使用者指南

Amazon Elastic VMware Service

Amazon Elastic VMware Service: 使用者指南

Table of Contents

什麼是 Amazon Elastic VMware Service？

您可以使用 Amazon Elastic VMware Service (Amazon EVS) 直接在 EC2 裸機執行個體 (VPC) 上部署和執行 VMware Cloud Foundation Amazon Virtual Private Cloud (VCF) 環境。

主題

Amazon EVS 的功能

以下是 Amazon EVS 的主要功能：

簡化並加速遷移至 AWS

消除遷移摩擦，並確保營運與訂閱可攜性和雲端中 VMware Cloud Foundation (VCF) 的自動化部署保持一致。擴充內部部署網路並遷移工作負載，而無需變更 IP 地址、重新訓練員工或重新撰寫操作 Runbook。

在雲端中保留對 VMware 架構的控制

完全控制您的 VMware 架構，並最佳化符合應用程式獨特需求的虛擬化堆疊，包括附加元件和第三方解決方案。

自我管理或利用 AWS 合作夥伴以獲得受管體驗

釋放自我管理的選擇和靈活性，或利用 AWS 合作夥伴的專業知識在 上管理和操作您的 VCF 環境 AWS ，以跨人才、時間和成本實現您的業務目標。

擴展並保護您的企業免於中斷

在最安全、可擴展且具彈性的雲端上增強可擴展性，以遷移和操作 VMware 型工作負載。

接受 AWS 創新以轉換您的應用程式和基礎設施

作為 AWS原生服務，Amazon EVS 透過 200 多種服務 （包括受管資料庫、分析、無伺服器和容器，以及生成式 AI) 簡化擴展和擴展 VMware 環境，以轉換您的業務。

開始使用 Amazon EVS

若要建立您的第一個 Amazon EVS 環境，請參閱 開始使用。一般而言，開始使用 Amazon EVS 需要完成以下步驟。

1. 完成 事前準備。如需詳細資訊，請參閱設定 Amazon Elastic VMware Service。
2. 建立 Amazon EVS 環境。在環境建立期間，Amazon EVS 會使用您指定的 CIDR 範圍建立所需的 VLAN 子網路，並將主機新增至環境。
3. 自訂 VCF。根據您的需求，在 vSphere 使用者介面中設定您的環境。這可能包括設定登入、政策、監控等。
4. 連線和遷移。將您的環境連接至內部部署資料中心，並將 VCF 工作負載遷移至 Amazon EVS。

存取 Amazon EVS

您可以使用下列界面來定義和設定 Amazon EVS 部署：

- Amazon EVS 主控台 - 提供建立 Amazon EVS 環境的 Web 界面。
- AWS CLI - 為 Windows、macOS AWS 服務 和 Linux 支援廣泛的 和 命令集。如需詳細資訊，請參閱AWS Command Line Interface。
- AWS CloudFormation - 提供每種資源類型的規格，例如 `AWS::EVS::Environment`。您可以使用資源規格建立範本，CloudFormation 會為您佈建和設定資源。

Amazon EVS 的概念和元件

本節說明一些重要的 Amazon EVS 概念和元件。

Amazon EVS 環境

Amazon EVS 環境是 VMware Cloud Foundation (VCF) 資源的邏輯容器，例如 vSphere 主機、vSAN、NSX 和 SDDC Manager。環境中包含一個具有 vSphere 叢集的合併式 VCF 網域，而叢集中裝載了用於管理、監控和執行個體化 VCF 軟體堆疊的元件。每個環境都會直接映射至 SDDC Manager 設備。如需詳細資訊，請參閱the section called “Architecture”。

Amazon EVS 主機

Amazon EVS 主機是在 Amazon EC2 裸機執行個體上執行的 VMware ESX 主機。Amazon EVS 主機會將本機 NVMe 執行個體存放磁碟區用於 vSAN 資料存放區，以存放您的管理和工作負載虛擬機器。

> **Warning**
>
> 執行個體存放區磁碟區是暫時性的。如果基礎 EC2 執行個體已停止或終止，則存放在這些磁碟區上的資料不會保留。在 VCF 內停用或終止 Amazon EVS 使用的 Amazon EC2 執行個體可能會導致資料遺失。
> 如需主機維護的詳細資訊，請參閱 the section called “主機維護”。

服務存取子網路

服務存取子網路是標準 VPC 子網路，可讓 Amazon EVS 存取 VCF 部署。在建立 Amazon EVS 環境期間，您可以指定 Amazon EVS 用於服務存取的 VPC 和子網路。

當您建立 Amazon EVS 環境時，Amazon EVS 會將彈性網路介面佈建至服務存取子網路，以促進與 VCF 設備及 ESX 主機的管理連線。Amazon EVS 需要此連線才能部署、管理和監控 VCF 部署。

Amazon EVS VLAN 子網路

Amazon EVS VLAN 子網路是由 Amazon EVS 管理的 Amazon VPC 子網路。VLAN 子網路為 Amazon EVS 主機和 VMware NSX、VMware HCX 和 VMware vCenter Server 等 VCF 設備提供 VPC 連線能力。每個 VLAN 子網路都有一個 VLAN 標籤，允許以邏輯方式分割 VLAN 網路流量。

Amazon EVS 會建立服務在建立 Amazon EVS 環境時使用的所有 VLAN 子網路。您可以提供 VLAN 子網路使用的 CIDR 區塊輸入。您應該確保 VLAN 子網路 CIDR 區塊根據將設定的主機數量適當調整大小，並考慮未來的擴展需求。CIDR 區塊的大小下限必須為 /28 網路遮罩，上限為 /24 網路遮罩。CIDR 區塊不得與與 VPC 相關聯的任何現有 CIDR 區塊重疊。

建立時，VLAN 子網路會隱含地與 VPC 的主要路由表建立關聯。部署後，您可以明確地將 VLAN 子網路與自訂路由表建立關聯。如需詳細資訊，請參閱the section called “Amazon EVS 網路考量事項”。

> **Important**
>
> Amazon EVS VLAN 子網路只能在 Amazon EVS 環境建立期間建立，且在環境建立之後無法修改。建立環境之前，您必須確定 VLAN 子網路 CIDR 區塊的大小正確。部署環境之後，您將無法新增 VLAN 子網路。

> **Important**
>
> EC2 安全群組規則不會在連接至 VLAN 子網路的 Amazon EVS 彈性網路介面上強制執行。若要控制往返 VLAN 子網路的流量，您必須使用網路存取控制清單。

主機管理 VLAN 子網路

主機管理 VLAN 子網路會將管理流量與使用者流量分開，並允許遠端管理主機。EVS 主機管理 vmkernel 網路介面會連線至此子網路。

vMotion VLAN 子網路

vMotion VLAN 子網路邏輯上會分割 VMware vMotion 流量，並在 vMotion 程序期間用來在主機之間移動虛擬機器。

vSAN VLAN 子網路

VMware vSAN 會使用 vSAN VLAN 子網路，將與 vSAN 儲存操作相關的流量與其他網路流量分開。

VTEP VLAN 子網路

VTEP VLAN 子網路使用 VMware NSX 虛擬通道端點 (VTEP) 來封裝和解封裝 Amazon EVS ESX 主機的覆蓋網路流量。

Edge VTEP VLAN 子網路

Edge VTEP VLAN 子網路是專用於 NSX Edge 設備覆蓋流量的專用 VTEP VLAN 子網路。此 VLAN 用於 NSX 邊緣和 ESX 主機之間的浮水印通訊。

管理 VM VLAN 子網路

Management VM VLAN 子網路用於管理虛擬設備，包括 NSX Manager、vCenter Server 和 SDDC Manager。

HCX 上行 VLAN 子網路

HCX 上行 VLAN 子網路用於 HCX Interconnect (HCX-IX) 和 HCX Network Extension (HCX-NE) 設備之間的通訊，並啟用建立 HCX 服務網格上行連結。

NSX 上行 VLAN 子網路

NSX 上行 VLAN 子網路用於將 NSX 覆蓋網路連接到 VPC 的其餘部分，以及您設定的任何其他外部網路。NSX 上行 VLAN 子網路是在 NSX Edge 節點上行連結上設定。

擴充 VLAN 子網路

擴充 VLAN 子網路可用來啟用其他 VCF 支援的函數，例如 NSX 聯合。Amazon EVS 會在環境建立期間建立兩個擴充 VLAN 子網路。

VMware NSX

VMware NSX 是一種軟體定義的聯網 (SDN) 平台，可啟用網路虛擬化。Amazon EVS 使用 VMware NSX 來建立和管理 VMware Cloud Foundation (VCF) 設備和工作負載執行所在的浮水印網路。Amazon EVS 部署一對作用中/待命 NSX Edge 節點，以及 NSX 覆蓋網路。Amazon EVS 會自動代表您設定所有 NSX 路由和上行連結，做為部署的一部分。如需常見 NSX 概念的詳細資訊，請參閱 VMware NSX 安裝指南中的關鍵概念。

VMware Hybrid Cloud Extension (HCX)

VMware Hybrid Cloud Extension (VMware HCX) 是一種應用程式行動性平台，旨在簡化應用程式遷移、重新平衡工作負載，以及最佳化資料中心和雲端的災難復原。您可以使用 HCX 將 VMware 型工作負載遷移至 Amazon EVS。

您可以使用 Direct Connect 搭配相關聯的傳輸閘道，或使用連接至傳輸閘道 AWS Site-to-Site VPN 連接，來設定 VMware HCX 的連線能力。如需詳細資訊，請參閱移轉。

Amazon EVS 架構

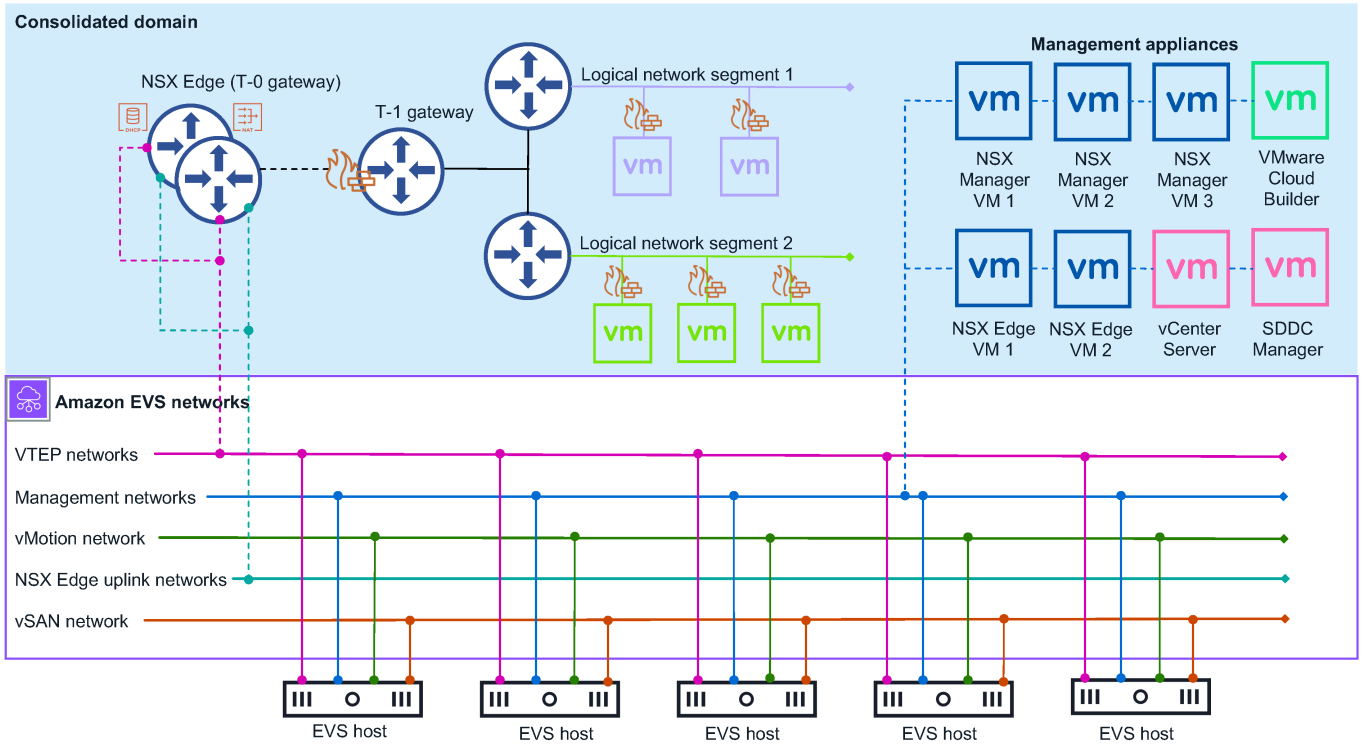
Amazon EVS 實作 VMware Cloud Foundation (VCF) 合併架構模型。在此模型中，VCF 管理元件和客戶工作負載會在合併網域上執行。Amazon EVS 環境是從單一 vCenter 伺服器管理，具有 vSphere 資源集區，可在管理和客戶工作負載之間提供隔離。

Amazon EVS 部署的合併網域包含下列 VCF 管理元件：

- ESX 主機
- vCenter 伺服器執行個體
- SDDC Manager

- vSAN 資料存放區
- 三節點 NSX Manager 叢集
- vSphere 叢集
- NSX Edge 叢集

下圖顯示已在 Amazon EVS 環境中部署的 Amazon EVS 架構範例，並顯示環境中的元件如何連線。在圖表中，具有合併網域架構的 Amazon EVS 環境會以藍色著色。底層 Amazon EVS 網路拓撲會在紫色實線中說明。



網路拓撲

Amazon EVS 環境有兩個不同的管理網路層：

Amazon VPC

在環境建立期間在 VPC 中建立的 Amazon VPC 和 Amazon EVS VLAN 子網路會形成 VCF 部署的底層網路。此基礎設施可為 NSX 覆蓋網路、主機管理、vMotion 和 VSAN 提供連線能力。Amazon VPC Route Server 可在底層網路和覆蓋網路之間啟用動態路由。如需詳細資訊，請參閱the section called “概念和元件”。

> **Note**
>
> Amazon EVS VLAN 子網路僅用於促進 VCF 底層通訊。執行客戶工作負載的訪客虛擬機器必須部署在 NSX 覆蓋網路上。不支援在 Amazon EVS VLAN 子網路底層網路上部署訪客虛擬機器。

VMware NSX 覆蓋網路

Amazon EVS 會代表您設定 NSX 覆蓋網路，做為部署的一部分。您可以設定其他 NSX 覆蓋網路，以在 Amazon EVS 環境中的不同工作負載或應用程式之間實現網路隔離。如需詳細資訊，請參閱 VMware Cloud Foundation 產品文件中的 VMware Cloud Foundation 的浮水印設計。 VMware

> **Note**
>
> 對於具有兩個 NSX Edge 節點的作用中/待命 NSX Edge 叢集，Amazon EVS 僅支援一個 tier-0 閘道。此 layer-0 閘道會連線至您設定用於 Amazon EVS 的所有浮水印網路，並公告這些浮水印網路。

這兩個網路層由具有兩個 NSX Edge 節點的作用中/待命 NSX Edge 叢集連接。NSX Edge 節點可在 VLANs 中的虛擬機器之間透過 VPC 進行通訊，以及網際網路連線，以及搭配傳輸閘道使用 Direct Connect or AWS Site-to-Site VPN 進行私有連線。

Amazon EVS 網路考量事項

管理網路需要下列聯網資源組態。您可以在 Amazon EVS 環境建立期間提供這些輸入。如需詳細資訊，請參閱the section called “概念和元件”。

- Amazon VPC。請確定您的 VPC IPv4 CIDR 區塊大小適當，以容納 Amazon EVS 在環境建立期間佈建的必要 VPC 子網路和 Amazon EVS VLAN 子網路。如需詳細資訊，請參閱the section called “Amazon EVS VLAN 子網路”。

  > **Note**
  >
  > Amazon EVS 目前不支援 IPv6。

- VPC 中的服務存取子網路。Amazon EVS 使用此子網路來維護與 SDDC Manager 設備的持久性連線。如需詳細資訊，請參閱the section called “服務存取子網路”。

> **Note**
>
> Amazon EVS 目前僅支援單一可用區部署。Amazon EVS 使用的所有 VPC 子網路都必須存在於提供服務的區域中的單一可用區域中。

> **Note**
>
> 所有 VPC 子網路都需要根據您組織的聯網需求設定的關聯路由表。

- VPC DHCP 選項集中的主要 DNS 伺服器 IP 地址和次要 DNS 伺服器 IP 地址，用於解析主機 IP 地址。Amazon EVS 還需要您為部署中的每個 VCF 管理設備及 Amazon EVS 主機建立具有 A 記錄的 DNS 正向查詢區域，以及具有 PTR 記錄的反向查詢區域。如需詳細資訊，請參閱the section called “設定 DNS 伺服器”。
- Amazon EVS 在環境建立期間為您佈建的每個 VLAN 子網路的 Amazon EVS VLAN 子網路 CIDR 區塊。CIDR 區塊的大小上限為 /28 網路遮罩，大小上限為 /24 網路遮罩。CIDR 區塊必須是非重疊的。
- 已啟用 Amazon VPC Route Server 傳播的 Route Server 執行個體。
- 服務存取子網路中的兩個 Route Server 端點。
- 兩個 Route Server 對等互連 Amazon EVS 與 Route Server 端點佈建的 NSX Edge 節點。

Tier-0 閘道

tier-0 閘道會處理邏輯和實體網路之間的所有南北流量，並在 NSX 覆蓋網路上建立。此 tier-0 閘道會建立為 Amazon EVS 部署的一部分。

> **Note**
>
> 對於具有兩個 NSX Edge 節點的作用中/待命 NSX Edge 叢集，Amazon EVS 僅支援一個 tier-0 閘道。

Tier-1 閘道

第 1 層閘道會處理環境中路由網路區段之間的東西流量，並在 NSX 覆蓋網路上建立。第 1 層閘道具有區段的下行連線，以及第 0 層閘道的上行連線。如果需要，您可以建立和設定其他 Tier-1 閘道。

NSX Edge 叢集

Amazon EVS 使用 NSX Manager 介面來部署具有兩個 NSX Edge 節點的 NSX Edge 叢集，這些節點在作用中/待命模式下執行。此 NSX Edge 叢集提供 Tier-0 和 Tier-1 閘道執行所在的平台，以及 IPsec VPN 連線及其 BGP 路由機制。

Amazon EVS 資源

Amazon EVS 會在環境建立期間佈建下列 AWS 資源。這些資源會出現在您允許 Amazon EVS 存取的 VPC 中，並在建立後顯示在 AWS 管理主控台 和 AWS CLI 中。

> **Important**
>
> 在 Amazon EVS 主控台和 API 之外修改這些資源可能會影響 Amazon EVS 環境的可用性和穩定性。

- Amazon EVS 彈性網路介面，可讓您連線至 VCF 設備與主機。
- 在 Amazon EC2 裸機執行個體上執行的 Amazon EVS ESX 主機。如需詳細資訊，請參閱the section called “Amazon EVS 主機”。

  > **Important**
  >
  > 您的 Amazon EVS 環境必須至少有 4 個主機，且不超過 16 個主機。Amazon EVS 僅支援具有 4-16 個主機的環境。

- 將您的 VPC 連接到 VCF 設備的 Amazon EVS VLAN 子網路。如需詳細資訊，請參閱the section called “Amazon EVS VLAN 子網路”。

設定 Amazon Elastic VMware Service

若要使用 Amazon EVS，您需要設定其他 AWS 服務，以及設定您的環境以符合 VMware Cloud Foundation (VCF) 需求。如需部署先決條件的摘要檢查清單，請參閱 the section called “部署檢查清單”。

主題

註冊 AWS

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個。

1. 開啟 https://portal.aws.amazon.com/billing/signup。
2. 請遵循線上指示進行。

建立 IAM 使用者

1. 選擇根使用者並輸入 AWS 您的帳戶電子郵件地址，以帳戶擁有者身分登入 IAM 主控台。在下一頁中，輸入您的密碼。

> **Note**
>
> 強烈建議您遵循下方 Administrator IAM 使用者最佳實務，並妥善鎖藏根使用者憑證。只在需要執行少數帳戶和服務管理任務時，才以根使用者身分登入。

2. 在導覽窗格中，選擇使用者，然後選擇建立使用者。
3. 在 User name (使用者名稱) 中輸入 Administrator。
4. 選取 AWS 管理主控台存取旁的核取方塊。然後選取 Custom password (自訂密碼)，接著在文字方塊中輸入您的新密碼。
5. （選用） 根據預設， AWS 要求新使用者在第一次登入時建立新密碼。您可以清除 User must create a new password at next sign-in (使用者下次登入必須建立新的密碼) 旁的核取方塊，讓新使用者登入時可以重設密碼。
6. 選擇 Next: Permissions (下一步：許可)。
7. 在 Set permissions (設定許可) 下，選擇 Add user to group (將使用者新增至群組)。
8. 選擇 Create group (建立群組)。
9. 在 Create group (建立群組) 對話方塊中，請於 Group name (群組名稱) 輸入 Administrators。
10. 選擇篩選政策，然後選取 AWS 受管 - 任務函數來篩選資料表內容。
11. 在政策清單中，勾選 AdministratorAccess 的核取方塊。接著選擇 Create group (建立群組)。

> **Note**
>
> 您必須啟用 Billing 的 IAM 使用者和角色存取權，才能使用AdministratorAccess許可來存取 AWS Billing and Cost Management 主控台。若要這樣做，請遵循委派對帳單主控台的存取權相關教學課程的步驟 1 中的指示。

12. 回到群組清單，選取新群組的核取方塊。必要時，選擇 Refresh (重新整理) 以顯示清單中的群組。
13. 選擇 Next: Tags (下一步：標籤)。
14. (選用) 藉由連接標籤做為索引鍵/值組，將中繼資料新增至使用者。如需有關在 IAM 中使用標籤的詳細資訊，請參閱《IAM 使用者指南》中的標記 IAM 實體。

15選擇 Next: Review (下一步：檢閱)，查看要新增至新使用者的群組成員資格清單。準備好繼續時，請選擇 Create user (建立使用者)。

您可以使用這個相同的程序來建立更多群組和使用者，並讓使用者存取 AWS 您的帳戶資源。若要了解如何使用將使用者許可限制為特定 AWS 資源的政策，請參閱存取管理和範例政策。

建立 IAM 角色以將 Amazon EVS 許可委派給 IAM 使用者

您可以使用 角色來委派對 AWS 資源的存取。透過 IAM 角色，您可以在信任帳戶和其他 AWS 信任帳戶之間建立信任關係。信任帳戶擁有要存取的資源，而信任的帳戶包含需要存取資源的使用者。

建立信任關係後，來自信任帳戶的 IAM 使用者或應用程式可以使用 AWS Security Token Service (AWS STS) `AssumeRole` API 操作。此操作提供暫時安全登入資料，可讓您存取帳戶中 AWS 的資源。如需詳細資訊，請參閱《 使用者指南 AWS Identity and Access Management 》中的建立角色以將許可委派給 IAM 使用者。

請依照下列步驟，使用允許存取 Amazon EVS 操作的許可政策來建立 IAM 角色。

> **Note**
>
> Amazon EVS 不支援使用執行個體描述檔將 IAM 角色傳遞至 EC2 執行個體。

Example

IAM console

1. 前往 IAM 主控台。
2. 在左側選單中，選擇政策。
3. 選擇建立政策。
4. 在政策編輯器中，建立啟用 Amazon EVS 操作的許可政策。如需政策範例，請參閱 the section called “建立和管理 Amazon EVS 環境”。若要檢視所有可用的 Amazon EVS 動作、資源和條件索引鍵，請參閱服務授權參考中的動作。
5. 選擇下一步。
6. 在政策名稱下，輸入有意義的政策名稱來識別此政策。
7. 檢閱此政策中定義的許可。
8. （選用）新增標籤以協助識別、組織或搜尋此資源。

9. 選擇建立政策。
10. 在左側功能表中，選擇角色。
11. 選擇建立角色。
12. 針對信任的實體類型，選擇 AWS 帳戶。
13. 在 AWS 帳戶 下，指定您要執行 Amazon EVS 動作的帳戶，然後選擇下一步。
14. 在新增許可頁面上，選取您先前建立的許可政策，然後選擇下一步。
15. 在角色名稱下，輸入有意義的名稱來識別此角色。
16. 檢閱信任政策，並確保將正確的 AWS 帳戶 列為委託人。
17. (選用) 新增標籤以協助識別、組織或搜尋此資源。
18. 選擇建立角色。

AWS CLI

1. 將下列內容複製到信任政策 JSON 檔案。對於委託人 ARN，請以`service-user`您自己的 AWS 帳戶 ID 和 IAM 使用者名稱取代範例 AWS 帳戶 ID 和名稱。

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/service-user"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. 建立角色。將 取代`evs-environment-role-trust-policy.json`為您的信任政策檔案名稱。

```
aws iam create-role \
  --role-name myAmazonEVSEnvironmentRole \
  --assume-role-policy-document file://"evs-environment-role-trust-policy.json"
```

3. 建立許可政策，以啟用 Amazon EVS 操作並將政策連接至角色。將 `myAmazonEVSEnvironmentRole` 取代為您的角色名稱。如需政策範例，請參閱 the section

called “建立和管理 Amazon EVS 環境”。若要檢視所有可用的 Amazon EVS 動作、資源和條件索引鍵，請參閱服務授權參考中的動作。

```
aws iam attach-role-policy \
  --policy-arn arn:aws:iam::aws:policy/AmazonEVSEnvironmentPolicy \
  --role-name myAmazonEVSEnvironmentRole
```

註冊 AWS 商業、 AWS Enterprise On-Ramp 或 AWS 企業支援計劃

Amazon EVS 要求客戶註冊 AWS Business、 AWS Enterprise On-Ramp 或 AWS Enterprise Support 計劃，以持續存取技術支援和架構指導。 AWS Business Support 是符合 Amazon EVS 要求的最低 AWS 支援層。如果您有業務關鍵工作負載，建議您註冊 AWS Enterprise On-Ramp 或 AWS Enterprise Support 計劃。如需詳細資訊，請參閱比較 AWS 支援計劃。

> **Important**
>
> 如果您不註冊 AWS Business、 AWS Enterprise On-Ramp 或 AWS Enterprise Support 計畫，Amazon EVS 環境建立會失敗。

檢查配額

若要啟用 Amazon EVS 環境建立，請確定您的帳戶具有所需的最低帳戶層級配額。如需詳細資訊，請參閱Service Quotas。

> **Important**
>
> 如果每個 EVS 環境配額的主機計數值不至少為 4，Amazon EVS 環境建立會失敗。

規劃 VPC CIDR 大小

建立 Amazon EVS 環境時，您必須指定 VPC CIDR 區塊。環境建立後，無法變更 VPC CIDR 區塊，而且需要預留足夠的空間來容納 Amazon EVS 在環境部署期間建立的必要 EVS 子網路和主機。因此，在部署之前，請務必仔細規劃 CIDR 區塊大小，並考量 Amazon EVS 需求和未來的擴展需求。Amazon EVS 需要 VPC CIDR 區塊，其大小下限為 /22 網路遮罩，以便為所需的 EVS 子網路和主機提供足夠的空間。如需詳細資訊，請參閱the section called “Amazon EVS 網路考量事項”。

Important

請確定您的 VPC 子網路和 Amazon EVS 為 VCF 設備建立的 VLAN 子網路有足夠的 IP 地址空間。VPC CIDR 區塊的大小下限必須為 /22 網路遮罩，以便為所需的 EVS 子網路和主機提供足夠的空間。

Note

Amazon EVS 目前不支援 IPv6。

使用子網路建立 VPC

Amazon EVS 會將您的環境部署到您提供的 VPC。此 VPC 必須包含 Amazon EVS 服務存取的子網路 (the section called “服務存取子網路”)。如需使用 Amazon EVS 子網路建立 VPC 的步驟，請參閱 the section called “使用子網路和路由表建立 VPC”。

設定 VPC 主要路由表

Amazon EVS VLAN 子網路會隱含地與 VPC 主路由表相關聯。若要啟用與 DNS 或內部部署系統等相依服務的連線，以便成功部署環境，您必須設定主要路由表，以允許這些系統的流量。如需詳細資訊，請參閱the section called “將 Amazon EVS VLAN 子網路明確關聯至 VPC 路由表”。

Important

Amazon EVS 只有在建立 Amazon EVS 環境之後，才支援使用自訂路由表。建立 Amazon EVS 環境期間不應使用自訂路由表，因為這可能會導致連線問題。

閘道路由需求

根據您的連線需求設定這些閘道類型的路由：

- NAT 閘道 (NGW)
  - 僅傳出網際網路存取為選用。
  - 必須位於具有網際網路閘道存取的公有子網路中。

  - 新增從私有子網路和 EVS VLAN 子網路到 NAT 閘道的路由。
  - 如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的使用 NAT 閘道。
- 傳輸閘道 (TGW)
  - 透過 AWS Direct Connect 和 AWS Site-to-Site進行內部部署連線時需要。
  - 新增內部部署網路範圍的路由。
  - 如果使用 BGP，請設定路由傳播。
  - 如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的 Amazon VPC Transit Gateways 中的 Transit Gateways。

最佳實務

- 記錄所有路由表組態。
- 使用一致的命名慣例。
- 定期稽核您的路由表。
- 進行變更後測試連線能力。
- 備份路由表組態。
- 監控路由運作狀態和傳播。

如需使用路由表的詳細資訊，請參閱《Amazon VPC 使用者指南》中的設定路由表。

設定 VPC 的 DHCP 選項集

> **Important**
>
> 如果您不符合這些 Amazon EVS 要求，您的環境部署會失敗：
>
> - 在 DHCP 選項集中包含主要 DNS 伺服器 IP 地址和次要 DNS 伺服器 IP 地址。
> - 在您的部署中包含具有每個 VCF 管理設備與 Amazon EVS 主機 A 記錄的 DNS 轉送查詢區域。
> - 包含 DNS 反向查詢區域，其中包含部署中每個 VCF 管理設備及 Amazon EVS 主機的 PTR 記錄。
> - 設定 VPC 的主要路由表，以確保 DNS 伺服器的路由存在。
> - 確認您的網域名稱註冊有效且未過期，並且沒有重複的主機名稱或 IP 位址。

- 設定您的安全群組和網路存取控制清單 (ACLs)，以允許 Amazon EVS 與下列通訊：
  - 透過 TCP/UDP 連接埠 53 的 DNS 伺服器。
  - 透過 HTTPS 和 SSH 的主機管理 VLAN 子網路。
  - 透過 HTTPS 和 SSH 管理 VLAN 子網路。

如需詳細資訊，請參閱the section called “使用 VPC DHCP 選項集設定 DNS 和 NTP 伺服器”。

建立和設定 VPC Route Server 基礎設施

Amazon EVS 使用 Amazon VPC Route Server 來啟用 BGP 型動態路由到您的 VPC 底層網路。您必須指定路由伺服器，將路由共用到服務存取子網路中至少兩個路由伺服器端點。路由伺服器對等項上設定的對等 ASN 必須相符，而且對等 IP 位址必須是唯一的。

Important

如果您不符合這些 Amazon EVS 對 VPC Route Server 組態的要求，您的環境部署會失敗：

- 您必須在服務存取子網路中設定至少兩個路由伺服器端點。
- 為 Tier-0 閘道設定邊界閘道協定 (BGP) 時，VPC Route Server 對等 ASN 值必須符合 NSX Edge 對等 ASN 值。
- 建立兩個路由伺服器對等時，您必須為每個端點使用來自 NSX 上行 VLAN 的唯一 IP 地址。這兩個 IP 地址會在 Amazon EVS 環境部署期間指派給 NSX 邊緣。
- 啟用路由伺服器傳播時，您必須確保所有要傳播的路由表至少有一個明確的子網路關聯。如果傳播的路由表沒有明確的子網路關聯，BGP 路由公告會失敗。

Note

對於 Route Server 對等活體偵測，Amazon EVS 僅支援預設的 BGP 保持連線機制。Amazon EVS 不支援多躍點雙向轉送偵測 (BFD)。

先決條件

開始之前，您需要：

- 路由伺服器的 VPC 子網路。
- 管理 VPC Route Server 資源的 IAM 許可。
- 路由伺服器的 BGP ASN 值 (Amazon 端 ASN)。此值必須介於 1-4294967295 的範圍內。
- 將路由伺服器與 NSX Tier-0 閘道對等的對等 ASN。在路由伺服器和 NSX Tier-0 閘道中輸入的對等 ASN 值必須相符。NSX Edge 設備的預設 ASN 為 65000。

步驟

如需設定 VPC Route Server 的步驟，請參閱 Route Server 入門教學課程。

> **Note**
>
> 如果您使用 NAT 閘道或傳輸閘道，請確定您的路由伺服器已正確設定，以將 NSX 路由傳播至 VPC 路由表 (VPC)。

> **Note**
>
> 建議您為路由伺服器執行個體啟用持續路由，持續時間介於 1-5 分鐘。如果啟用，即使所有 BGP 工作階段都結束，路由仍會保留在路由伺服器的路由資料庫中。

> **Note**
>
> 在部署和操作 Amazon EVS 環境之前，BGP 連線狀態將會關閉。

建立內部部署連線的傳輸閘道

您可以使用 Direct Connect 搭配相關聯的傳輸閘道，或使用 AWS Site-to-Site VPN 連接至傳輸閘道，設定現場部署資料中心與 AWS 基礎設施的連線能力。如需詳細資訊，請參閱the section called “設定內部部署網路連線 （ 選用 ）”。

建立 Amazon EC2 容量保留

Amazon EVS 會在您的 Amazon EVS 環境中啟動代表 ESX 主機的 Amazon EC2 i4i.metal 執行個體。為了確保在需要時有足夠的 i4i.metal 執行個體容量，我們建議您請求 Amazon EC2 容量保留。您可以

隨時建立容量保留，並選擇開始時間。您可以請求立即使用的容量保留，也可以請求未來日期的容量保留。如需詳細資訊，請參閱《Amazon Elastic Compute Cloud 使用者指南》中的使用 EC2 隨需容量保留保留運算容量。

