



入門指南

AWS Management Console



版本 1.0

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

AWS Management Console: 入門指南

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

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

Table of Contents

什麼是 AWS Management Console ?	1
使用您選擇的裝置	1
配置 AWS Management Console	2
使用小工具	2
.....	2
指定統一設定	3
存取統一設定	4
重設統一設定	5
編輯整合設定	5
變更的視覺模式 AWS Management Console	6
在整合設定中變更預設語言	6
選擇區域	7
新增與移除我的最愛	7
變更您的密碼	8
變更的語言 AWS Management Console	9
服務入門	11
統一搜尋	12
與 Amazon Q 聊天	13
開始使用 Amazon Q	13
範例問題	13
我的應用程式 AWS	14
myApplications 的功能	14
相關服務	14
存取 myApplications	15
定價	15
支援地區	15
選擇加入區域	16
開始使用 myApplications	16
步驟 1：建立 應用程式	16
步驟 2：檢視應用程式	18
管理應用程式	19
編輯應用程式	19
刪除應用程式	20
建立程式碼片段	20

管理資源	20
新增資源	21
移除資源	21
myApplications 儀表板	22
應用程式儀表板安裝小工具	22
應用程式摘要小工具	22
運算小工具	22
成本和用量小工具	22
AWS 安全小工具	23
DevOps 小工具	23
監控和操作小工具	24
標籤小工具	24
AWS Management Console 私人存取	25
支援 AWS 區域的服務主控台和功能	25
AWS Management Console 私人存取安全性控制概觀	29
來自您網路的 AWS Management Console 帳戶限制	29
從您的網路到網際網路的連線	29
必要的 VPC 端點和 DNS 組態	29
DNS配置 AWS Management Console 和 AWS 登入	30
VPC 端點和服務的DNSAWS 組態	32
實作服務控制政策和 VPC 端點政策	33
搭配 AWS Organizations 服務控制原則使用 AWS Management Console 私人存取	33
僅允許 AWS Management Console 使用預期的帳戶和組織 (受信任的身分)	33
實作以身分為基礎的政策以及其他政策類型	35
支援的 AWS 全域條件上下文鍵	35
AWS Management Console 私人訪問如何與 aws 配合使用 : SourceVpc	35
如何反映不同的網路路徑 CloudTrail	36
嘗試 AWS Management Console 私人訪問	37
使用 Amazon EC2 進行測試設定	37
使用 Amazon 測試設置 WorkSpaces	51
以 IAM 政策測試 VPC 設定	68
參考架構	69
在主控台工具列上啟動 AWS CloudShell	71
取得帳單資訊	72
降價在 AWS	73
段落、行距和水平線	73

標題	74
文字格式	74
連結	74
清單	74
表格和按鈕 (CloudWatch 儀表板)	75
故障診斷	77
頁面未正確載入	77
連接到我的瀏覽器時顯示「訪問被拒絕」錯誤 AWS Management Console	78
連接到時，我的瀏覽器顯示超時錯誤 AWS Management Console	78
我想變更 AWS Management Console 的語言，但是找不到頁面底部的語言選擇選單	79
文件歷史紀錄	80
AWS 詞彙表	82
.....	lxxxiii

什麼是 AWS Management Console ？

這 [AWS Management Console](#) 是一個 Web 應用程式，它包含並引用了用於管理 AWS 資源的廣泛服務控制台集合。若是首次登入，這時主控台頁面將會顯示。此首頁會提供每個服務主控台的存取權，同時提供單一位置來存取執行 AWS 相關作業所需的資訊。它也可讓您新增、移除和重新排列小工具 (例如「最近造訪」、「AWS Health 全狀況」等)，以自訂「主機首頁」體驗。

Note

語言選擇選項已移至新的「統一設定」頁面。如需詳細資訊，請參閱 [變更 AWS Management Console 的語言](#)。

另一方面，個別服務的主控台提供多種雲端運算工具，以及您帳戶和 [計費](#) 的相關資訊。

使用您選擇的裝置

[AWS Management Console](#) 的設計目的是能用於平板電腦以及其他類型的裝置：

- 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。

也可作為安卓系統和 iOS 的 AWS Management Console 應用程式使用。這個應用程式提供了有助於實現完整 Web 體驗的行動相關任務。例如，您可以從手機輕鬆檢視和管理現有的 Amazon EC2 執行個體和 Amazon CloudWatch 警示。

您可以從 [Amazon 應用商店](#) 下載 AWS 控制台移動應用程式，[谷歌播放](#)，或 [iTunes](#)。

配置 AWS Management Console

本主題說明如何設定您的，以 AWS Management Console 及如何使用 [整合設定] 頁面來設定套用至所有服務主控台的預設值。同時也說明 Widget，這是主控台首頁儀表板的一項功能，可讓您新增自訂元件，以追蹤 AWS 服務和資源的相關資訊。

主題

- [使用小工具](#)
- [指定統一設定](#)
- [選擇區域](#)
- [新增與移除我的最愛](#)
- [變更您的密碼](#)
- [變更的語言 AWS Management Console](#)

使用小工具

主控台首頁控制面板包含 Widget，可顯示有關您 AWS 環境的重要資訊，並提供服務捷徑。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。

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 (在小工具標題列左上角以六個垂直點表示)，然後將其拖曳至「主控台首頁」儀表板。

若要移除小工具

1. 選擇刪節號 (在小工具右上角以三個垂直點表示)。
2. 選擇 Remove widget (移除 Widget)。

重新排列您的小工具

- 選擇拖曳指標 (在小工具標題列左上角以六個垂直點表示)，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 Management Console。

指定統一設定

您可以從「AWS Management Console 整合設定」頁面設定設定和預設值，例如顯示、語言和地區。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

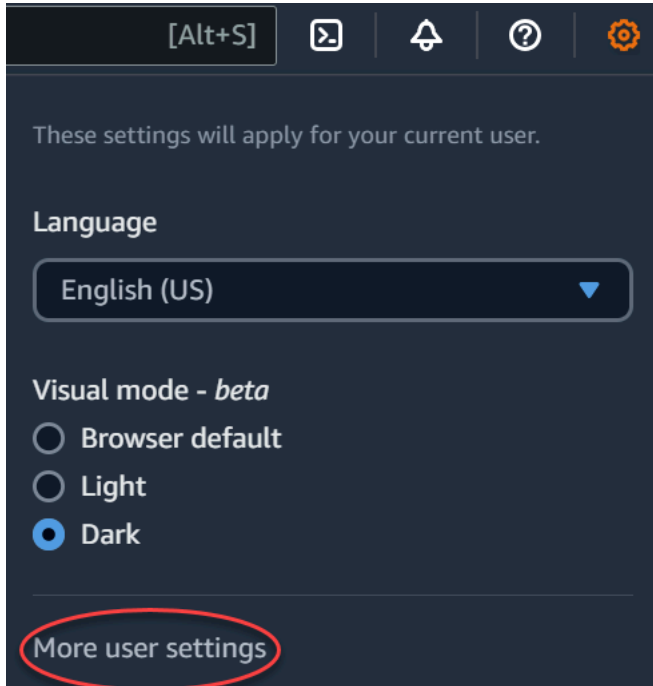
為了確保您的設定、我的最愛服務和最近造訪的服務全域持續存在，此資料會儲存在所有資料中 AWS 區域，包括預設為停用的區域。這些區域是非洲 (開普敦)、亞太區域 (香港)、亞太區域 (海德拉巴)、亞太區域 (雅加達)、歐洲 (米蘭)、歐洲 (西班牙)、歐洲 (蘇黎世)、中東 (巴林) 和中東 (阿拉伯聯合大公國)。如想存取特定區域，然後在該區域中建立和管理資源，您仍然必須 [手動啟用區域](#)。如果您不想全部儲存此資料 AWS 區域，請選擇 [全部重設] 以清除設定，然後在 [設定] 管理中選擇不記住最近造訪過的服務。

存取統一設定

下列程序說明如何存取整合設定。

如何存取統一設定

1. 登入 [AWS Management Console](#)。
2. 在導覽列中，選擇齒輪圖示。
3. 若要開啟統一設定頁面，請選擇更多使用者設定。



重設統一設定

您可以刪除所有整合設定組態，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，包括瀏覽中的我的最愛服務和 [服務] 功能表、[主控台首頁] Widget 上最近造訪過的服務 AWS Console Mobile Application，以及跨服務套用的所有設定，例如預設語言、預設地區和視覺模式。

