策	使用新的 UXC 許可更新 AWSManagementConsoleAdministratorAccess 和 AWSManagementConsoleBasicUserAccess 政策。如需詳細資訊，請參閱???。	2026 年 3 月 26 日
已新增頁面	新增頁面以說明建議的動作。如需詳細資訊，請參閱???。	2025 年 10 月 15 日
新的 AWS 受管政策	新增兩個新政策，以限制使用、設定和自訂 的許可 AWS 管理主控台範圍。 • AWSManagementConsoleBasicUserAccess • AWSManagementConsoleAdministratorAccess	2025 年 8 月 14 日
使用者體驗自訂 (UXC)	可用的新服務。	2025 年 8 月 14 日
頁面已更新	您現在可以從服務功能表檢視 myApplications 中的應用程式。如需詳細資訊，請參閱???。	2025 年 7 月 29 日
已新增頁面	新增新頁面以說明多工作階段功能。如需詳細資訊，請參閱???。	2024 年 12 月 6 日
頁面已更新	變更您的密碼頁面已更新。如需詳細資訊，請參閱???。	2024 年 6 月 18 日

變更	描述	Date
已新增新頁面	新增頁面以說明如何存取服務功能表和 AWS 事件通知。如需詳細資訊，請參閱???及???。	2024 年 6 月 18 日
頁面已更新	什麼是 AWS 管理主控台？ 頁面已更新。如需詳細資訊，請參閱???。	2024 年 6 月 18 日
取得支援	新增頁面，說明如何取得支援。如需詳細資訊，請參閱???。	2024 年 6 月 18 日
統一導覽和 AWS Console Home	新增頁面以說明如何使用 主控台。如需詳細資訊，請參閱???及???。	2024 年 6 月 18 日
與 Amazon Q 聊天	新的設定頁面，詳細說明使用者如何向 Amazon Q Developer AWS 提出問題。如需詳細資訊，請參閱與 Amazon Q Developer 聊天。	2024 年 5 月 29 日
myApplications	介紹 myApplications 的新頁面。如需詳細資訊，請參閱 myApplications 是什麼 AWS？。	2023 年 11 月 29 日
指定統一設定	新的設定頁面，用於指定套用至目前使用者 (包括語言和區域) 的設定和預設值。如需詳細資訊，請參閱指定統一設定。	2022 年 4 月 6 日

變更	描述	Date
新的 AWS Console Home UI	新的 AWS Console Home UI，其中包含小工具，用於顯示 AWS 服務的重要用量資訊和捷徑。如需詳細資訊，請參閱使用小工具。	2022 年 2 月 25 日
變更主控台語言	為 AWS 管理主控台選擇其他語言。如需詳細資訊，請參閱變更 AWS 管理主控台的語言。	2021 年 4 月 1 日
啟動 CloudShell	AWS CloudShell 從 開啟 AWS 管理主控台 並執行 AWS CLI 命令。如需詳細資訊，請參閱啟動 AWS CloudShell。	2021 年 3 月 22 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。