設定 AWS CLI

AWS CLI 是使用 的命令列工具 AWS 服務，包括 Amazon EVS。它也用於驗證 IAM 使用者或角色，以便從本機電腦存取 Amazon EVS 虛擬化環境和其他 AWS 資源。若要從命令列佈建 AWS 資源，您需要取得要在命令列中使用的 AWS 存取金鑰 ID 和私密金鑰。然後您需要在 AWS CLI中對這些憑證進行設定。如需詳細資訊，請參閱《 第 2 版 AWS Command Line Interface 使用者指南》中的設定 AWS CLI 。

建立 Amazon EC2 金鑰對

Amazon EVS 會使用您在環境建立期間提供的 Amazon EC2 金鑰對來連線至主機。若要建立金鑰對，請遵循 Amazon Elastic Compute Cloud 《 使用者指南》中為 Amazon EC2 執行個體建立金鑰對的步驟。

為 VMware Cloud Foundation (VCF) 準備您的環境

部署 Amazon EVS 環境之前，您的環境必須符合 VMware Cloud Foundation (VCF) 基礎設施需求。如需詳細的 VCF 先決條件，請參閱 VMware Cloud Foundation 產品文件中的規劃和準備工作手冊。

您也應該熟悉 VCF 5.2.x 要求。如需相關版本資訊，請參閱 VCF 5.2.x 版本備註。

> **Note**
>
> 如需 Amazon EVS 提供的 VCF 版本的相關資訊，請參閱 the section called “VCF 版本和 EC2 執行個體”。

取得 VCF 授權金鑰

若要使用 Amazon EVS，您需要提供 VCF 解決方案金鑰和 vSAN 授權金鑰。VCF 解決方案金鑰必須至少有 256 個核心。vSAN 授權金鑰必須至少有 110 TiB 的 vSAN 容量。如需 VCF 授權的詳細資訊，請參閱 VMware Cloud Foundation 管理指南中的在 VMware Cloud Foundation 中管理授權金鑰。VMware

> **Important**
>
> 使用 SDDC Manager 使用者介面來管理 VCF 解決方案和 vSAN 授權金鑰。Amazon EVS 會要求您在 SDDC Manager 中維護有效的 VCF 解決方案和 vSAN 授權金鑰，服務才能正常運作。

> **Note**
>
> 您的 VCF 授權將可供所有 AWS 區域的 Amazon EVS 使用，以符合授權規範。Amazon EVS 不會驗證授權金鑰。若要驗證授權金鑰，請造訪 Broadcom 支援。

VMware HCX 先決條件

您可以使用 VMware HCX 將現有的 VMware 型工作負載遷移至 Amazon EVS。將 VMware HCX 與 Amazon EVS 搭配使用之前，請確定已完成下列先決條件任務。

> **Note**
>
> VMware HCX 預設不會安裝在 EVS 環境中。

- 您必須先符合最低網路底層需求，才能將 VMware HCX 與 Amazon EVS 搭配使用。如需詳細資訊，請參閱 VMware HCX 使用者指南中的網路底層最低需求。
- 確認 VMware NSX 已在環境中安裝和設定。如需詳細資訊，請參閱 VMware NSX 安裝指南。
- 確定已在環境中啟用並安裝 VMware HCX。如需啟用和安裝 VMware HCX 的詳細資訊，請參閱《VMware HCX 入門指南》中的 VMware HCX VMware 入門。
- 如果您需要 HCX 網際網路連線，您必須完成下列先決條件任務：
  - 請確定 Amazon 提供的連續公有 IPv4 CIDR 區塊網路遮罩長度的 IPAM 配額為 /28 或更高。

    > **Important**
    >
    > 對於 HCX 網際網路連線，Amazon EVS 需要使用來自公有 IPAM 集區的 IPv4 CIDR 區塊，網路遮罩長度為 /28 或更高。使用任何網路遮罩長度小於 /28 的 CIDR 區塊會導致 HCX 連線問題。如需增加 IPAM 配額的詳細資訊，請參閱 IPAM 的配額。

- 使用網路遮罩長度下限為 /28 的 CIDR 建立 IPAM 和公有 IPv4 IPAM 集區。
- 從 IPAM 集區為 HCX Manager 和 HCX Interconnect (HCX-IX) 設備配置至少兩個彈性 IP 地址 (EIPs)。為您需要部署的每個 HCX 網路設備配置額外的彈性 IP 地址。
- 將公有 IPv4 CIDR 區塊新增為 VPC 的額外 CIDR。

如需 HCX 設定的詳細資訊，請參閱 the section called “選擇您的 HCX 連線選項”和 the section called “HCX 連線選項”。

Amazon EVS 部署先決條件檢查清單

本節包含必須完成才能成功部署 Amazon EVS 環境的先決條件清單。

VCF 授權金鑰資訊

元件	Description	最低需求	範例值 (s)
站台 ID	由 Broadcom 提供的站台 ID，用於存取 Broadcom 支援入口網站。	必須在 EVS 環境建立請求中提供來自 Broadcom 的網站 ID。	01234567
VCF 解決方案金鑰	單一 VCF 授權金鑰，可解鎖整個 VCF 堆疊的功能，包括 vSphere、NSX、SDDC Manager 和 vCenter Server。	必須在 EVS 環境建立請求中提供有效的作用中 VCF 解決方案金鑰。現有 EVS 環境不能正在使用金鑰。	ABCDE-FGHIJ-KLMNO-PQRSTU-VWXYZ
vSAN 授權金鑰	vSAN 授權金鑰可讓您在 VCF 環境中啟用和使用 vSAN 軟體。	必須在 EVS 環境建立請求中提供有效的作用中 vSAN 授權金鑰。現有 EVS 環境不能正在使用金鑰。	ABCDE-FGHIJ-KLMNO-PQRSTU-VWXYZ

AWS 帳戶和區域資訊

元件	Description	最低需求	範例值 (s)
AWS 帳戶 ID 號碼	AWS 帳戶可讓您建立和管理 AWS 資源和存取 AWS 服務。	必須能夠存取 AWS 帳戶。	999999999999
AWS 區域	實體地理區域，其中 AWS 維護多個稱為可用區域的隔離資料中心。	必須指定要部署的 Amazon EVS AWS 區域。如需目前可使用 Amazon EVS 的區域清單，請參閱《AWS 一般參考指南》中的 Amazon Elastic VMware Service 端點和配額。	美國西部 (奧勒岡)

AWS 內部部署資料中心連線的 Transit Gateway

元件	Description	最低需求	範例值 (s)
傳輸閘道 ID	傳輸閘道可做為區域虛擬路由器，讓流量在您的 VPC 和內部部署網路之間流動。	必須使用傳輸閘道將 Amazon EVS 環境連線至您的內部部署網路。	tgw-0262a0e521EXAMPLE
連線方法	若要將內部部署網路連線至 Amazon EVS 環境，您必須搭配 AWS Direct Connect 或 AWS Site-to-Site使用傳輸閘道。	決定您要使用 AWS Direct Connect、AWS Site-to-Site VPN，還是兩者的組合。如需搭配 Direct Connect Site-to-Site VPN 的詳細資訊，請參閱搭配 AWS Direct Connect 的私	使用 AWS Direct Connect AWS Site-to-Site VPN

元件	Description	最低需求	範例值 (s)
		有 IP AWS Site-to-Site VPN。	

Amazon EVS 環境的 VPC

元件	Description	最低需求	範例值 (s)
VPC ID	VPC 是一種虛擬網路，與您要在自己的資料中心操作的傳統網路非常相似。	任何 Amazon VPC 都可用於環境部署。	vpc-0abcdef1234567890
VPC CIDR 區塊	在 Amazon VPC 中，CIDR 區塊會定義 VPC 中可用的 IP 地址範圍。	RFC 1918 CIDR 區塊，大小下限為 /22 網路遮罩。VPC CIDR 區塊的大小必須適當，以容納要在 VPC 中部署的所有 EVS 子網路和主機。此 CIDR 區塊在您的環境中應該是唯一的。	10.1.0.0/20

EVS 環境的 VPC 子網路

元件	Description	最低需求	範例值 (s)
服務存取子網路 ID	服務存取子網路是啟用 Amazon EVS 服務存取的標準 VPC 子網路。如需詳細資訊，請參閱the section called “服務存取子網路”。	可以使用任何 VPC 子網路，前提是子網路的大小在 VPC 內適當。我們建議指定網路遮罩為 /24 的 VPC 子網路 CIDR 區塊。	subnet-abcdef1234567890e

元件	Description	最低需求	範例值 (s)
服務存取子網路 CIDR	VPC 子網路 CIDR 區塊是使用 CIDR 表示法定義的 IP 地址範圍，配置給 VPC 內的特定子網路。	服務存取子網路的大小必須適當，以容納要在 VPC 中部署的其他 EVS 子網路和主機。我們建議指定網路遮罩為 /24 的 VPC 子網路 CIDR 區塊。	10.1.0.0/24
AWS 區域內的可用區域 ID	AWS 區域內的不同位置，旨在與其他 AZs 中的故障隔離，並由一或多個資料中心組成。	您可以指定 VPC 子網路在子網路建立期間部署到的可用區域。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的建立子網路。	us-west-2a

EVS 環境的 EVS VLAN 子網路

元件	Description	最低需求	範例值 (s)
主機管理 VLAN CIDR	主機管理 VLAN 子網路的 CIDR 區塊。如需詳細資訊，請參閱the section called “主機管理 VLAN 子網路”。	大小下限必須為 /28 網路遮罩，上限為 /24 網路遮罩。不得與與 VPC 相關聯的任何現有 CIDR 區塊重疊。	10.1.1.0/24
vMotion VLAN CIDR	vMotion VLAN 子網路的 CIDR 區塊。如需詳細資訊，請參閱the section called “vMotion VLAN 子網路”。	大小必須與主機管理 VLAN 相同。	10.1.2.0/24

元件	Description	最低需求	範例值 (s)
vSAN VLAN CIDR	vSAN VLAN 子網路的 CIDR 區塊。如需詳細資訊，請參閱the section called “vSAN VLAN 子網路”。	大小必須與主機管理 VLAN 相同。	10.1.3.0/24
VTEP VLAN CIDR	VTEP VLAN 子網路的 CIDR 區塊。如需詳細資訊，請參閱the section called “VTEP VLAN 子網路”。	大小必須與主機管理 VLAN 相同。	10.1.4.0/24
Edge VTEP VLAN CIDR	邊緣 VTEP VLAN 子網路的 CIDR 區塊。如需詳細資訊，請參閱the section called “Edge VTEP VLAN 子網路”。	大小下限必須為 /28 網路遮罩，上限為 /24 網路遮罩。不得與與 VPC 相關聯的任何現有 CIDR 區塊重疊。	10.1.5.0/24
管理 VM VLAN CIDR	管理 VM VLAN 子網路的 CIDR 區塊。如需詳細資訊，請參閱the section called “管理 VM VLAN 子網路”。	大小下限必須為 /28 網路遮罩，上限為 /24 網路遮罩。不得與與 VPC 相關聯的任何現有 CIDR 區塊重疊。	10.1.6.0/24
HCX 上行 VLAN CIDR	HCX 上行 VLAN 子網路的 CIDR 區塊。如需詳細資訊，請參閱the section called “HCX 上行 VLAN 子網路”。	大小下限必須為 /28 網路遮罩，上限為 /24 網路遮罩。不得與與 VPC 相關聯的任何現有 CIDR 區塊重疊。	10.1.7.0/24

元件	Description	最低需求	範例值 (s)
NSX 上行 VLAN CIDR	NSX 上行 VLAN 子網路的 CIDR 區塊。如需詳細資訊，請參閱the section called “NSX 上行 VLAN 子網路”。	大小下限必須為 /28 網路遮罩，上限為 /24 網路遮罩。不得與與 VPC 相關聯的任何現有 CIDR 區塊重疊。	10.1.8.0/24
擴充 VLAN 1 CIDR	擴充 VLAN 子網路的 CIDR 區塊。如需詳細資訊，請參閱the section called “擴充 VLAN 子網路”。	大小下限必須為 /28 網路遮罩，上限為 /24 網路遮罩。不得與與 VPC 相關聯的任何現有 CIDR 區塊重疊。	10.1.9.0/24
擴充 VLAN 2 CIDR	擴充 VLAN 子網路的 CIDR 區塊。如需詳細資訊，請參閱the section called “擴充 VLAN 子網路”。	大小下限必須為 /28 網路遮罩，上限為 /24 網路遮罩。不得與與 VPC 相關聯的任何現有 CIDR 區塊重疊。	10.1.10.0/24

DNS 和 NTP 基礎設施

元件	Description	最低需求	範例值 (s)
主要 DNS 伺服器 IP 地址	主要網域名稱系統 (DNS) 伺服器，做為所有網域 DNS 記錄的真實來源。	您可以使用可用主機範圍內任何有效、未使用的 IPv4 地址。	10.1.1.10
次要 DNS 伺服器 IP 地址	網域 DNS 記錄的備份 DNS 伺服器。	您可以使用可用主機範圍內任何有效、未使用的 IPv4 地址。	10.1.5.25
NTP 伺服器 IP 地址	網路時間通訊協定 (NTP) 伺服器是使用 NTP 標準同步網路內	您可以使用預設 Amazon Time Sync Service 搭配本機 `169.254.169.123`	169.254.169.123 (Amazon Time Sync Service)

元件	Description	最低需求	範例值 (s)
	時鐘的裝置或應用程式。	IP 地址或其他 NTP 伺服器 IP 地址。	
適用於 VCF 部署的 FQDN	完整網域名稱 (FQDN) 是網路上裝置的絕對名稱。FQDN 包含主機名稱和網域名稱。	FQDN 只能包含英數字元、減號 (-)，以及做為標籤之間分隔符號的句點。必須是有效且未過期的唯一 FQDN。	evs.local

VPC DHCP 選項集

元件	Description	最低需求	範例值 (s)
DHCP 選項集 ID	DHCP 選項集是 VPC 中的資源 (例如 EC2 執行個體) 用於透過虛擬網路進行通訊的一組網路設定。	必須至少包含 2 個 DNS 伺服器。您可以使用 Route 53 或自訂 DNS 伺服器。還必須包含您的 DNS 網域名稱和 NTP 伺服器。	dopt-0a1b2c3d

EC2 key pair (EC2 金鑰對)

元件	Description	最低需求	範例值 (s)
EC2 金鑰對名稱	EC2 金鑰對是一組安全登入資料，用於安全地連線至 Amazon EC2 執行個體。	金鑰對名稱必須是唯一的。	`my-ec2-key-pair`

VPC 路由表

元件	Description	最低需求	範例值 (s)
主路由表 ID	在 Amazon VPC 中，主要路由表是使用 VPC 自動建立的預設路由表，並管理未明確與不同路由表相關聯之任何 VPC 子網路的流量。當 Amazon EVS 建立 VPC 的主要路由表時，EVS VLAN 子網路會隱含關聯。	必須設定為啟用與相依服務的連線，例如 DNS 或內部部署系統，才能成功部署環境。	rtb-0123456789abcdef0

網路存取控制清單 (ACL)

元件	Description	最低需求	範例值 (s)
網路 ACL ID	網路存取控制清單 (ACL) 允許或拒絕子網路層級的傳入或傳出流量。	必須允許 Amazon EVS 與下列通訊： • 透過 TCP/UDP 連接埠 53 的 DNS 伺服器。 • 透過 HTTPS 和 SSH 的主機管理 VLAN 子網路。 • 透過 HTTPS 和 SSH 管理 VM VLAN 子網路。	acl-0f62c640e793a38a3

VCF 元件的 DNS 記錄

元件	Description	最低需求	IP 地址範例	範例主機名稱
ESX 主機 1	ESX 主機 1 的 A 記錄和 PTR 記錄中定義的 IP 地址和主機名稱。	Amazon EVS 需要具有 A 記錄的 DNS 轉送查詢區域，以及具有為每個 EVS 部署中每個 ESX 主機建立的 PTR 記錄的反向查詢區域。	10.1.0.10	esxi01
ESX 主機 2	ESX 主機 2 的 A 記錄和 PTR 記錄中定義的 IP 地址和主機名稱。	Amazon EVS 需要具有 A 記錄的 DNS 轉送查詢區域，以及具有為每個 EVS 部署中每個 ESX 主機建立的 PTR 記錄的反向查詢區域。	10.1.0.11	esxi02
ESX 主機 3	ESX 主機 3 的 A 記錄和 PTR 記錄中定義的 IP 地址和主機名稱。	Amazon EVS 需要具有 A 記錄的 DNS 轉送查詢區域，以及具有為每個 EVS 部署中每個 ESX 主機建立的 PTR 記錄的反向查詢區域。	10.1.0.12	esxi03
ESX 主機 4	ESX 主機 4 的 A 記錄和 PTR 記錄中定義的 IP 地址和主機名稱。	Amazon EVS 需要具有 A 記錄的 DNS 轉送查詢區域，以及具有為每個 EVS 部署中每個 ESX 主機建	10.1.0.13	esxi04

元件	Description	最低需求	IP 地址範例	範例主機名稱
		立的 PTR 記錄的反向查詢區域。		
vCenter 伺服器設備	vCenter Server 設備的 A 記錄和 PTR 記錄中定義的 IP 地址和主機名稱。	Amazon EVS 需要具有 A 記錄的 DNS 轉送查詢區域，以及具有為每個 EVS 部署中的每個 VCF 管理設備建立的 PTR 記錄的反向查詢區域。	10.1.5.10	vc01
NSX Manager 叢集	NSX Manager 叢集 A 記錄和 PTR 記錄中定義的 IP 地址和主機名稱。	Amazon EVS 需要具有 A 記錄的 DNS 轉送查詢區域，以及具有為每個 EVS 部署中的每個 VCF 管理設備建立的 PTR 記錄的反向查詢區域。	10.1.5.11	nsx
SDDC Manager 設備	在 SDDC Manager 設備的 A 記錄和 PTR 記錄中定義的 IP 地址和主機名稱。	Amazon EVS 需要具有 A 記錄的 DNS 轉送查詢區域，以及具有為每個 EVS 部署中的每個 VCF 管理設備建立的 PTR 記錄的反向查詢區域。	10.1.5.12	sddcm01

元件	Description	最低需求	IP 地址範例	範例主機名稱
雲端建置器設備	雲端建置器設備的 A 記錄和 PTR 記錄中定義的 IP 地址和主機名稱。	Amazon EVS 需要具有 A 記錄的 DNS 轉送查詢區域，以及具有為每個 EVS 部署中的每個 VCF 管理設備建立的 PTR 記錄的反向查詢區域。	10.1.5.13	cb01
NSX Edge 1 設備	NSX Edge 1 設備的 A 記錄和 PTR 記錄中定義的 IP 地址和主機名稱。	Amazon EVS 需要具有 A 記錄的 DNS 轉送查詢區域，以及具有為每個 EVS 部署中的每個 VCF 管理設備建立的 PTR 記錄的反向查詢區域。	10.1.5.14	edge01
NSX Edge 2 設備	NSX Edge 2 設備的 A 記錄和 PTR 記錄中定義的 IP 地址和主機名稱。	Amazon EVS 需要具有 A 記錄的 DNS 轉送查詢區域，以及具有為每個 EVS 部署中的每個 VCF 管理設備建立的 PTR 記錄的反向查詢區域。	10.1.5.15	edge02

元件	Description	最低需求	IP 地址範例	範例主機名稱
NSX Manager 1 設備	NSX Manager 1 設備的 A 記錄和 PTR 記錄中定義的 IP 地址和主機名稱。	Amazon EVS 需要具有 A 記錄的 DNS 轉送查詢區域，以及具有為每個 EVS 部署中的每個 VCF 管理設備建立的 PTR 記錄的反向查詢區域。	10.1.5.16	nsx01
NSX Manager 2 設備	NSX Manager 2 設備的 A 記錄和 PTR 記錄中定義的 IP 地址和主機名稱。	Amazon EVS 需要具有 A 記錄的 DNS 轉送查詢區域，以及具有為每個 EVS 部署中的每個 VCF 管理設備建立的 PTR 記錄的反向查詢區域。	10.1.5.17	nsx02
NSX Manager 3 設備	NSX Manager 3 設備的 A 記錄和 PTR 記錄中定義的 IP 地址和主機名稱。	Amazon EVS 需要具有 A 記錄的 DNS 轉送查詢區域，以及具有為每個 EVS 部署中的每個 VCF 管理設備建立的 PTR 記錄的反向查詢區域。	10.1.5.18	nsx03

VPC Route Server 基礎設施

元件	Description	最低需求	範例值 (s)
路由伺服器 ID	Amazon EVS 使用 Amazon VPC Route Server 來啟用 BGP 型動態路由到您的 VPC 底層網路。	您必須指定路由伺服器，將路由共用到服務存取子網路中至少兩個路由伺服器端點。在路由伺服器和 NSX Edge 對等上設定的對等 ASN 必須相符，且對等 IP 地址必須是唯一的。	rs-0a1b2c3d4e5f67890
路由伺服器關聯	路由伺服器與 VPC 之間的連線。	您的路由伺服器必須與 VPC 相關聯。	`{ "RouteServerAssociation": { "RouteServerId": "rs-0a1b2c3d4e5f67890", "VpcId": "vpc-1", "State": "associating" } }`
VPC Route Server 端的 BGP ASN (Amazon 端 ASN)	Amazon 端 ASN 代表 VPC 路由伺服器與 NSX Edge 對等之間的 BGP 工作階段的 AWS 一側。您可以在建立路由伺服器時指定此 BGP ASN。如需詳細資訊，請參閱《Amazon VPC 使用	此值必須是唯一的，而且在 1-4294967295. AWS recommends 範圍內，使用 64512–65534 (16 位元 ASN) 或 4200000000–4294967294 (32 位元 ASN) 範圍內的私有 ASN。	65001

元件	Description	最低需求	範例值 (s)
	者指南》中的建立路由伺服器。		
路由伺服器端點 1 ID	路由伺服器端點是子網路內的 AWS受管元件，可促進路由伺服器與 BGP 對等之間的 BGP （邊界閘道通訊協定） 連線。	必須將路由伺服器端點部署到服務存取子網路。	rse-0123456789abcdef0
路由伺服器對等 1 ID	路由伺服器對等是路由伺服器端點與部署在 AWS (NSX Edge) 中的裝置之間的 BGP 對等互連工作階段。	路由伺服器對等中指定的對等 ASN 值必須符合用於 NSX Edge Tier-0 閘道的對等 ASN 值。	rsp-0123456789abcdef0
路由伺服器對等 1 IP 地址 (EVS NSX Edge 1 端）	路由伺服器對等 () 的 IP 地址`PeerAddress` 。	必須使用來自 NSX 上行 VLAN 的唯一未使用 IP 地址。Amazon EVS 會將此 IP 地址套用至 NSX Edge 1，作為部署的一部分，並與路由伺服器端點對等互連。	10.1.7.10
路由伺服器對等 1 端點 ENI 地址	路由伺服器對等 () 的端點 ENI IP 地址`EndpointEniAddress` 。	由路由伺服器在對等建立時自動產生。	10.1.7.11
路由伺服器端點 2 ID	路由伺服器端點是子網路內的 AWS受管元件，可促進路由伺服器與 BGP 對等之間的 BGP （邊界閘道通訊協定） 連線。	必須將路由伺服器端點部署到服務存取子網路。	rse-fedcba9876543210f

元件	Description	最低需求	範例值 (s)
路由伺服器對等 2 ID (EVS NSX Edge 2 端)	路由伺服器對等是路由伺服器端點與部署在 AWS (NSX Edge) 中的裝置之間的 BGP 對等互連工作階段。	路由伺服器對等中指定的對等 ASN 值必須符合用於 NSX Edge Tier-0 閘道的對等 ASN 值。	rsp-fedcba9876543210f
路由伺服器對等 2 IP 地址	路由伺服器對等 () 的 IP 地址`PeerAddress` 。	必須使用來自 NSX 上行 VLAN 的唯一 IP 地址。Amazon EVS 會將此 IP 地址套用至 NSX Edge 2，做為部署的一部分，並與路由伺服器端點對等互連。	10.1.7.200
路由伺服器對等 2 端點 ENI 地址	路由伺服器對等 () 的端點 ENI IP 地址`EndpointEniAddress` 。	由路由伺服器在對等建立時自動產生。	10.1.7.201
路由伺服器傳播	Route Server 傳播會在您指定的路由表的 FIB 中安裝路由。	必須指定與服務存取子網路相關聯的路由表。Amazon EVS 目前僅支援 IPv4 聯網。	`{ "RouteServerEndpoint": { "RouteServerId": "rs-1", "RouteServerEndpointId": "rse-1", "VpcId": "vpc-1", "SubnetId": "subnet-1", "State": "pending" } }`

元件	Description	最低需求	範例值 (s)
NSX 對等端的 BGP ASN	連線 NSX 端的 BGP ASN。	建議使用 NSX 預設 ASN 65000	65000

HCX 網際網路存取資源 （選用）

元件	Description	最低需求	範例值 (s)
IPAM ID	用於管理 HCX 網際網路存取 IP 地址的 Amazon VPC IP Address Manager (IPAM)。	必須設定為提供公有 IPv4 地址。僅適用於 HCX 網際網路存取組態。	ipam-0123456789abcdef0
IPAM 集區 ID	Amazon 擁有的公有 IPv4 IPAM 集區，可為 HCX 元件提供地址。	必須設定為公有 IPv4 集區。僅適用於 HCX 網際網路存取組態。	ipam-pool-0123456789abcdef0
HCX 公有 VLAN CIDR 區塊	從 IPAM 集區為 HCX 公有 VLAN 子網路配置的次要公有 IPv4 CIDR 區塊。	必須擁有 /28 網路遮罩，並從 Amazon 擁有的 IPAM 公有集區配置。僅適用於 HCX 網際網路存取組態。	18.97.137.0/28
彈性 IP 位址	從 HCX 元件的 IPAM 集區配置的連續彈性 IP 地址。	HCX Manager、HCX Interconnect Appliance (HCX-IX) 和 HCX Network Extension (HCX-NE) 的相同 IPAM 集區至少 3 EIPs。僅適用於 HCX 網際網路存取組態。	eipalloc-0123456789abcdef0、eipalloc-0123456789abcdef1、eipalloc-0123456789abcdef2

Amazon Elastic VMware Service 入門

使用本指南來開始使用 Amazon Elastic VMware Service (Amazon EVS)。您將了解如何在自己的 Amazon Virtual Private Cloud (VPC) 中使用主機建立 Amazon EVS 環境。

完成後，您將擁有 Amazon EVS 環境，可用來將 VMware vSphere 型工作負載遷移至 AWS 雲端。

Important

為了盡可能簡單快速地開始使用，本主題包含建立 VPC 的步驟，並指定 DNS 伺服器組態和 Amazon EVS 環境建立的最低需求。建立這些資源之前，建議您規劃符合需求的 IP 地址空間和 DNS 記錄設定。您也應該熟悉 VCF 5.2.x 要求。如需相關版本資訊，請參閱 VCF 5.2.x 版本備註。

Important

如需 Amazon EVS 提供的 VCF 版本的相關資訊，請參閱 the section called “VCF 版本和 EC2 執行個體”。

主題

先決條件

開始使用之前，您必須完成 Amazon EVS 先決條件任務。如需詳細資訊，請參閱設定 Amazon Elastic VMware Service。

使用子網路和路由表建立 VPC

> **Note**
>
> VPC、子網路和 Amazon EVS 環境都必須在同一個帳戶中建立。Amazon EVS 不支援跨帳戶共用 VPC 子網路或 Amazon EVS 環境。

Example

Amazon VPC console

1. 開啟 Amazon VPC 主控台。
2. 在 VPC 儀表板上，選擇 Create VPC (建立 VPC)。
3. 針對 Resources to create (建立資源)，選擇 VPC and more (VPC 等)。
4. 保持選取自動產生名稱標籤以建立 VPC 資源的「名稱」標籤，或將其清除以提供您自己的 VPC 資源「名稱」標籤。
5. 針對 IPv4 CIDR 區塊，輸入 IPv4 CIDR 區塊。VPC 必須具有 IPv4 CIDR 區塊。請確定您建立的 VPC 大小足以容納 Amazon EVS 子網路。如需詳細資訊，請參閱the section called “Amazon EVS 網路考量事項”。

   > **Note**
   >
   > Amazon EVS 目前不支援 IPv6。

6. 將租用保留為 `Default`。選取此選項後，在此 VPC 中啟動的 EC2 執行個體將使用啟動執行個體時指定的租用屬性。Amazon EVS 會代表您啟動裸機 EC2 執行個體。
7. 對於 Number of Availability Zones (AZs) (可用區域 (AZ) 的數量)，選擇 1。

> **Note**
>
> Amazon EVS 目前僅支援單一可用區部署。

8. 展開自訂 AZs，並為您的子網路選擇 AZ。

> **Note**
>
> 您必須部署在支援 Amazon EVS 的 AWS 區域中。如需 Amazon EVS 區域可用性的詳細資訊，請參閱《 AWS 一般參考指南》中的 Amazon Elastic VMware Service 端點和配額。

9. （選用）如果您需要網際網路連線，請針對公有子網路數量選擇 1。

10針對私有子網路的數量，選擇 1。此私有子網路將用作您在環境建立步驟期間提供給 Amazon EVS 的服務存取子網路。如需詳細資訊，請參閱the section called “服務存取子網路”。

11若要選擇子網路的 IP 地址範圍，請展開自訂子網路 CIDR 區塊。

> **Note**
>
> Amazon EVS VLAN 子網路也需要從此 VPC CIDR 空間建立。請確定您在 VPC CIDR 區塊中為服務所需的 VLAN 子網路保留足夠的空間。如需詳細資訊，請參閱the section called “Amazon EVS 網路考量事項”

12.（選用）若要透過 IPv4 將網際網路存取權授予資源，請在 1 個可用區域中選擇 NAT 閘道。請注意，存在與 NAT 閘道關聯的成本。如需詳細資訊，請參閱 NAT 閘道的定價。

> **Note**
>
> Amazon EVS 需要使用 NAT 閘道來啟用傳出網際網路連線。

13對於 VPC endpoints (VPC 端點)，選擇 None (無)。

> **Note**
>
> Amazon EVS Amazon S3 目前不支援 的閘道 VPC 端點。若要啟用 Amazon S3 連線，您必須使用 AWS PrivateLink 為 設定介面 VPC 端點 Amazon S3。如需詳細資訊，請參

閱《Amazon Simple Storage Service 使用者指南》中的 AWS PrivateLink 的 Amazon S3 。

14對於 DNS 選項，請保持選取預設值。Amazon EVS 需要您的 VPC 具備所有 VCF 元件的 DNS 解析功能。

15(選用) 若要將標籤新增至 VPC，請展開其他標籤，選擇新增標籤，然後輸入標籤金鑰和標籤值。

16選擇建立 VPC。

> **Note**
>
> 在 VPC 建立期間， Amazon VPC 會自動建立主要路由表，並依預設隱含地將子網路與其建立關聯。

AWS CLI

1. 開啟終端機工作階段。
2. 在單一可用區域中建立具有私有子網路和選用公有子網路的 VPC。

```
aws ec2 create-vpc \
  --cidr-block 10.0.0.0/16 \
  --instance-tenancy default \
  --tag-specifications 'ResourceType=vpc,Tags=[{Key=Name,Value=evs-vpc}]'
---
. Store the VPC ID for use in subsequent commands.
+
[source,bash]
```

VPC_ID=$(aws ec2 describe-vpcs \ --filters Name=tag：Name，Values=evs-vpc \ --query 'Vpcs【0】。VpcId' \ --輸出文字 ） ---

3. 啟用 DNS 主機名稱和 DNS 支援。

```
aws ec2 modify-vpc-attribute \
  --vpc-id $VPC_ID \
  --enable-dns-hostnames
aws ec2 modify-vpc-attribute \
  --vpc-id $VPC_ID \
  --enable-dns-support
```

4. 在 VPC 中建立私有子網路。

```
aws ec2 create-subnet \
  --vpc-id $VPC_ID \
  --cidr-block 10.0.1.0/24 \
  --availability-zone us-west-2a \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=evs-private-
subnet}]'
```

5. 存放私有子網路 ID 以供後續命令使用。

```
PRIVATE_SUBNET_ID=$(aws ec2 describe-subnets \
  --filters Name=tag:Name,Values=evs-private-subnet \
  --query 'Subnets[0].SubnetId' \
  --output text)
```

6. （選用）如果需要網際網路連線，請建立公有子網路。

```
aws ec2 create-subnet \
  --vpc-id $VPC_ID \
  --cidr-block 10.0.0.0/24 \
  --availability-zone us-west-2a \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=evs-public-
subnet}]'
```

7. （選用）存放公有子網路 ID 以供後續命令使用。

```
PUBLIC_SUBNET_ID=$(aws ec2 describe-subnets \
  --filters Name=tag:Name,Values=evs-public-subnet \
  --query 'Subnets[0].SubnetId' \
  --output text)
```

8. （選用）如果建立公有子網路，請建立並連接網際網路閘道。

```
aws ec2 create-internet-gateway \
  --tag-specifications 'ResourceType=internet-gateway,Tags=[{Key=Name,Value=evs-
igw}]'

IGW_ID=$(aws ec2 describe-internet-gateways \
  --filters Name=tag:Name,Values=evs-igw \
  --query 'InternetGateways[0].InternetGatewayId' \
  --output text)
```

```
aws ec2 attach-internet-gateway \
  --vpc-id $VPC_ID \
  --internet-gateway-id $IGW_ID
```

9. （選用）如果需要網際網路連線，請建立 NAT 閘道。

```
aws ec2 allocate-address \
  --domain vpc \
  --tag-specifications 'ResourceType=elastic-ip,Tags=[{Key=Name,Value=evs-nat-
eip}]'

EIP_ID=$(aws ec2 describe-addresses \
  --filters Name=tag:Name,Values=evs-nat-eip \
  --query 'Addresses[0].AllocationId' \
  --output text)

aws ec2 create-nat-gateway \
  --subnet-id $PUBLIC_SUBNET_ID \
  --allocation-id $EIP_ID \
  --tag-specifications 'ResourceType=natgateway,Tags=[{Key=Name,Value=evs-nat}]'
```

10建立和設定必要的路由表。

```
aws ec2 create-route-table \
  --vpc-id $VPC_ID \
  --tag-specifications 'ResourceType=route-table,Tags=[{Key=Name,Value=evs-
private-rt}]'

PRIVATE_RT_ID=$(aws ec2 describe-route-tables \
  --filters Name=tag:Name,Values=evs-private-rt \
  --query 'RouteTables[0].RouteTableId' \
  --output text)

aws ec2 create-route-table \
  --vpc-id $VPC_ID \
  --tag-specifications 'ResourceType=route-table,Tags=[{Key=Name,Value=evs-public-
rt}]'

PUBLIC_RT_ID=$(aws ec2 describe-route-tables \
  --filters Name=tag:Name,Values=evs-public-rt \
  --query 'RouteTables[0].RouteTableId' \
  --output text)
```