重設所有整合設定

1. 登入 [AWS Management Console](#)。
2. 在導覽列中，選擇齒輪圖示。
3. 選擇 [更多使用者設定] 以開啟 [整合設定] 頁面。
4. 選擇「全部重設」。

編輯整合設定

下列程序說明如何編輯偏好的設定。

若要編輯整合設定

1. 登入 [AWS Management Console](#)。
2. 在導覽列中，選擇齒輪圖示。
3. 選擇 [更多使用者設定] 以開啟 [整合設定] 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 Management Console](#)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)：
 - 記住最近訪問過的服務可讓您選擇是否 AWS Management Console 記住您最近訪問的服務。關閉此功能也會刪除您最近造訪的服務歷程記錄，因此您不會再在 [服務] 功能表或 [主控台首頁] Widget 中看到最近造訪過的服務。AWS Console Mobile Application

5. 選擇儲存變更。

變更的視覺模式 AWS Management Console

您的視覺模式會將主機設定為淺色模式、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 Management Console](#)。
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。

在整合設定中變更預設語言

下列程序說明如何使用導覽列變更預設語言。

從導覽列變更預設語言

1. 登入 [AWS Management Console](#)。
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偏好的語言。

選擇區域

對於許多服務，您可以選擇 AWS 區域 指定管理資源的位置。地區是位於相同地理區域的 AWS 資源集。您不需要為某些服務（例如）選擇「區域」AWS Identity and Access Management。[AWS Management Console](#)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](#)。

選擇區域

1. 登入 [AWS Management Console](#)。
2. [選擇服務](#)即可前往該服務的主控台。
3. 在導覽列上選擇目前顯示區域的名稱，然後選擇您要切換的區域。

若要選擇預設區域

1. 在導覽列中選擇設定圖示，然後選擇更多使用者設定，以瀏覽至統一設定頁面。
2. 選擇位於 Localization and default Region (本地化和預設區域) 旁的 Edit (編輯)。
3. 選取您的預設地區，然後選擇 [儲存設定]。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。
4. (選擇性) 選擇 [前往新的預設區域]，立即前往新的預設區域。

Note

如果您已建立 AWS 資源，但在主控台中看不到這些資源，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，若要查看這些區域，請使用區域選擇工具選擇包含您資源的區域。

新增與移除我的最愛

若要更快地存取您經常使用的服務，您可以將其服務主控台儲存到 Favorites (我的最愛) 清單中。

若要新增服務到 Favorites (我的最愛) 清單

1. 登入 [AWS Management Console](#)。
2. 選擇位於頁面右上角或右下角的 Add widgets (新增小工具) 按鈕。
3. 在新增小工具 選單中，選擇 我的最愛 以新增至主控台，然後選擇 新增。

我的最愛新增於主機首頁底部。您可以透過選擇小工具頂部的標題列來拖曳我的最愛，然後將小工具拖曳到頁面上的新位置。

4. 在導覽列上選擇 Services (服務)。
5. 在最近造訪清單或所有服務清單中，將游標暫留在您要新增為我的最愛的服務名稱上。
6. 選取服務名稱左側的星號。
7. 重複前兩個步驟，即可新增更多服務到 Favorites (我的最愛) 清單。

若要從 Favorites (我的最愛) 清單中移除服務

1. 在導覽列上選擇 Services (服務)。
2. 執行以下任意一項：
 - 在我的最愛清單中，將游標暫留在服務名稱上。然後選擇服務名稱右側的 ×。
 - 在 Recently visited (最近用過) 清單或 All services (所有服務) 清單中，依照 Favorites (我的最愛) 清單中的服務名稱，取消選取名稱旁邊的星號。

變更您的密碼

如果您是帳戶擁有者，您可以從中變更您的 AWS 帳戶密碼 [AWS Management Console](#)。

變更您的密碼

1. 登入 [AWS Management Console](#)。
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. 顯示的選項將根據您的 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)。

變更的語言 AWS Management Console

體 AWS Console Home 驗包括「整合設定」頁面，您可以在其中變更中 AWS 服務的預設語言 AWS Management Console。您還可以從設定選單快速變更預設語言，從導覽列即可存取該選單。您可以從主控台的任何位置執行這項變更。

Note

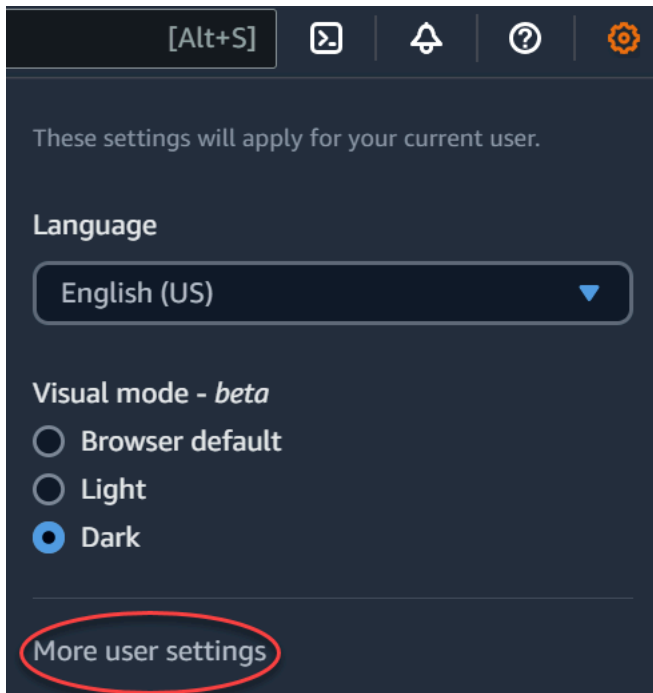
這項程序會變更所有主控台的語言，但不會變更 AWS 文件的語言。若要變更文件的語言，請使用文件頁面右上方的語言選單選擇所需語言。

目 AWS Management Console 前支援下列語言：

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

在統一設定中變更預設語言

1. 登入 [AWS Management Console](#)。
2. 在導覽列中，選擇設定圖示。
3. 若要開啟統一設定頁面，請選擇更多使用者設定。



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 服務的主控台文字都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 Management Console 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 服務的主控台文字都會以您偏好的語言顯示。

從導覽列變更預設語言

1. 登入 [AWS Management Console](#)。
2. 在導覽列中，選擇設定圖示。
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。

服務入門

[AWS Management Console](#) 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

執行下列任意一項：

- 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 [使用整合搜尋來搜尋產品、服務、功能等](#)。
- 在 Recently visited services (最近用過的服務) 小工具中，選擇服務名稱。
- 在 Recently visited services (最近用過的服務) 小工具中，選擇 View all AWS services (檢視所有 AWS 服務)。然後，在 All AWS services (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)。

使用整合搜尋來搜尋產品、服務、功能等

導覽列中的搜尋方塊提供整合的搜尋工具，可方便您追蹤 AWS 服務與功能、服務文件以及 AWS Marketplace。只要輸入幾個字元，即可查看所有類別的結果。您輸入的字元越多，搜尋作業越能提供更準確的結果。

若要搜尋服務、功能、文件或 AWS Marketplace 產品

1. 在的導覽列上的搜尋方塊中 AWS Management Console，輸入全部或部分搜尋字詞。
2. 執行下列任一操作，以縮小搜尋範圍並取得更多詳細資訊：
 - 若要將結果範圍縮小至您需要的內容類型，請選擇左側的任何一種類別。
 - 若要查看特定類別的更多搜尋結果，請依各個類別標題選擇 See all *n* results (查看所有 *n* 個結果)。若要返回主要的結果清單，請選擇左上角的 Back (返回)。
 - 若要快速導覽至服務的熱門功能，請將游標停留在結果中的服務名稱上，然後選擇連結。
 - 若要取得有關文件或 AWS Marketplace 結果的詳細資訊，請暫停結果標題。
3. 選擇任一連結即可瀏覽至您需要的服務、主題，或 AWS Marketplace 頁面。

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。

與 Amazon Q 開發人員聊天

Amazon Q Developer 是採用生成式人工智慧 (AI) 的交談助理，可協助您了解、建置、擴充和操作 AWS 應用程式。您可以向 Amazon Q 詢問任何有關 AWS 架構、資源、最佳實務、文件等的問題。您還可以創建支持案例並從實時代理獲得幫助。如需詳細資訊，請參閱[什麼是 Amazon Q?](#) 在 Amazon Q 開發人員用戶指南中。

開始使用 Amazon Q

您可以選擇六角形的 Amazon Q 圖示 AWS Management Console，在 AWS 文件、AWS 網站、網站或 Con AWS sole Mobile Application 中開始與 Amazon Q 聊天。如需詳細資訊，請參閱[Amazon Q 開發人員使用指南](#)中的 Amazon Q 開發人員入門。

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?

什麼是我的 AWS 應用程式？

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。您可以從中的一個檢視存取帳戶中的所有應用程式、跨所有應用程式的關鍵指標，以及成本、安全性和作業指標的概觀，以及來自多個服務主控台的見解 AWS Management Console。myApplications 包括以下內容：

- 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

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「我的應用程式」中，因此您可以在 API AWS Management Console、CLI 和 SDK 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 是可用的 IaC 工具，包括 AWS CloudFormation 和地形。
- **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。
- **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、金絲雀和服務層級目標來評估應用程式的健康狀態和效能 Amazon CloudWatch AWS Security Hub、來自的發現結果和成本趨勢。AWS Cost Explorer Service 您也可以從中找到運算指標摘要和最佳化，以及管理資源符合性和組態狀態。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
- 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 Management Console](#) 中存取 myApplications。

定價

我的應用程式在 AWS 提供，不收取額外費用。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。

支援地區

我的應用程式可在下列項目中使用：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)
- 亞太區域 (孟買)
- 亞太區域 (大阪)
- 亞太區域 (首爾)
- 亞太區域 (新加坡)
- 亞太區域 (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。如需有關的詳細資訊 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)
- 亞太區域 (香港)
- 亞太區域 (海德拉巴)
- 亞太區域 (雅加達)
- 亞太區域 (墨爾本)
- 歐洲 (米蘭)
- 歐洲 (西班牙)
- 歐洲 (蘇黎世)
- Middle East (Bahrain)
- 中東 (阿拉伯聯合大公國)
- 以色列 (特拉維夫)

開始使用 myApplications

若要開始使用 myApplications 建立、監視和管理應用程式，請使用下列步驟。

步驟 1：建立 應用程式

建立新的應用程式或在 2023 年 11 月 8 日之前建立的現有 AppRegistry 應用程式上載，以開始使用「我的應用程式」。

Create an application

建立應用程式

1. 登入 [AWS Management Console](#)。
2. 在左側邊欄中，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

應用 AWS 程式標籤會自動套用至新建立的應用程式，並可用來識別與您的應用程式相關聯的資源。如需詳細資訊，請參閱 [《AWS Service Catalog AppRegistry 管理指南》](#) 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) 新增現有資源：

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 [開始使用 AWS 資源總管](#)。
所有新增的資源都會以 AWS 應用程式標籤加上標籤。

- a. 選擇選取資源。
- b. (選用) 選擇 [檢視](#)。
- c. 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

如果找不到所需的資源，請使用 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](#)。

- d. 選取要新增之資源旁的核取方塊。
 - e. 選擇新增。
 - f. 選擇下一步。
10. 檢閱選擇。
 11. 如果要關聯 AWS CloudFormation 堆疊，請選取頁面底部的核取方塊。

 Note

將 AWS CloudFormation 堆疊新增至應用程式需要進行堆疊更新，因為新增至應用程式的所有資源都會標記 AWS 應用程式標記。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《AWS CloudFormation 使用者指南》中的[更新堆疊資源的行為](#)。

12. 選擇建立應用程式。

Onboard existing application

將現有的 AppRegistry 應用程式上載

1. 登入 [AWS Management Console](#)。
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. 如果要建立 CloudFormation 堆疊關聯，請選取警告方塊中的核取方塊。
7. 選擇加入應用程式。

步驟 2：檢視應用程式

您可以在卡片或資料表檢視中，檢視所有區域或特定區域的應用程式及其相關資訊。

檢視應用程式

1. 在左側邊欄中，選擇 myApplications。
2. 在地區中，選取目前地區或支援的區域。

3. 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。
4. (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。

管理應用程式

本主題說明如何管理應用程式。

編輯應用程式

編輯您的應用程式隨即開啟，AppRegistry 讓您可以更新其說明。您也可以使用 AppRegistry 來編輯應用程式的標籤和屬性群組。

編輯應用程式

1. 開啟 [AWS Management Console](#)。
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 myApplications 儀表板上選擇動作，然後選擇編輯應用程式。
5. 在編輯應用程式說明中更新說明，然後選擇儲存變更。

編輯標籤

- 請遵循《管理AWS Service Catalog AppRegistry 員指南》中的「[管理標籤](#)」中的步驟。

編輯屬性群組

- 請遵循《管理員指南》中的 [〈編輯屬性群組AWS Service CatalogAppRegistry〉](#) 中的步驟。

刪除應用程式

如果已不再需要應用程式，則可將其刪除。

如欲刪除應用程式

1. 開啟 [AWS Management Console](#)。
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. 選擇刪除。
7. 確認刪除，然後選擇刪除應用程式。

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標記 AWS 應用程式標籤，以便將其與您的應用程式相關聯。

建立應用程式的程式碼片段

1. 開啟 [AWS Management Console](#)。
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。

管理資源

本主題介紹如何管理資源。

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。

新增資源

1. 開啟 [AWS Management Console](#)。
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

如果找不到所需的資源，請使用 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。

移除資源

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 Management Console](#)。
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

如果找不到所需的資源，請使用 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。

myApplications 儀表板

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、安全性和操作小器具，可顯示來自多個 AWS 服務的見解。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[使用小工具](#)。

應用程式儀表板安裝小工具

此 Widget 包含建議的入門活動清單，您可以用來協助您設定管理應 AWS 服務 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 EC2 執行個體 CPU 使用率和 Lambda 叫用的資源效能指標趨勢圖。
Amazon CloudWatch

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 Widget 會顯示應用程式資源的 AWS 成本和使用情況資料。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 Widget 只會彙總標記為 AWS 應用程式標籤的資源成本，不包括稅

金、費用和其他與資源無直接關聯的共用成本。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

若要設定成本和使用量 Widget，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 Widget 會顯示應用程式安全 AWS 性中的安全性發現項目。AWS 安全性為您的應用程式提供中安全性發現項目的全面檢視 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](#)。

配置安 AWS 全小器具

要配置 AWS 安全小部件，請 AWS Security Hub 為您的應用程序和帳戶進行設置。如需詳細資訊，請參閱[什麼是 AWS Security Hub?](#) 在《AWS Security Hub 使用者指南》中。如需定價資訊，請參閱《AWS Security Hub 使用者指南》中的 [AWS Security Hub 免費試用、用量和定價](#)。

AWS Security Hub 要求您 Con AWS fig 配置錄製。此服務提供與您 AWS 帳戶相關聯之資源的詳細檢視。如需詳細資訊，請參閱《AWS Systems Manager 使用者指南》中的 [AWS Systems Manager](#)。

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

配置 DevOps 小器具

若要設定 DevOps Widget，請 AWS Systems Manager OpsCenter 為您的應用程式和帳戶啟用。如需詳細資訊，請參閱「[Systems Manager 總管入門](#)」和「[AWS Systems Manager 使用者指南](#)」

OpsCenter 中的。啟用 OpsCenter AWS Systems Manager Explorer 允許配置，AWS Config 並 Amazon CloudWatch 使其事件 OpsItems 根據常用的規則和事件自動創建。若要取得更多資訊，請參閱 [《使用指南》 OpsCenter 中的 AWS Systems Manager 〈設置〉](#)。

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 AWS Systems Manager 式管理員，為應用程式設定 Amazon EC2 執行個體的自動修補。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 應用程式訊號