11將必要的路由新增至路由表。

```
aws ec2 create-route \
  --route-table-id $PUBLIC_RT_ID \
  --destination-cidr-block 0.0.0.0/0 \
  --gateway-id $IGW_ID

aws ec2 create-route \
  --route-table-id $PRIVATE_RT_ID \
  --destination-cidr-block 0.0.0.0/0 \
  --nat-gateway-id $NAT_GW_ID
```

12將路由表與您的子網路建立關聯。

```
aws ec2 associate-route-table \
  --route-table-id $PRIVATE_RT_ID \
  --subnet-id $PRIVATE_SUBNET_ID

aws ec2 associate-route-table \
  --route-table-id $PUBLIC_RT_ID \
  --subnet-id $PUBLIC_SUBNET_ID
```

> **Note**
>
> 在 VPC 建立期間， Amazon VPC 會自動建立主要路由表，並依預設隱含地將子網路與其建立關聯。

選擇您的 HCX 連線選項

為您的 Amazon EVS 環境選擇一個連線選項：

- 私有連線：為 HCX 提供高效能網路路徑，將可靠性和一致性最佳化。需要使用 AWS Direct Connect Site-to-Site進行外部網路連線。
- 網際網路連線：使用公有網際網路建立快速設定的彈性遷移路徑。需要使用 VPC IP Address Manager (IPAM) 和彈性 IP 地址。

如需詳細分析，請參閱 the section called “HCX 連線選項”。

選擇您的選項：

- 選項 A：僅限私有連線 → 繼續至 the section called “設定 VPC 主要路由表”。
- 選項 B：網際網路連線 → 繼續前往 the section called “HCX 網際網路連線設定”。

HCX 網際網路連線設定

> **Note**
>
> 如果您選擇 HCX 私有連線並繼續 ，請略過本節the section called “設定 VPC 主要路由表”。

若要啟用 Amazon EVS 的 HCX 網際網路連線，您必須：

- 請確定 Amazon 提供的連續公有 IPv4 CIDR 區塊網路遮罩長度的 VPC IP Address Manager (IPAM) 配額為 /28 或更高。

  > **Important**
  >
  > 使用任何 Amazon 提供的連續公有 IPv4 CIDR 區塊，且網路遮罩長度小於 /28，將導致 HCX 連線問題。如需增加 IPAM 配額的詳細資訊，請參閱 IPAM 的配額。

- 使用網路遮罩長度下限為 /28 的 CIDR 建立 IPAM 和公有 IPv4 IPAM 集區。
- 從 IPAM 集區為 HCX Manager 和 HCX Interconnect (HCX-IX) 設備配置至少兩個彈性 IP 地址 (EIPs)。為您需要部署的每個 HCX 網路設備配置額外的彈性 IP 地址。
- 將公有 IPv4 CIDR 區塊新增為 VPC 的額外 CIDR。

如需在環境建立後管理 HCX 網際網路連線的詳細資訊，請參閱 the section called “HCX 公有連線”。

建立 IPAM

請依照下列步驟建立 IPAM。

> **Note**
>
> 您可以使用 IPAM 免費方案來建立 IPAM 資源，以搭配 Amazon EVS 使用。雖然 IPAM 本身是免費方案，但您必須負責其他與 IPAM 搭配使用之 AWS 服務的費用，例如 NAT 閘道，以及您使用且超過免費方案限制的任何公有 IPv4 地址。如需 IPAM 定價的詳細資訊，請參閱 Amazon VPC 定價頁面。

> **Note**
>
> Amazon EVS 目前不支援私有 IPv6 全域單點傳送地址 (GUA) CIDRs。

建立公有 IPv4 IPAM 集區

請依照下列步驟建立公有 IPv4 集區。

IPAM console

1. 開啟 IAM 主控台。
2. 在導覽窗格中選擇 Pools (集區)。
3. 選擇公有範圍。如需範圍的詳細資訊，請參閱 IPAM 的運作方式。
4. 選擇建立集區。
5. (選用) 新增集區的 Name tag (名稱標籤) 和集區的 Description (說明)。
6. 在 Address family (地址系列) 下，選擇 IPv4。
7. 在 Resource planning (資源規劃) 下，將 Plan IP space within the scope (規劃範圍內的 IP 空間) 保留選取狀態。
8. 在 Locale (區域設定) 下，選擇該集區的區域設定。地區設定是您希望此 IPAM 集區可用於配置 AWS 的區域。您選擇的地區設定必須符合 VPC 部署所在的 AWS 區域。
9. 在 Service (服務) 下，選擇 EC2 (EIP/VPC)。這將公告從此集區為 Amazon EC2 服務配置的 CIDRs （適用於彈性 IP 地址）。
10. 在 公有 IP 來源 下，選擇 Amazon 擁有。
11. 在要佈建CIDRs 下，選擇新增 Amazon 擁有的公有 CIDR。
12. 在網路遮罩下，選擇 CIDR 網路遮罩長度。/28 是所需的最小網路遮罩長度。
13. 選擇建立集區。

AWS CLI

1. 開啟終端機工作階段。
2. 從 IPAM 取得公有範圍 ID。

```
SCOPE_ID=$(aws ec2 describe-ipam-scopes \
  --filters Name=ipam-scope-type,Values=public \
  --query 'IpamScopes[0].IpamScopeId' \
```

```
  --output text)
```

3. 在公有範圍內建立 IPAM 集區。

```
aws ec2 create-ipam-pool \
  --ipam-scope-id $SCOPE_ID \
  --address-family ipv4 \
  --no-auto-import \
  --locale us-east-2 \
  --description "Public IPv4 pool for HCX" \
  --tag-specifications 'ResourceType=ipam-pool,Tags=[{Key=Name,Value=evs-hcx-
public-pool}]' \
  --public-ip-source amazon \
  --aws-service ec2
```

4. 存放用於後續命令的集區 ID。

```
POOL_ID=$(aws ec2 describe-ipam-pools \
  --filters Name=tag:Name,Values=evs-hcx-public-pool \
  --query 'IpamPools[0].IpamPoolId' \
  --output text)
```

5. 從集區佈建 CIDR 區塊，網路遮罩長度下限為 /28。

```
aws ec2 provision-ipam-pool-cidr \
  --ipam-pool-id $POOL_ID \
  --netmask-length 28
```

從 IPAM 集區配置彈性 IP 地址

請依照下列步驟，從 HCX Service Mesh 設備的 IPAM 集區配置彈性 IP 地址 (EIPs)。

Amazon VPC console

1. 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Elastic IPs (彈性 IP)。
3. 選擇 Allocate Elastic IP address (配置彈性 IP 地址)。
4. 選取使用 IPv4 IPAM 集區配置。
5. 選取您先前設定的 Amazon 擁有公有 IPv4 集區。
6. 在配置 IPAM 方法下，選擇 IPAM 集區中的手動輸入地址。

> **Important**
>
> 您無法將公有 IPAM CIDR 區塊的前兩個 EIPs 或最後一個 EIP 與 VLAN 子網路建立關聯。這些 EIPs會保留為網路、預設閘道和廣播地址。如果您嘗試將這些 EIPs 與 VLAN 子網路建立關聯，Amazon EVS 會擲回驗證錯誤。

> **Important**
>
> 手動輸入 IPAM 集區中的地址，以確保未配置 Amazon EVS 保留EIPs。如果您允許 IPAM 選擇 EIP，IPAM 可能會配置 Amazon EVS 保留的 EIP，導致 EIP 與 VLAN 子網路的關聯失敗。

7. 指定要從 IPAM 集區配置的 EIP。
8. 選擇 Allocate (配置)。
9. 重複此程序來配置您需要的其餘 EIPs。您必須從 IPAM 集區為 HCX Manager 和 HCX Interconnect (HCX-IX) 設備配置至少兩個 EIPs。為您需要部署的每個 HCX 網路設備配置額外的 EIP。

AWS CLI

1. 開啟終端機工作階段。
2. 取得您先前建立的 IPAM 集區 ID。

```
POOL_ID=$(aws ec2 describe-ipam-pools \
  --filters Name=tag:Name,Values=evs-hcx-public-pool \
  --query 'IpamPools[0].IpamPoolId' \
  --output text)
```

3. 從 IPAM 集區配置彈性 IP 地址。您必須從 IPAM 集區為 HCX Manager 和 HCX Interconnect (HCX-IX) 設備配置至少兩個 EIPs。為您需要部署的每個 HCX 網路設備配置額外的 EIP。

> **Important**
>
> 您無法將公有 IPAM CIDR 區塊的前兩個 EIPs 或最後一個 EIP 與 VLAN 子網路建立關聯。這些 EIPs會保留為網路、預設閘道和廣播地址。如果您嘗試將這些 EIPs 與 VLAN 子網路建立關聯，Amazon EVS 會擲回驗證錯誤。

> **Important**
>
> 手動輸入 IPAM 集區中的地址，以確保未配置 Amazon EVS 保留EIPs。如果您允許 IPAM 選擇 EIP，IPAM 可能會配置 Amazon EVS 保留的 EIP，導致 EIP 與 VLAN 子網路的關聯失敗。

```
aws ec2 allocate-address \
  --domain vpc \
  --tag-specifications 'ResourceType=elastic-ip,Tags=[{Key=Name,Value=evs-hcx-
manager-eip}]' \
  --ipam-pool-id $POOL_ID \
  --address xx.xx.xxx.3

aws ec2 allocate-address \
  --domain vpc \
  --tag-specifications 'ResourceType=elastic-ip,Tags=[{Key=Name,Value=evs-hcx-ix-
eip}]' \
  --ipam-pool-id $POOL_ID \
  --address xx.xx.xxx.4

aws ec2 allocate-address \
  --domain vpc \
  --tag-specifications 'ResourceType=elastic-ip,Tags=[{Key=Name,Value=evs-hcx-ne-
eip}]' \
  --ipam-pool-id $POOL_ID \
  --address xx.xx.xxx.5
```

將公有 IPv4 CIDR 區塊從 IPAM 集區新增至 VPC 以獲得 HCX 網際網路一致性

若要啟用 HCX 網際網路連線，您必須將公有 IPv4 CIDR 區塊從 IPAM 集區新增至 VPC，做為額外的 CIDR。Amazon EVS 使用此 CIDR 區塊將 VMware HCX 連線至您的網路。請依照下列步驟，將 CIDR 區塊新增至 VPC。

> **Important**
>
> 您必須手動輸入您新增至 VPC 的 IPv4 CIDR 區塊。Amazon EVS 目前不支援使用 IPAM 配置的 CIDR 區塊。使用 IPAM 配置的 CIDR 區塊可能會導致 EIP 關聯失敗。

Amazon VPC console

1. 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Your VPCs (您的 VPC)。
3. 選取您先前建立的 VPC，然後選擇動作、編輯 CIDRs。
4. 選擇新增 IPV4 CIDR。
5. 選取 IPV4 CIDR 手動輸入。
6. 從您先前建立的公有 IPAM 集區指定 CIDR 區塊。

AWS CLI

1. 開啟終端機工作階段。
2. 取得 IPAM 集區 ID 和佈建 CIDR 區塊。

```
POOL_ID=$(aws ec2 describe-ipam-pools \
  --filters Name=tag:Name,Values=evs-hcx-public-pool \
  --query 'IpamPools[0].IpamPoolId' \
  --output text)

CIDR_BLOCK=$(aws ec2 get-ipam-pool-cidrs \
  --ipam-pool-id $POOL_ID \
  --query 'IpamPoolCidrs[0].Cidr' \
  --output text)
```

3. 將 CIDR 區塊新增至您的 VPC。

```
aws ec2 associate-vpc-cidr-block \
  --vpc-id $VPC_ID \
```

```
  --cidr-block $CIDR_BLOCK
```

設定 VPC 主要路由表

Amazon EVS VLAN 子網路會隱含地與 VPC 主路由表相關聯。若要啟用與 DNS 或內部部署系統等相依服務的連線，以便成功部署環境，您必須設定主要路由表，以允許這些系統的流量。主要路由表必須包含 VPC CIDR 的路由。只有初始 Amazon EVS 環境部署才需要使用主路由表。部署環境之後，您可以將環境設定為使用自訂路由表。如需詳細資訊，請參閱the section called “設定自訂路由表”。

部署環境之後，您必須明確地將每個 Amazon EVS VLAN 子網路與 VPC 中的路由表建立關聯。如果您的 VLAN 子網路未明確與 VPC 路由表相關聯，NSX 連線會失敗。強烈建議您在環境部署之後，明確地將子網路與自訂路由表建立關聯。如需詳細資訊，請參閱the section called “設定 VPC 主要路由表”。

Important

Amazon EVS 只有在建立 Amazon EVS 環境之後，才支援使用自訂路由表。建立 Amazon EVS 環境期間不應使用自訂路由表，因為這可能會導致連線問題。

使用 VPC DHCP 選項集設定 DNS 和 NTP 伺服器

Important

如果您不符合這些 Amazon EVS 要求，您的環境部署會失敗：

- 在 DHCP 選項集中包含主要 DNS 伺服器 IP 地址和次要 DNS 伺服器 IP 地址。
- 在您的部署中包含具有每個 VCF 管理設備與 Amazon EVS 主機 A 記錄的 DNS 轉送查詢區域。
- 包含 DNS 反向查詢區域，其中包含部署中每個 VCF 管理設備及 Amazon EVS 主機的 PTR 記錄。
- 設定 VPC 的主要路由表，以確保 DNS 伺服器的路由存在。
- 確認您的網域名稱註冊有效且未過期，並且沒有重複的主機名稱或 IP 位址。
- 設定您的安全群組和網路存取控制清單 (ACLs)，以允許 Amazon EVS 與下列通訊：
  - 透過 TCP/UDP 連接埠 53 的 DNS 伺服器。
  - 透過 HTTPS 和 SSH 的主機管理 VLAN 子網路。

- 透過 HTTPS 和 SSH 管理 VLAN 子網路。

Amazon EVS 使用您 VPC 的 DHCP 選項集來擷取下列項目：

- 用於主機 IP 地址解析的網域名稱系統 (DNS) 伺服器。
- DNS 解析的網域名稱。
- 用於時間同步的網路時間通訊協定 (NTP) 伺服器。

您可以使用 Amazon VPC 主控台或 建立 DHCP 選項集 AWS CLI。如需詳細資訊，請參閱 Amazon VPC 《使用者指南》中的建立 DHCP 選項集。

設定 DNS 伺服器

DNS 組態可在 Amazon EVS 環境中啟用主機名稱解析。若要成功部署 Amazon EVS 環境，VPC 的 DHCP 選項集必須具有下列 DNS 設定：

- DHCP 選項集中的主要 DNS 伺服器 IP 地址和次要 DNS 伺服器 IP 地址。
- 部署中每個 VCF 管理設備與 Amazon EVS 主機具有 A 記錄的 DNS 轉送查詢區域。
- 部署中每個 VCF 管理設備及 Amazon EVS 主機具有 PTR 記錄的反向查詢區域。對於 NTP 組態，您可以使用預設的 Amazon NTP 地址 `169.254.169.123`，或您偏好的另一個 IPv4 地址。

如需在 DHCP 選項集中設定 DNS 伺服器的詳細資訊，請參閱建立 DHCP 選項集。

為內部部署連線設定 DNS

對於內部部署連線，建議使用 Route 53 私有託管區域搭配傳入解析程式。此設定會啟用混合 DNS 解析，您可以在 VPC 內將 Route 53 用於內部 DNS，並將其與現有的現場部署 DNS 基礎設施整合。這可讓 VPC 內的資源解析內部部署網路上託管的網域名稱，反之亦然，而不需要複雜的組態。如有需要，您也可以使用自己的 DNS 伺服器搭配 Route 53 傳出解析程式。如需設定步驟，請參閱《Amazon Route 53 開發人員指南》中的建立私有託管區域和將傳入 DNS 查詢轉送到您的 VPC。

> **Note**
>
> 在 DHCP 選項集中同時使用 Route 53 和自訂網域名稱系統 (DNS) 伺服器可能會導致意外行為。

> **Note**
>
> 如果您使用 中私有託管區域中定義的自訂 DNS 網域名稱 Route 53，或搭配介面 VPC 端點 (AWS PrivateLink) 使用私有 DNS，則必須同時將 `enableDnsHostnames`和 `enableDnsSupport` 屬性設定為 `true`。如需詳細資訊，請參閱 VPC 的 DNS 屬性。

故障診斷 DNS 連線能力問題

Amazon EVS 需要持續連線至您 VPC DHCP 選項集中的 SDDC Manager 和 DNS 伺服器，才能存取 DNS 記錄。如果 SDDC Manager 的持續連線無法使用，Amazon EVS 將無法再驗證環境狀態，而且您可能會失去環境存取權。如需疑難排解此問題的步驟，請參閱 the section called “連線能力檢查失敗”。

設定 NTP 伺服器

NTP 伺服器向網路提供時間。Amazon EC2 執行個體上一致且準確的時間參考對於許多 VCF 環境任務和程序至關重要。時間同步對於下列項目至關重要：

- 系統記錄和稽核
- 安全營運
- 分散式系統管理
- 疑難排解

您可以在 VPC 的 DHCP 選項集中輸入最多四個 NTP 伺服器的 IPv4 地址。您可以在 IPv4 地址 指定 Amazon Time Sync Service`169.254.169.123`。根據預設，Amazon EVS 部署的 Amazon EC2 執行個體會使用位於 IPv4 地址 的 Amazon Time Sync Service`169.254.169.123`。

如需 NTP 伺服器的詳細資訊，請參閱 RFC 2123。如需 Amazon Time Sync Service 的詳細資訊，請參閱 EC2 執行個體中的精密時鐘和時間同步，以及 VMware Cloud Foundation 文件中的在 VMware Cloud Foundation 主機上設定 NTP。

設定 NTP 設定

1. 選擇您的 NTP 來源：
   - Amazon Time Sync Service （ 建議 ）
   - 自訂 NTP 伺服器

2. 將 NTP 伺服器新增至 DHCP 選項集。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的建立 DHCP 選項集。
3. 驗證時間同步。如需 DHCP 選項集組態的詳細資訊，請參閱 the section called “設定 VPC 的 DHCP 選項集”。

設定內部部署網路連線（選用）

您可以使用 Direct Connect 搭配相關聯的傳輸閘道，或使用 AWS Site-to-Site VPN 連接至傳輸閘道，設定現場部署資料中心與 AWS 基礎設施的連線能力。

若要啟用內部部署系統的連線，以成功部署環境，您必須設定 VPC 的主要路由表，以允許這些系統的流量。如需詳細資訊，請參閱the section called “設定 VPC 主要路由表”。

建立 Amazon EVS 環境之後，您必須使用在 Amazon EVS 環境中建立的 VPC CIDRs 更新傳輸閘道路由表。如需詳細資訊，請參閱the section called “為內部部署連線設定傳輸閘道路由表和 Direct Connect 字首（選用）”。

如需設定 Direct Connect 連線的詳細資訊，請參閱Direct Connect 閘道和傳輸閘道關聯。如需將 AWS Site-to-Site與 AWS 傳輸閘道搭配使用的詳細資訊，請參閱 Amazon VPC 《傳輸閘道使用者指南》中的AWSAmazon VPC 傳輸閘道中的Site-to-Site VPN 連接。

> **Note**
>
> Amazon EVS 不支援透過 AWS Direct Connect 私有虛擬介面 (VIF) 或透過直接終止至底層 VPC AWS Site-to-Site VPN 連線進行連線。

使用端點和對等設定 VPC Route Server 執行個體

Amazon EVS 使用 Amazon VPC Route Server 來啟用 BGP 型動態路由到您的 VPC 底層網路。您必須指定路由伺服器，將路由共用到服務存取子網路中至少兩個路由伺服器端點。路由伺服器對等項上設定的對等 ASN 必須相符，而且對等 IP 位址必須是唯一的。

如果您要設定 Route Server for HCX 網際網路連線，則必須為您在此程序的第一個步驟中建立的服務存取子網路和公有子網路設定 Route Server 傳播。

> **Important**
>
> 如果您不符合這些 Amazon EVS 對 VPC Route Server 組態的要求，您的環境部署會失敗：

- 您必須在服務存取子網路中設定至少兩個路由伺服器端點。
- 為 Tier-0 閘道設定邊界閘道協定 (BGP) 時，VPC Route Server 對等 ASN 值必須符合 NSX Edge 對等 ASN 值。
- 建立兩個路由伺服器對等時，您必須為每個端點使用來自 NSX 上行 VLAN 的唯一 IP 地址。這兩個 IP 地址會在 Amazon EVS 環境部署期間指派給 NSX 邊緣。
- 啟用路由伺服器傳播時，您必須確保所有要傳播的路由表至少有一個明確的子網路關聯。如果傳播的路由表沒有明確的子網路關聯，BGP 路由公告會失敗。

如需設定 VPC Route Server 的詳細資訊，請參閱 Route Server 入門教學課程。

Important

啟用路由伺服器傳播時，請確保要傳播的所有路由表至少有一個明確的子網路關聯。如果路由表確實具有明確的子網路關聯，則 BGP 路由公告會失敗。

Note

對於 Route Server 對等活體偵測，Amazon EVS 僅支援預設的 BGP 保持連線機制。Amazon EVS 不支援多躍點雙向轉送偵測 (BFD)。

Note

建議您為路由伺服器執行個體啟用持續路由，持續時間介於 1-5 分鐘。如果啟用，即使所有 BGP 工作階段都結束，路由仍會保留在路由伺服器的路由資料庫中。如需詳細資訊，請參閱 Amazon VPC 《使用者指南》中的建立路由伺服器。

Note

如果您使用 NAT 閘道或傳輸閘道，請確定您的路由伺服器已正確設定，以將 NSX 路由傳播至 VPC 路由表 (VPC)。

疑難排解

如果您遇到問題：

- 確認每個路由表都有明確的子網路關聯。
- 檢查為路由伺服器輸入的對等 ASN 值和 NSX Tier-0 閘道是否相符。
- 確認 Route Server 端點 IP 地址是唯一的。
- 檢閱路由表中的路由傳播狀態。
- 使用 VPC Route Server 對等記錄來監控 BGP 工作階段運作狀態，並疑難排解連線問題。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的路由伺服器對等記錄。

建立網路 ACL 以控制 Amazon EVS VLAN 子網路流量

Amazon EVS 使用網路存取控制清單 (ACL) 來控制往返 Amazon EVS VLAN 子網路的流量。您可以使用 VPC 的預設網路 ACL，或者您可以使用類似於安全群組規則的規則為您的 VPC 建立自訂網路 ACL，以新增一層安全層。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的為您的 VPC 建立網路 ACL。

如果您打算設定 HCX 網際網路連線，請確定您設定的網路 ACL 規則允許 HCX 元件的必要傳入和傳出連線。如需 HCX 連接埠需求的詳細資訊，請參閱 VMware HCX 使用者指南。

> **Important**
>
> 如果您是透過網際網路連線，則將彈性 IP 地址與 VLAN 建立關聯可提供該 VLAN 子網路上所有資源的直接網際網路存取。確保您已設定適當的網路存取控制清單，以根據您的安全需求來限制存取。

> **Important**
>
> EC2 安全群組無法在連接到 Amazon EVS VLAN 子網路的彈性網路介面上運作。若要控制往返 Amazon EVS VLAN 子網路的流量，您必須使用網路存取控制清單。

建立 Amazon EVS 環境

> **Important**
>
> 為了盡可能簡單快速地開始使用，本主題包含使用預設設定建立 Amazon EVS 環境的步驟。建立環境之前，建議您先熟悉所有設定，並使用符合您需求的設定來部署環境。環境只能在初始環境建立期間設定。環境建立之後就無法修改。如需所有可能 Amazon EVS 環境設定的概觀，請參閱 Amazon EVS API 參考指南。

> **Note**
>
> 您的環境 ID 將提供給所有 AWS 區域的 Amazon EVS，以滿足 VCF 授權合規需求。

> **Note**
>
> Amazon EVS 環境必須部署到與 VPC 和 VPC 子網路相同的區域和可用區域。

完成此步驟，以建立具有主機和 VLAN 子網路的 Amazon EVS 環境。

Example

Amazon EVS console

1. 前往 Amazon EVS 主控台。

   > **Note**
   >
   > 請確定主控台右上角顯示的 AWS 區域是 AWS 您要建立環境的區域。如果不是，請選擇 AWS 區域名稱旁的下拉式清單，然後選擇您要使用的 AWS 區域。

2. 在導覽窗格中，選擇 Environments (環境)。
3. 選擇 Create environment (建立環境)。
4. 在驗證 Amazon EVS 需求頁面上，檢查是否符合服務需求。如需詳細資訊，請參閱設定 Amazon Elastic VMware Service。
   a. （選用）針對名稱，輸入環境名稱。

b. 針對環境版本，選擇您的 VCF 版本。如需 Amazon EVS 提供的 VCF 版本的相關資訊，請參閱 the section called “VCF 版本和 EC2 執行個體”。

c. 在站台 ID 中，輸入您的 Broadcom 站台 ID。

d. 針對 VCF 解決方案金鑰，輸入 VCF 解決方案金鑰 (VMware vSphere 8 Enterprise Plus for VCF)。此授權金鑰不能由現有環境使用。

> **Note**
>
> VCF 解決方案金鑰必須至少有 256 個核心。

> **Note**
>
> 您的 VCF 授權將可供所有 AWS 區域的 Amazon EVS 使用，以符合授權規範。Amazon EVS 不會驗證授權金鑰。若要驗證授權金鑰，請造訪 Broadcom 支援。

> **Note**
>
> Amazon EVS 會要求您在 SDDC Manager 中維護有效的 VCF 解決方案金鑰，服務才能正常運作。如果您使用 vSphere 用戶端部署後管理 VCF 解決方案金鑰，您必須確保金鑰也會出現在 SDDC Manager 使用者介面的授權畫面中。

e. 針對 vSAN 授權金鑰，輸入 vSAN 授權金鑰。此授權金鑰不能由現有環境使用。

> **Note**
>
> vSAN 授權金鑰必須至少有 110 TiB 的 vSAN 容量。

> **Note**
>
> 您的 VCF 授權將可供所有 AWS 區域的 Amazon EVS 使用，以符合授權規範。Amazon EVS 不會驗證授權金鑰。若要驗證授權金鑰，請造訪 Broadcom 支援。

> **Note**
>
> Amazon EVS 要求您在 SDDC Manager 中維護有效的 vSAN 授權金鑰，以選擇可正常運作的服務。如果您使用 vSphere 用戶端部署後管理 vSAN 授權金鑰，您必須確保金鑰也會出現在 SDDC Manager 使用者介面的授權畫面中。

f. 如需 VCF 授權條款，請勾選核取方塊以確認您已購買 ，並將繼續維持所需的 VCF 軟體授權數量，以涵蓋 Amazon EVS 環境中的所有實體處理器核心。Amazon EVS 中 VCF 軟體的相關資訊將與 Broadcom 共用，以驗證授權合規性。

g. 選擇下一步。

5. 在指定主機詳細資訊頁面上，完成以下步驟四次，將四個主機新增至環境。Amazon EVS 環境需要四個主機來進行初始部署。

   a. 選擇新增主機詳細資訊。

   b. 針對 DNS 主機名稱，輸入主機的主機名稱。

   c. 針對執行個體類型，選擇 EC2 執行個體類型。

   d. 對於 ESX 主機版本，在環境建立期間，將使用所選 VCF 版本的預設 ESX 版本。如需詳細資訊，請參閱the section called “VCF 版本和 EC2 執行個體”。

   > **Important**
   >
   > 請勿停止或終止 Amazon EVS 部署的 EC2 執行個體。此動作會導致資料遺失。

   > **Note**
   >
   > Amazon EVS 目前僅支援 i4i.metal EC2 執行個體。

   e. 針對 SSH 金鑰對，選擇 SSH 金鑰對以存取主機。

   f. 選擇新增主機。

6. 在設定網路和連線頁面上，執行下列動作。

   a. 針對 HCX 連線需求，選取您要搭配私有連線使用 HCX，還是透過網際網路使用。

   b. 針對 VPC，選擇您先前建立的 VPC。

   c. （僅適用於 HCX Internet Connectivy) 對於 HCX 網路 ACL，請選擇將與 HCX VLAN 相關聯的網路 ACL。

> **Important**
>
> 我們強烈建議您建立專用於 HCX VLAN 的自訂網路 ACL。如需詳細資訊，請參閱the section called “設定網路 ACL”。

d. 針對服務存取子網路，選擇您建立 VPC 時建立的私有子網路。

e. 對於安全群組 - 選用 ，您可以選擇最多兩個安全群組來控制 Amazon EVS 控制平面和 VPC 之間的通訊。如果未選擇安全群組，Amazon EVS 會使用預設安全群組。

> **Note**
>
> 請確定您選擇的安全群組提供 DNS 伺服器和 Amazon EVS VLAN 子網路的連線。

f. 在管理連線下，輸入要用於 Amazon EVS VLAN 子網路的 CIDR 區塊。對於 HCX 上行 VLAN CIDR 區塊，如果設定公有 HCX VLAN，您必須指定網路遮罩長度剛好為 /28 的 CIDR 區塊。如果為公有 HCX VLAN 指定任何其他 CIDR 區塊大小，Amazon EVS 會擲回驗證錯誤。對於私有 HCX VLAN 和所有其他 VLANs CIDR 區塊，您可以使用的最小網路遮罩長度為 /28，最大值為 /24。

> **Important**
>
> Amazon EVS VLAN 子網路只能在 Amazon EVS 環境建立期間建立，且在環境建立之後無法修改。建立環境之前，您必須確定 VLAN 子網路 CIDR 區塊的大小正確。部署環境之後，您將無法新增 VLAN 子網路。如需詳細資訊，請參閱the section called “Amazon EVS 網路考量事項”。

g. 在擴展 VLANs下，輸入其他 Amazon EVS VLAN 子網路的 CIDR 區塊，可用於在 Amazon EVS 內擴展 VCF 功能，例如啟用 NSX 聯合。

h. 在工作負載/VCF 連線下，輸入 NSX 上行 VLAN 的 CIDR 區塊，然後選擇兩個透過 NSX 上行對等至 Route Server 端點的 VPC Route Server 對等 IDs。

> **Note**
>
> 在 EVS 部署之前，Amazon EVS 需要與兩個 Route Server 端點和兩個 Route Server 對等相關聯的 VPC Route Server 執行個體。此組態會透過 NSX 上行連結啟用動態

BGP 型路由。如需詳細資訊，請參閱the section called “使用端點和對等設定 VPC Route Server 執行個體”。

i. 選擇下一步。

7. 在指定管理 DNS 主機名稱頁面上，執行下列動作。

a. 在管理設備 DNS 主機名稱下，輸入虛擬機器的 DNS 主機名稱來託管 VCF 管理設備。如果使用 Route 53 做為 DNS 提供者，也請選擇包含 DNS 記錄的託管區域。

b. 在登入資料下，選擇您要使用 Secrets Manager 的 AWS 受管 KMS 金鑰，還是您提供的客戶受管 KMS 金鑰。此金鑰用於加密使用 SDDC Manager、NSX Manager 和 vCenter 設備所需的 VCF 憑證。

> **Note**
>
> 客戶受管 KMS 金鑰有相關的使用成本。如需詳細資訊，請參閱 AWS KMS 定價頁面。

c. 選擇下一步。

8. （選用）在新增標籤頁面上，新增您要指派給此環境的任何標籤，然後選擇下一步。

> **Note**
>
> 建立為此環境一部分的主機將會收到下列標籤：`DoNotDelete-EVS-<environmentid>-<hostname>`。

> **Note**
>
> 與 Amazon EVS 環境相關聯的標籤不會傳播到基礎 AWS 資源，例如 EC2 執行個體。您可以使用個別的服務主控台或 在基礎 AWS 資源上建立標籤 AWS CLI。

9. 在檢閱和建立頁面上，檢閱您的組態，然後選擇建立環境。

> **Important**
>
> 在環境部署期間，Amazon EVS 會建立 EVS VLAN 子網路，並隱含地將其與主路由表建立關聯。部署完成後，您必須明確地將 Amazon EVS VLAN 子網路與路由表建立關聯，

以便進行 NSX 連線。如需詳細資訊，請參閱the section called “將 Amazon EVS VLAN 子網路明確關聯至 VPC 路由表”。

> **Note**
>
> Amazon EVS 部署 VMware Cloud Foundation 的最近綁定版本，其中可能不會包含個別產品更新，稱為非同步修補程式。完成此部署後，我們強烈建議您使用 Broadcom 的非同步修補程式工具 (AP 工具） 或 SDDC Manager 產品內 LCM 自動化來檢閱和更新個別產品。NSX 升級必須在 SDDC Manager 之外完成。

> **Note**
>
> 環境建立可能需要幾個小時。

AWS CLI

1. 開啟終端機工作階段。
2. 建立 Amazon EVS 環境。以下是範例`aws evs create-environment`請求。

> **Important**
>
> 在執行 `aws evs create-environment`命令之前，請檢查是否符合所有 Amazon EVS 先決條件。如果未符合先決條件，則環境部署會失敗。如需詳細資訊，請參閱設定 Amazon Elastic VMware Service。

> **Important**
>
> 在環境部署期間，Amazon EVS 會建立 EVS VLAN 子網路，並隱含地將其與主路由表建立關聯。部署完成後，您必須明確地將 Amazon EVS VLAN 子網路與路由表建立關聯，以便進行 NSX 連線。如需詳細資訊，請參閱the section called “將 Amazon EVS VLAN 子網路明確關聯至 VPC 路由表”。

> **Note**
>
> Amazon EVS 部署 VMware Cloud Foundation 的最近綁定版本，其中可能不會包含個別產品更新，稱為非同步修補程式。完成此部署後，我們強烈建議您使用 Broadcom 的非同步修補程式工具 (AP 工具） 或 SDDC Manager 產品內 LCM 自動化來檢閱和更新個別產品。NSX 升級必須在 SDDC Manager 之外完成。

> **Note**
>
> 環境部署可能需要幾個小時。

- 針對 `--vpc-id`，指定您先前建立且 IPv4 CIDR 範圍下限為 /22 的 VPC。
- 針對 `--service-access-subnet-id`，指定您建立 VPC 時所建立私有子網路的唯一 ID。
- 對於 `--vcf-version`，請參閱 the section called “VCF 版本和 EC2 執行個體” 以取得 Amazon EVS 提供的 VCF 版本，
- 使用 `--terms-accepted`，您確認您已購買並將繼續維持所需的 VCF 軟體授權數量，以涵蓋 Amazon EVS 環境中的所有實體處理器核心。Amazon EVS 中 VCF 軟體的相關資訊將與 Broadcom 共用，以驗證授權合規性。
- 針對 `--license-info`，輸入您的 VCF 解決方案金鑰 (VMware vSphere 8 Enterprise Plus for VCF) 和 vSAN 授權金鑰。

> **Note**
>
> VCF 解決方案金鑰必須至少有 256 個核心。vSAN 授權金鑰必須至少有 110 TiB 的 vSAN 容量。

> **Note**
>
> Amazon EVS 會要求您在 SDDC Manager 中維護有效的 VCF 解決方案金鑰和 vSAN 授權金鑰，服務才能正常運作。如果您使用 vSphere 用戶端部署後管理這些授權金鑰，您必須確保它們也會出現在 SDDC Manager 使用者介面的授權畫面中。

> **Note**
>
> 現有 Amazon EVS 環境無法使用 VCF 解決方案金鑰和 vSAN 授權金鑰。

- 對於 ，`--initial-vlans`指定 Amazon EVS 代表您建立之 Amazon EVS VLAN 子網路的 CIDR 範圍。這些 VLANs用於部署 VCF 管理設備。如果設定公有 HCX VLAN，您必須指定網路遮罩長度剛好為 /28 的 CIDR 區塊。如果為公有 HCX VLAN 指定任何其他 CIDR 區塊大小，Amazon EVS 會擲回驗證錯誤。對於私有 HCX VLAN 和所有其他 VLANs CIDR 區塊，您可以使用的最小網路遮罩長度為 /28，最大值為 /24。
- `hcxNetworkAclId` 如果設定 HCX 網際網路連線，則會使用 。為公有 HCX VLAN 指定自訂網路 ACL。

> **Important**
>
> 我們強烈建議您建立專用於 HCX VLAN 的自訂網路 ACL。如需詳細資訊，請參閱the section called “設定網路 ACL”。

> **Important**
>
> Amazon EVS VLAN 子網路只能在 Amazon EVS 環境建立期間建立，且在環境建立之後無法修改。建立環境之前，您必須確定 VLAN 子網路 CIDR 區塊的大小正確。部署環境後，您將無法新增 VLAN 子網路。如需詳細資訊，請參閱the section called “Amazon EVS 網路考量事項”。

- 針對 `--hosts`，指定 Amazon EVS 環境部署所需的主機詳細資訊。包含每個主機的 DNS 主機名稱、EC2 SSH 金鑰名稱和 EC2 執行個體類型。專用主機 ID 是選用的。

> **Important**
>
> 請勿停止或終止 Amazon EVS 部署的 EC2 執行個體。此動作會導致資料遺失。

> **Note**
>
> Amazon EVS 目前僅支援 i4i.metal EC2 執行個體。

- 針對 `--connectivity-info`，指定您在上一個步驟中建立的 2 個 VPC Route Server 對等 IDs。

> **Note**
>
> 在 EVS 部署之前，Amazon EVS 需要與兩個 Route Server 端點和兩個 Route Server 對等相關聯的 VPC Route Server 執行個體。此組態會透過 NSX 上行連結啟用動態 BGP 型路由。如需詳細資訊，請參閱the section called “使用端點和對等設定 VPC Route Server 執行個體”。

- 針對 `--vcf-hostnames`，輸入虛擬機器的 DNS 主機名稱來託管 VCF 管理設備。
- 針對 `--site-id`，輸入您唯一的 Broadcom 網站 ID。具有此 ID 才能進入 Broadcom 入口網站，而 Broadcom 會在軟體合約結束或續約時提供給您。
- （選用）針對 `--region`，輸入要部署環境的區域。如果未指定區域，則會使用您的預設區域。

```
aws evs create-environment \
--environment-name testEnv \
--vpc-id vpc-1234567890abcdef0 \
--service-access-subnet-id subnet-01234a1b2cde1234f \
--vcf-version VCF-5.2.2 \
--terms-accepted \
--license-info "{
      \"solutionKey\": \"00000-00000-00000-abcde-11111\",
      \"vsanKey\": \"00000-00000-00000-abcde-22222\"
    }" \
   --initial-vlans "{
      \"isHcxPublic\": true,
      \"hcxNetworkAclId\": \"nacl-abcd1234\",
      \"vmkManagement\": {
        \"cidr\": \"10.10.0.0/24\"
      },
      \"vmManagement\": {
        \"cidr\": \"10.10.1.0/24\"
```

```
      },
      \"vMotion\": {
        \"cidr\": \"10.10.2.0/24\"
      },
      \"vSan\": {
        \"cidr\": \"10.10.3.0/24\"
      },
      \"vTep\": {
        \"cidr\": \"10.10.4.0/24\"
      },
      \"edgeVTep\": {
        \"cidr\": \"10.10.5.0/24\"
      },
      \"nsxUplink\": {
        \"cidr\": \"10.10.6.0/24\"
      },
      \"hcx\": {
        \"cidr\": \"10.10.7.0/24\"
      },
      \"expansionVlan1\": {
        \"cidr\": \"10.10.8.0/24\"
      },
      \"expansionVlan2\": {
          \"cidr\": \"10.10.9.0/24\"
      }
    }" \
--hosts "[
    {
      \"hostName\": \"esx01\",
      \"keyName\": \"sshKey-04-05-45\”,
      \"instanceType\": \"i4i.metal\",
      \"dedicatedHostId\": \"h-07879acf49EXAMPLE\"
    },
    {
      \"hostName\": \"esx02\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\",
      \"dedicatedHostId\": \"h-07878bde50EXAMPLE\"
    },
    {
      \"hostName\": \"esx03\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\",
      \"dedicatedHostId\": \"h-07877eio51EXAMPLE\"
```

```
    },
    {
      \"hostName\": \"esx04\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\",
      \"dedicatedHostId\": \"h-07863ghi52EXAMPLE\"
    }
  ]" \
--connectivity-info "{
    \"privateRouteServerPeerings\": [\"rsp-1234567890abcdef0\",\"rsp-
abcdef01234567890\"]
  }" \
  --vcf-hostnames "{
    \"vCenter\": \"vcf-vc01\",
    \"nsx\": \"vcf-nsx\",
    \"nsxManager1\": \"vcf-nsxm01\",
    \"nsxManager2\": \"vcf-nsxm02\",
    \"nsxManager3\": \"vcf-nsxm03\",
    \"nsxEdge1\": \"vcf-edge01\",
    \"nsxEdge2\": \"vcf-edge02\",
    \"sddcManager\": \"vcf-sddcm01\",
    \"cloudBuilder\": \"vcf-cb01\"
  }" \
--site-id my-site-id \
--region us-east-2
```

以下是範例回應。

```
{
    "environment": {
        "environmentId": "env-abcde12345",
        "environmentState": "CREATING",
        "stateDetails": "The environment is being initialized, this operation
 may take some time to complete.",
        "createdAt": "2025-04-13T12:03:39.718000+00:00",
        "modifiedAt": "2025-04-13T12:03:39.718000+00:00",
        "environmentArn": "arn:aws:evs:us-east-2:111122223333:environment/env-
abcde12345",
        "environmentName": "testEnv",
        "vpcId": "vpc-1234567890abcdef0",
        "serviceAccessSubnetId": "subnet-01234a1b2cde1234f",
        "vcfVersion": "VCF-5.2.2",
        "termsAccepted": true,
```

```
        "licenseInfo": [
            {
                "solutionKey": "00000-00000-00000-abcde-11111",
                "vsanKey": "00000-00000-00000-abcde-22222"
            }
        ],
        "siteId": "my-site-id",
        "connectivityInfo": {
            "privateRouteServerPeerings": [
                "rsp-1234567890abcdef0",
                "rsp-abcdef01234567890"
            ]
        },
        "vcfHostnames": {
            "vCenter": "vcf-vc01",
            "nsx": "vcf-nsx",
            "nsxManager1": "vcf-nsxm01",
            "nsxManager2": "vcf-nsxm02",
            "nsxManager3": "vcf-nsxm03",
            "nsxEdge1": "vcf-edge01",
            "nsxEdge2": "vcf-edge02",
            "sddcManager": "vcf-sddcm01",
            "cloudBuilder": "vcf-cb01"
        }
    }
}
```

驗證 Amazon EVS 環境建立

Example

Amazon EVS console

1. 前往 Amazon EVS 主控台。
2. 在導覽窗格中，選擇 Environments (環境)。
3. 選取環境。
4. 選取詳細資訊索引標籤。
5. 檢查環境狀態是否已通過，且環境狀態是否已建立。這可讓您知道環境已就緒可供使用。

> **Note**
>
> 環境建立可能需要幾個小時。如果環境狀態仍顯示建立，請重新整理頁面。

AWS CLI

1. 開啟終端機工作階段。
2. 使用您環境的環境 ID 和包含 資源的區域名稱，執行下列命令。當 environmentState為 時，環境即可供使用CREATED。

> **Note**
>
> 環境建立可能需要幾個小時。如果 environmentState仍然顯示 CREATING，請再次執行 命令以重新整理輸出。

```
aws evs get-environment  --environment-id env-abcde12345
```

以下是範例回應。

```
{
    "environment": {
        "environmentId": "env-abcde12345",
        "environmentState": "CREATED",
        "createdAt": "2025-04-13T13:39:49.546000+00:00",
        "modifiedAt": "2025-04-13T13:40:39.355000+00:00",
        "environmentArn": "arn:aws:evs:us-east-2:111122223333:environment/env-
abcde12345",
        "environmentName": "testEnv",
        "vpcId": "vpc-0c6def5b7b61c9f41",
        "serviceAccessSubnetId": "subnet-06a3c3b74d36b7d5e",
        "vcfVersion": "VCF-5.2.2",
        "termsAccepted": true,
        "licenseInfo": [
            {
                "solutionKey": "00000-00000-00000-abcde-11111",
                "vsanKey": "00000-00000-00000-abcde-22222"
            }
```

```
        ],
        "siteId": "my-site-id",
        "checks": [],
        "connectivityInfo": {
            "privateRouteServerPeerings": [
                "rsp-056b2b1727a51e956",
                "rsp-07f636c5150f171c3"
            ]
        },
        "vcfHostnames": {
            "vCenter": "vcf-vc01",
            "nsx": "vcf-nsx",
            "nsxManager1": "vcf-nsxm01",
            "nsxManager2": "vcf-nsxm02",
            "nsxManager3": "vcf-nsxm03",
            "nsxEdge1": "vcf-edge01",
            "nsxEdge2": "vcf-edge02",
            "sddcManager": "vcf-sddcm01",
            "cloudBuilder": "vcf-cb01"
        },
        "credentials": []
    }
}
```

將 Amazon EVS VLAN 子網路明確關聯至 VPC 路由表

將每個 Amazon EVS VLAN 子網路與 VPC 中的路由表明確建立關聯。此路由表用於允許 AWS 資源與使用 Amazon EVS 執行的 NSX 網路區段上的虛擬機器進行通訊。如果您已建立公有 HCX VLAN，請務必明確地將公有 HCX VLAN 子網路與 VPC 中路由至網際網路閘道的公有路由表建立關聯。

Example

Amazon VPC console

1. 前往 VPC 主控台。
2. 在導覽窗格中，選擇 Route tables (路由表)。
3. 選擇您要與 Amazon EVS VLAN 子網路建立關聯的路由表。
4. 選取子網路關聯索引標籤。
5. 在明確子網路關聯下，選取編輯子網路關聯。
6. 選取所有 Amazon EVS VLAN 子網路。

7. 選擇 Save associations (儲存關聯)。

AWS CLI

1. 開啟終端機工作階段。
2. 識別 Amazon EVS VLAN IDs。

```
aws ec2 describe-subnets
```

3. 將 Amazon EVS VLAN 子網路與 VPC 中的路由表建立關聯。

```
aws ec2 associate-route-table \
--route-table-id rtb-0123456789abcdef0 \
--subnet-id subnet-01234a1b2cde1234f
```

將 EIPs 與 HCX 公有 VLAN 子網路建立關聯 （ 用於 HCX 網際網路連線 ）

請依照下列步驟，將彈性 IP 地址 (EIPs) 從 IPAM 集區關聯至 HCX 公有 VLAN 以進行 HCX 網際網路連線。您必須為 HCX Manager 和 HCX Interconnect (HCX-IX) 設備建立至少兩個 EIPs 的關聯。為您需要部署的每個 HCX 網路設備建立額外的 EIP 關聯。您最多可以從與 HCX 公有 VLAN 相關聯的 IPAM 集區中擁有 13 EIPs。

Important

如果您未從 IPAM 集區將至少兩個 EIPs 與 HCX 公有 VLAN 子網路建立關聯，HCX 公有網際網路連線會失敗。

Note

Amazon EVS 目前僅支援將 EIPs 與 HCX VLAN 建立關聯。

> **Note**
>
> 您無法將公有 IPAM CIDR 區塊的前兩個 EIPs 或最後一個 EIP 與 VLAN 子網路建立關聯。這些 EIPs會保留為網路、預設閘道和廣播地址。如果您嘗試將這些 EIPs 與 VLAN 子網路建立關聯，Amazon EVS 會擲回驗證錯誤。

Amazon EVS console

1. 前往 Amazon EVS 主控台。
2. 在導覽功能表中，選擇環境。
3. 選取環境。
4. 在網路和連線索引標籤下，選取 HCX 公有 VLAN。
5. 選擇將 EIP 與 VLAN 建立關聯。
6. 選取要與 HCX 公有 VLAN 建立關聯的彈性 IP 地址 （多個）。
7. 選擇關聯 EIPs。
8. 檢查 EIP 關聯以確認 EIPs已與 HCX 公有 VLAN 建立關聯。

AWS CLI

1. 若要將彈性 IP 地址與 VLAN 建立關聯，請使用範例`associate-eip-to-vlan`命令。
   - `environment-id` - Amazon EVS 環境的 ID。
   - `vlan-name` - 要與彈性 IP 地址建立關聯的 VLAN 名稱。
   - `allocation-id` - 彈性 IP 地址的配置 ID。

   ```
   aws evs associate-eip-to-vlan \
     --environment-id "env-605uove256" \
     --vlan-name "hcx" \
     --allocation-id "eipalloc-0429268f30c4a34f7"
   ```

   命令會傳回有關 VLAN 的詳細資訊，包括新的 EIP 關聯：

   ```
   {
       "vlan": {
           "vlanId": 80,
           "cidr": "18.97.137.0/28",
   ```

```
        "availabilityZone": "us-east-2c",
        "functionName": "hcx",
        "subnetId": "subnet-02f9a4ee9e1208cfc",
        "createdAt": "2025-08-22T23:42:16.200000+00:00",
        "modifiedAt": "2025-08-23T13:42:28.155000+00:00",
        "vlanState": "CREATED",
        "stateDetails": "VLAN successfully created",
        "eipAssociations": [
            {
                "associationId": "eipassoc-09e966faad7ecc58a",
                "allocationId": "eipalloc-0429268f30c4a34f7",
                "ipAddress": "18.97.137.2"
            }
        ],
        "isPublic": true,
        "networkAclId": "acl-02fa8ab4ad3ddfb00"
    }
}
```


`eipAssociations` 陣列會顯示新的關聯，包括：

- `associationId` - 此 EIP 關聯的唯一 ID，用於取消關聯。
- `allocationId` - 相關聯彈性 IP 地址的配置 ID。
- `ipAddress` - 指派給 VLAN 的 IP 地址。

2. 重複此步驟來建立其他 EIPs關聯。

為內部部署連線設定傳輸閘道路由表和 Direct Connect 字首 （選用）

如果您使用具有傳輸閘道的 Direct Connect or AWS Site-to-Site VPN 來設定內部部署網路連線，則必須使用在 Amazon EVS 環境中建立的 VPC CIDRs 來更新傳輸閘道路由表。如需詳細資訊，請參閱 Amazon VPC Transit Gateways 中的傳輸閘道路由表。

如果您使用的是 AWS Direct Connect，您可能需要更新 Direct Connect 字首，才能從 VPC 傳送和接收更新的路由。如需詳細資訊，請參閱允許 AWS Direct Connect 閘道的字首互動。

擷取 VCF 登入資料並存取 VCF 管理設備

Amazon EVS 使用 AWS Secrets Manager 在您的帳戶中建立、加密和存放受管秘密。這些秘密包含安裝和存取 VCF 管理設備所需的 VCF 登入資料，例如 vCenter Server、NSX 和 SDDC Manager，

以及 ESX 根密碼。如需擷取秘密的詳細資訊，請參閱《 AWS Secrets Manager 使用者指南》中的從 Secrets Manager 取得 AWS 秘密。

> **Note**
>
> Amazon EVS 不提供您的私密的受管輪換。建議您定期在設定的輪換時段輪換您的私密，以確保私密不會長期存在。

從 AWS Secrets Manager 擷取 VCF 登入資料後，您可以使用它們來登入您的 VCF 管理設備。如需詳細資訊，請參閱 VMware 產品文件中的登入 SDDC Manager 使用者介面和如何使用和設定 vSphere 用戶端。

設定 EC2 序列主控台 （選用）

根據預設，Amazon EVS 會在新部署的 Amazon EVS 主機上啟用 ESX Shell。此組態允許透過 ECAmazon EC22 執行個體的序列連接埠，您可以用來對開機、網路組態和其他問題進行疑難排解。序列主控台不需要您的執行個體具有任何網路功能。使用序列主控台，您可以將命令輸入執行中的 EC2 執行個體，就像您的鍵盤和監視器直接連接到執行個體的序列連接埠一樣。

您可以使用 EC2 主控台或 存取 EC2 序列主控台 AWS CLI。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的執行個體的 EC2 序列主控台。 Amazon EC2

> **Note**
>
> EC2 序列主控台是唯一支援 Amazon EVS 的機制，可存取直接主控台使用者介面 (DCUI)，以在本機與 ESX 主機互動。

> **Note**
>
> Amazon EVS 預設會停用遠端 SSH。如需啟用 SSH 存取遠端 ESX Shell 的詳細資訊，請參閱 VMware vSphere 產品文件中使用 SSH 進行遠端 ESX Shell 存取。

連接至 EC2 序列主控台

若要連線至 EC2 序列主控台並使用您選擇的工具進行故障診斷，必須完成某些先決條件任務。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的 EC2 序列主控台和連線至 EC2 序列主控台的先決條件。 EC2 Amazon EC2

> **Note**
>
> 若要連線至 EC2 序列主控台，您的 EC2 執行個體狀態必須為 `running`。如果執行個體處於 `pending`、`stopping`、`shutting-down`、 或 `terminated` 狀態`stopped`，則無法連線至序列主控台。如需執行個體狀態變更的詳細資訊，請參閱《Amazon EC2 使用者指南》中的 Amazon EC2 執行個體狀態變更。 Amazon EC2

設定對 EC2 序列主控台的存取

若要設定 EC2 序列主控台的存取權，您或您的管理員必須在帳戶層級授予序列主控台存取權，然後設定 IAM 政策以將存取權授予您的使用者。對於 Linux 執行個體，您還必須在每個執行個體上設定密碼型使用者，以便您的使用者可以使用序列主控台進行故障診斷。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的設定 EC2 序列主控台的存取權。 Amazon EC2

清除

請依照下列步驟刪除已建立 AWS 的資源。

刪除 Amazon EVS 主機和環境

請依照下列步驟刪除 Amazon EVS 主機和環境。此動作會刪除在您的 Amazon EVS 環境中執行的 VMware VCF 安裝。

> **Note**
>
> 若要刪除 Amazon EVS 環境，您必須先刪除環境中的所有主機。如果有與環境相關聯的主機，則無法刪除環境。

Example

Amazon EVS console

1. 前往 Amazon EVS 主控台。
2. 在導覽窗格中，選擇環境。
3. 選取包含要刪除之主機的環境。

4. 選取主機索引標籤。
5. 選取主機，然後在主機索引標籤中選擇刪除。對環境中的每個主機重複此步驟。
6. 在環境頁面頂端，選擇刪除，然後選擇刪除環境。

> **Note**
>
> 環境刪除也會刪除您建立的 Amazon EVS. AWS resources 所建立的 Amazon EVS VLAN 子網路和 AWS Secrets Manager 秘密。這些資源可能會繼續產生成本。

7. 如果您已經有不再需要的 Amazon EC2 容量保留，請確定您已取消它們。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的容量保留機群。

AWS CLI

1. 開啟終端機工作階段。
2. 識別包含要刪除之主機的環境。

```
aws evs list-environments
```

以下是範例回應。

```
{
    "environmentSummaries": [
        {
            "environmentId": "env-abcde12345",
            "environmentName": "testEnv",
            "vcfVersion": "VCF-5.2.2",
            "environmentState": "CREATED",
            "createdAt": "2025-04-13T14:42:41.430000+00:00",
            "modifiedAt": "2025-04-13T14:43:33.412000+00:00",
            "environmentArn": "arn:aws:evs:us-east-2:111122223333:environment/env-
abcde12345"
        },
        {
            "environmentId": "env-edcba54321",
            "environmentName": "testEnv2",
            "vcfVersion": "VCF-5.2.2",
            "environmentState": "CREATED",
            "createdAt": "2025-04-13T13:39:49.546000+00:00",
            "modifiedAt": "2025-04-13T13:52:13.342000+00:00",
```

```
            "environmentArn": "arn:aws:evs:us-east-2:111122223333:environment/env-
edcba54321"
        }
    ]
}
```

3. 從環境刪除主機。以下是範例`aws evs delete-environment-host`請求。

> **Note**
>
> 若要能夠刪除環境，您必須先刪除環境中包含的所有主機。

```
aws evs delete-environment-host \
--environment-id env-abcde12345 \
--host esx01
```

4. 重複上述步驟，刪除您環境中剩餘的主機。
5. 刪除環境。

```
aws evs delete-environment --environment-id env-abcde12345
```

> **Note**
>
> 環境刪除也會刪除 Amazon EVS VLAN 子網路和 Amazon EVS 建立的 AWS Secrets Manager 秘密。不會刪除您建立的其他 AWS 資源。這些資源可能會繼續產生成本。

6. 如果您已經有不再需要的 Amazon EC2 容量保留，請確定您已取消它們。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的容量保留機群。

刪除 IPAM 資源（用於 HCX 網際網路連線）

如果您已設定 HCX 網際網路連線，請依照下列步驟刪除 IPAM 資源。

1. 從公有 IPAM 集區發行 EIP 配置。如需詳細資訊，請參閱《VPC IP Address Manager 使用者指南》中的發行配置。
2. 從 IPAM 集區取消佈建公有 IPv4 CIDR。如需詳細資訊，請參閱《VPC IP Address Manager 使用者指南》中的從集區取消佈建 CIDRs。

3. 刪除公有 IPAM 集區。如需詳細資訊，請參閱《VPC IP Address Manager 使用者指南》中的刪除集區。
4. 刪除 IPAM。如需詳細資訊，請參閱《VPC IP Address Manager 使用者指南》中的刪除 IPAM。

刪除 VPC Route Server 元件

如需刪除您建立之 Amazon VPC Route Server 元件的步驟，請參閱《Amazon VPC 使用者指南》中的 Route Server 清除。

刪除網路存取控制清單 (ACL)

如需刪除網路存取控制清單的步驟，請參閱《Amazon VPC 使用者指南》中的刪除 VPC 的網路 ACL。

取消關聯和刪除子網路路由表

如需取消關聯和刪除子網路路由表的步驟，請參閱《Amazon VPC 使用者指南》中的子網路路由表。

刪除子網路

刪除 VPC 子網路，包括服務存取子網路。如需刪除 VPC 子網路的步驟，請參閱《Amazon VPC 使用者指南》中的刪除子網路。

> **Note**
>
> 如果您將 Route 53 用於 DNS，請在嘗試刪除服務存取子網路之前移除傳入端點。否則，您將無法刪除服務存取子網路。

> **Note**
>
> 刪除環境時，Amazon EVS 會代表您刪除 VLAN 子網路。只有在刪除環境時，才能刪除 Amazon EVS VLAN 子網路。

刪除 VPC

如需刪除 VPC 的步驟，請參閱《Amazon VPC 使用者指南》中的刪除您的 VPC。

後續步驟

使用 VMware Hybrid Cloud Extension (VMware HCX) 將工作負載遷移至 Amazon EVS。如需詳細資訊，請參閱移轉。

使用 VMware HCX 將工作負載遷移至 Amazon EVS

部署 Amazon EVS 之後，您可以使用私有或公有網際網路連線來部署 VMware HCX，以便將工作負載遷移至 Amazon EVS。如需詳細資訊，請參閱 VMware HCX 使用者指南中的 VMware HCX 入門。

> **Important**
>
> HCX 網際網路型遷移通常不建議用於：
>
> - 對網路抖動或延遲敏感的應用程式。
> - 時間關鍵 vMotion 操作。
> - 具有嚴格效能需求的大規模遷移。
>
> 對於這些案例，我們建議您使用 HCX 私有連線。相較於以網際網路為基礎的連線，私有專用連線可提供更可靠的效能。

HCX 連線選項

您可以使用具有 AWS Direct Connect 或 Site-to-Site VPN 連線的私有連線，或使用公有連線，將工作負載遷移至 Amazon EVS。

根據您的情況和連線選項，您可能偏好使用公有或私有連線搭配 HCX。例如，某些網站可能有具有更高效能一致性的私有連線，但由於 VPN 加密或有限的連結速度，輸送量較低。同樣地，您可能具有高輸送量的公有網際網路連線，其效能差異更大。透過 Amazon EVS，您可以選擇使用最適合您的連線選項。

下表比較 HCX 私有與公有連線之間的差異。

私有連線	公有連線
概觀	**概觀**
僅使用 VPC 內的私有連線。您可以選擇使用 AWS Direct Connect 或 Site-to-Site VPN 搭配外部網路連線的傳輸閘道。	搭配彈性 IP 地址使用公有網際網路連線，無需專用私有連線即可啟用遷移。

私有連線	公有連線
最適合	最適合
• 時間敏感的 vMotion 操作。 • 大規模遷移。 • 對延遲/抖動敏感的應用程式。 • 大量資料傳輸。 • 具有現有 AWS Direct Connect/AWS Site-to-Site VPN 的組織。	• 沒有 AWS Direct Connect/AWS Site-to-Site VPN 的位置。 • 成本敏感的專案。
主要優點	主要優點
• 一致的低延遲連線。 • 專用頻寬配置。 • 更可靠的網路效能。 • 可針對私有環境停用預設 HCX 加密，以最佳化效能。 • 不需要公有 IP 管理。	• 設定速度比私有連線速度更快。 • 更小的遷移符合成本效益。
重要考量事項	重要考量事項
• 更複雜的初始設定。 • 較高的前期基礎設施成本。 • 較長的實作時間表。 • 任何 HCX 元件沒有直接網際網路連線。	• 更多可變網路效能。 • 頻寬限制是可能的。 • 延遲高於私有連線。 • 每個元件都需要從公有 IPAM 集區配置的專用彈性 IP 地址。 • EIP 關聯可為每個 HCX 元件啟用直接網際網路連線。

HCX 私有連線架構

HCX 私有連線解決方案整合了數個元件：

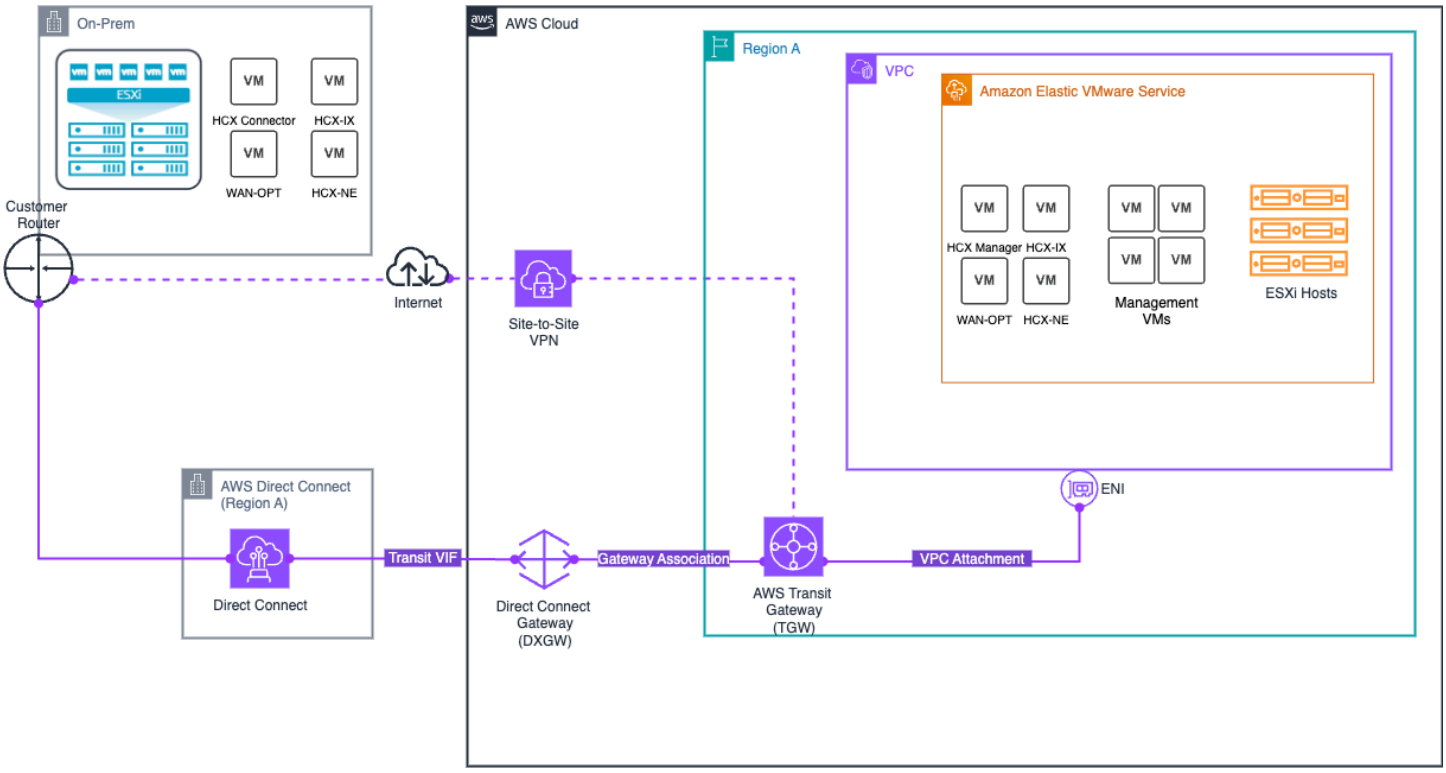
- Amazon EVS 網路元件

- 僅使用私有 VLAN 子網路進行安全通訊，包括私有 HCX VLAN。
- 支援流量控制的網路 ACLs。
- 支援透過私有 VPC 路由伺服器進行路由的動態 BGP 傳播。

- AWS 內部部署連線的受管網路傳輸選項
  - AWS Direct Connect + AWS Transit Gateway 可讓您透過私有專用連線，將內部部署網路連線至 Amazon EVS。如需詳細資訊，請參閱 AWS Direct Connect + AWS Transit Gateway。
  - AWS Site-to-Site VPN + AWS Transit Gateway 提供在遠端網路與透過網際網路的傳輸閘道之間建立 IPsec VPN 連線的選項。如需詳細資訊，請參閱 AWS Transit Gateway + AWS Site-to-Site VPN。

> **Note**
>
> Amazon EVS 不支援透過 AWS Direct Connect 私有虛擬介面 (VIF) 或透過直接終止至底層 VPC AWS Site-to-Site VPN 連線進行連線。

下圖說明 HCX 私有連線架構，示範如何使用 AWS Direct Connect 和 Site-to-Site VPN 搭配傳輸閘道，透過私有專用連線啟用安全工作負載遷移。



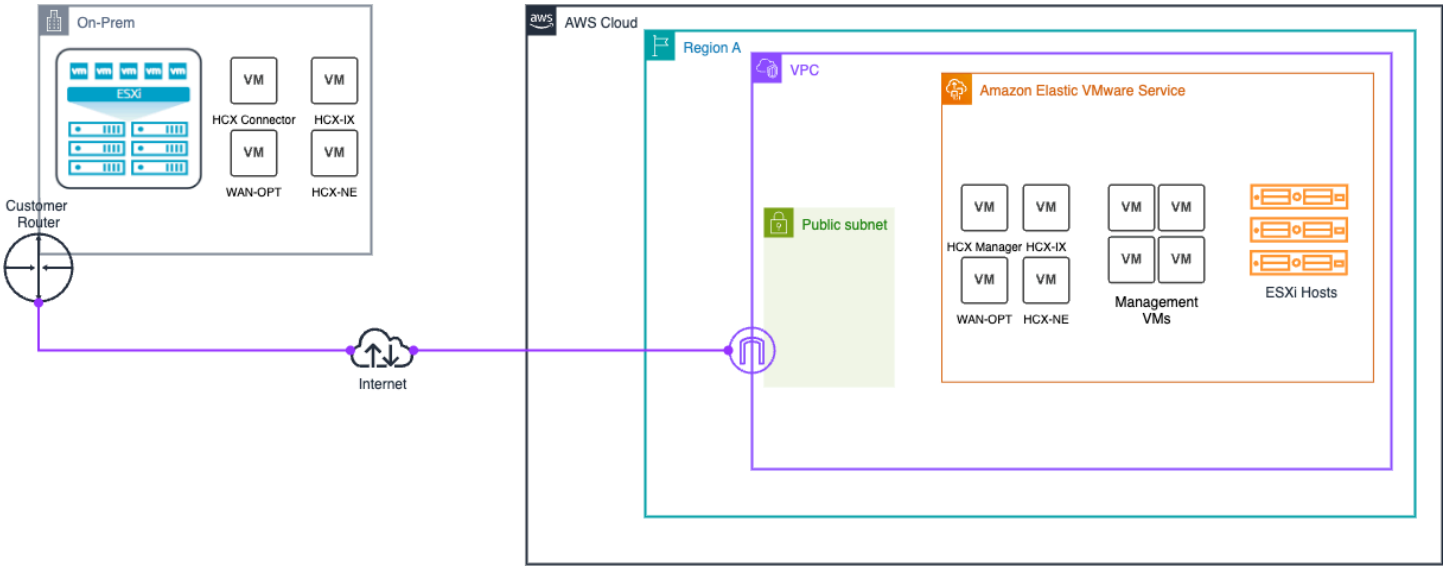
HCX 網際網路連線架構

HCX 網際網路連線解決方案包含數個共同運作的元件：

- Amazon EVS 網路元件
  - 使用隔離的公有 HCX VLAN 子網路來啟用 Amazon EVS 與內部部署 HCX 設備之間的網際網路連線。
  - 支援流量控制的網路 ACLs。
  - 支援透過公有 VPC 路由伺服器進行路由的動態 BGP 傳播。
- IPAM 和公有 IP 管理
  - Amazon VPC IP Address Manager (IPAM) 會從 Amazon 擁有的公有 IPAM 集區管理公有 IPv4 地址配置。
  - 次要 VPC CIDR 區塊 (/28) 從 IPAM 集區配置，建立與主要 VPC CIDR 分開的隔離公有子網路。