設定監控和操作小工具

要配置監視和操作小部件，請在您的 AWS 帳戶中創建 CloudWatch 警報和金絲雀。如需詳細資訊，請參閱 [Amazon 使用 CloudWatch 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 Canary 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 應用程式訊號的詳細資訊，請參閱 [Amazon CloudWatch 使用者指南中的啟用 Amazon CloudWatch 應用程式深入解析](#)。

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 [什麼是標籤？](#) 在標記 AWS 資源 AWS 白皮書的最佳做法中。

AWS Management Console 私人存取

AWS Management Console 私人存取是一項進階安全性功能，可控制對 AWS Management Console。AWS Management Console 當您想要防止使用者從您的網路中登入意外 AWS 帳戶時，「私人存取」非常有用。使用此功能，您可以限制 AWS Management Console 只存取一組指定的已知流量來自您的網路 AWS 帳戶時。

主題

- [支援 AWS 區域的服務主控台和功能](#)
- [AWS Management Console 私人存取安全性控制概觀](#)
- [必要的 VPC 端點和 DNS 組態](#)
- [實作服務控制政策和 VPC 端點政策](#)
- [實作以身分為基礎的政策以及其他政策類型](#)
- [嘗試 AWS Management Console 私人訪問](#)
- [參考架構](#)

支援 AWS 區域的服務主控台和功能

AWS Management Console 私有存取僅支援區域和 AWS 服務的子集。AWS Management Console 中不受支援的服務主控台將處於非作用中。此外，使用 AWS Management Console 私人存取時，某些 AWS Management Console 功能可能會停用，例如「整合設定」中的「[預設區域](#)」選項。

支援下列區域和服務主控台。

支援地區

- 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)
- 亞太區域 (海德拉巴)
- 亞太區域 (孟買)
- 亞太區域 (首爾)
- 亞太區域 (大阪)

- 亞太區域 (新加坡)
- 亞太區域 (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)
- 非洲 (開普敦)
- Asia Pacific (Hong Kong)
- 亞太區域 (雅加達)
- 亞太區域 (墨爾本)
- 加拿大西部 (卡加利)
- 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
- Amazon Athena
- AWS Auto Scaling
- AWS Billing Conductor
- AWS Certificate Manager

- AWS Cloud Map
- Amazon CloudFront
- Amazon CloudWatch
- AWS CodeArtifact
- AWS CodeBuild
- Amazon CodeGuru
- Amazon Comprehend
- Amazon Comprehend Medical
- AWS Compute Optimizer
- AWS Console Home
- AWS Database Migration Service
- AWS DeepRacer
- 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
- Amazon ElastiCache
- Amazon EMR
- Amazon EventBridge
- Amazon GameLift
- AWS Global Accelerator
- AWS Glue DataBrew
- AWS Ground Station

- Amazon GuardDuty
- 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 數據 Firehose
- Amazon Kinesis Video Streams
- AWS Lambda
- Amazon Lex
- AWS License Manager
- Amazon Managed Grafana
- 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 Manager
- Amazon OpenSearch 服務
- AWS Organizations
- Amazon S3 on Outposts
- Amazon SageMaker 運行
- Amazon SageMaker 合成數據
- AWS Secrets Manager
- Service Quotas
- AWS Signer
- Amazon Simple Email Service
- Amazon Simple Queue Service

- Amazon Simple Storage Service (Amazon S3)
- AWS SQL Workbench
- AWS Step Functions
- AWS Support
- AWS Systems Manager
- AWS Transfer Family
- 統一設定
- Amazon VPC IP 地址管理員

AWS Management Console 私人存取安全性控制概觀

來自您網路的 AWS Management Console 帳戶限制

AWS Management Console 如果您只想將網路的存取限制為組織中已知的 AWS Management Console 指定集合，則 Private Access AWS 帳戶 在情況下很有用。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 Management Console 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

您的網路仍需要網際網路連線，才能存取所使用的資產 AWS Management Console，例如靜態內容 (CSS JavaScript、影像)，以及所有 AWS 服務 未啟用的資產 [AWS PrivateLink](#)。如需使用的頂層網域清單 AWS Management Console，請參閱 [故障診斷](#)。

Note

目前，AWS Management Console 私人存取不支援 `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 Management Console 私人存取每個區域需要以下兩個 VPC 端點。以您自己的區域資訊取代 `#`。

1. COM. 亞馬遜。##. 控制台 AWS Management Console
2. COM. 亞馬遜。##. 登入 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 Management Console 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](#)。

DNS配置 AWS Management Console 和 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 Management Console 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`：

- 區域 CNAME 記錄 (所有區域中)
- 區域登入指向登入區域中的 VPC 人雲端端點 AWS 登入 DNS
- 指向控制台區域中的 VPC 人雲端端點 AWS Management Console 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。
 - 指向美國東部 (維吉尼亞北部) 的 AWS 登入 VPC 端點 (us-east-1)
 - 指向美國東部 (維吉尼亞北部) 的 AWS Management Console VPC 端點 (us-east-1)

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](#)。

某些 AWS 主控台 (包括 Amazon S3) 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

若要將此流量導向至您的 AWS Management Console 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。但是，這不是使用 AWS Management Console 私人訪問所必需的。

下列 json 檔案包含要設定每個區域的 AWS 服務完整清單和主控台端點。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-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 Management Console 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.signin.aws.amazon.com
- support.console.aws.amazon.com
- global.console.aws.amazon.com
- 之前列出的 JSON 檔案中存在的其他記錄

VPC 端點和服務的DNSAWS 組態

AWS 服務 通過直接瀏覽器請求和 Web 服務器代理請求的組合進行 AWS Management Console 調用。若要將此流量導向至您的 AWS Management Console 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 檔案。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-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，因為我們增加對更多服務主控台的 AWS Management Console 私人存取支援。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

您可以針對 AWS Management Console 私人存取使用服務控制原則 (SCP) 和 VPC 端點原則，限制允許 AWS Management Console 從 VPC 及其連線的內部部署網路中使用的帳戶集。

搭配 AWS Organizations 服務控制原則使用 AWS Management Console 私人存取

如果您的 AWS 組織使用允許特定服務的服務控制原則 (SCP)，您必須新增 `signin:*` 至允許的動作。需要此權限，因為 AWS Management Console 透過私有存取 VPC 端點登入會執行 IAM 授權，SCP 在未經許可的情況下封鎖。例如，以下服務控制政策允許在組織中使用 Amazon EC2 和 CloudWatch 服務，包括使用 AWS Management Console 私有存取端點存取服務的時間。

```
{
  "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 AWS Management Console 使用預期的帳戶和組織 (受信任的身分)

AWS Management Console 並 AWS 登入 支援專門控制已登入帳戶身分的 VPC 端點策略。

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，而不會控制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 (例如 Amazon EC2 主控台) 時，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。相反地，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

VPC 端點 AWS Management Console 和 VPC 端點的 SignIn VPC 端點原則僅支援有限的政策公式子集。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 端點使用下列策略。

此 VPC 端點策略允許在指定 AWS 組織 AWS 帳戶 中登錄並阻止登錄到任何其他帳戶。

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

此 VPC 端點策略將登錄限制為特定列表，AWS 帳戶 並阻止登錄到任何其他帳戶。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
```



```
"Action": "*",
"Resource": "*",
"Condition": {
  "StringEquals": {
    "aws:PrincipalAccount": [ "111122223333", "222233334444" ]
  }
}
]
```

限制 AWS Management Console 和登入 VPC 端點上限制 AWS 帳戶 或組織的政策會在登入時進行評估，並針對現有工作階段定期重新評估。

實作以身分為基礎的政策以及其他政策類型

您可以 AWS 透過建立政策並將其附加到 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。本頁說明原則與 AWS Management Console 私人存取一起使用時的運作方式。

支援的 AWS 全域條件上下文鍵

AWS Management Console 私有訪問不支持 `aws:SourceVpce` 和 `aws:VpcSourceIp` AWS 全局條件上下文鍵。使用 AWS Management Console 私有存取時，您可以改為在政策中使用 `aws:SourceVpc` IAM 條件。