如需詳細資訊，請參閱the section called “HCX 公有連線”。

下圖說明 HCX 網際網路連線架構。



HCX 遷移設定

本教學課程說明如何設定 VMware HCX 將工作負載遷移至 Amazon EVS。

先決條件

將 VMware HCX 與 Amazon EVS 搭配使用之前，請確定已符合 HCX 先決條件。如需詳細資訊，請參閱the section called “VMware HCX 先決條件”。

> **Important**
>
> Amazon EVS 對 HCX 公有網際網路連線有獨特的要求。
> 如果您需要 HCX 公有連線，您必須符合下列要求：
>
> - 使用網路遮罩長度下限為 /28 的 CIDR 建立 IPAM 和公有 IPv4 IPAM 集區。
> - 從 IPAM 集區為 HCX Manager 和 HCX Interconnect (HCX-IX) 設備配置至少兩個彈性 IP 地址 (EIPs)。為您需要部署的每個 HCX 網路設備配置額外的彈性 IP 地址。
> - 將公有 IPv4 CIDR 區塊新增為 VPC 的額外 CIDR。
>
> 如需詳細資訊，請參閱the section called “HCX 網際網路連線設定”。

檢查 HCX VLAN 子網路的狀態

系統會為 HCX 建立 VLAN，做為標準 Amazon EVS 部署的一部分。請依照下列步驟檢查 HCX VLAN 子網路是否已正確設定。

Example

Amazon EVS console

1. 前往 Amazon EVS 主控台。
2. 在導覽窗格中，選擇 Environments (環境)。
3. 選取 Amazon EVS 環境。
4. 選取網路和連線索引標籤。
5. 在 VLANs下，識別 HCX VLAN，並檢查狀態是否已建立且公有為 true。

AWS CLI

1. 使用您環境的環境 ID 和包含 資源的區域名稱，執行下列命令。

```
aws evs list-environment-vlans  --region <region-name> --environment-id env-
abcde12345
```

2. 在回應輸出中，識別具有 functionName的 VLAN，hcx並檢查 vlanState是 CREATED且 isPublic 設定為 true。以下是範例回應。

```
{
    "environmentVlans": [{
            "vlanId": 50,
            "cidr": "10.10.4.0/24",
            "availabilityZone": "us-east-2b",
            "functionName": "vTep",
            "subnetId": "subnet-0ce640ac79e7f4dbc",
            "createdAt": "2025-09-09T12:09:37.526000-07:00",
            "modifiedAt": "2025-09-09T12:35:00.596000-07:00",
            "vlanState": "CREATED",
            "stateDetails": "VLAN successfully created",
            "eipAssociations": [],
            "isPublic": false
        },
        {
            "vlanId": 80,
            "cidr": "18.97.141.240/28",
            "availabilityZone": "us-east-2b",
            "functionName": "hcx",
            "subnetId": "subnet-0f080c94782cc74b4",
            "createdAt": "2025-09-09T12:09:37.675000-07:00",
            "modifiedAt": "2025-09-09T12:35:00.359000-07:00",
            "vlanState": "CREATED",
            "stateDetails": "VLAN successfully created",
            "eipAssociations": [{
                    "assocationId": "eipassoc-0be981accbbdf443a",
                    "allocationId": "eipalloc-0cef80396f4a0cc24",
                    "ipAddress": "18.97.141.245"
                },
                {
                    "assocationId": "eipassoc-0d5572f66b7952e9d",
                    "allocationId": "eipalloc-003fc9807d35d1ad3",
                    "ipAddress": "18.97.141.244"
                }
            ],
            "isPublic": true
```

```
        }
    ]
}
```

檢查 HCX VLAN 子網路是否與網路 ACL 相關聯

請依照下列步驟檢查 HCX VLAN 子網路是否與網路 ACL 相關聯。如需網路 ACL 關聯的詳細資訊，請參閱 the section called “建立網路 ACL 以控制 Amazon EVS VLAN 子網路流量”。

> **Important**
>
> 如果您是透過網際網路連線，則將彈性 IP 地址與 VLAN 建立關聯可提供該 VLAN 上所有資源的直接網際網路存取。確保您已設定適當的網路存取控制清單，以根據您的安全需求來限制存取。

> **Important**
>
> EC2 安全群組無法在連接到 Amazon EVS VLAN 子網路的彈性網路介面上運作。若要控制往返 Amazon EVS VLAN 子網路的流量，您必須使用網路存取控制清單 (ACL)。

Example

Amazon VPC console

1. 前往 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Network ACLs (網路 ACL)。
3. 選取與 VLAN 子網路相關聯的網路 ACL。
4. 選取子網路關聯索引標籤。
5. 檢查 HCX VLAN 子網路是否在關聯的子網路中列出。

AWS CLI

1. 使用`Values`篩選條件中的 HCX VLAN 子網路 ID 執行下列命令。

```
aws ec2 describe-network-acls --filters "Name=subnet-id,Values=subnet-
abcdefg9876543210"
```

2. 檢查回應中是否傳回正確的網路 ACL。

檢查 EVS VLAN 子網路是否明確與路由表相關聯

Amazon EVS 要求所有 EVS VLAN 子網路都必須明確與 VPC 中的路由表建立關聯。對於 HCX 網際網路連線，您的 HCX 公有 VLAN 子網路必須與 VPC 中路由至網際網路閘道的公有路由表明確關聯。請依照下列步驟檢查明確的路由表關聯。

Example

Amazon VPC console

1. 前往 VPC 主控台。
2. 在導覽窗格中，選擇 Route tables (路由表)。
3. 選擇應該明確與 EVS VLAN 子網路建立關聯的路由表。
4. 選取子網路關聯索引標籤。
5. 在明確子網路關聯下，檢查是否已列出所有 EVS VLAN 子網路。如果此處未列出 VLAN 子網路，則 VLAN 子網路會隱含地與主路由表相關聯。若要讓 Amazon EVS 正常運作，您必須明確地將所有 VLAN 子網路與路由表建立關聯。對於 HCX 公有 VLAN 子網路，您必須擁有具有網際網路閘道做為目標的相關聯公有路由表。若要解決此問題，請選擇編輯子網路關聯 （ 並新增遺失的 VLAN 子網路 ）。

AWS CLI

1. 開啟終端機工作階段。
2. 執行下列範例命令來擷取所有 EVS VLAN 子網路的詳細資訊，包括路由表關聯。如果此處未列出 VLAN 子網路，則 VLAN 子網路會隱含地與主路由表相關聯。若要讓 Amazon EVS 正常運作，您必須明確地將所有 VLAN 子網路與路由表建立關聯。對於 HCX 公有 VLAN 子網路，您必須擁有具有網際網路閘道做為目標的相關聯公有路由表。

```
aws ec2 describe-subnets
```

3. 明確地將 EVS VLAN 子網路與 VPC 中的路由表建立關聯。以下是範例命令。

```
aws ec2 associate-route-table \
--route-table-id rtb-0123456789abcdef0 \
--subnet-id subnet-01234a1b2cde1234f
```

（對於 HCX 網際網路連線）檢查 EIPs是否與 HCX VLAN 子網路相關聯

對於您部署的每個 HCX 網路設備，您必須擁有與 HCX 公有 VLAN 子網路相關聯的 IPAM 集區中的 EIP。您必須為 HCX Manager 和 HCX Interconnect (HCX-IX) 設備建立至少兩個 EIPs 與 HCX 公有 VLAN 子網路的關聯。請依照下列步驟檢查是否存在必要的 EIP 關聯。

Important

如果您未從 IPAM 集區將至少兩個 EIPs 與 HCX 公有 VLAN 子網路建立關聯，HCX 公有網際網路連線會失敗。

Note

您無法將公有 IPAM CIDR 區塊的前兩個 EIPs 或最後一個 EIP 與 VLAN 子網路建立關聯。這些 EIPs會保留為網路、預設閘道和廣播地址。如果您嘗試將這些 EIPs與 VLAN 子網路建立關聯，Amazon EVS 會擲回驗證錯誤。

Example

Amazon EVS console

1. 前往 Amazon EVS 主控台。
2. 在導覽功能表中，選擇環境。
3. 選取環境。
4. 在網路和連線索引標籤下，選取 HCX 公有 VLAN。
5. 檢查 EIP 關聯索引標籤，確認 EIPs已與 HCX 公有 VLAN 建立關聯。

AWS CLI

1. 若要檢查哪些 EIPs 與 HCX VLAN 子網路相關聯，請使用 `list-environment-vlans`命令。對於 `environment-id`，請針對包含 HCX VLAN 的 EVS 環境使用唯一的 ID。

```
aws evs list-environment-vlans \
  --environment-id "env-605uove256" \
```

命令會傳回 VLAN VLANs 的詳細資訊，包括 EIP 關聯：

```
{
  "environmentVlans": [
    {
      "vlanId": 80,
      "cidr": "18.97.137.0/28",
      "availabilityZone": "us-east-2c",
      "functionName": "hcx",
      "subnetId": "subnet-02f9a4ee9e1208cfc",
      "createdAt": "2025-08-26T22:15:00.200000+00:00",
      "modifiedAt": "2025-08-26T22:20:28.155000+00:00",
      "vlanState": "CREATED",
      "stateDetails": "VLAN successfully created",
      "eipAssociations": [
        {
          "associationId": "eipassoc-09876543210abcdef",
          "allocationId": "eipalloc-0123456789abcdef0",
          "ipAddress": "18.97.137.3"
        },
        {
          "associationId": "eipassoc-12345678901abcdef",
          "allocationId": "eipalloc-1234567890abcdef1",
          "ipAddress": "18.97.137.4"
        },
        {
          "associationId": "eipassoc-23456789012abcdef",
          "allocationId": "eipalloc-2345678901abcdef2",
          "ipAddress": "18.97.137.5"
        }
      ],
      "isPublic": true,
      "networkAclId": "acl-0123456789abcdef0"
    },
```

```
    ...
  ]
}
```

`eipAssociations` 陣列會顯示 EIP 關聯，包括：

- `associationId` - 此 EIP 關聯的唯一 ID。
- `allocationId` - 相關聯彈性 IP 地址的配置 ID。
- `ipAddress` - 指派給 VLAN 的 IP 地址。

使用 HCX 公有上行 VLAN ID 建立分散式連接埠群組

前往 vSphere 用戶端界面，並依照新增分散式連接埠群組中的步驟，將分散式連接埠群組新增至 vSphere 分散式交換器。

在 vSphere 用戶端界面內設定容錯回復時，請確定 uplink1 是作用中上行連結，而 uplink2 是待命上行連結，以啟用作用中/待命容錯移轉。針對 vSphere Client 介面中的 VLAN 設定，輸入您先前識別的 HCX VLAN ID。

（選用）設定 HCX WAN 最佳化

> **Note**
>
> HCX 4.11.3 不再提供 WAN 最佳化功能。如需詳細資訊，請參閱 HCX 4.11.3 版本備註。

HCX WAN 最佳化服務 (HCX-WO) 透過套用資料縮減和 WAN 路徑調節等 WAN 最佳化技術，改善私有線路或網際網路路徑的效能特性。對於無法專用 10Gbit 路徑進行遷移的部署，建議使用 HCX WAN 最佳化服務。在 10Gbit 中，使用 WAN 最佳化的低延遲部署可能無法改善遷移效能。如需詳細資訊，請參閱 VMware HCX 部署考量事項和最佳實務。

HCX WAN 最佳化服務會與 HCX WAN Interconnect 服務設備 (HCX-IX) 一起部署。HCX-IX 負責企業環境與 Amazon EVS 環境之間的資料複寫。

若要搭配 Amazon EVS 使用 HCX WAN 最佳化服務，您需要在 HCX VLAN 子網路上使用分散式連接埠群組。使用先前步驟中建立的分散式連接埠群組。

（選用）啟用 HCX 行動性最佳化網路

HCX Mobility Optimized Networking (MON) 是 HCX Network Extension Service 的一項功能。啟用 MON 的網路擴充功能可在 Amazon EVS 環境中啟用選擇性路由，藉此改善遷移虛擬機器的流量流程。MON 可讓您在延伸第 2 層網路時，設定將工作負載流量遷移至 Amazon EVS 的最佳路徑，避免經過來源閘道的長往返網路路徑。此功能適用於所有 Amazon EVS 部署。如需詳細資訊，請參閱 VMware HCX 使用者指南中的設定行動最佳化網路。

Important

啟用 HCX MON 之前，請閱讀下列限制和不支援的 HCX 網路延伸組態。
網路延伸模組的限制和條件
行動最佳化網路拓撲的限制

Important

啟用 HCX MON 之前，請確定您已在 NSX 界面中設定目的地網路 CIDR 的路由重新分佈。如需詳細資訊，請參閱 VMware NSX 文件中的設定 BGP 和路由重新分佈。

驗證 HCX 連線

VMware HCX 包含內建診斷工具，可用於測試連線能力。如需詳細資訊，請參閱《VMware HCX 使用者指南》中的 VMware HCX 故障診斷。 VMware

設定 HCX 公有網際網路連線

您可以將彈性 IP 地址與 VLAN 建立關聯，以設定 HCX 公有 VLAN 的公有網際網路存取。這可為需要網際網路存取以進行遷移操作的 VMware HCX 設備和工作負載啟用直接網際網路連線。

相關主題

本主題涵蓋管理 HCX 公有 VLAN 的網際網路存取。如需完整實作：

1. 完成 中的先決條件設定 Amazon Elastic VMware Service。
2. 在 中設定初始設定開始使用。
3. 設定網際網路存取 （本主題）。

關於 HCX VLAN 網際網路存取

您可以為 VMware HCX 設備設定網際網路存取，讓您透過網際網路將工作負載執行 HCX 遷移至 Amazon EVS。

此方法：

- 啟用虛擬機器遷移，而不需要專用私有連線。
- 提供彈性且符合成本效益的遷移解決方案。

> **Important**
>
> HCX 網際網路型遷移通常不建議用於：
>
> - 對網路抖動或延遲敏感的應用程式。
> - 時間關鍵 vMotion 操作。
> - 具有嚴格效能需求的大規模遷移。
>
> 對於這些案例，我們建議使用 HCX 私有連線。相較於以網際網路為基礎的連線，私有專用連線可提供更可靠的效能。

網際網路連線概觀

檢閱下列考量事項。

HCX 網路需求和 DNAT

HCX 有特定的聯網限制，會影響您設定公有網際網路存取的方式。

HCX 不支援目的地網路地址轉譯 (DNAT)。相反地，HCX 要求上行網路可使用預設閘道 IP 地址進行路由。

Amazon EVS VLAN 子網路包含與其他 VPC 子網路相同的預設閘道 IP 地址。不過，即使您在 RFC1918 地址範圍之外使用 CIDR 區塊，這些子網路一律是私有子網路。

啟用 HCX 網際網路連線

若要啟用沒有 DNAT 的網際網路連線，Amazon EVS 會使用特定的 CIDR 組態方法：

- 網際網路可路由 CIDR 需求：Amazon EVS 需要符合 HCX VLAN 子網路 CIDR 的網際網路可路由 CIDR。
- IPAM 配置：Amazon EVS 使用 IPAM 配置的公有 CIDR，網路遮罩長度下限為 /28，做為網際網路可路由 CIDR。
- VPC 組態：您必須手動將公有 IPAM 配置 CIDR 新增至 VPC，做為次要 VPC CIDR。
- VLAN 子網路部署：設定 IPAM 和 VPC 之後，您可以在 Amazon EVS 部署期間，在 HCX VLAN 子網路中使用公有 IPAM 配置 CIDR。
- 彈性 IP 組態：Amazon EVS 需要下列組態：
  - 配置彈性 IPs：您可以從 IPAM 配置的 CIDR 配置彈性 IPs。您必須從 IPAM 集區為 HCX Manager 和 HCX Interconnect (HCX-IX) 設備配置至少兩個彈性 IP 地址 (EIPs)。為您需要部署的每個 HCX 網路設備配置額外的彈性 IP 地址。
  - 與 VLAN 建立關聯：您可以將要與 HCX 設備搭配使用的每個彈性 IP 與 HCX VLAN 子網路建立關聯。使用 Amazon EVS 主控台或 AWS CLI 進行此關聯。
  - 設定閘道地址：來自 CIDR 的第一個可用地址會成為您在 HCX 設備中設定的閘道地址。
  - 流量路由：每個相關聯彈性 IP 的流量會直接路由至具有相同 IP 地址的目的地 HCX 設備，而不含 DNAT。

如需使用 Amazon EVS 環境部署的網際網路連線設定 HCX 的步驟，請參閱 設定 Amazon Elastic VMware Service和 開始使用。

操作考量

- HCX 公有 VLAN CIDR 區塊必須具有 /28 網路遮罩長度。
- 使用 Amazon EVS 主控台或 進行部署後，EIPs 可以與 HCX 公有 VLAN 建立關聯或取消關聯 AWS CLI，但必須來自相同的 IPAM 集區。
- 每個 EIP 關聯都有自己的唯一關聯 ID。
- 您最多可以從與 /28 HCX 公有 VLAN 相關聯的公有 IPAM 集區中擁有 13 EIPs。您無法將公有 IPAM 配置 CIDR 區塊的前兩個 EIPs 或最後一個 EIP 與 HCX 公有 VLAN 子網路建立關聯。這些 EIPs會保留為網路、預設閘道和廣播地址。如果您嘗試將這些 EIPs 與 VLAN 建立關聯，Amazon EVS 會擲回驗證錯誤。

安全考量

- 網路存取控制清單 (ACLs) 仍然適用於流經 HCX 公有 VLAN 子網路的流量。

- 安全群組規則不適用於 HCX 公有 VLAN 子網路上的流量。使用網路 ACLs進行流量控制。

> **Important**
>
> 如果您是透過網際網路連線，則將彈性 IP 地址與 VLAN 建立關聯可提供該 VLAN 上所有資源的直接網際網路存取。確保您已設定適當的網路存取控制清單，以根據您的安全需求來限制存取。

管理 VLANs的彈性 IP 地址

您可以使用 Amazon EVS 主控台或 ，將彈性 IP 地址與 HCX 公有 VLAN 建立關聯和取消關聯 AWS CLI。

> **Note**
>
> Amazon EVS 目前僅支援將彈性 IP 地址與 HCX 公有 VLAN 建立關聯和取消關聯。

將彈性 IP 地址與 VLAN 建立關聯

先決條件

請確定您有下列項目：

- 彈性 IP 地址是從 Amazon 擁有的公有 IPAM 集區配置。
- Amazon EVS 環境已建立。

Example

Amazon EVS console

1. 前往 Amazon EVS 主控台。
2. 在導覽功能表中，選擇環境。
3. 選取環境。
4. 在網路和連線索引標籤下，選取 HCX 公有 VLAN。

> **Note**
>
> Amazon EVS 目前僅支援將 EIPs 與 HCX VLAN 建立關聯。

5. 選擇將 EIP 與 VLAN 建立關聯。
6. 選取要與 HCX 公有 VLAN 建立關聯的彈性 IP 地址 （ 多個 ）。
7. 選擇關聯 EIPs。您最多可以有 13 EIPs。

> **Note**
>
> 您無法將公有 IPAM CIDR 區塊的前兩個 EIPs 與 VLAN 子網路建立關聯。這些 EIPs會保留為網路和預設閘道地址。

8. 檢查 EIP 關聯以確認 EIPs已與 HCX 公有 VLAN 建立關聯。

AWS CLI

1. 若要將彈性 IP 地址與 VLAN 建立關聯，請使用範例`associate-eip-to-vlan`命令。
   - `environment-id` - Amazon EVS 環境的 ID。
   - `vlan-name` - 必須是 `hcx`。Amazon EVS 目前僅支援與 HCX VLAN 的 EIP 關聯。
   - `allocation-id` - 彈性 IP 地址的配置 ID。

   ```
   aws evs associate-eip-to-vlan \
     --environment-id "env-605uove256" \
     --vlan-name "hcx" \
     --allocation-id "eipalloc-0429268f30c4a34f7"
   ```

   命令會傳回有關 VLAN 的詳細資訊，包括新的 EIP 關聯：

   ```
   {
       "vlan": {
           "vlanId": 80,
           "cidr": "18.97.137.0/28",
           "availabilityZone": "us-east-2c",
           "functionName": "hcx",
           "subnetId": "subnet-02f9a4ee9e1208cfc",
           "createdAt": "2025-08-22T23:42:16.200000+00:00",
   ```

```
        "modifiedAt": "2025-08-23T13:42:28.155000+00:00",
        "vlanState": "CREATED",
        "stateDetails": "VLAN successfully created",
        "eipAssociations": [
            {
                "associationId": "eipassoc-09e966faad7ecc58a",
                "allocationId": "eipalloc-0429268f30c4a34f7",
                "ipAddress": "18.97.137.2"
            }
        ],
        "isPublic": true,
        "networkAclId": "acl-02fa8ab4ad3ddfb00"
    }
}
```


`eipAssociations` 陣列會顯示新的關聯，包括：

- `associationId` - 此 EIP 關聯的唯一 ID，用於取消關聯。
- `allocationId` - 相關聯彈性 IP 地址的配置 ID。
- `ipAddress` - 指派給 VLAN 的 IP 地址。

2. 重複此步驟來建立其他 EIPs關聯。您最多可以有 13 EIPs。

取消彈性 IP 地址與 VLAN 的關聯

先決條件

請確定您有下列項目：

- Amazon EVS 環境已建立。
- EIP 與 Amazon EVS 環境相關聯。

Example

Amazon EVS console

1. 前往 Amazon EVS 主控台。
2. 在導覽功能表中，選擇環境。
3. 選取環境。
4. 在網路和連線索引標籤下，選取 HCX 公有 VLAN。

5. 選擇取消 EIP 與 VLAN 的關聯。
6. 選取要與 HCX 公有 VLAN 取消關聯的彈性 IP 地址 （多個）。

> **Important**
> 取消 EIPs的關聯可能會導致使用公有 VLAN 子網路之設備的網際網路連線中斷。

7. 選擇取消關聯 EIPs。
8. 檢查 EIP 關聯以確認 EIPs已與 HCX 公有 VLAN 取消關聯。

AWS CLI

若要取消彈性 IP 地址與 VLAN 的關聯，請使用範例`disassociate-eip-from-vlan`命令。

- `environment-id` - Amazon EVS 環境的 ID。
- `vlan-name` - 必須是 `hcx`。Amazon EVS 目前僅支援與 HCX VLAN 的 EIP 關聯。
- `association-id` - 要移除之 EIP 關聯的關聯 ID。

> **Important**
> 取消 EIPs的關聯可能會導致使用公有 VLAN 子網路之設備的網際網路連線中斷。

```
aws evs disassociate-eip-from-vlan \
  --environment-id "env-605uove256" \
  --vlan-name "hcx" \
  --association-id "eipassoc-09e966faad7ecc58a"
```

命令會傳回移除 EIP 關聯的 VLAN 詳細資訊：

```
{
    "vlan": {
        "vlanId": 80,
        "cidr": "18.97.137.0/28",
        "availabilityZone": "us-east-2c",
        "functionName": "hcx",
        "subnetId": "subnet-02f9a4ee9e1208cfc",
        "createdAt": "2025-08-22T23:42:16.200000+00:00",
```

```
        "modifiedAt": "2025-08-23T13:48:49.846000+00:00",
        "vlanState": "CREATED",
        "stateDetails": "VLAN successfully created",
        "eipAssociations": [],
        "isPublic": true,
        "networkAclId": "acl-02fa8ab4ad3ddfb00"
    }
}
```

空`eipAssociations`陣列會確認彈性 IP 地址已成功與 VLAN 取消關聯。

關於網際網路型遷移的 HCX WAN 最佳化

> **Note**
>
> HCX 4.11.3 不再提供 WAN 最佳化功能。如需詳細資訊，請參閱 HCX 4.11.3 版本備註。

透過網際網路執行遷移時，HCX WAN 最佳化 (HCX-WO) 可以改善遷移效能。此服務可與 HCX Interconnect 設備 (HCX-IX) 搭配使用，以：

- 套用資料縮減技術，將頻寬使用量降至最低。
- 實作 WAN 路徑調節以最佳化網路效能。
- 透過高延遲網際網路連線改善遷移速度。
- 增強網際網路型遷移的可靠性。

HCX WAN 最佳化特別適用於網際網路型遷移，其中：

- 網路延遲可能高於私有連線選項。
- 可用的頻寬可能有限或可變。
- 網路條件可能會因網際網路流量模式而波動。

如需設定網際網路連線後設定 HCX WAN 最佳化的詳細說明，請參閱 the section called “（選用）設定 HCX WAN 最佳化”。

> **Note**
>
> 雖然 WAN 最佳化可以大幅改善網際網路型遷移效能，但在具有專用 10Gbit 低延遲連線的環境中，可能無法提供額外的優勢。在決定是否啟用此功能時，請考慮您的網路特性。

管理 Amazon EVS 環境

本章包含下列主題，可協助您管理環境。

- the section called “VCF 訂閱” - 說明 VCF 訂閱如何與 Amazon EVS 搭配運作，以及 VCF 訂閱管理的客戶責任。
- the section called “VCF 版本和 EC2 執行個體” - 描述支援的 VCF 和 ESX 版本，以及如何檢查 Amazon EVS 中的版本可用性。
- the section called “生命週期管理” - 描述 Amazon EVS 環境中的生命週期管理責任，包括基礎基礎設施管理、VCF 升級管理、ESX 主機生命週期管理。
- the section called “環境維護” - 說明如何執行 Amazon EVS 環境的常見維護任務，包括聯網組態、ESX 主機維護、檢查環境狀態，以及管理 VCF 憑證的秘密輪換排程。
- the section called “建立主機” - 說明如何在環境部署後建立 Amazon EVS 主機，並將主機新增至叢集。
- the section called “刪除主機” - 說明如何刪除 Amazon EVS 主機並將其從叢集中移除。

VCF 訂閱

> **Note**
>
> Amazon EVS 不支援永久 vSphere 授權。您必須擁有有效且作用中的 VMware Cloud Foundation 訂閱，才能使用 Amazon EVS。

Amazon EVS 使用 VMware Cloud Foundation (VCF) 訂閱，具有您帶到 AWS (BYOS) 的授權可移轉權利。若要成功部署 Amazon EVS 環境，您需要在環境建立請求中提供有效的 VCF 解決方案金鑰和 vSAN 授權金鑰。vSphere 授權金鑰做為 VCF 的解決方案金鑰。每個 VCF 授權金鑰只能用於一個 Amazon EVS 環境。如果您嘗試使用已在另一個環境中使用的 VCF 授權金鑰，環境建立會失敗。

您的 VCF 解決方案金鑰必須至少有 256 個核心，才能為 Amazon EVS 在環境建立時部署的四個初始 EC2 i4i.metal 主機提供足夠的核心容量。每個 i4i.metal 主機都需要 64 個核心。vSAN 授權金鑰必須至少有 110 TiB 的 vSAN 容量。如果您嘗試使用規模過小的授權金鑰，環境建立會失敗。

> **Note**
>
> 您的 VCF 訂閱將可供所有 AWS 區域的 Amazon EVS 使用，以符合授權規範。Amazon EVS 不會驗證授權金鑰。若要驗證授權金鑰，請造訪 Broadcom 支援。

> **Note**
>
> Amazon EVS 中 VCF 軟體的相關資訊將與 Broadcom 共用，以驗證授權合規性。

訂閱管理

您負責管理您的 VCF 訂閱。您的 VCF 訂閱必須在 SDDC Manager 中管理。從 SDDC Manager 移除您的授權金鑰或以使用中的授權金鑰取代它們會導致環境狀態檢查失敗，讓您無法將主機新增至 Amazon EVS 環境。如需環境狀態檢查和 the section called “監控環境狀態” 的詳細資訊the section called “故障診斷失敗的環境狀態檢查”。如需 VCF 授權金鑰的詳細資訊，請參閱 VMware Cloud Foundation 文件中的管理 VMware Cloud Foundation 中的授權金鑰。 VMware

> **Important**
>
> 使用 SDDC Manager 使用者介面來管理 VCF 解決方案和 vSAN 授權金鑰。Amazon EVS 會要求您在 SDDC Manager 中維護有效的 VCF 解決方案和 vSAN 授權金鑰，服務才能正常運作。雖然金鑰必須使用 vSphere 用戶端指派給主機和 vSAN 叢集，但您必須確定這些金鑰也會出現在 SDDC Manager 使用者介面的授權畫面中。

新增 VCF 授權金鑰

在 Broadcom 支援入口網站中，您可以購買其他 VCF 授權金鑰，如果您已有大型金鑰，您可以分割授權金鑰，或合併多個授權金鑰。這可讓您授權在初始部署後新增至環境的主機，或授權其他環境。確定已購買的授權金鑰已新增至 vCenter Sever 和 SDDC Manager 庫存中。如果新增主機，請確定您的授權已指派給 vSphere 中的正確主機，且有足夠的核心和 vSAN 儲存容量。Amazon EVS 不支援未授權的主機。如需詳細資訊，請參閱 VMware 文件中的在 vSphere 用戶端中設定資產的授權設定。

新的未過期授權金鑰必須在授權金鑰的評估期間到期之前指派給 vCenter Server，才能保持作用中狀態。成功設定 Amazon EVS 環境需要作用中的授權金鑰。如果提供過期的授權金鑰，您的環境將無法

部署。如需 VCF 授權金鑰建立的詳細資訊，請參閱 VMware 文件中的建立新的授權。如果您新增的授權金鑰發生問題，請參閱 the section called “金鑰涵蓋範圍檢查失敗”。

移除 VCF 授權金鑰

您可以從 SDDC Manager 庫存中移除 VCF 授權金鑰，以便在刪除環境中的主機後減少核心和 vSAN 容量。若要保持符合您與 vSphere 搭配使用之產品的授權模式，您必須從庫存中移除所有未指派的授權金鑰。如果您在 Broadcom Support Portal 中擁有分割、合併或升級的授權金鑰，則必須移除舊的授權金鑰。如需詳細資訊，請參閱 VMware 文件中的移除授權。

Amazon EVS 提供的 VCF 版本和 EC2 執行個體類型

Amazon EVS 提供多個版本的 VMware Cloud Foundation (VCF)、ESX 和 EC2 執行個體類型，您可以在建立環境和建立主機時加以選取。

檢查提供的 VCF 版本、ESX 版本和 EC2 執行個體類型

AWS 主控台會在建立環境精靈中顯示 Amazon EVS 提供的 VCF 版本清單。當您選取執行個體類型，同時將主機新增至現有環境時，即可看見可用的 ESX 版本。您也可以使用 CLI 檢視 VCF 版本、ESX 版本和 EC2 執行個體類型。

Example

Amazon EVS console

1. 前往 Amazon EVS 主控台。
2. 在導覽功能表中，選擇環境。
3. 執行以下任意一項：

   若要檢查 VCF 版本：

   a. 選取建立環境。

   b. 在驗證 Amazon EVS 要求下，選擇您的 VCF 版本，以查看狀態是否可用或受到限制。

   若要檢查 ESX 版本：

   a. 選取現有的環境。

   b. 選擇 Create host (建立主機)。

   c. 選取執行個體類型以查看可用的 ESX 版本。

AWS CLI

執行下列命令來擷取 VCF 和 ESX 版本的相關資訊：

```
aws evs get-versions --region <region-name>
```

回應範例：

```
{
   "instanceTypeEsxVersions": [
      {
         "esxVersions": [ "ESXi-8.0U3b-24280767","ESXi-8.0U3g-24859861" ],
         "instanceType": "i4i.metal"
      }
   ],
   "vcfVersions": [
      {
            "vcfVersion": "VCF-5.2.1",
            "status": "RESTRICTED",
            "defaultEsxVersion": "ESXi-8.0U3b-24280767",
            "instanceTypes": ["i4i.metal"]
      },
      {
            "vcfVersion": "VCF-5.2.2",
            "status": "AVAILABLE",
            "defaultEsxVersion": "ESXi-8.0U3g-24859861",
            "instanceTypes": ["i4i.metal"]
      }
   ]
}
```

> **Note**
>
> 如果您需要的版本顯示 RESTRICTED，且您有特定需求，請參閱 以取得如何存取該版本the section called “請求存取受限的 VCF 版本”的詳細資訊。

Amazon EVS 中的目前 VCF 版本

Amazon EVS 目前提供下列 VCF 版本來建立環境：

VCF 版本	預設 ESX 版本	狀態	EC2 執行個體類型
VCF-5.2.2	ESXi-8.0U3g-24859861	AVAILABLE	i4i.metal
VCF-5.2.1	ESXi-8.0U3b-24280767	受限	i4i.metal

> **Note**
>
> 建立新的 Amazon EVS 環境時，您必須指定 VCF 版本。

ESX 版本考量事項

每個 VCF 版本都有以 Broadcom VCF 物料清單 (BOM) 為基礎的預設 ESX 版本。建立新環境時，您無法選擇特定的 ESX 版本。會自動套用所選 VCF 版本的預設 ESX 版本。

不過，將主機新增至環境時，您可以為所選執行個體類型選取可用的 ESX 版本。如果您未指定版本，Amazon EVS 會使用與您環境 VCF 版本相關聯的預設 ESX 版本。

新增主機之後，只能使用 vCenter Lifecycle Manager 升級其 ESX 版本。

> **Note**
>
> Amazon EVS 不提供由 Broadcom 發行的所有 VCF 和 ESX 版本。如需軟體互通性資訊，請參閱 Broadcom 互通性矩陣。如需與 AWS EC2 執行個體的完整硬體相容性，請參閱《Broadcom 相容性指南》。

請求存取受限的 VCF 版本

如果您需要存取`RESTRICTED`狀態為 的 VCF 版本，請聯絡 AWS Support 並提供下列資訊：

- AWS 您的帳戶 ID
- AWS 區域
- 您需要的特定 VCF 版本

- 您的使用案例和業務理由 （例如安全/合規、相容性/相依性等）

AWS 支援會檢閱您的請求，並核准或請求其他資訊。核准後，版本狀態會在 AWS 主控台或 `get-versions` API 回應`AVAILABLE`中變更為 。

Amazon EVS 環境生命週期管理

此頁面說明您在 Amazon EVS 環境中的生命週期管理責任。

Amazon EVS 的主要優點是您可以完全控制雲端中的 VMware 架構。您可以最佳化 VMware Cloud Foundation (VCF) 軟體堆疊，以滿足應用程式的獨特需求。由於 Amazon EVS 是自我管理的服務，因此您必須負責 Amazon EVS 環境中所用 VMware 軟體的生命週期管理和維護，例如 ESX、vSphere、vSAN、NSX 和 SDDC Manager。您也必須負責維護任何第三方整合，例如整合到 Amazon EVS 主機的資料保護解決方案。

您必須負責 Amazon EVS 使用的基礎 AWS 網路元件組態，包括 VPC 路由表、安全群組和網路存取控制清單 (ACL) 規則、VPC Route Server 組態、網際網路閘道、NAT 閘道和傳輸閘道 （用於內部部署連線）。

AWS 負責使用您提供的聯網組態來部署 Amazon EVS 環境。環境部署包括下列項目：

- 引導 Amazon EVS 環境的網路組態。
- 使用您提供的 VPC Route Server 執行個體啟用南北路由。
- 部署所需的 EVS VLAN 子網路、彈性網路介面和四個初始 ESX 主機。
- 使用 Tier-0 閘道和 Tier-1 閘道設定 NSX 覆蓋網路。
- 在作用中/待命模式下部署具有兩個 NSX Edge 節點的 NSX Edge 叢集。
- 建立和設定初始 vSAN 叢集並掛載資料存放區。

您必須負責 VMware NSX 組態，包括網路區段、分散式防火牆規則和負載平衡器。您也需要負責在部署 EVS 環境後，使用 Amazon EVS 實作的任何整合解決方案的組態，包括 VMware HCX 組態和其他 NSX Tier-1 閘道。

如需 AWS 和客戶責任的詳細資訊，請參閱AWS 共同責任模型。

> **Note**
>
> 在 Amazon EVS 環境部署中，會建立和設定 Tier-0 閘道和 Tier-1 閘道。Amazon EVS 目前僅支援單一 Tier-0 閘道。這些邏輯路由器或 NSX 節點 VMs 的任何修改都可能會影響連線能力，因此應避免。

VMware 軟體更新

> **Warning**
>
> 如果您在 Amazon EVS 環境部署之後已更新 ESX 版本，則 SDDC 管理員可能會在委託主機步驟中的 VCF 主機驗證期間失敗。如需疑難排解此問題的步驟，請參閱 the section called “SDDC Manager 在主機測試期間未通過 VCF 主機驗證”。

如需 Amazon EVS 提供的 VCF 版本的相關資訊，請參閱 the section called “VCF 版本和 EC2 執行個體”。根據AWS 共同責任模型，您有責任在 EVS 環境中套用 VCF 軟體的任何修補程式、更新或升級，包括 ESX、vCenter Server、vSAN、NSX、SDDC Manager 和其他整合解決方案。部署後，我們建議您檢閱 Amazon EVS 部署的 VCF 軟體版本，並視需要更新。您可以透過 Broadcom 支援入口網站取得 VCF 更新。我們也建議您建立並遵守更新和修補程式的定期維護排程。

> **Note**
>
> Amazon EVS 目前不支援 VMware Cloud Foundation 9。

> **Note**
>
> Amazon EVS 不提供由 Broadcom 發行的所有 VCF 和 ESX 版本。如需軟體互通性資訊，請參閱 Broadcom 互通性矩陣。如需與 AWS EC2 執行個體的完整硬體相容性，請參閱《Broadcom 相容性指南》。

某些修補程式、更新或升級可能會影響您環境中執行的工作負載。在修補、更新或升級 VCF 軟體之前，建議您檢閱 VCF 生命週期管理指南，以了解這些變更將如何影響您的環境。我們也建議您在部署到生產環境之前，先在預備環境中測試變更。您可以檢閱 VCF 5.2.x 版本備註，以了解最新的 VCF 5.2.x 更新。

ESX 主機生命週期和維護

您負責 Amazon EVS 環境中的 ESX 主機生命週期管理和維護，包括監控主機運作狀態和修復主機問題。如需詳細資訊，請參閱the section called “環境維護”。

AWS 對基礎 i4i.metal EC2 執行個體執行排程維護，以確保基礎設施的可靠性、可用性和效能。如需詳細資訊，請參閱the section called “關於 EC2 執行個體的 AWS 排程維護”。

在您的環境中執行維護

本節說明如何執行 Amazon EVS 環境的常見維護任務。

主題

- 監控您環境的狀態和資源
- AMI 維護
- Amazon EVS 主機維護
- 設定 Amazon EVS 子網路的自訂路由表
- 設定網路存取控制清單以控制 Amazon EVS VLAN 子網路流量
- 秘密管理生命週期

監控您環境的狀態和資源

您可以使用 Amazon EVS 主控台或 監控 Amazon EVS 環境和基礎 AWS 資源的各個層面 AWS CLI。

> **Note**
>
> VMware Cloud Foundation (VCF) 元件會在 SDDC Manager 中監控。您無法使用 Amazon EVS 主控台或 監控 VCF 元件 AWS CLI。如需有關使用 SDDC Manager 監控 VMware Cloud Foundation (VCF) 元件的資訊，請參閱 SDDC Manager 入門。

檢視環境狀態和資源

環境狀態可協助您判斷您的環境是否遇到需要注意的問題。請依照此程序檢查您環境的狀態，並檢視基礎資源。

Example

Amazon EVS console

1. 開啟 Amazon EVS 主控台。
2. 在導覽窗格中，選擇 Environments (環境)。
3. 選擇您的環境 ID 以開啟環境詳細資訊頁面。
4. 在詳細資訊下，檢視環境狀態。

   如果您的環境運作狀態良好，狀態會顯示為已通過。如果發生問題，狀態會顯示為失敗。當狀態為失敗時，您可以檢視顯示四個環境狀態檢查結果的快顯視窗：

   - 金鑰重複使用 - 顯示通過或失敗，以指出 VCF 授權金鑰是否有效。
   - 主機計數 - 顯示不明、已通過或失敗，以指出主機連線的狀態。
   - 金鑰涵蓋範圍 - 顯示通過或失敗，以指出 VCF 授權金鑰是否涵蓋所有主機。
   - 可連線性 - 顯示已通過或失敗，表示可連線至 SDDC Manager。

     如需有關對環境狀態檢查失敗進行故障診斷的資訊，請參閱 疑難排解。

     檢視您環境中的資源

     選擇下列其中一個索引標籤：

   - 主機 - 顯示您環境中的主機。
   - 網路與連線 - 顯示與您環境相關聯的 VPC、EVS 子網路和 VPC Route Server 資源。
   - 管理設備 - 顯示您環境中的 VCF 管理設備及其 DNS 主機名稱和相關登入資料。
   - 標籤 - 顯示與您的環境相關聯的標籤。

AWS CLI

您可以使用 AWS CLI 來檢查您的環境狀態和資源。

列出所有環境及其狀態

```
aws evs list-environments
```

> **Tip**
>
> 使用 `--query` 參數篩選輸出。例如：

```
aws evs list-environments --query 'Environments[*].[EnvironmentId,Status]'
```

列出環境主機

```
aws evs list-environment-hosts \
    --environment-id environment-id
```

列出環境 VLANs

```
aws evs list-environment-vlans \
    --environment-id environment-id
```

如需 API 操作的詳細資訊，請參閱《Amazon EVS API 參考指南》中的以下內容：

- ListEnvironments
- ListEnvironmentHosts
- ListEnvironmentVlans

AMI 維護

Amazon EVS 使用自訂 EVS Amazon Machine Image (AMI) 部署 ESX 主機。AMI 包含自訂廠商附加元件，其中包含在 Amazon EC2 上執行 ESX 所需的套件。

故障診斷由於不相容的叢集映像而新增主機失敗

當您將主機新增至您的環境時，主機具有最新版本的 EVS 自訂廠商附加元件。如果您的環境使用具有較舊附加元件版本的主機，新增主機會失敗，並顯示新主機與叢集映像不相容的錯誤。如需修正此問題的詳細步驟，請參閱 the section called “新增主機因不相容的叢集映像而失敗”。

Amazon EVS 主機維護

由於 Amazon EVS 是自我管理的服務，因此您必須負責維護在主機上執行的 VMware Cloud Foundation (VCF) 軟體、監控主機運作狀態，以及修復主機問題，包括主機故障時的主機替換。如需

在 VMware Cloud Foundation (VCF) 中管理 ESX 主機的詳細資訊，請參閱 VMware Cloud Foundation 文件中的主機管理。

檢查基礎 EC2 執行個體的運作狀態

Amazon EC2 會在每一次執行 EC2 執行個體時執行自動化檢查，以識別硬體和軟體問題。您可以在 EC2 主控台中檢視這些狀態檢查的結果 AWS CLI ，或識別特定且可偵測的問題。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的檢視 Amazon EC2 執行個體的狀態檢查，以及《 AWS CLI 命令列參考》中的 describe-instance-status。 Amazon EC2

您可以建立 CloudWatch 警示，在特定執行個體上的狀態檢查失敗時提醒您。如需詳細資訊，請參閱《tje Amazon EC2 使用者指南》中的為狀態檢查失敗的 Amazon EC2 執行個體建立 CloudWatch 警示。 Amazon EC2

關於 EC2 執行個體的 AWS 排程維護

AWS 會對基礎 EC2 執行個體執行排程維護，以確保可靠性、可用性和效能。EC2 裸機執行個體的排程事件類型與其他 EC2 執行個體相同。 AWS 可以排程事件以重新啟動、停止和淘汰您的執行個體，因為基礎硬體問題或排程維護。這些事件不會頻繁發生。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的排程事件類型。

> **Note**
>
> 在任何排定的重新啟動事件之前，您應該將主機置於 vSphere 用戶端中的維護模式。

如果您的其中一個執行個體將受到排程事件的影響， 會使用與您相關聯的電子郵件地址，事先透過電子郵件 AWS 通知您 AWS 帳戶。 AWS 也會傳送 AWS 運作狀態事件，您可以使用 Amazon EventBridge 來監控和管理該事件。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的使用 Amazon EventBridge 監控 AWS 運作狀態中的事件和 Amazon EC2 執行個體的排程事件。 Amazon EC2 Amazon EC2

您可以隨時重新排程事件，使其在適合您的特定日期和時間發生。事件最晚可以重新排程到事件截止日期。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的重新排程 EC2 執行個體的排程事件。 Amazon EC2

使用 EC2 隨需容量預留

您可以使用 EC2 隨需容量預留，以確保您的叢集在維護期間有足夠的容量。您可以保留特定可用區域中任何持續時間的容量。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的使用 EC2 隨需容量保留保留運算容量。 Amazon EC2

如需建立容量保留的步驟，請參閱《Amazon EC2 使用者指南》中的建立容量保留。

> **Note**
>
> 如果您使用 EC2 隨需容量預留或 EC2 專用主機，我們建議您為關鍵任務工作負載保留備用主機。雖然容量保留可確保您可以在指定的可用區域中存取特定數量的 EC2 執行個體容量，但讓備用主機提供額外的備援層，這對於關鍵任務工作負載至關重要。對於專用主機，擁有備用主機可確保您維護關鍵任務工作負載的環境，即使主要主機需要維護或遇到問題。

準備 AWS 排程 **system-maintenance**和 **instance-retirement**事件

AWS 會排程兩種類型的`system-maintenance`事件：網路維護和電源維護。

- 在網路維護期間，排程執行個體會暫時遺失網路連線能力。維護完成後，便會還原您執行個體的一般網路連線能力。
- 在電源維護期間，排程執行個體會暫時離線，然後重新開機。在 EC2 裸機執行個體上執行重新啟動時，不會保留執行個體存放磁碟區資料。

AWS 當偵測到託管 EC2 執行個體的基礎硬體降級時， 會排程 EC2 `instance-retirement`事件。

若要修復 `system-maintenance`和 `instance-retirement`事件，請在發生維護事件之前，使用 Amazon EVS 主控台或 AWS CLI 和 SDDC Manager 將失敗的主機取代為新主機。如果您等待發生維護事件，且需要重新啟動 EC2 執行個體，則會遺失存放在執行個體儲存體磁碟區中的 vSAN 資料。如需詳細步驟，請參閱the section called “取代 Amazon EVS 主機”。

> **Important**
>
> EC2 主控台不應用於管理 Amazon EVS 主機的狀態，包括停止、啟動和終止。請勿嘗試啟動、停止或終止 Amazon EVS 部署的 EC2 執行個體。此動作會導致 vSAN 資料遺失。

取代 Amazon EVS 主機

請依照此程序來取代 Amazon EVS 主機。

> **Warning**
>
> Amazon EVS 主機使用自訂廠商附加元件來提供重要的主機功能。當您將主機新增至您的環境時，將會有最新版本的 Amazon EVS 自訂附加元件。如果您的環境使用具有較舊附加元件版本的主機，將主機新增至 vSphere 叢集會導致叢集映像修復失敗。如需疑難排解此問題的步驟，請參閱 the section called “故障診斷由於不相容的叢集映像而新增主機失敗”。

> **Warning**
>
> 如果您已在部署後更新 ESX 版本，SDDC 管理員可能會在委託主機步驟中的 VCF 主機驗證期間失敗。如需疑難排解此問題的步驟，請參閱 the section called “SDDC Manager 在主機測試期間未通過 VCF 主機驗證”。

> **Note**
>
> 請確定每個 EVS 環境配額的 Amazon EVS 主機計數已正確設定，以確保成功建立主機。如果此配額值少於您嘗試在單一 Amazon EVS 環境中佈建的主機數量，則主機建立會失敗。您可能需要為需要主機替換的維護操作請求提高配額。如需詳細資訊，請參閱Service Quotas。

Example

Amazon EVS console and SDDC Managuer UI

1. 前往 Amazon EVS 主控台。
2. 在導覽窗格中，選擇環境。
3. 選取包含要取代之主機的環境。
4. 選取主機索引標籤。
5. 選擇 Create host (建立主機)。
6. 指定主機詳細資訊，然後選擇建立主機。
7. 若要驗證完成，請檢查主機狀態是否已變更為已建立。

8. 從 AWS Secrets Manager 擷取 ESX 根密碼的憑證。如需擷取秘密的詳細資訊，請參閱《AWS Secrets Manager 使用者指南》中的從 Secrets Manager 取得 AWS 秘密。
9. 移至 SDDC Manager。
10. 使用您在上一個步驟中擷取的 ESX 根登入資料，在 SDDC Manager 中委任新主機。如需詳細資訊，請參閱 VMware Cloud Foundation 文件中的 Commission Hosts。
11. 將新主機新增至叢集。如需詳細資訊，請參閱 vSphere 文件中的如何使用快速入門工作流程將 ESX 主機新增至 vSphere 叢集。 vSphere
12. 停用 SDDC Manager 中您要從 SDDC Manager 移除的舊主機。如需詳細資訊，請參閱 VMware Cloud Foundation 文件中的停用主機。
13. 返回 Amazon EVS 主控台。
14. 在主機索引標籤下，選取失敗的主機，然後選擇刪除 > 刪除主機。

AWS CLI and SDDC Manager UI

1. 開啟新的終端機工作階段。
2. 建立新的主機。如需參考，請參閱以下命令範例。

```
aws evs create-environment-host \
    --environment-id "env-abcde12345" \
    --host '{ \
        "hostName": "esxi-host-05", \
        "keyName": "your-ec2-keypair-name", \
        "instanceType": "i4i.metal" \
        "esxVersion": "ESXi-8.0U3g-24859861"\
    }'
```

3. 從 AWS Secrets Manager 擷取 ESX 根密碼的憑證。如需擷取秘密的詳細資訊，請參閱《AWS Secrets Manager 使用者指南》中的從 Secrets Manager 取得 AWS 秘密。
4. 移至 SDDC Manager。
5. 使用您在上一個步驟中擷取的 ESX 根登入資料，在 SDDC Manager 中委任新主機。如需詳細資訊，請參閱 VMware Cloud Foundation 文件中的 Commission Hosts。
6. 將新主機新增至包含受損主機的叢集。
7. 在 SDDC Manager 中停用受損的主機。如需詳細資訊，請參閱 VMware Cloud Foundation 文件中的停用主機。
8. 返回終端機。
9. 刪除失敗的主機。如需參考，請參閱以下命令範例。

```
aws evs delete-environment-host --environment-id "env-abcde12345" --host-name
 "esxi-host-05"
```

疑難排解

如需疑難排解指引，請參閱 疑難排解。如果您在檢閱疑難排解指引後仍遇到問題，請聯絡 AWS Support 以取得進一步協助。

設定 Amazon EVS 子網路的自訂路由表

Amazon EVS 只有在建立 Amazon EVS 環境之後，才支援使用自訂路由表。若要成功建立環境，您必須設定主要路由表，以允許對 DNS 和內部部署系統等相依服務的流量。這是因為 Amazon EVS VLAN 子網路在環境部署期間隱含地與我們 VPC 的主要路由表相關聯。

環境部署之後，您必須明確地將每個 Amazon EVS VLAN 子網路與 VPC 中的路由表建立關聯。如果您的 VLAN 子網路未明確與 VPC 路由表相關聯，NSX 連線會失敗。我們強烈建議您明確地將子網路與自訂路由表建立關聯。自訂路由表可讓您更精細地控制 VPC 內的網路流量路由，為特定子網路或閘道提供量身打造的路由規則。如需建立自訂路由表的詳細資訊，請參閱《Amazon VPC 使用者指南》中的為您的 VPC 建立路由表。

設定網路存取控制清單以控制 Amazon EVS VLAN 子網路流量

網路存取控制清單 (ACL) 會允許或拒絕子網層級的特定傳入或傳出流量。您可以使用網路 ACLs 來控制 Amazon EVS VLAN 子網路的傳入和傳出流量。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的為您的 VPC 建立網路 ACL。

> **Important**
>
> EC2 安全群組無法在連接至 Amazon EVS VLAN 子網路的彈性網路介面上運作。若要控制往返 Amazon EVS VLAN 子網路的流量，您必須使用網路存取控制清單。

> **Warning**
>
> Amazon EVS 需要存取您的 VCF 部署。您必須設定安全群組和網路存取控制清單 (ACLs)，以允許 Amazon EVS 與下列項目通訊：
>
> - 透過 TCP/UDP 連接埠 53 的 DNS 伺服器。

- 透過 HTTPS 和 SSH 的主機管理 VLAN 子網路。
- 透過 HTTPS 和 SSH 管理 VM VLAN 子網路。

如果您的安全群組和網路 ACLs 不允許此存取，Amazon EVS 環境部署將會失敗，且現有環境的合規狀態可能會降低。

秘密管理生命週期

Amazon EVS 使用 AWS Secrets Manager 在初始環境部署時，在您的帳戶中建立、加密和存放秘密。這些秘密包含安裝和存取 VCF 管理設備所需的 VCF 登入資料，例如 vCenter Server、NSX 和 SDDC Manager，以及 ESX 主機根密碼。刪除 EVS 環境時，Amazon EVS 也會代表您刪除受管秘密。

您負責秘密生命週期管理，包括秘密輪換。Amazon EVS 不提供您的私密的受管輪換。建議您定期在設定的輪換時段輪換秘密，以確保秘密不會過久。如需詳細資訊，請參閱 AWS Secrets Manager 使用者指南中的輪換排程。

建立 Amazon EVS 主機

在 Amazon EVS 環境部署之後，您可以新增主機以增加容量和工作負載彈性。Amazon EVS 支援每個環境 4-16 個主機。此動作只能在部署 Amazon EVS 環境之後使用。

> **Note**
>
> 您必須在 SDDC Manager 使用者介面中指派和委託主機。

建立 Amazon EVS 主機

請依照下列步驟建立 Amazon EVS 主機。

> **Warning**
>
> Amazon EVS 主機使用自訂廠商附加元件來提供重要的主機功能。當您將主機新增至您的環境時，將會有最新版本的 Amazon EVS 自訂附加元件。如果您的環境使用具有較舊附加元件版本的主機，將主機新增至 vSphere 叢集會導致叢集映像修復失敗。如需疑難排解此問題的步驟，請參閱 the section called “故障診斷由於不相容的叢集映像而新增主機失敗”。

Warning

如果您在 Amazon EVS 環境部署之後已更新 ESX 版本，則 SDDC 管理員可能會在委託主機步驟中的 VCF 主機驗證期間失敗。如需疑難排解此問題的步驟，請參閱 the section called “SDDC Manager 在主機測試期間未通過 VCF 主機驗證”。

Note

請確定每個 EVS 環境配額的 Amazon EVS 主機計數已正確設定，以確保成功建立主機。如果此配額值少於您嘗試在單一 Amazon EVS 環境中佈建的主機數量，則主機建立會失敗。若要提高配額，您可以請求提高配額。如需詳細資訊，請參閱Service Quotas。

Note

如果您在將主機新增至環境時未指定 ESX 版本，Amazon EVS 會自動使用與環境 VCF 版本相關聯的預設 ESX 版本。如需詳細資訊，請參閱the section called “VCF 版本和 EC2 執行個體”。

Important

新增 ESX 主機時，請選取符合您目標 vSphere 叢集的 ESX 版本。如果相同版本無法使用，請使用 vSphere Lifecycle Manager 部署較舊版本並升級。如需詳細資訊，請參閱the section called “SDDC Manager 在主機測試期間未通過 VCF 主機驗證”。升級可能需要重新啟動主機，並增加委託主機所需的時間。

具有比 vSphere 叢集映像 ESX 版本更新的 ESX 版本的主機無法降級。您需要刪除主機，並使用正確的 ESX 版本重新建立主機。

Example

Amazon EVS console and SDDC Managuer UI

1. 前往 Amazon EVS 主控台。
2. 在導覽窗格中，選擇環境。

3. 選取您要建立主機的環境。
4. 選取主機索引標籤。
5. 選擇 Create host (建立主機)。
6. 指定主機詳細資訊，然後選擇建立主機。
7. 若要驗證完成，請檢查主機狀態是否已變更為已建立。
8. 移至 SDDC Manager。
9. 在 SDDC Manager 中委任新主機。如需詳細資訊，請參閱 VMware Cloud Foundation 文件中的 Commission Hosts。
10. 使用 SDDC Manager 將新主機新增至叢集。如需詳細資訊，請參閱 vSphere 文件中的如何使用快速入門工作流程將 ESX 主機新增至 vSphere 叢集。 vSphere

AWS CLI and SDDC Manager UI

1. 開啟新的終端機工作階段。
2. 建立新的主機。如需參考，請參閱以下命令範例。

```
aws evs create-environment-host \
    --environment-id "env-abcde12345" \
    --host '{ \
        "hostName": "esxi-host-05", \
        "keyName": "your-ec2-keypair-name", \
        "instanceType": "i4i.metal",\
        "esxVersion": "ESXi-8.0U3g-24859861"\
    }'
```

3. 移至 SDDC Manager。
4. 在 SDDC Manager 中委任新主機。如需詳細資訊，請參閱 VMware Cloud Foundation 文件中的 Commission Hosts。
5. 使用 SDDC Manager 將新主機新增至叢集。如需詳細資訊，請參閱 vSphere 文件中的如何使用快速入門工作流程將 ESX 主機新增至 vSphere 叢集。 vSphere

刪除 Amazon EVS 主機

當不再需要主機時，您可以從環境刪除 Amazon EVS 主機。Amazon EVS 要求您的環境至少要有四個主機。Amazon EVS 不支援主機少於四個的環境。

> **Warning**
>
> 刪除未停用的主機會在 vCenter 和 SDDC Manager 中保留過時的資料，這可能需要額外的清理工作。在 Amazon EVS 主控台或 API 中刪除主機之前，請確定您的主機已解除委任。

> **Warning**
>
> 一律使用 Amazon EVS 主控台或 API 來移除您的 Amazon EVS 主機。從 EC2 主控台刪除主機可能會讓您的環境處於不一致狀態。

刪除 Amazon EVS 主機

請依照下列步驟刪除 Amazon EVS 主機。

Example

SDDC Managuer UI and Amazon EVS console

1. 移至 SDDC Manager。
2. 從 SDDC Manager 移除叢集。
3. 在 SDDC Manager 中停用主機。如需詳細資訊，請參閱 VMware Cloud Foundation 文件中的停用主機。
4. 前往 Amazon EVS 主控台。
5. 在導覽窗格中，選擇環境。
6. 選取包含要刪除之主機的環境。
7. 選取主機索引標籤。
8. 選擇刪除主機。
9. 選取主機，然後在主機索引標籤中選擇刪除。針對您要刪除的每個主機重複此步驟。

SDDC Manager UI and AWS CLI

1. 移至 SDDC Manager。
2. 從 SDDC Manager 移除叢集。

3. 在 SDDC Manager 中停用主機。如需詳細資訊，請參閱 VMware Cloud Foundation 文件中的停用主機。
4. 開啟新的終端機工作階段。
5. 刪除主機。如需參考，請參閱以下命令範例。

```
aws evs delete-environment-host \
--environment-id env-abcdefghij \
--host-name my-evs-host.example.com
```

Amazon Elastic VMware Service 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，該架構專為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。共同責任模型將此描述為雲端本身的安全和雲端內部的安全：

- 雲端的安全性 – AWS 負責保護在 AWS 服務 中執行的基礎設施 AWS 雲端。 AWS 也為您提供可安全使用的服務。在 AWS 合規計劃中，第三方稽核員會定期測試並驗證我們的安全功效。若要了解適用於 Amazon Elastic VMware Service (Amazon EVS) 的合規計劃，請參閱AWS 服務 合規計劃範圍中的 。
- 雲端的安全性 – 您的責任取決於您使用 AWS 服務 的 。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 Amazon EVS 時套用共同責任模型。它說明如何設定 Amazon EVS 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 Amazon EVS 資源。

目錄

Amazon EVS 中的資料保護

AWS 共同責任模型適用於 Amazon Elastic VMware Service 中的資料保護。如此模型所述， AWS 負責保護執行所有 AWS 雲端的 全球基礎設施。您有責任控制在此基礎設施上託管的內容，包括 VMware Cloud Foundation (VCF) 元件。您也必須負責 AWS 服務 您使用之 的安全組態和管理任務。如需有關資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。如需歐洲資料保護的相關資訊，請參閱安全AWS 部落格上的共同責任模型和 GDPR 部落格文章。 AWS

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

- 每個帳戶均要使用多重要素驗證 (MFA)。

- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 設定 API 和使用者活動記錄 AWS CloudTrail。如需有關使用 CloudTrail 線索擷取 AWS 活動的資訊，請參閱 AWS CloudTrail 《 使用者指南》中的使用 CloudTrail 線索。

> **Note**
>
> Amazon EVS 不會記錄非AWS 元件的使用者活動，例如 VCF 環境中的活動。這些活動會記錄在各種 VMware 主控台中，例如 vSphere 和 NSX Manager。如果需要集中式 VCF 記錄，您可以設定 VCF 監控解決方案，例如 VMware Aria Operations 或 VMware Tanzu 可觀測性，以實現此結果。如需詳細資訊，請參閱 VCF 文件中的 VMware Cloud Foundation with VMware Tanzu and VMware Aria Suite Lifecyle in VMware Cloud Foundation mode。

- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 AWS 服務。
- 使用進階受管安全服務 Amazon Macie，例如 ，協助探索和保護存放在其中的敏感資料 Amazon S3。
- 如果您在 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-3 驗證的密碼編譯模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-3。

我們強烈建議您絕對不要將敏感的識別資訊，例如客戶的電子郵件地址，放入標籤或任意格式的文字欄位中，例如名稱欄位。這包括當您 AWS 服務 使用 Amazon EVS 或使用主控台、API AWS CLI或 AWS SDKs的其他 時。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

靜態加密

Amazon EVS 部署 i4i.metal EC2 執行個體，其預設針對存放在執行個體存放區磁碟區上的資料使用透明 AES-256 加密。Amazon EVS 目前不支援 EBS 開機磁碟區加密。

Amazon EBS 開機磁碟區

Amazon EVS i4i.metal 執行個體使用 Amazon EBS 開機磁碟區。開機磁碟區包含作業系統和其他必要檔案，以供 EC2 執行個體開機和執行。開機磁碟區未加密。Amazon EVS 目前不支援開機磁碟區加密。開機磁碟區不包含來自虛擬機器的使用者資料。

執行個體儲存體磁碟區

Amazon EVS i4i.metal EC2 執行個體隨附本機 NVMe SSD 儲存體，這是執行個體硬體的一部分。Amazon EVS 使用 NVMe 執行個體存放區磁碟區做為 vSAN 資料存放區的磁碟。在您部署 Amazon EVS 環境之後，vSAN 資料存放區會保留您的管理和工作負載虛擬機器。

NVMe 執行個體儲存體磁碟區上的資料會以執行個體上的硬體模組中實作的 XTS-AES-256 區塊編碼器來加密。用於加密寫入本機連接 NVMe 儲存裝置之資料的金鑰是依客戶和磁碟區而定。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的靜態加密。

部署 Amazon EVS 環境之後，您可以為 vSAN 資料存放區中存放的所有資料、個別虛擬機器 (VMs) 或 VMs 中的個別檔案啟用 vSAN data-at-rest資料加密。當某些 VMs 需要加密，而其他則不需要加密，或當 VM 中的特定磁碟或檔案需要加密時，此精細控制非常有用。如需詳細資訊，請參閱 VMware vSAN 文件中的 vSAN Data-At-Rest Encryption 如何運作。

傳輸中加密

根據預設，Amazon EVS 不會加密傳輸中流量。若要加密周遊 Amazon EVS 的傳輸中資料，您可以使用應用程式層加密搭配 Transport Layer Security (TLS) 等通訊協定。若要了解 EC2 執行個體流量加密，請參閱《Amazon EC2 使用者指南》中的傳輸中加密。

> **Note**
>
> Nitro 網路加密不適用於 Amazon EVS 部署的 EC2 執行個體。Amazon EVS 不支援主機間流量的傳輸中加密。

內部部署連線的傳輸中加密選項

若要加密內部部署資料中心與 Amazon EVS 之間的流量，您可以將 AWS Direct Connect 和 AWS Site-To-Site與 AWS Transit Gateway 結合使用。這種組合可提供 IPsec 加密的私有連線，同時降低網路成本、增加頻寬輸送量，並提供比一般網際網路 VPN 連線更一致的網路體驗。如需詳細資訊，請參閱使用 AWS Direct Connect 的私有 AWS Site-to-Site VPN。

> **Note**
>
> Amazon EVS 不支援透過 AWS Direct Connect 私有虛擬介面 (VIF) 或透過直接終止至底層 VPC AWS Site-to-Site VPN 連線進行連線。Amazon EVS 支援在 NSX Edge Tier-0 或 Tier-1

閘道上終止 IPSec VPN。如需詳細資訊，請參閱 VMware NSX 文件中的新增 NSX IPSec VPN 服務。

MAC Security (MACsec) 是 IEEE 標準，提供資料機密性、資料完整性和資料來源真實性。您可以使用支援 MACsec 的 AWS Direct Connect 連線，將您的資料從公司資料中心加密到 AWS Direct Connect 位置。如需詳細資訊，請參閱 AWS Direct Connect 使用者指南中的 Direct Connect 中的 MAC 安全性。 AWS

VMware 網路資料的傳輸中加密

在 Amazon EVS 環境部署之後，您有多個選項可在 VMware VCF 層強制執行傳輸中加密資料：

- VMware vDefend 分散式防火牆 - 可讓您在虛擬機器之間實作精細的網路分割，並強制執行 TLS/SSL 加密。如需詳細資訊，請參閱 VMware VCF 文件中的使用使用者介面設定分散式防火牆的安全設定。
- vSAN data-in-transit加密 - 可用於加密 vSAN 叢集中主機之間的所有資料和中繼資料。如需詳細資訊，請參閱 VMware vSAN 文件中的 vSAN Data-In-Transit加密。
- 加密的 vSphere vMotion - 保護使用 vSphere vMotion 傳輸之資料的機密性、完整性和真實性。如需詳細資訊，請參閱 vSphere 文件中的什麼是加密 vSphere vMotion。 vSphere

金鑰和秘密管理

在 Amazon EVS 環境部署期間，Amazon EVS 會使用 AWS Secrets Manager 來建立、加密和存放秘密，其中包含安裝和存取 VMware VCF 管理設備所需的 VCF 登入資料，以及 ESX 根密碼。刪除 EVS 環境時，Amazon EVS 也會代表您刪除受管秘密。如需詳細資訊，請參閱 Secrets Manager 使用者指南中的 Secrets Manager 秘密中的內容。 AWS

Secrets Manager 使用信封加密搭配 AWS KMS 金鑰和資料金鑰來保護每個秘密值。除非另有指定，否則會使用 Secrets Manager 的預設 AWS 受管金鑰。或者，您可以在環境建立期間指定客戶受管金鑰，以加密您的秘密。如需詳細資訊，請參閱《Secrets Manager 使用者指南》中的 AWS Secrets Manager 中的秘密加密和解密。 AWS

> **Note**
>
> 客戶受管金鑰需支付額外的使用費。預設 AWS 受管金鑰是免費提供的。如需詳細資訊，請參閱 AWS Secrets Manager 使用者指南中的定價。

Amazon EVS 不會在部署後，同步 AWS Secrets Manager 和 VCF 軟體之間的登入資料。您有責任確保與 Amazon EVS 環境相關聯的秘密與 SDDC Manager 中的登入資料保持同步，以避免 VCF 密碼過期和無法存取 VCF 軟體。