AWS Management Console 私人訪問如何與 `aws` 配合使用：SourceVpc

本節說明您所產生之要求 AWS Management Console 可以採取的各種網路路徑 AWS 服務。一般而言，AWS 服務主控台是以 AWS Management Console 網路伺服器代理的直接瀏覽器要求和要求混合來實作。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，建議您針對要從 VPC 使用的所有服務 (無論是直接還是透過 AWS Management Console 私人存取) 設定 VPC 端點。此外，您必須在政策中使用 `aws:SourceVpc` IAM 條件，而不是使用 AWS Management Console 私人存取功能的特定 `aws:SourceVpce` 值。本節提供不同網路路徑如何運作的詳細資訊。

使用者登入之後 AWS Management Console，他們會 AWS 服務 透過直接瀏覽器要求和由 AWS Management Console 網頁伺服器代理到伺服器的要求的組合來 AWS 發出要求。例如，CloudWatch 圖形資料要求是直接從瀏覽器發出。有些 AWS 服務主控台請求 (例如 Amazon S3) 是由網路伺服器代理至 Amazon S3。

對於直接瀏覽器請求，使用 AWS Management Console 私人訪問不會改變任何內容。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 設定為的 VPC 端點 `com.amazonaws.region.monitoring`，則會透過 CloudWatch 過該 CloudWatch VPC 端點傳送要求。如果沒有用於的 VPC 端點 CloudWatch，請求將透過 CloudWatch 過 VPC 上的 Internet Gateway 到達其公用端點。CloudWatch 透過 CloudWatch VPC 端點到達的請求將具有 IAM 條件 `aws:SourceVpc` 並 `aws:SourceVpce` 設定為各自的值。CloudWatch 透過其公用端點到達的使用者將會 `aws:SourceIp` 設定為要求的來源 IP 位址。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 Management Console 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，Amazon S3 主控台發出的請求)，網路路徑會有所不同。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。但是，當您將 AWS Management Console 私有存取與支援的服務搭配使用時，這些請求 (例如，對 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，其中部署用於登入和主控台的 AWS Management Console 私人存取端點。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 Management Console 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 Management Console 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)。

如何反映不同的網路路徑 CloudTrail

由您產生的要求所使用的不同網路路徑會反映 AWS Management Console 在您的 CloudTrail 事件歷史記錄中。

對於直接瀏覽器請求，使用 AWS Management Console 私人訪問不會改變任何內容。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 端點識別碼。

對於 AWS Management Console Web 伺服器代理的要求，CloudTrail 事件不會包含任何 VPC 相關詳細資料。不過，建立瀏覽器工作階段所需的初始要求 (例如 `AwsConsoleSignIn` 事件類型) 會在事件詳細資料中包含 AWS 登入 VPC 端點識別碼。AWS 登入

嘗試 AWS Management Console 私人訪問

本節說明如何在新帳戶中設定和測試 AWS Management Console 私人存取。

AWS Management Console 私人存取是一項進階安全性功能，需要有關網路和設定 VPC 的先進知識。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 Management Console 私有存取。

主題

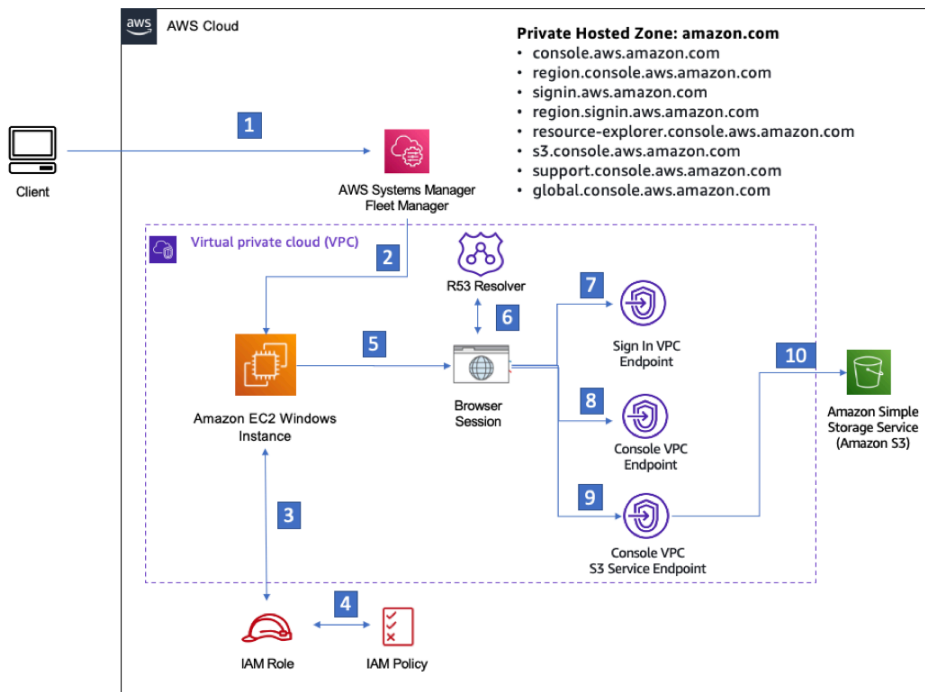
- [使用 Amazon EC2 進行測試設定](#)
- [使用 Amazon 測試設置 WorkSpaces](#)
- [以 IAM 政策測試 VPC 設定](#)

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。

本指南示範用於設定和體驗從 Amazon Amazon EC2 執行個體到 Amazon 簡單儲存服務的 AWS Management Console 私有存取連線的測試環境。本教學課程 AWS CloudFormation 用於建立和設定 Amazon EC2 使用的網路設定，以視覺化此功能。

下圖說明使用 Amazon EC2 存取 AWS Management Console 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。



- 1 Client connects to the Fleet manager using Key pair.
- 2 Authenticated session connection to Windows Server using the Remote Desktop Protocol (RDP).
- 3 EC2 instance confirms credentials for IAM role in use as instance profile.
- 4 EC2 instance profile role permissions check.
- 5 Initiate browser session in EC2 instance.
- 6 Route53 resolver with endpoint address.
- 7 Private Sign in endpoint.
- 8 Private Console endpoint.
- 9 S3 service private endpoint.
- 10 Connected to S3 service via private endpoint.

複製以下 AWS CloudFormation 範本並將其儲存至您將在「設定網路」程序的步驟三中使用的檔案。

Note

此 AWS CloudFormation 範本使用目前在以色列 (特拉維夫) 區域不支援的組態。

AWS Management Console 私有訪問環境 Amazon EC2 AWS CloudFormation 模板

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: 't2.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
```

```
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
```

```
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 [AWS 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 AWS 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，請確認它們不與 AWS 帳戶
6. 對於 EC2 KeyPair 參數，請從帳戶中現有的 Amazon EC2 金鑰配對中選取一個。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 key pair](#)。
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，選取範本建立的主控台 VPCE 測試執行個體 AWS CloudFormation。然後選擇 連線。