Amazon EVS 不會代表您輪換秘密。您有責任輪換與環境相關聯的秘密。我們強烈建議在建立環境後立即輪換您的秘密，並實作輪換排程以定期更新秘密。如需輪換 AWS Secrets Manager 秘密的詳細資訊，請參閱《 AWS Secrets Manager 使用者指南》中的依 Lambda 函數輪換。如需 VCF 密碼管理的詳細資訊，請參閱 VMware Cloud Foundation 文件中的密碼管理。

Important

Amazon EVS 不會在部署後，同步 AWS Secrets Manager 和 VCF 軟體之間的登入資料。如果部署後使用 AWS Secrets Manager，您必須在 AWS Secrets Manager 和 SDDC Manager 之間保持憑證同步，以避免 VCF 密碼過期問題。如果 SDDC Manager 登入資料未保持在最新狀態，您可能會無法存取 VCF 軟體。

Note

Amazon EVS 不提供秘密的受管輪換。

Note

針對 AWS Secrets Manager 秘密輪換使用 Lambda 函數會產生費用。如需詳細資訊，請參閱 AWS Secrets Manager 使用者指南中的定價。

網際網路流量隱私權

Amazon EVS 使用客戶提供的 VPC 在 Amazon EVS 環境中的資源之間建立邊界，並控制它們、您的內部部署網路和網際網路之間的流量。如需 Amazon VPC 安全性的詳細資訊，請參閱 Amazon VPC 《 使用者指南》中的確保 中的網際網路流量隱私權 Amazon VPC。

根據預設，Amazon EVS 會在環境建立期間建立拒絕直接網際網路存取的私有 VLAN 子網路。若要將另一層安全性新增至 VPC，您可以使用進一步限制網際網路連線的規則，為您的 VPC 建立自訂網路存取控制清單。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的為您的 VPC 建立網路 ACL。

> **Important**
>
> EC2 安全群組無法在連接至 Amazon EVS VLAN 子網路的彈性網路介面上運作。若要控制往返 Amazon EVS VLAN 子網路的流量，您必須使用網路存取控制清單。

如果您是 NSX 管理員，您可以設定下列 NSX 功能來保護網路流量：

- VMware vDefend Gateway Firewall - 保護網路周邊，防止外部威脅（南北流量）。如需詳細資訊，請參閱 VMware NSX 文件中的新增閘道防火牆政策和規則。
- VMware vDefend 分散式防火牆 - 防止來自內部網路（東西流量）的攻擊。如需詳細資訊，請參閱 VMware NSX 文件中的新增分散式防火牆。

Amazon Elastic VMware Service 的身分和存取管理

AWS Identity and Access Management (IAM) 是 AWS 服務 ，可協助管理員安全地控制對 AWS resources 的存取。 IAM 管理員可控制誰可以經過身分驗證（登入）和授權（具有許可）來使用 Amazon Elastic VMware Service (Amazon EVS) 資源。 IAM 是您可以免費使用 AWS 服務 的 。

主題

目標對象

使用方式 AWS Identity and Access Management (IAM) 會有所不同，取決於您在 Amazon EVS 中執行的工作。

服務使用者 – 如果您使用 Amazon EVS 服務來執行任務，您的管理員會為您提供所需的登入資料和許可。當您使用更多 Amazon EVS 功能來執行工作時，您可能需要額外的許可。了解存取許可的管理方式可協助您向管理員請求正確的許可。

如果您無法存取 Amazon EVS 中的功能，請參閱 the section called “對 Amazon EVS 身分和存取進行故障診斷”。

服務管理員 - 如果您在公司負責 Amazon EVS 資源，您可能擁有 Amazon EVS 的完整存取權。您的任務是判斷服務使用者應存取的 Amazon EVS 功能和資源。然後，您必須向 IAM 管理員提交請求，以變更服務使用者的許可。檢閱此頁面上的資訊，以了解 的基本概念 IAM。若要進一步了解貴公司如何 IAM 搭配 Amazon EVS 使用 ，請參閱 the section called “Amazon EVS 如何使用 IAM”。

IAM 管理員 - 如果您是 IAM 管理員，建議您了解如何撰寫政策以管理 Amazon EVS 存取的詳細資訊。若要檢視您可以在 中使用的 Amazon EVS 身分型政策範例 IAM，請參閱 the section called “Amazon EVS 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 透過擔任 IAM 角色來驗證 （ 登入 AWS)。

您可以使用透過身分來源提供的登入資料，以聯合身分 AWS 的形式登入 。 AWS IAM Identity Center (IAM Identity Center) 使用者、您公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料，都是聯合身分的範例。當您以聯合身分身分登入時，您的管理員先前會使用 IAM 角色設定聯合身分。當您使用聯合 AWS 身分存取 時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS 管理主控台 或 AWS 存取入口網站。如需登入的詳細資訊 AWS，請參閱 AWS 《 登入使用者指南》中的如何登入您的 AWS 帳戶 。

如果您以 AWS 程式設計方式存取 ， AWS 會提供軟體開發套件 (SDK) 和命令列界面 (CLI)，以使用您的登入資料以密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，則必須自行簽署請求。如需使用建議方法自行簽署請求的詳細資訊，請參閱《 AWS 一般參考》中的 Signature 第 4 版簽署程序。

無論您使用何種身分驗證方法，您可能還需要提供額外的安全性資訊。例如， AWS 建議您使用多重驗證 (MFA) 來提高帳戶的安全性。若要進一步了解，請參閱《 AWS IAM Identity Center (AWS 單一登入的後繼者 ） 使用者指南》中的多重要素驗證，以及《IAM 使用者指南》中的在 中使用多重要素驗證 (MFA) AWS。

AWS 帳戶根使用者

當您第一次建立 時 AWS 帳戶，您會從單一登入身分開始，該身分可完整存取帳戶中的所有 AWS 服務和資源。此身分稱為 AWS 帳戶根使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常作業。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需需要您以根使用者身分登入的任務完整清單，請參閱《帳戶管理參考指南》中的需要根使用者憑證的任務。

聯合身分

根據最佳實務， 要求人類使用者，包括需要管理員存取權的使用者，使用 聯合身分提供者 AWS 服務來使用臨時憑證來存取 。

聯合身分是來自您的企業使用者目錄、Web 身分提供者、 AWS Directory Service、 Identity Center 目錄，或 AWS 服務 是透過身分來源提供的登入資料存取的任何使用者。當聯合身分存取時 AWS 帳戶，它們會擔任 角色，而角色會提供臨時登入資料。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連接並同步到您自己的身分來源中的一組使用者 AWS 帳戶 和群組，以便在所有 和應用程式中使用。如需有關 IAM Identity Center 的資訊，請參閱《IAM Identity Center （單一登入的後續） 使用者指南》中的什麼是 AWS IAM Identity Center AWS ？。

IAM 使用者 和 群組

IAM 使用者 是您 中的身分 AWS 帳戶 ，具有單一人員或應用程式的特定許可。如果可能，我們建議依賴臨時登入資料，而不是建立擁有密碼和存取金鑰等長期登入資料 IAM 使用者 的人員。不過，如果您有特定的使用案例需要使用長期憑證 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱《IAM 使用者指南》中的為需要長期憑證的使用案例定期輪換存取金鑰。

IAM 群組是指定 集合的身分 IAM 使用者。您無法以群組身分登入。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有名為 IAMAdmins 的群組，並授予該群組管理 IAM 資源的許可。

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

IAM 角色

IAM 角色是 中具有特定許可 AWS 帳戶 的身分。它類似於 IAM 使用者，但不與特定人員相關聯。您可以 AWS 管理主控台 切換 IAM 角色，暫時在 中擔任 角色。您可以透過呼叫 AWS CLI 或 AWS API 操

作或使用自訂 URL 來擔任角色。如需使用角色方法的詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM 角色。

IAM 具有臨時登入資料的 角色在下列情況下非常有用：

- 聯合身分使用者存取 – 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱 IAM 使用者指南中的為第三方身分提供者建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM中的角色相關聯。如需有關許可集的資訊，請參閱《 AWS IAM Identity Center (AWS 單一登入的後續）使用者指南》中的許可集。
- 暫時 IAM 使用者 許可 – IAM 使用者 可以擔任 IAM 角色，暫時接受特定任務的不同許可。
- 跨帳戶存取 – 您可以使用 IAM 角色，允許不同帳戶中的某人 （信任的委託人） 存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。不過，對於某些 AWS 服務，您可以直接將政策連接到資源 （而不是使用角色做為代理）。若要了解跨帳戶存取的角色和資源型政策之間的差異，請參閱《IAM 使用者指南》中的IAM 角色與資源型政策的差異。
- 跨服務存取 – 有些 AWS 服務 使用其他 中的功能 AWS 服務。例如，當您在服務中呼叫 時，該服務通常會在 中執行應用程式 Amazon EC2 或將物件存放在其中 Amazon S3。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 委託人許可 – 當您使用 IAM 使用者 或 角色在 中執行動作時 AWS，您會被視為委託人。政策能將許可授予主體。當您使用某些服務時，您可能會執行一個動作，然後在不同的服務中觸發另一個動作。在此情況下，您必須具有執行這兩個動作的許可。
  - 服務角色 – 服務角色是服務擔任以代表您執行動作 IAM 的角色。 IAM 管理員可以從內部建立、修改和刪除服務角色 IAM。如需詳細資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務服務。
  - 服務連結角色 – 服務連結角色是連結至 的一種服務角色 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶 ，並由服務擁有。 IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 上執行 Amazon EC2 的應用程式 – 您可以使用 IAM 角色來管理在 Amazon EC2 執行個體上執行之應用程式的臨時登入資料，以及提出 AWS CLI 或 AWS API 請求。最好將存取金鑰存放在 Amazon EC2 執行個體中。若要將 AWS 角色指派給 Amazon EC2 執行個體並將其提供給其所有應用程式，您可以建立連接至執行個體的執行個體描述檔。執行個體描述檔包含 角色，並可讓在 Amazon EC2 執行個體上執行的程式取得臨時登入資料。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM 角色將許可授予在 Amazon EC2 執行個體上執行的應用程式。

若要了解如何使用 IAM 角色，請參閱《IAM 使用者指南》中的何時建立 IAM 角色 （而非使用者）。

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。政策是 中的物件， AWS 當與身分或資源建立關聯時， 會定義其許可。當委託人（使用者、根使用者或角色工作階段）發出請求時， 會 AWS 評估這些政策。政策中的許可決定是否允許或拒絕請求。大多數政策會以 JSON 文件 AWS 形式存放在 中。如需 JSON 政策文件結構和內容的詳細資訊，請參閱《IAM 使用者指南》中的 JSON 政策概觀。

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。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。

每個 IAM 實體（使用者或角色）都從沒有許可開始。根據預設，使用者什麼都不做，甚至無法變更自己的密碼。若要授予使用者執行動作的許可，管理員必須將許可政策附加到使用者。或者，管理員可以將使用者新增到具備預定許可的群組。當管理員將許可授予群組時，該群組中的所有使用者都會獲得這些許可。

IAM 無論您用來執行操作的方法為何， 政策都會定義動作的許可。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該政策的使用者可以從 AWS 管理主控台 AWS CLI、 或 AWS API 取得角色資訊。

身分型政策

身分型政策是您可以連接到身分的 JSON 許可政策文件，例如 IAM 使用者、 角色或 群組。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接嵌入單一使用者、群組或角色。受管政策是獨立的政策，您可以連接到 中的多個使用者、群組和角色 AWS 帳戶。受管政策包括 AWS 受管政策和客戶受管政策。如需了解如何在受管政策及內嵌政策間選擇，請參閱 IAM 使用者指南中的在受管政策和內嵌政策間選擇。

資源型政策

以資源為基礎的政策是您連接到資源的 JSON 政策文件，例如 儲存 Amazon S3 貯體。服務管理員可使用這些政策來定義指定委託人 (帳戶成員、使用者或角色) 可以在什麼情況下對該資源執行什麼動作。資源型政策是內嵌政策。不存在受管的資源型政策。

存取控制清單 (ACL)

存取控制清單 (ACL) 是可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源之許可的政策類型。ACL 類似於以資源為基礎的政策，雖然它們不使用 JSON 政策文件格式。 Amazon S3 AWS

WAF， 和 Amazon VPC 是支援 ACLs的服務範例。如需進一步瞭解 ACL，請參閱《Amazon Simple Storage Service 開發人員指南》中的存取控制清單 (ACL) 概觀。

其他政策類型

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

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

多種政策類型

當多種類型的政策套用到請求時，產生的許可會更複雜而無法理解。若要了解如何 AWS 在涉及多個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。

Amazon EVS 如何使用 IAM

在您使用 IAM 管理 Amazon EVS 的存取權之前，請先了解哪些 IAM 功能可與 Amazon EVS 搭配使用。

IAM 功能	Amazon EVS 支援
the section called “Amazon EVS 的身分型政策”	是
the section called “Amazon EVS 中的資源型政策”	否

IAM 功能	Amazon EVS 支援
the section called “Amazon EVS 的政策動作”	是
the section called “Amazon EVS 的政策資源”	部分
the section called “Amazon EVS 的政策條件索引鍵”	是
the section called “Amazon EVS 中的存取控制清單 (ACLs)”	否
the section called “使用 Amazon EVS 的屬性型存取控制 (ABAC)”	是
the section called “搭配 Amazon EVS 使用臨時憑證”	是
the section called “轉送 Amazon EVS 的存取工作階段”	是
the section called “Amazon EVS 的服務角色”	否
the section called “Amazon EVS 的服務連結角色”	是

若要取得 Amazon EVS 和其他 AWS 服務 使用方式的高階檢視 IAM，請參閱《IAM 使用者指南》中的 AWS 服務 使用 IAM 。

Amazon EVS 的身分型政策

支援身分型政策：是

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，以及允許或拒絕動作的條件。您無法在身分型政策中指定委託人，因為它適用於其連接的 使用者或角色。若要了解您在 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。

Amazon EVS 的身分型政策範例

若要檢視 Amazon EVS 身分型政策的範例，請參閱 the section called “Amazon EVS 身分型政策範例”。

Amazon EVS 中的資源型政策

支援資源型政策：否

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

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

Amazon EVS 的政策動作

支援動作 是

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。

IAM 身分型政策的 `Action`元素說明政策允許或拒絕的特定動作。政策動作通常具有與相關聯 AWS API 操作相同的名稱。政策會使用動作來授予執行相關聯操作的許可。

Amazon EVS 中的政策動作在動作之前使用下列字首：`evs:`。例如，若要授予某人使用 Amazon EVS `CreateEnvironment` API 操作建立環境的許可，請在其政策中包含 `evs:CreateEnvironment`動作。政策陳述式必須包含 `Action` 或 `NotAction` 元素。Amazon EVS 會定義自己的一組動作，描述您可以使用此服務執行的任務。

若要在單一陳述式中指定多個動作，請用逗號分隔，如下所示：

```
"Action": [
      "evs:action1",
      "evs:action2"
```

您也可以使用萬用字元 (*) 來指定多個動作。例如，若要指定開頭是 List 文字的所有動作，請包含以下動作：

```
"Action": "evs:List*"
```

若要查看 Amazon EVS 動作的清單，請參閱《服務授權參考》中的 Amazon EVS 定義的動作。

Amazon EVS 的政策資源

支援政策資源：部分

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。

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

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

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

若要查看 Amazon EVS 資源類型及其 ARNs，請參閱《服務授權參考》中的 Amazon Elastic VMware Service 定義的資源。若要了解您可以使用哪些動作指定每個資源的 ARN，請參閱 Amazon Elastic VMware Service 定義的動作。

有些 Amazon EVS API 動作支援多個資源。例如，在呼叫 ListEnvironments API 動作時，可以參考多個環境。若要在單一陳述式中指定多項資源，請使用逗號分隔 ARN。

```
"Resource": [
      "EXAMPLE-RESOURCE-1",
      "EXAMPLE-RESOURCE-2"
```

例如，Amazon EVS 環境資源具有下列 ARN：

```
arn:${Partition}:evs:${Region}:${Account}:environment/${EnvironmentId}
```

若要在陳述式my-environment-2中指定環境my-environment-1和 ，請使用下列範例 ARNs：

```
"Resource": [
        "arn:aws:evs:us-east-1:123456789012:environment/my-environment-1",
```

```
        "arn:aws:evs:us-east-1:123456789012:environment/my-environment-2"
```

若要指定屬於特定帳戶的所有環境，請使用萬用字元 (*)：

```
"Resource": "arn:aws:evs:us-east-1:123456789012:environment/*"
```

Amazon EVS 的政策條件索引鍵

支援服務特定政策條件金鑰：是

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

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

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

您也可以在指定條件時使用預留位置變數。例如，只有當資源以其 IAM 使用者 名稱標記時，您才能授予存取資源的 IAM 使用者 許可。如需詳細資訊，請參閱《IAM 使用者指南》中的IAM 政策元素：變數和標籤。

Amazon EVS 會定義自己的一組條件金鑰，也支援使用一些全域條件金鑰。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的AWS 全域條件內容索引鍵。

所有 Amazon EC2 動作都支援 aws:RequestedRegion和 ec2:Region條件金鑰。如需詳細資訊，請參閱範例：限制對特定區域的存取。

若要查看 Amazon EVS 條件金鑰清單，請參閱《服務授權參考》中的 Amazon EVS 的條件金鑰。若要了解您可以使用條件金鑰的動作和資源，請參閱 Amazon EVS 定義的動作。

Amazon EVS 中的存取控制清單 (ACLs)

支援 ACL：否

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

使用 Amazon EVS 的屬性型存取控制 (ABAC)

支援 ABAC (政策中的標籤)：是

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。在 中 AWS，這些屬性稱為標籤。您可以將標籤連接至 IAM 實體 （使用者或角色） 和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。然後，您可以設計 ABAC 政策，以便在委託人的標籤與其嘗試存取的資源上的標籤相符時允許操作。

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

您可以將標籤連接至 Amazon EVS 資源，或在請求中將標籤傳遞至 Amazon EVS。如需根據標籤控制存取，請使用 `aws:ResourceTag/<key-name>`、`aws:RequestTag/<key-name>` 或 `aws:TagKeys` 條件索引鍵，在政策的條件元素中，提供標籤資訊。如需您可以在條件索引鍵中使用標籤之動作的詳細資訊，請參閱《服務授權參考》中的 Amazon EVS 定義的動作。

搭配 Amazon EVS 使用臨時憑證

支援臨時憑證：是

當您使用臨時登入資料登入時，有些 AWS 服務 無法運作。如需詳細資訊，包括哪些 AWS 服務 使用臨時登入資料，請參閱《AWS 服務 IAM 使用者指南》中的使用 IAM 的 。

如果您 AWS 管理主控台 使用使用者名稱和密碼以外的任何方法登入 ，則會使用臨時登入資料。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取 時，該程序會自動建立臨時登入資料。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱《IAM 使用者指南》中的從使用者切換至 IAM 角色 (主控台)。

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

轉送 Amazon EVS 的存取工作階段

支援轉寄存取工作階段 (FAS)：是

當您使用 IAM 使用者或角色在 中執行動作時 AWS，您會被視為委託人。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫 的委託人許可 AWS 服務，結合 AWS 服務 請求向下游服務提出請求。只有當服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱轉發存取工作階段。

Amazon EVS 的服務角色

支援服務角色：否

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

Amazon EVS 的服務連結角色

支援服務連結角色：是

服務連結角色是連結至 的一種服務角色 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶 ，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需建立或管理 Amazon EVS 服務連結角色的詳細資訊，請參閱 the section called “使用服務連結角色”。

Amazon EVS 身分型政策範例

根據預設， IAM 使用者 和 角色沒有建立或修改 Amazon EVS 資源的許可。他們也無法使用 AWS 管理主控台 AWS CLI或 AWS API 執行任務。 IAM 管理員必須建立 IAM 政策，授予使用者和角色對所需指定資源執行特定 API 操作的許可。然後，管理員必須將這些政策連接到需要這些許可的 IAM 使用者或 群組。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的使用 JSON 編輯器建立政策。

主題

- 政策最佳實務
- 使用 Amazon EVS 主控台
- 允許使用者檢視他們自己的許可
- 建立和管理 Amazon EVS 環境
- 取得並列出 Amazon EVS 環境、主機和 VLANs

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 Amazon EVS 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 受管政策並轉向最低權限許可 – 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 – 當您使用 IAM 政策設定許可時，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 套用許可的詳細資訊，請參閱《IAM 使用者指南》中的 中的政策和許可 IAM。
- 使用 IAM 政策中的條件來進一步限制存取 – 您可以將條件新增至政策，以限制對動作和資源的存取。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 驗證您的 IAM 政策以確保安全和功能許可 – IAM Access Analyzer 驗證新的和現有的政策，以便政策遵守 IAM 政策語言 (JSON) 和 IAM 最佳實務。 IAM Access Analyzer 提供超過 100 個政策檢查和可行的建議，以協助您撰寫安全和功能政策。如需詳細資訊，請參閱《IAM 使用者指南》中的IAM Access Analyzer 政策驗證。
- 需要多重要素驗證 (MFA) – 如果您的案例需要帳戶中的 IAM 使用者 或根使用者，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。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 API 存取。

使用 Amazon EVS 主控台

若要存取 Amazon EVS 主控台，IAM 主體必須擁有一組最低許可。這些許可必須允許委託人列出和檢視您 中 Amazon EVS 資源的詳細資訊 AWS 帳戶。如果您建立比最低必要許可更嚴格的身分型政策，則對於具有該政策的主體而言，主控台將無法如預期運作。

為了確保您的 IAM 主體仍然可以使用 Amazon EVS 主控台，請使用您自己的唯一名稱建立政策，例如 `AmazonEVSAdminPolicy`。將政策連接至主體。如需詳細資訊，請參閱《IAM 使用者指南》中的新增許可到使用者。

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

```
            "Sid": "EVSServiceLinkedRole",
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/evs.amazonaws.com/
AWSServiceRoleForEVS",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "evs.amazonaws.com"
                }
            }
        }
    ]
}
```

對於僅呼叫 AWS CLI 或 AWS API 的使用者，您不需要允許最低主控台許可。反之，只需允許存取符合您嘗試執行之 API 作業的動作就可以了。

允許使用者檢視他們自己的許可

此範例示範如何建立政策， IAM 使用者 允許 檢視連接至其使用者身分的內嵌和受管政策。此政策包含在主控台或使用 或 AWS CLI AWS API 以程式設計方式完成此動作的許可。

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

```
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

建立和管理 Amazon EVS 環境

此範例政策包含建立和刪除 Amazon EVS 環境所需的許可，以及在建立環境之後新增或刪除主機。

您可以將 AWS 區域 取代為您要 AWS 區域 在其中建立環境的 。如果您的帳戶已具有 AWSServiceRoleForAmazonEVS 角色，您可以移除來自政策的 `iam:CreateServiceLinkedRole` 動作。如果您曾經在帳戶中建立 Amazon EVS 環境，除非您刪除，否則具有這些許可的角色已存在。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ReadOnlyDescribeActions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeHosts",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeAddresses",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeSubnets",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeInstances",
                "ec2:DescribeRouteServers",
                "ec2:DescribeRouteServerEndpoints",
                "ec2:DescribeRouteServerPeers",
                "ec2:DescribePlacementGroups",
```

```
                "ec2:DescribeVolumes",
                "ec2:DescribeSecurityGroups",
                "support:DescribeServices",
                "support:DescribeSupportLevel",
                "servicequotas:GetServiceQuota",
                "servicequotas:ListServiceQuotas"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ModifyNetworkInterfaceStatement",
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "ModifyNetworkInterfaceStatementForSubnetAssociation",
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyNetworkInterfaceAttribute"
            ],
            "Resource": "arn:aws:ec2:*:*:subnet/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "CreateNetworkInterfaceWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
```

```
            ],
            "Condition": {
                "Null": {
                    "aws:RequestTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "CreateNetworkInterfaceAdditionalResources",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:security-group/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "TagOnCreateEC2Resources",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*",
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:volume/*",
                "arn:aws:ec2:*:*:subnet/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": [
                        "CreateNetworkInterface",
                        "RunInstances",
                        "CreateSubnet",
                        "CreateVolume"
                    ]
                },
```

```
                "Null": {
                    "aws:RequestTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "DetachNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:DetachNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*",
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "RunInstancesWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Condition": {
                "Null": {
                    "aws:RequestTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "RunInstancesWithTagResource",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
```

```
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "RunInstancesWithoutTag",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:image/*",
                "arn:aws:ec2:*:*:security-group/*",
                "arn:aws:ec2:*:*:key-pair/*",
                "arn:aws:ec2:*:*:placement-group/*"
            ]
        },
        {
            "Sid": "TerminateInstancesWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:TerminateInstances",
                "ec2:ModifyInstanceAttribute"
            ],
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "CreateSubnetWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSubnet"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*"
```

```
            ],
            "Condition": {
                "Null": {
                    "aws:RequestTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "CreateSubnetWithoutTagForExistingVPC",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSubnet"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:vpc/*"
            ]
        },
        {
            "Sid": "DeleteSubnetWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteSubnet"
            ],
            "Resource": "arn:aws:ec2:*:*:subnet/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "VolumeDeletion",
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteVolume"
            ],
            "Resource": "arn:aws:ec2:*:*:volume/*",
             "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
```

```
            "Sid": "VolumeDetachment",
            "Effect": "Allow",
            "Action": [
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "RouteServerAccess",
            "Effect": "Allow",
            "Action": [
                "ec2:GetRouteServerAssociations"
            ],
            "Resource": "arn:aws:ec2:*:*:route-server/*"

        },
        {
            "Sid": "EVSServiceLinkedRole",
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/evs.amazonaws.com/
AWSServiceRoleForEVS",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "evs.amazonaws.com"
                }
            }
        },
        {
            "Sid": "SecretsManagerCreateWithTag",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:CreateSecret"
            ],
```

```
            "Resource": "arn:aws:secretsmanager:*:*:secret:*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/AmazonEVSManaged": "true"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AmazonEVSManaged"
                    ]
                }
            }
        },
        {
            "Sid": "SecretsManagerTagging",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:TagResource"
            ],
            "Resource": "arn:aws:secretsmanager:*:*:secret:*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/AmazonEVSManaged": "true",
                    "aws:ResourceTag/AmazonEVSManaged": "true"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AmazonEVSManaged"
                    ]
                }
            }
        },
        {
            "Sid": "SecretsManagerOps",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:DeleteSecret",
                "secretsmanager:GetSecretValue",
                "secretsmanager:UpdateSecret"
            ],
            "Resource": "arn:aws:secretsmanager:*:*:secret:*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
```

```
            }
        },
        {
            "Sid": "SecretsManagerRandomPassword",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetRandomPassword"
            ],
            "Resource": "*"
        },
        {
            "Sid": "EVSPermissions",
            "Effect": "Allow",
            "Action": [
                "evs:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KMSKeyAccessInConsole",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey"
            ],
            "Resource": "arn:aws:kms:*:*:key/*"
        },

        {
            "Sid": "KMSKeyAliasAccess",
            "Effect": "Allow",
            "Action": [
                "kms:ListAliases"
            ],
            "Resource": "*"
        }
    ]
}
```

取得並列出 Amazon EVS 環境、主機和 VLANs

此範例政策包含管理員取得和列出 us-east-2 中指定帳戶內所有 Amazon EVS 環境、主機和 VLANs 所需的最低許可 AWS 區域。

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

對 Amazon EVS 身分和存取進行故障診斷

使用以下資訊來協助您診斷和修正使用 Amazon EVS 和 時可能遇到的常見問題 IAM。

主題

- AccessDeniedException
- 我想要允許 以外的人員 AWS 帳戶 存取我的 Amazon EVS 資源

AccessDeniedException

如果您在呼叫 AWS API 操作`AccessDeniedException`時收到 ，則您使用的 IAM 主體憑證沒有發出該呼叫所需的許可。

```
An error occurred (AccessDeniedException) when calling the CreateEnvironment operation:
User: arn:aws:iam::111122223333:user/user_name is not authorized to perform:
evs:CreateEnvironment on resource: arn:aws:evs:region:111122223333:environment/my-env
```

在先前的範例訊息中，使用者沒有呼叫 Amazon EVS `CreateEnvironment` API 操作的許可。若要提供 Amazon EVS 管理員許可給 IAM 主體，請參閱 the section called “Amazon EVS 身分型政策範例”。

如需 IAM 的一般資訊，請參閱《IAM 使用者指南》中的使用 政策控制對 AWS 資源的存取。

我想要允許 以外的人員 AWS 帳戶 存取我的 Amazon EVS 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要了解 Amazon EVS 是否支援這些功能，請參閱 the section called “Amazon EVS 如何使用 IAM”。
- 若要了解如何在您擁有 AWS 帳戶 的 資源間提供存取，請參閱《IAM 使用者指南》中的AWS 帳戶 在您擁有的另一個 IAM 使用者 中提供存取。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的將存取權提供給第三方 AWS 帳戶 擁有。
- 若要了解如何透過聯合身分提供存取權，請參閱《IAM 使用者指南》中的提供存取權給外部驗證的使用者 （ 聯合身分 ）。
- 若要了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的IAM 角色與資源型政策的差異。

AWS Amazon EVS 的 受管政策

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 AWS 受管政策中定義的許可，則更新會影響政策連接的所有主體身分 （ 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：AmazonEVSServiceRolePolicy

您不得將 AmazonEVSServiceRolePolicy 連接到 IAM 實體。此政策會連接到服務連結角色，允許 Amazon EVS 代表您執行動作。如需詳細資訊，請參閱the section called “使用服務連結角色”。當您使用具有 iam:CreateServiceLinkedRole許可的 IAM 主體建立環境時，服務AWSServiceRoleforAmazonEVS連結角色會自動為您建立並連接此政策。

此政策允許AWSServiceRoleForAmazonEVS服務連結角色 AWS 服務 代表您呼叫 。

許可詳細資訊

此政策包含下列許可，允許 Amazon EVS 完成下列任務。

- ec2 - 探索 VPC 聯網元件，包括子網路和 VPCs。建立、修改、標記和刪除彈性網路介面，這些介面用於在您的 VPC 子網路中建立 Amazon EVS 和 VMware Virtual Cloud Foundation (VCF) SDDC Manager 設備之間的持久性連線。Amazon EVS 需要此連線才能部署、管理和監控 VCF 部署。
- ec2 - 刪除 Amazon EVS 在您提出 EVS 主機刪除請求時建立的 EC2 執行個體。描述和修改 EC2 執行個體屬性，以便在需要時停用預設 EC2 執行個體終止和停止保護，以支援 EVS 主機刪除。
- ec2 - 管理 Cloud Builder 安裝和清除的 EBS 磁碟區。在環境建立期間，Cloud Builder 會安裝在其中一個 Amazon EVS 部署的主機上，以執行 VCF 組態變更。完成後，Amazon EVS 會透過分離和刪除儲存所在的 EC2 磁碟區來移除 Cloud Builder。
- ec2 - 如果您請求刪除環境，請代表您刪除 EVS VLAN 子網路。
- secretsmanager - 刪除 Amazon EVS 在環境建立期間在 AWS Secrets Manager 中建立和存放的 VCF 密碼。如果環境建立失敗或您請求刪除環境，Amazon EVS 會刪除服務在您帳戶中建立的所有秘密。當您透過提供 AWS 秘密 ARN 設定 vCenter 連接器時，從 Secrets Manager 擷取 vCenter 登入資料。許可的範圍具有資源標籤條件EvsAccess=true，以確保 Amazon EVS 僅存取明確標記用於 Amazon EVS vCenter 存取的秘密。
- kms - 當存放在 Secrets Manager 中的 vCenter 登入資料使用 KMS 金鑰加密時，解密秘密並描述 KMS 金鑰。許可的範圍包含資源標籤條件EvsAccess=true，以確保 Amazon EVS 僅存取明確標記用於 vCenter 存取的 KMS 金鑰。
- cloudwatch - 針對具有配額 CloudWatch 的 Amazon EVS 資源，將 AWS 用量指標發佈至 。

若要檢視政策的詳細資訊，包括最新版本的 JSON 政策文件，請參閱《 AWS 受管政策參考指南》中的 AmazonEVSServiceRolePolicy。

AWS 受管政策的 Amazon EVS 更新

檢視自此服務開始追蹤 Amazon EVS AWS 受管政策更新以來的詳細資訊。如需有關此頁面變更的自動提醒，請訂閱 文件歷史紀錄 頁面的 RSS 摘要。

變更	描述	Date
AmazonEVSServiceRolePolicy — 政策已更新	Amazon EVS 已更新政策，以允許服務從 AWS Secrets	2026 年 3 月 23 日

變更	描述	Date
	Manager 擷取 vCenter 憑證，並解密使用 KMS 金鑰加密的秘密。如需詳細資訊，請參閱 the section called “AWS 受管政策：AmazonEVSServiceRolePolicy”。	
AmazonEVSServiceRolePolicy — 政策已更新	Amazon EVS 已更新政策，新增完整的資源管理功能，包括 EC2 執行個體管理、EBS 磁碟區操作和 AWS Secrets Manager 整合。如需詳細資訊，請參閱 the section called “AWS 受管政策：AmazonEVSServiceRolePolicy”。	2025 年 8 月 14 日
AmazonEVSServiceRolePolicy — 政策已更新	Amazon EVS 已更新政策，以允許服務刪除 EVS VLAN 子網路，並將 Amazon EVS 用量指標發佈至其中 CloudWatch。如需詳細資訊，請參閱 the section called “AWS 受管政策：AmazonEVSServiceRolePolicy”。	2025 年 7 月 14 日
AmazonEVSServiceRolePolicy — 新增的政策	Amazon EVS 新增了允許服務連線到客戶帳戶中 VPC 子網路的新政策。服務功能需要此連線。如需詳細資訊，請參閱 the section called “AWS 受管政策：AmazonEVSServiceRolePolicy”。	2025 年 6 月 9 日
Amazon EVS 已開始追蹤變更	Amazon EVS 開始追蹤其 AWS 受管政策的變更。	2025 年 6 月 9 日

使用 Amazon EVS 的服務連結角色

Amazon Elastic VMware Service 使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至 Amazon EVS 的唯一 IAM 角色類型。服務連結角色是由 Amazon EVS 預先定義，並包含該服務代表您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可讓您更輕鬆地設定 Amazon EVS，因為您不必手動新增必要的許可。Amazon EVS 會定義其服務連結角色的許可，除非另有定義，否則只有 Amazon EVS 可以擔任其角色。定義的許可包括信任政策和許可政策，且該許可政策無法附加至其他 IAM 實體。