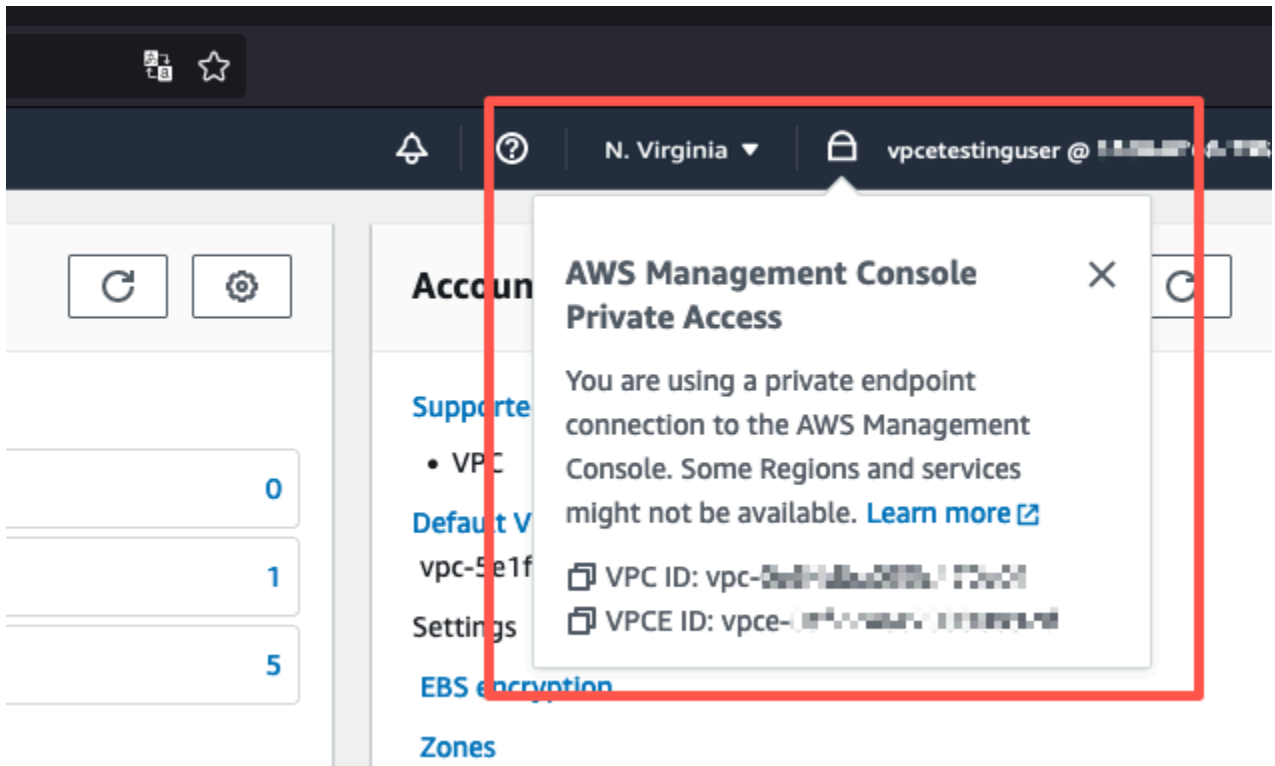
Note

此範例使用「叢集管理員」(的 AWS Systems Manager Explorer 功能) 來連線到 Windows 伺服器。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 AWS CloudFormation 範本時使用的 Amazon EC2 key pair 相關聯的私密金鑰。
7. 從 Amazon EC2 視窗執行個體，在瀏覽器 AWS Management Console 中開啟。
8. 使用登入 AWS 資料登入後，開啟 [Amazon S3 主控台](#) 並確認您已使用 AWS Management Console 私人存取連線。

若要測試 AWS Management Console 私人存取設定

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 測試設置 WorkSpaces

Amazon 使您 WorkSpaces 能夠佈建虛擬, 基於雲的視窗, Amazon Linux, 或 Ubuntu Linux 桌面為您的用戶, 被稱為 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](#)。

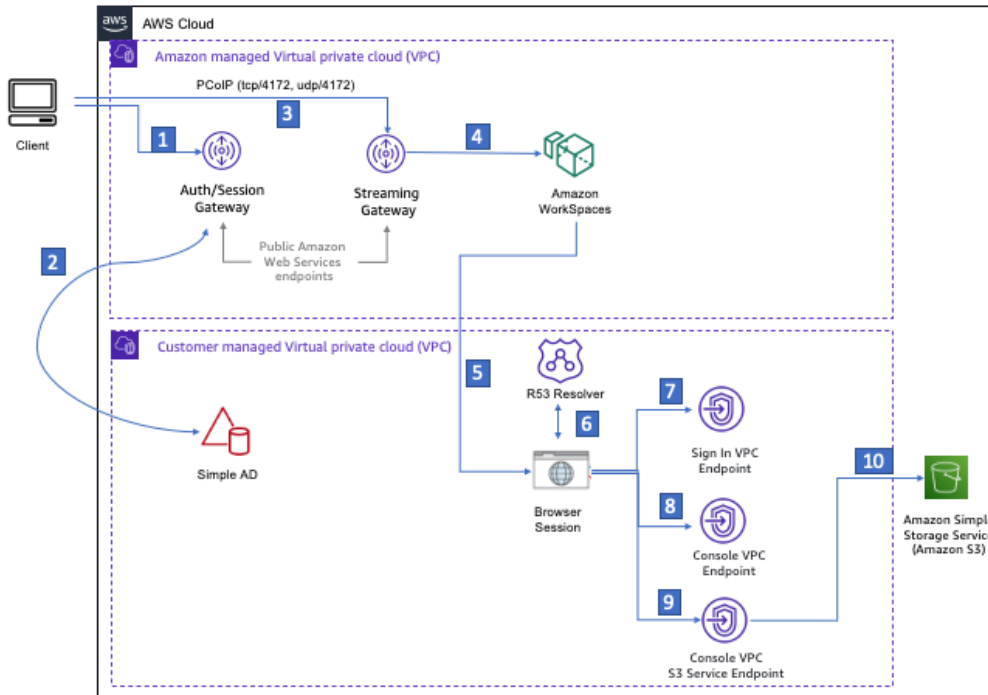
本節中的範例說明測試環境, 在此環境中, 使用者環境使用在上執行的 WorkSpace 網頁瀏覽器登入 AWS Management Console Private Access。然後, 使用者會造訪 Amazon Simple Storage Service 主控台。這 WorkSpace 是為了模擬企業用戶在連接 VPC 的網絡上使用筆記本電腦的體驗, AWS Management Console 從他們的瀏覽器訪問。

本教程使 AWS CloudFormation 用創建和配置網絡設置和一個簡單的活動目錄由一步一步的說明一 WorkSpaces 起使用來設置 WorkSpace 使用 AWS Management Console。

下圖說明使用 a WorkSpace 測試 AWS Management Console 私人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。

Private Hosted Zone: amazon.com

- console.aws.amazon.com
- region.console.aws.amazon.com
- signin.aws.amazon.com
- region.signin.aws.amazon.com
- resource-explorer.console.aws.amazon.com
- s3.console.aws.amazon.com
- support.console.aws.amazon.com
- global.console.aws.amazon.com



- 1 Login information sent to authentication gateway
- 2 Authentication against Simple AD
- 3 Streaming Traffic to Streaming gateway
- 4 Each Workspace is connected to two networks simultaneously, Amazon-managed VPC for streaming traffic and Customer managed VPC handling all other traffic.
- 5 Initiate browser session
- 6 Route53 resolver with endpoint address.
- 7 Private Sign in endpoint
- 8 Private Console endpoint
- 9 S3 service private endpoint
- 10 Connected to S3 service via private endpoint

複製以下 AWS CloudFormation 範本並將其儲存至您將在設定網路程序的步驟 3 中使用的檔案。

AWS Management Console 私有存取環境 AWS 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

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::VPCEGatewayAttachment
```

```
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

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

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: "ADAdminSecret"
    Description: "Password for directory services admin"
    GenerateSecretString:
      SecretStringTemplate: '{"username": "Admin"}'
      GenerateStringKey: password
      PasswordLength: 30
      ExcludeCharacters: '"@/\`'

WorkspaceSimpleDirectory:
  Type: AWS::DirectoryService::SimpleAD

```

```
DependsOn: AppVPC
DependsOn: PrivateSubnetA
DependsOn: PrivateSubnetB
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 [AWS 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 AWS 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，請確認它們不與 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 and Workspace Simple Directory 的值。請注意這些值，因為您將在下一個程序的步驟四中使用它們來建立和配置 WorkSpace。

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。

PrivateConsoleNetworkForS3



Delete

Update

Stack actions ▼

Create stack ▼

Stack info

Events

Resources

Outputs

Parameters

Template

Change sets

Outputs (4)



Search outputs

< 1 >

Key ▲	Value ▼	Description ▼	Export name
PrivateSubnetA	subnet-0dbb336fdb5467891	Private Subnet A	-
PrivateSubnetB	subnet-00ad943c5d84fd13a	Private Subnet B	-
WorkspacesAdminPassword	arn:aws:secretsmanager:us-east-1:425341151473:secret:ADAdminSecret-HR1MHT	The ARN of the Workspaces admin's password. Navigate to the Secrets Manager in the AWS Console to view the value.	-
WorkspaceSimpleDirectory	d-90679724b4	Directory to be used for Workspaces	-

現在您已經建立了網路，請使用下列程序來建立和存取 WorkSpace。

若要建立 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。

Directory ID	Directory name	Organization name	Directory type	Registered
d-90679724b4	corp.awsconsole.com	d-90679724b4	Simple AD	True

4. 若要在中使用目錄 WorkSpaces，您必須註冊它。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 AWS 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，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 登錄信息發送到此電子郵件地址。
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使用者自訂的預設設定，檢閱並選擇建立工作區。在Pending狀態 WorkSpace 開始，並在大約 20 分鐘Available內轉換。
14. 當可用時，您將收到一封電子郵件，其中包含您在步驟 9 中提供的電子郵件地址訪問它的說明。
WorkSpace

登入後 WorkSpace，您可以測試您是否正在使用 AWS Management Console 私人存取權存取。

若要存取 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. WorkSpaces 使用您在步驟三中建立的登入資料登入 Amazon。

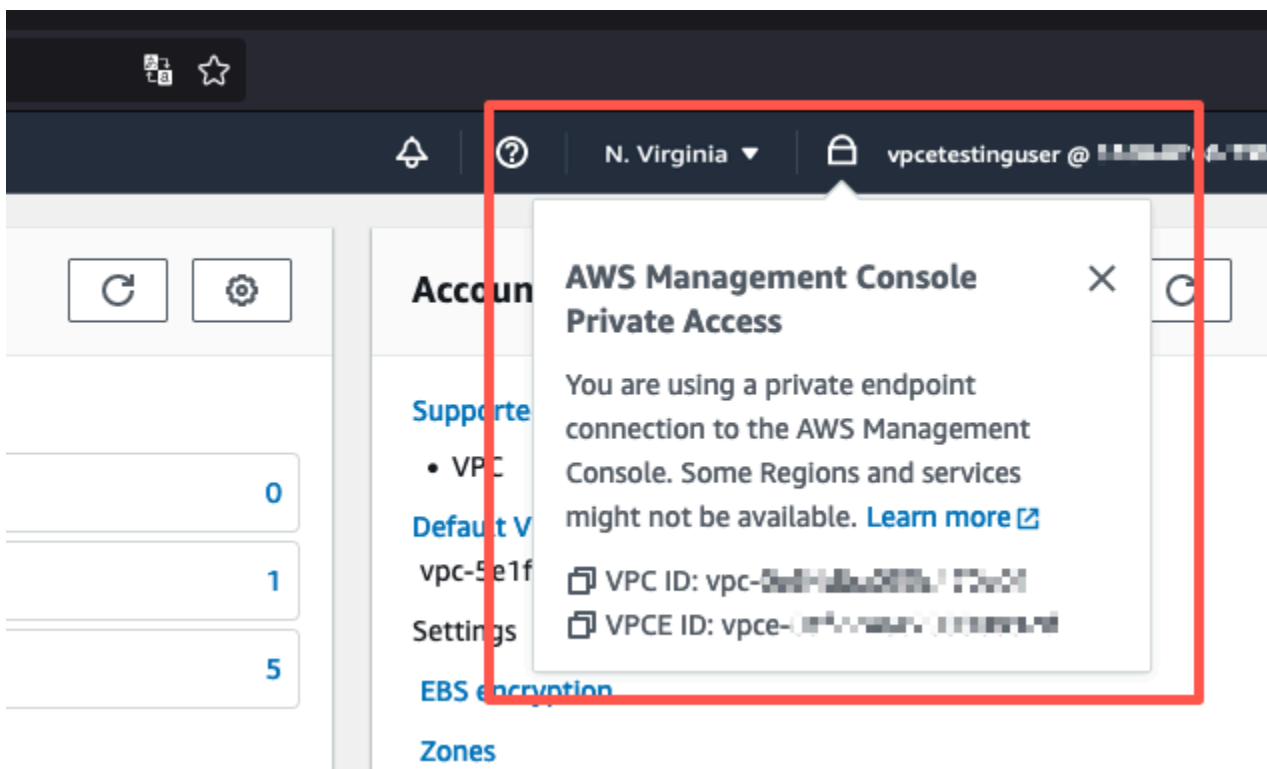
若要測試 AWS Management Console 私人存取設定

1. 在您的瀏覽器中 WorkSpace，開啟瀏覽器。然後，導覽至 [AWS Management Console](#) 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](#)，您可以在其中確認是否使用 AWS Management Console 私有存取連線。
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

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

下列政策會拒絕存取 Amazon S3，除非它使用您指定的 VPC。

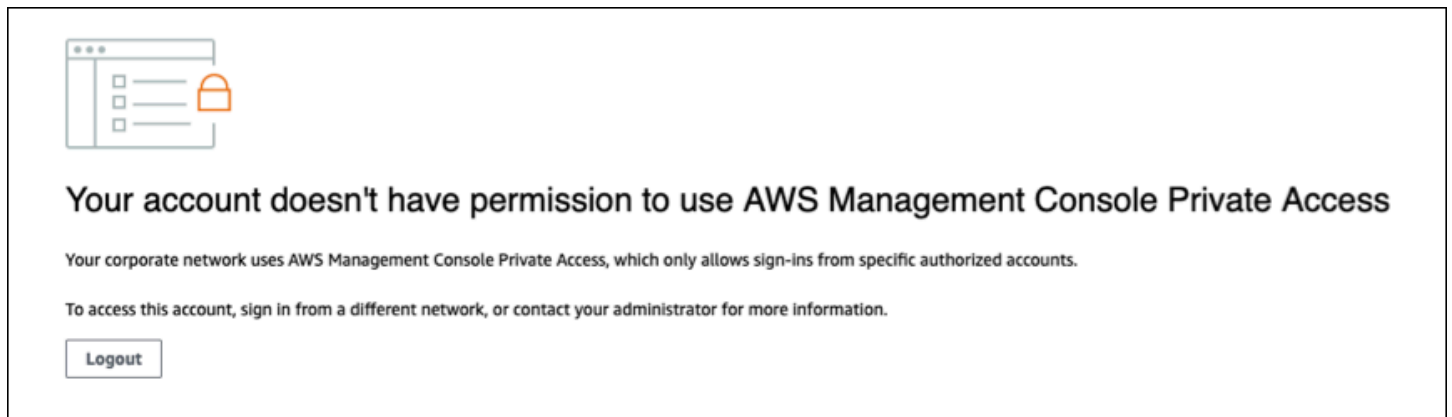
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "S3:*",
      "Resource": "*",
      "Condition": {
        "StringNotEqualsIfExists": {
          "aws:SourceVpc": "sourceVPC"
        },
        "Bool": {
          "aws:ViaAwsService": "false"
        }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