您必須先刪除服務連結角色的相關資源，才能將其刪除。這可保護您的 Amazon EVS 資源，因為您不會不小心移除存取資源的許可。

如需關於支援服務連結角色的其他服務的資訊，請參閱可搭配 IAM 運作的AWS 服務，尋找 Service-Linked Role (服務連結角色) 欄中顯示為 Yes (是) 的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

Amazon EVS 的服務連結角色許可

Amazon EVS 使用名為 的服務連結角色AWSServiceRoleForAmazonEVS。此角色允許 Amazon EVS 管理您帳戶中的環境。連接的政策允許角色管理下列資源：EVS 彈性網路介面、EVS VLAN 子網路、EVS 主機、VPCs 和 CloudWatch 指標。

AWSServiceRoleForAmazonEVS 服務連結角色信任下列服務以擔任角色：

- evs.amazonaws.com

角色許可政策允許 Amazon EVS 對指定的資源完成下列動作：

- AmazonEVSServiceRolePolicy

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的服務連結角色許可。

為 Amazon EVS 建立服務連結角色

您不需要手動建立一個服務連結角色。當您在 AWS 管理主控台、 CLI 或 AWS API AWS 中建立環境時，Amazon EVS 會為您建立服務連結角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您建立環境時，Amazon EVS 會再次為您建立服務連結角色。

編輯 Amazon EVS 的服務連結角色

Amazon EVS 不允許您編輯AWSServiceRoleForAmazonEVS服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱《IAM 使用者指南》中的編輯服務連結角色。

刪除 Amazon EVS 的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。然而，務必清除您的服務連結角色，之後才能以手動方式將其刪除。

清除服務連結角色

在您使用 IAM 刪除服務連結角色之前，您必須先刪除該角色所使用的任何資源。如需使用主機刪除 Amazon EVS 環境的步驟，請參閱 the section called “刪除 Amazon EVS 主機和環境”。

> **Note**
>
> 如果您嘗試刪除資源時，Amazon EVS 服務正在使用該角色，則刪除可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

手動刪除 服務連結角色

使用 IAM 主控台、CLI AWS 或 AWS API 來刪除AWSServiceRoleForAmazonEVS服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

Amazon EVS 服務連結角色支援的區域

Amazon EVS 支援在提供服務的所有區域中使用服務連結角色。如需詳細資訊，請參閱《 AWS 一般參考指南》中的 Amazon Elastic VMware Service 端點和配額。

Amazon EVS 中的彈性

AWS 全球基礎設施是以 AWS 區域 和 可用區域為基礎建置。 AWS 區域 提供多個實體隔離和隔離的可用區域，這些區域透過低延遲、高輸送量和高度備援聯網進行連接。透過可用區域，您可以設計與操

作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

Amazon EVS 環境可在單一 AWS 可用區域中使用。為了確保 Amazon EVS 單一可用區域基礎設施的高可用性，Amazon EVS 提供下列功能：

> **Note**
>
> Amazon EVS 目前僅支援單一可用區部署。

- Amazon EVS 支援使用 AWS Elastic Disaster Recovery 來自動化資料的備份和復原。
- Amazon EVS 部署作用中/待命 NSX Edge 叢集，每個 VCF 需求有兩個 NSX Edge 節點。NSX Edge 節點會在不同的主機上執行，以確保高可用性，並在 NSX Edge 節點失敗的罕見情況下允許快速容錯移轉。
- Amazon EVS 會部署四個 ESX 主機的最低環境，這是 VCF 所需的。您可以在部署後新增其他主機。這是 VMware 設計需求，以確保適當的 vSAN 規定人數，並在維護操作和主機故障期間維持可用性。如需詳細資訊，請參閱 VMware Cloud Foundation 文件中的 vSphere Cluster Design for VMware Cloud Foundation。
- Amazon EVS 支援對 EC2 主機使用 EC2 分割區置放群組或叢集置放群組。分割區置放群組會將 EC2 執行個體分散到邏輯分割區，讓一個分割區中的執行個體群組不會與不同分割區中的執行個體群組共用基礎硬體。此策略有助於降低大型分散式工作負載相關硬體故障的可能性。叢集置放群組用於將您的 EC2 執行個體放置在相同的實體機架中，以確保低延遲。如需詳細資訊，請參閱 Amazon EC2 《使用者指南》中的分割區置放群組。

如需 AWS 區域和可用區域的詳細資訊，請參閱 AWS 全球基礎設施。

VMware 元件彈性

Amazon EVS 客戶負責設定在 Amazon EVS 上執行的 VMware 元件，以確保虛擬機器 (VMs) 和工作負載彈性的高可用性。

Amazon EVS 支援下列 VMware Cloud Foundation (VCF) 彈性功能：

- vSphere 複寫 - 為災難復原和工作負載遷移目的提供以主機為基礎的非同步 VMs 複寫。如需詳細資訊，請參閱 VMware vSphere 複寫文件中 vSphere 複寫的運作方式。 vSphere
- vSAN 資料保護 - 可讓您使用 vSAN 叢集上本機儲存的原生快照，快速從勒索軟體攻擊的操作失敗中復原 VMs。如需詳細資訊，請參閱 vSAN 文件中的使用 vSAN 資料保護。

- vSphere HA - 在主機故障時為 VMs 提供自動容錯移轉。如需詳細資訊，請參閱 VCF 文件中的適用於 VMware Cloud Foundation 的 vCenter Server 高可用性設計。
- vSphere 容錯能力 (FT) - 透過建立和維護另一個相同且持續可用的 VM，在容錯移轉情況下予以取代，為關鍵任務 VMs 提供持續可用性。如需詳細資訊，請參閱 vSphere 文件中的容錯如何運作。
- vSAN 容錯率失敗 (FTT) - 一種 vSAN 設定，可決定 VM 在無法存取之前可承受多少主機故障。這會定義 vSAN 叢集內虛擬機器的備援和容錯能力層級。如需詳細資訊，請參閱 vSAN 文件中的在 vSAN 叢集中使用故障網域來容忍其他故障。

將 Amazon EVS 與其他 AWS 服務搭配使用

Amazon EVS 與其他 整合 AWS 服務 ，以提供其他解決方案。本主題識別 Amazon EVS 用來新增功能的一些服務。

主題

- 使用 AWS CloudFormation 建立 Amazon EVS 資源
- 使用 Amazon FSx for NetApp ONTAP 執行高效能工作負載

使用 AWS CloudFormation 建立 Amazon EVS 資源

Amazon EVS 已與 AWS CloudFormation 整合，這項服務可協助您建立和設定 AWS 資源，以減少建立和管理資源和基礎設施的時間。您可以建立範本來描述您想要的所有 AWS 資源，例如 Amazon EVS 環境， AWS CloudFormation 會負責為您佈建和設定這些資源。

當您使用 AWS CloudFormation 時，您可以重複使用範本來一致且重複地設定 Amazon EVS 資源。只需描述您的資源一次，然後在多個 AWS 帳戶 和 區域中逐一佈建相同的資源。

Amazon EVS 和 AWS CloudFormation 範本

若要佈建和設定 Amazon EVS 和相關服務的資源，您必須了解 AWS CloudFormation 範本。範本是以 JSON 或 YAML 格式化的文本檔案。這些範本說明您想要在 AWS CloudFormation 堆疊中佈建的資源。如果您不熟悉 JSON 或 YAML，您可以使用 AWS CloudFormation 設計工具來協助您開始使用 AWS CloudFormation 範本。如需詳細資訊，請參閱《AWS CloudFormation 使用者指南》中的什麼是 CloudFormation 設計工具？。 AWS CloudFormation

Amazon EVS 支援在 AWS CloudFormation 中建立環境。如需詳細資訊，包括您環境的 JSON 和 YAML 範本範例，請參閱《 AWS CloudFormation 使用者指南》中的 Amazon EVS 資源類型參考。

進一步了解 AWS CloudFormation

若要進一步了解 AWS CloudFormation，請參閱下列資源：

- AWS CloudFormation
- AWS CloudFormation 使用者指南
- AWS CloudFormation 命令列界面使用者指南

使用 Amazon FSx for NetApp ONTAP 執行高效能工作負載

Amazon FSx for NetApp ONTAP 是一種儲存服務，允許您在雲端中啟動和執行全受管的 ONTAP 檔案系統。ONTAP 是 NetApp 的檔案系統技術，提供受到廣泛採用的資料存取和資料管理功能。FSx for ONTAP 提供內部部署 NetApp 檔案系統的功能、效能和 APIs，具有全受管 AWS 服務的靈活性、可擴展性和簡易性。如需詳細資訊，請參閱《FSx for ONTAP 使用者指南》。

Amazon EVS 支援使用 Amazon FSx for NetApp ONTAP 做為 NFS/iSCSI 資料存放區，以及做為在 Amazon EVS 上執行 VMware 虛擬機器的訪客連線儲存體。

將 FSx for NetApp ONTAP 設定為 NFS 資料存放區

下列程序詳細說明使用 FSx 主控台和在 Amazon EVS 上執行的 VMware vSphere 用戶端界面，將 FSx for NetApp ONTAP 設定為 Amazon EVS 的 NFS 資料存放區所需的最低步驟。

先決條件

將 Amazon EVS 與 Amazon FSx for NetApp ONTAP 搭配使用之前，請確定已完成下列先決條件任務。

- Amazon EVS 環境會部署在您的 Virtual Private Cloud (VPC) 中。如需詳細資訊，請參閱開始使用。
- 您可以存取在 Amazon EVS 上執行的 vSphere 用戶端。
- 您或您的儲存管理員必須擁有必要的許可，才能在 VPC 中建立和管理 FSx for ONTAP 檔案系統。如需詳細資訊，請參閱 Amazon FSx for NetApp ONTAP 的身分和存取管理。

您的 IAM 主體具有適當的許可，可在 VPC 中建立和管理 FSx for ONTAP 檔案系統。如需詳細資訊，請參閱the section called “建立和管理 Amazon EVS 環境”。

建立 FSx for NetApp ONTAP 檔案系統

1. 前往 Amazon FSx 主控台。
2. 選擇 Create file system (建立檔案系統)。
3. 選取 Amazon FSx for NetApp ONTAP。
4. 選擇下一步。
5. 選取標準建立。
6. 針對部署類型，選取單一可用區部署選項。

> **Note**
>
> Amazon EVS 目前僅支援單一可用區部署。

7. 對於 SSD 儲存容量，請指定 1024 GiB。
8. 針對輸送量容量，選擇指定輸送量容量。針對單一可用區 1 選擇至少 512 MB/s，或針對單一可用區 2 選擇至少 768 MB/s。
9. 選取可連線至 Amazon EVS VLAN 子網路的 Amazon EVS VPC。
10. 選取安全群組，允許 ONTAP NFS 流量到 Amazon EVS 主機 VMkernel 管理 VLAN 子網路的所有必要 FSx。 VMkernel
11. 選取將部署檔案系統的 Amazon EVS 服務存取子網路。如需詳細資訊，請參閱the section called "服務存取子網路"。
12. 對於 Junction 路徑，指定有意義的名稱，例如 `/vol1`以在 vSphere 中識別此磁碟區。
13. 在預設磁碟區組態中，將儲存效率設定為已啟用。
14. 將剩餘的設定保留為預設值，然後選擇下一步。
15. 檢閱檔案系統屬性，然後選擇建立檔案系統。

擷取儲存虛擬機器的 NFS DNS 名稱

1. 前往 Amazon FSx 主控台。
2. 在左側選單中，選取檔案系統。
3. 選擇新建立的檔案系統。
4. 選取儲存虛擬機器索引標籤。
5. 選擇儲存虛擬機器。
6. 選取端點索引標籤。
7. 複製網路檔案系統 (NFS) DNS 名稱以供稍後在 VMware Vsphere 中使用。

使用 FSx for ONTAP 磁碟區在 vSphere 中建立 NFS 資料存放區 FSx

遵循在 vSphere 環境中建立 NFS 資料存放區中的指示，將 Amazon FSx for NetApp ONTAP 設定為 VMware vSphere 的外部儲存。對於 vSphere 用戶端界面中的伺服器設定，請使用您在上一個步驟中複製的儲存虛擬機器 (SVM) NFS DNS 名稱。

將 FSx for NetApp ONTAP FSx 設定為 iSCSI 資料存放區

下列程序詳細說明使用 FSx 主控台和在 Amazon EVS 上執行的 VMware vSphere 用戶端界面，將 FSx for NetApp ONTAP 設定為 Amazon EVS 的 iSCSI 資料存放區所需的最低步驟。

先決條件

將 Amazon EVS 與 Amazon FSx for NetApp ONTAP 搭配使用之前，請確定已完成下列先決條件任務。

- Amazon EVS 環境會部署在您的 Virtual Private Cloud (VPC) 中。如需詳細資訊，請參閱開始使用。
- 您可以存取在 Amazon EVS 上執行的 vSphere 用戶端。
- 您或您的儲存管理員必須擁有必要的許可，才能在 VPC 中建立和管理 FSx for ONTAP 檔案系統。如需詳細資訊，請參閱 Amazon FSx for NetApp ONTAP 的身分和存取管理。

建立 FSx for NetApp ONTAP 檔案系統

1. 前往 Amazon FSx 主控台。
2. 選擇 Create file system (建立檔案系統)。
3. 選取 Amazon FSx for NetApp ONTAP。
4. 選擇下一步。
5. 選取標準建立。
6. 針對部署類型，選取單一可用區部署選項。

> **Note**
>
> Amazon EVS 目前僅支援單一可用區部署。

7. 對於 SSD 儲存容量，請指定 1024 GiB。
8. 針對輸送量容量，選擇指定輸送量容量。針對單一可用區 1 選擇至少 512 MB/s，或針對單一可用區 2 選擇至少 768 MB/s。
9. 選取可連線至 Amazon EVS VLAN 子網路的 Amazon EVS VPC。
10. 選取安全群組，允許 ONTAP iSCSI 流量到 Amazon EVS 主機 VMkernel 管理 VLAN 子網路的所有必要 FSx。
11. 選取將部署檔案系統的 Amazon EVS 服務存取子網路。如需詳細資訊，請參閱the section called “服務存取子網路”。

12.在預設磁碟區組態中，將儲存效率設定為已啟用。

13.將剩餘的設定保留為預設值，然後選擇下一步。

14.檢閱檔案系統屬性，然後選擇建立檔案系統。

在 vSphere 中為 ESX 主機儲存體設定軟體 iSCSI 轉接器

對於每個 ESX 主機，您必須設定軟體 iSCSI 轉接器，ESX 主機才能使用它來存取 iSCSI 儲存。如需在 vSphere 中為 ESX 主機設定軟體 iSCSI 轉接器的說明，請參閱 VMware vSphere 產品文件中的新增或移除軟體 iSCSI 轉接器。

設定軟體 iSCSI 轉接器之後，請複製與 iSCSI 轉接器相關聯的 iSCSI 合格名稱 (IQN)。這些值將在稍後使用。

建立 iSCSI LUN

FSx for ONTAP 可讓您建立專門用於 iSCSI 存取的邏輯單位編號 (LUNs)，為 ESX 主機提供共用區塊儲存。您可以使用 NetApp ONTAP CLI 來建立 LUN。

以下是範例命令。

> **Note**
>
> 建議將 LUN 大小設定為磁碟區大小的 90%。

```
lun create -vserver <your_svm_name> \
-path /vol/<your_volume_name>/<lun_name> \
-size <required_datastore_capacity> \
-ostype vmware
```

如需詳細資訊，請參閱《FSx for ONTAP 使用者指南》中的建立 iSCSI LUN。

設定啟動器群組並將其對應至 iSCSI LUN

現在您已建立 iSCSI LUN，程序的下一個步驟是建立啟動器群組 (igroup)，將磁碟區連接到叢集，並將 LUN 映射到啟動器群組。您可以使用 NetApp ONTAP CLI 來執行這些動作。

1. 設定啟動器群組。

以下是範例命令。對於 `--initiator`，請使用您在上一個步驟中複製的 iSCSI 轉接器 IQNs。

```
igroup create <svm_name> \
-igroup <initiator_group_name> \
-protocol iscsi \
-ostype vmware \
-initiator <esxi_iqn_1>,<esxi_iqn_2>,<esxi_iqn_3>,<esxi_iqn_4>
```

2. 確認 `igroup`存在。

```
lun igroup show
```

3. 將 LUN 映射至啟動器群組。以下是範例命令。

```
lun mapping create -vserver <svm_name> \
-path /vol/<vol_name>/<lun_name> \
-igroup <initiator_group_name> \
-lun-id <scsi_lun_number_for this_datastore>
```

4. 使用 `lun show -path`命令來確認 LUN 已建立、上線和映射。

```
lun show -path /vol/<vol_name>/<lun_name> -fields state,mapped,serial-hex
```

如需詳細資訊，請參閱《FSx for ONTAP 使用者指南》中的佈建 Linux 的 iSCSI 或佈建 Windows 的 iSCSI。 FSx

在 vSphere 中設定 iSCSI LUN 的動態探索

若要允許 ESX 主機查看 iSCSI LUN，您必須為 vSphere 用戶端界面中的每個主機設定動態探索。在 iSCSI 伺服器欄位中，輸入您在上一個步驟中複製的 (NFS) DNS 名稱。如需詳細資訊，請參閱 VMware vSphere 產品文件中的設定 iSCSI 的動態或靜態探索和 ESX 主機上的 iSER。

使用 iSCSI LUN 在 VMware vSphere 中建立 VMFS 資料存放區

虛擬機器檔案系統 (VMFS) 資料存放區可做為 VMware 虛擬機器的儲存庫。遵循建立 vSphere VMFS 資料存放區中的指示，使用您先前設定的 iSCSI LUN 在 VMware vSphere 中設定 VMFS 資料存放區。

疑難排解

本章詳細說明在建立或管理 Amazon EVS 環境時遇到的一些常見問題。

故障診斷失敗的環境狀態檢查

Amazon EVS 會在您的環境中執行自動檢查，以識別問題。您可以檢視環境的狀態，以識別特定和可偵測到的問題。

檢閱環境狀態檢查資訊

使用 Amazon EVS 主控台調查受損的環境

1. 開啟 Amazon EVS 主控台。
2. 在導覽窗格中，選擇環境，然後選取您的環境。
3. 選取詳細資訊索引標籤以查看環境的概觀。
4. 檢查環境狀態。將滑鼠暫留在此欄位上，以展開包含每個環境狀態檢查個別結果的快顯視窗。

連線能力檢查失敗

連線能力檢查會驗證 Amazon EVS 是否持續連線至 SDDC Manager。如果 Amazon EVS 無法到達環境，則此檢查會失敗。

如果此檢查失敗，Amazon EVS 將無法再連接 SDDC Manager 來驗證環境狀態，並且無法再將主機加入到環境中。可連線性失敗也會導致授權金鑰重複使用，以及金鑰涵蓋範圍檢查失敗，而且主機計數檢查會傳回未知回應。

若要確保可連線性，請檢查下列項目：

- 確認您的憑證有效且未過期。您可以使用 SDDC Manager UI 或 vSphere 用戶端來管理 VCF 環境中的憑證。部署後，建議您取代 VMware Cloud Foundation 管理網域的所有憑證。如需詳細資訊，請參閱 VMware Cloud Foundation 文件中的管理 VMware Cloud Foundation 中的憑證。
- 確保您的 DNS 伺服器可從服務存取子網路存取、DNS 記錄有效，而且不存在重複的主機名稱或 IP 地址。
- 如果您想要建立自己的防火牆規則，請遵循下列準則：
  - 允許 TCP/UDP 存取 DNS 伺服器。

- 允許 HTTPS/SSH 存取主機管理 VLAN 子網路。
- 允許 HTTPS/SSH 存取管理 VM VLAN 子網路。

如果您在遵循本指南後仍無法解決問題，我們建議您聯絡 AWS Support 以取得進一步協助。

主機計數檢查失敗

此檢查會確認您的環境至少有四個主機，這是 VCF 5.2.x 的需求。

如果此檢查失敗，您將需要新增主機，以使您的環境符合此最低要求。Amazon EVS 僅支援具有 4 至 16 部主機的環境。

金鑰重複使用檢查失敗

此檢查會驗證 VCF 授權金鑰並未由其他 Amazon EVS 環境使用。VCF 授權只能在一個 Amazon EVS 環境中使用。如果您在已經由另一個環境使用的環境建立請求中提供 VCF 授權金鑰，則此檢查會失敗。

如果此檢查失敗，您會收到無法建立 Amazon EVS 環境的錯誤回應。若要解決此問題，請在 SDDC Manager 中檢閱授權設定，並以未使用的授權取代任何先前使用的授權。

> **Important**
>
> 使用 SDDC Manager 使用者介面來管理 VCF 解決方案和 vSAN 授權金鑰。Amazon EVS 會要求您在 SDDC Manager 中維護有效的 VCF 解決方案和 vSAN 授權金鑰，服務才能正常運作。雖然金鑰必須使用 vSphere 用戶端指派給主機和 vSAN 叢集，但您必須確定這些金鑰也會出現在 SDDC Manager 使用者介面的授權畫面中。

金鑰涵蓋範圍檢查失敗

此檢查會驗證指派給 vCenter Server 的 VCF 授權金鑰，是否為所有部署的主機配置足夠的 vCPU 核心和 vSAN 儲存容量 (TiB)。

如果此檢查失敗，您會收到無法建立 Amazon EVS 環境的錯誤回應。金鑰涵蓋失敗可能表示存在下列其中一個問題：

- VCF 授權未正確指派給 vCenter 伺服器。您必須在評估期到期或目前指派的授權到期前，將授權指派給 vCenter Server。如果是這個問題，請檢閱 SDDC Manager 中的授權指派情況。

- 目前的 VCF 授權不涵蓋 vCPU 核心和 vSAN 儲存容量需求。VCF 解決方案金鑰必須至少有 256 個核心。vSAN 授權金鑰必須至少有 110 TiB 的 vSAN 容量。如果是這個問題，請在 SDDC Manager 中新增 vSAN 授權，直到滿足您的使用需求為止。

如果上述動作無法解決問題，請聯絡 AWS Support 以取得進一步協助。

> **Important**
>
> 使用 SDDC Manager 使用者介面來管理 VCF 解決方案和 vSAN 授權金鑰。Amazon EVS 會要求您在 SDDC Manager 中維護有效的 VCF 解決方案和 vSAN 授權金鑰，服務才能正常運作。雖然金鑰必須使用 vSphere 用戶端指派給主機和 vSAN 叢集，但您必須確定這些金鑰也會出現在 SDDC Manager 使用者介面的授權畫面中。

此主機上的 vSphere HA 代理程式無法到達隔離地址

在 vCenter 使用者介面中，選取 ESX 主機時，您會看到「此主機上的 vSphere HA 代理程式無法到達隔離地址 <IPv6 address>」訊息。

此錯誤訊息表示主機上的 vSphere HA 代理程式無法連線到 vSphere HA 用於活動訊號檢查的預設 IPv6 隔離地址。錯誤訊息並不表示問題，只會因為 Amazon EVS 目前不支援 IPv6 而發生。Amazon EVS 缺少 IPV6 支援不會影響 vSphere HA 的核心功能。

ESX 主機叢集的 vSAN 升級預先檢查失敗

嘗試使用 SDDC Manager 升級 ESX 主機叢集時，vSAN 磁碟相關的預先檢查可能會失敗。這是因為 Amazon EVS 使用 vSAN Express Storage Architecture (ESA)，且升級預先檢查不適用於 vSAN ESA。如需詳細資訊，請參閱本主題的 Broadcom 知識庫文章。

新增主機因不相容的叢集映像而失敗

問題

當您將主機新增至您的環境時，主機具有最新版本的 EVS 自訂廠商附加元件。如果您的環境使用具有較舊附加元件版本的主機，新增主機會失敗，並顯示新主機與叢集映像不相容的錯誤。若要修正此問題，您必須使用 vSphere Lifecyle Manager 從新增的主機擷取最新的可用附加元件版本。

解決方案

請遵循下列步驟。

1. 前往 VMware vCenter Server 中的主機和叢集庫存。
2. 透過建立暫時空白叢集，從新增的主機擷取附加元件。
3. 在基本概念下，選取從 vCenter 庫存中的現有主機匯入映像，然後建立叢集。將所有其他設定保留為預設值。
4. 使用擷取的映像建立此臨時叢集後，您可以刪除臨時叢集。附加元件現在可在 vSphere Lifecycle Manager 儲存庫中使用。
5. 前往您的環境叢集，然後選取更新索引標籤。
6. 編輯叢集映像，並將附加元件版本變更為新擷取的版本。
7. 選擇儲存。
8. 在 SDDC Manager 中，重試失敗的新增主機任務。這將修復您的叢集主機，將所有主機更新為最新的附加元件版本。叢集映像修復需要主機重新啟動。

SDDC Manager 在主機測試期間未通過 VCF 主機驗證

問題

如果您在 Amazon EVS 環境部署之後已更新 ESX 版本，則 SDDC 管理員可能會在委託主機步驟中的 VCF 主機驗證期間失敗。若要修正此問題，您必須使用 vSphere Lifecyle Manager 在新增的主機上升級 ESX。

解決方案

請遵循下列步驟。

> **Important**
>
> 這些步驟需要暫時將主機新增至 SDDC Manager 外部的 vCenter。將 vSphere Lifecyle Manager 用於 ESX 升級以外的任何操作可能會使您的主機無法使用，並要求您刪除和建立新的 Amazon EVS 主機。

1. 前往 VMware vCenter Server 中的主機和叢集庫存。
2. 將主機暫時新增至您的虛擬資料中心，確保使用 映像選取管理主機。ESX 升級完成後，稍後的步驟會移除主機。如需詳細資訊，請參閱 vSphere 文件中的如何將主機新增至 vSphere 資料中心或資料夾。 vSphere

3. 將主機新增至 vSphere 後，請升級主機上的 ESX 版本。這可以在主機的更新索引標籤中完成。編輯主機映像以符合叢集的 ESX 版本。
4. 升級完成後，請從 vCenter 庫存中移除主機。如需詳細資訊，請參閱 vSphere 文件中的如何從 vCenter 伺服器執行個體移除 ESX 主機。
5. 在 SDDC 管理員中委託您的主機。如需詳細資訊，請參閱 VMware Cloud Foundation 文件中的 Commission Hosts。
6. 委託主機之後，請使用 SDDC Manager 將主機新增至叢集。

使用 AWS CloudTrail 記錄 Amazon EVS API 呼叫

Amazon EVS 已與 AWS CloudTrail 整合，CloudTrail 是一種服務，可提供 IAM 使用者、IAM 角色或 Amazon EVS 中 AWS 服務所採取動作的記錄。CloudTrail 會將 Amazon EVS 的所有 AWS API 呼叫擷取為事件。擷取的呼叫包括來自 Amazon EVS 主控台的呼叫，以及對 Amazon EVS API 操作的程式碼呼叫。如果您建立線索，則可以將 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 Amazon EVS 的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台中的事件歷史記錄檢視最新事件。您可以使用 CloudTrail 所收集的資訊，判斷對 Amazon EVS 提出的請求、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱《AWS CloudTrail 使用者指南》。

> **Note**
>
> Amazon EVS 不會記錄非AWS 元件的使用者活動，例如 VCF 環境中的活動。這些活動會記錄在各種 VMware 主控台中，例如 vSphere 和 NSX Manager。
> 如果需要集中式 VCF 記錄，您可以設定 VCF 監控解決方案，例如 VMware Cloud Foundation Operations，以實現此結果。

CloudTrail 中的 Amazon EVS 資訊

當您建立 AWS 帳戶時，會在您的帳戶上啟用 CloudTrail。當活動在 Amazon EVS 中發生時，該活動會與事件歷史記錄中的其他 AWS 服務事件一起記錄在 CloudTrail 事件中。您可以在 AWS 帳戶中檢視、搜尋和下載最近的事件。如需詳細資訊，請參閱《使用 CloudTrail 事件歷史記錄檢視事件》https://docs.aws.amazon.com/awscloudtrail/latest/userguide/view-cloudtrail-events.html。

若要持續記錄您 AWS 帳戶中的事件，包括 Amazon EVS 的事件，請建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。根據預設，當您在主控台中建立線索時，線索會套用至所有 AWS 區域。線索會記錄 AWS 分割區中所有區域的事件，並將日誌檔案傳送到您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務和整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 從多個區域接收 CloudTrail 日誌檔案

- 從多個帳戶接收 CloudTrail 日誌檔案

CloudTrail 會記錄所有 Amazon EVS 動作，並記錄在 Amazon EVS API 參考中。例如，對 `CreateEnvironment`、`GetEnvironment` 和 `DeleteEnvironment` 動作發出的呼叫會在 CloudTrail 記錄檔案中產生專案。

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

- 是否使用根或 AWS Identity and Access Management (IAM) 使用者登入資料提出請求。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 請求是否由其他 AWS 服務提出。

如需詳細資訊，請參閱 CloudTrail userIdentity 元素。

了解 Amazon EVS 日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

Amazon EVS 服務配額

Amazon EVS 已與 Service Quotas 整合，您可以使用 AWS 服務 它從中央位置檢視和管理配額。如需詳細資訊，請參閱Service Quotas 使用者指南中的什麼是 Service Quotas？。

透過 Service Quotas 整合，您可以使用 AWS 管理主控台 或 AWS CLI 來查詢 Amazon EVS 配額的值，並請求提高配額以調整配額。如需詳細資訊，請參閱《Service Quotas 使用者指南》中的請求增加配額和《 AWS CLI 命令參考》中的 request-service-quota-increase。

如需 Amazon EVS 服務配額的詳細資訊，請參閱《 AWS 一般參考指南》中的 Amazon EVS 配額。

Important

確保您的 EC2 執行中隨需標準執行個體配額反映您在 Amazon EVS 上使用的所有 EC2 執行個體所需的 vCPUs 數量。每個 i4i.metal 執行個體使用 128 vCPUs。如需增加 EC2 服務配額的詳細資訊，請參閱《Amazon EC2 使用者指南》中的請求增加。

Note

如果您計劃將 EC2 專用主機用於 Amazon EVS 環境，請確保您的 EC2 專用 i4i 主機配額反映您想要用於所需區域的專用主機數量。如需增加 EC2 服務配額的詳細資訊，請參閱《Amazon EC2 使用者指南》中的請求增加。

Note

如果設定 HCX 網際網路連線，Amazon 提供的連續公有 IPv4 CIDR 區塊網路遮罩長度的 IPAM 配額必須為 /28 或更高。如需詳細資訊，請參閱 IPAM 的配額。

Note

Amazon CloudWatch 會收集具有配額 （ 環境和主機 ） 的 Amazon EVS 資源 AWS 用量指標。如需詳細資訊，請參閱《Amazon CloudWatch 使用者指南》中的 CloudWatch 用量指標。 Amazon CloudWatch

在 中檢視 Amazon EVS 服務配額 AWS 管理主控台

1. 開啟 Service Quotas 主控台。
2. 在左側導覽窗格中，選擇 AWS 服務。
3. 從 AWS 服務清單中，搜尋並選取 Amazon Elastic VMware Service。
4. 選擇檢視配額。

   在服務配額清單中，您可以看到服務配額名稱、套用值（如果有的話）、 AWS 預設配額，以及配額值是否可以調整。
5. 若要檢視服務配額的其他資訊 (例如說明)，請選擇配額名稱。
6. （選用）若要請求增加配額，請選取您要增加的配額，選取在帳戶層級請求增加，輸入或選取所需資訊，然後選取請求。

若要使用 進一步處理服務配額 AWS 管理主控台，請參閱 Service Quotas 使用者指南。若要請求提升配額，請參閱《Service Quotas 使用者指南》中的請求提升配額。

使用 CLI 檢視 Amazon EVS AWS 服務配額

執行下列命令以檢視您的 Amazon EVS 配額。

```
aws service-quotas list-aws-default-service-quotas \
    --query 'Quotas[*].
{Adjustable:Adjustable,Name:QuotaName,Value:Value,Code:QuotaCode}' \
    --service-code evs \
    --output table
```

> **Note**
>
> 傳回的配額是可在目前 AWS 區域中此帳戶中建立的 Amazon EVS 環境或主機數量。

若要使用 CLI AWS 使用更多服務配額，請參閱 AWS CLI 命令參考中的服務配額。若要請求提高配額，請參閱 CLI 命令參考中的 request-service-quota-increase 命令。 AWS

Amazon Elastic VMware Service 使用者指南的文件歷史記錄

下表說明 Amazon Elastic VMware Service 的文件版本。

變更	描述	日期
已更新 AmazonEVSServiceRolePolicy	Amazon EVS 已更新 受管政策`AmazonEVSServiceRolePolicy` ，以允許服務從 AWS Secrets Manager 擷取 vCenter 憑證，並解密使用客戶受管 KMS 金鑰加密的秘密。	2026 年 3 月 23 日
已更新 AmazonEVSServiceRolePolicy	Amazon EVS 已更新 受管政策`AmazonEVSServiceRolePolicy` ，新增完整的資源管理功能，包括 EC2 執行個體管理、EBS 磁碟區操作和 AWS Secrets Manager 整合。如需詳細資訊，請參閱 Amazon EVS AWS 受管政策的更新。	2025 年 8 月 14 日
已更新 AmazonEVSServiceRolePolicy	已更新 AWS 受管政策 AmazonEVSServiceRolePolicy。	2025 年 8 月 4 日
已釋出每個 AWS 帳戶配額的環境計數	每個 AWS 帳戶配額的 Amazon EVS 發行環境計數。 每個 AWS 帳戶配額的環境計數代表可在指定帳戶和區域中建立的 Amazon EVS 環境數量上限。	2025 年 7 月 8 日
歐洲（愛爾蘭）區域發行的 Amazon EVS	Amazon EVS 在歐洲（愛爾蘭）區域發行。	2025 年 6 月 18 日

已發行的 AmazonEVSServiceRolePolicy	已發佈 AWS 受管政策 AmazonEVSServiceRolePolicy。	2025 年 6 月 9 日
初始使用者指南版本	Amazon Elastic VMware Service 使用者指南已發佈。 Amazon EVS 使用者指南說明所有 Amazon EVS 概念，並提供搭配主控台和命令列界面使用各種功能的指示。	2025 年 6 月 9 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。