下列政策會針對登入端點使用 AWS Management Console 私人存取政策，限制登入選取的 AWS 帳戶 ID。

```
{
  "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。



Your account doesn't have permission to use AWS Management Console Private Access

Your corporate network uses AWS Management Console Private Access, which only allows sign-ins from specific authorized accounts.

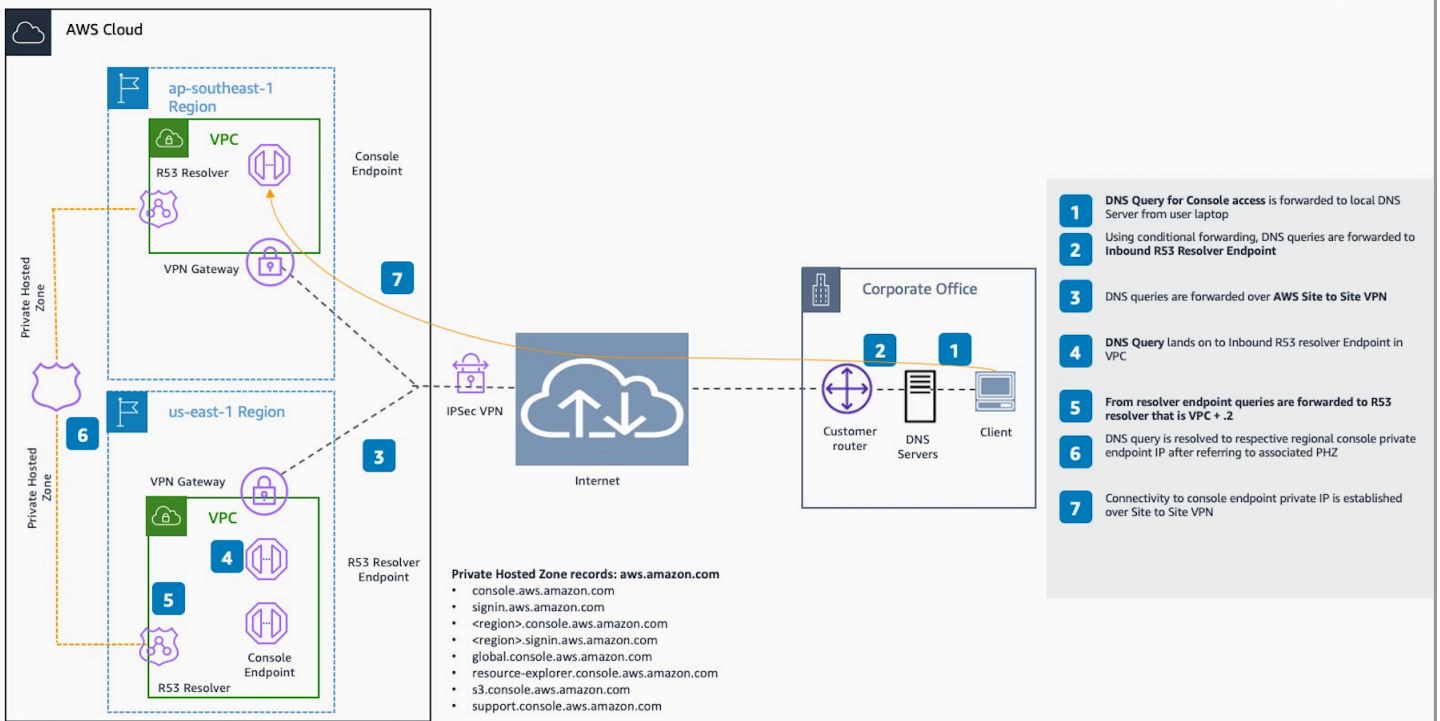
To access this account, sign in from a different network, or contact your administrator for more information.

[Logout](#)

參考架構

若要從內部部署網路 AWS Management Console 私密連線到私人存取，您可以利用 AWS Site-to-Site VPN 到 AWS 虛擬私人閘道 (VGW) 連線選項。AWS Site-to-Site VPN 透過建立連線並設定路由以透過連線傳遞流量，以便從 VPC 存取遠端網路。如需詳細資訊，請參閱[AWS 網站間 VPN 使用者指南中的 AWS Site-to-Site VPN 是什麼](#)。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 前往 AWS 虛擬私有閘道 (VGW)



此參考架構設計中的一個重要組成部分是 Amazon Route 53 Resolver，特別是入站解析器。在建立 AWS Management Console 私人存取端點的 VPC 中進行設定時，會在指定的子網路中建立解析器端點 (網路介面)。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 Management Console，它們會路由到 AWS Management Console 私人存取端點的私有 IP。

在設定與 AWS Management Console Private Access 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以及美國東部 (維吉尼亞北部) 區域中設定 AWS Management Console 私人存取端點，以及設定私有託管區域。AWS Management Console

在主控台工具列上啟動 AWS CloudShell

AWS CloudShell 是以瀏覽器為基礎、預先驗證身分的殼層，您可以直接在主控台工具列上的 AWS Management Console 進行啟動。您可以使用您偏好的 Shell (Bash , PowerShell 或 Z shell) ，對服務執行 AWS CLI 命令。

您可以下列兩個方法的其中一個在 Console Toolbar 上啟動 CloudShell：

- 選擇主控台左下角的 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 區域 (其中可用 AWS CloudShell) 的相關資訊，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。

取得帳單資訊

如果擁有必要的許可，則您可以從主控台獲得 AWS 費用的相關資訊。

取得您的帳單資訊

1. 在導覽列上，選擇您的帳戶名稱。
2. 選擇 Billing Dashboard (帳單儀表板)。
3. 使用 AWS Billing and Cost Management 儀表板，尋找每月開支的摘要和明細。若要進一步了解，請參閱 [AWS Billing 使用者指南](#)。

在主控台中使用 Markdown

中的某些服務 (例如 Amazon CloudWatch) 支援在某些欄位中使用 [Markdown](#)。AWS Management Console 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](#)
- [標題](#)
- [文字格式](#)
- [連結](#)
- [清單](#)
- [表格和按鈕 \(CloudWatch 儀表板 \)](#)

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：

```
&nbsp;
&nbsp;
```

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 儀表板文字元件支援降價表格和按鈕。

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 Widget 中，您也可以設定超連結的格式，使其顯示為按鈕。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)
```

故障診斷

請參閱本節，以尋找與 AWS Management Console。

您也可以使用 Amazon Q 開發人員診斷和疑難排解部分 AWS 服務的常見錯誤。如需詳細資訊，請參閱 Amazon Q 開發人員使用指南中的 [Amazon Q 開發人員在主控台中診斷常見錯誤](#)。

主題

- [頁面未正確載入](#)
- [連接到我的瀏覽器時顯示「訪問被拒絕」錯誤 AWS Management Console](#)
- [連接到時，我的瀏覽器顯示超時錯誤 AWS Management Console](#)
- [我想變更 AWS Management Console 的語言，但是找不到頁面底部的語言選擇選單](#)

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，或嘗試使用不同的網頁瀏覽器。
- 如果所有受影響的用戶都來自同一個團隊，則可能是隱私瀏覽器擴展或安全防火牆問題。隱私瀏覽器擴展程序和安全防火牆可以阻止對 AWS Management Console。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 Management Console 使用網域的尾碼，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 不再支持互聯網資源管理器 11。我們建議您搭 AWS Management Console 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](#)。

連接到我的瀏覽器時顯示「訪問被拒絕」錯誤 AWS Management Console

如果您使用下列所有項目，最近對主機所做的變更可能會影響您的存取權限：

- VPC 內的瀏覽器。
- VPC 端端點。
- 包含aws:SourceIp全域條件金鑰的 IAM 政策。

在主控台中，前往 IAM 政策頁面。建議您檢閱包含aws:SourceIp全域條件金鑰的 IAM 政策並新增aws:SourceVpc金鑰。

或者，您可以考慮使用「AWS Management Console 私人存取」功能，AWS Management Console 透過 VPC 端點存取，並使用原aws:SourceVpc則中的條件。如需詳細資訊，請參閱 [AWS Management Console 私人存取](#)。

連接到時，我的瀏覽器顯示超時錯誤 AWS Management Console

如果您的預設服務中斷 AWS 區域，您的瀏覽器可能會在嘗試連線到 AWS Management Console。若要 AWS Management Console 從不同區域登入，請在 URL 中指定替代地區端點。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-code.console.aws.amazon.com
```

如需詳細資訊，請參閱 AWS 一般參考 中的 [AWS Management Console 服務端點](#)。

若要檢視全部的狀態 AWS 服務，包括 AWS Management Console，請參閱 [AWS Health Dashboard](#)。

我想變更 AWS Management Console 的語言，但是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 Management Console，請[瀏覽至 \[整合設定\] 頁面](#)，然後選擇主控台的語言。

如需詳細資訊，請參閱[變更 AWS Management Console 的語言](#)。

文件歷史紀錄

下表說明 AWS Management Console 入門指南 自 2021 年 3 月開始生效的重要變更。

變更	描述	日期
與 Amazon Q 聊天	新的設定頁面，詳細說明使用者如何向 Amazon Q 開發人員提出 AWS 問題。如需詳細資訊，請參閱 與 Amazon Q 開發人員聊天 。	2024年5月29 日
我的應用	介紹我的應用程序的新頁面。如需詳細資訊，請參閱 什麼是我的應用程式？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
新 AWS Console Home 用戶界面	新的 AWS Console Home UI，其中包括用於顯示重要使用信息和 AWS 服務捷徑的小部件。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 Management Console 選擇其他語言。如需詳細資訊，請參閱 變更 AWS Management Console 的語言 。	2021 年 4 月 1 日
啟動 CloudShell	AWS CloudShell 從開啟 AWS Management Console 並執行 AWS CLI 命令。如需詳細資訊	2021 年 3 月 22 日

變更	描述	日期
	, 請參閱 啟動 AWS CloudShell !。	

AWS 詞彙表

如需最新的 AWS 術語，請參閱《AWS 詞彙表 參考》中的 [AWS 詞彙表](#)。

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。