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？ 1
Amazon EVS 的功能 1
開始使用 Amazon EVS 2
存取 Amazon EVS 2
概念和元件 2
Amazon EVS 環境 3
Amazon EVS 主機 3
服務存取子網路 3
Amazon EVS VLAN 子網路 3
VMware NSX 5
VMware Hybrid Cloud Extension (HCX) 5
架構 5
網路拓撲 7
Amazon EVS 資源 9
設定 Amazon Elastic VMware Service 11
註冊 AWS 11
建立 IAM 使用者 12
建立 IAM 角色以將 Amazon EVS 許可委派給 IAM 使用者 13
註冊 AWS 商業、 AWS Enterprise On-Ramp 或 AWS 企業支援計劃 15
檢查配額 15
規劃 VPC CIDR 大小並設定 VPC 元件 15
主路由表 16
DHCP 選項集 16
建立 VPC Route Server 基礎設施 16
為內部部署連線建立傳輸閘道 17
建立 Amazon EC2 容量保留 17
設定 AWS CLI 17
建立 Amazon EC2 金鑰對 17
為 VMware Cloud Foundation (VCF) 準備您的環境 17
取得 VCF 授權金鑰 18
VMware HCX 先決條件 18
開始使用 20
先決條件 21
使用子網路和路由表建立 VPC 21

設定 VPC 主要路由表 23
使用 VPC DHCP 選項集設定 DNS 和 NTP 伺服器 23
DNS 伺服器組態 24
NTP 伺服器組態 24
（選用） 設定內部部署網路連線 25
使用端點和對等設定 VPC Route Server 執行個體 26
建立 Amazon EVS 環境 27
驗證 Amazon EVS 環境建立 38
將 Amazon EVS VLAN 子網路明確關聯至 VPC 路由表 40
（選用） 設定傳輸閘道路由表和 Direct Connect 字首以進行內部部署連線 40
建立網路 ACL 以控制 Amazon EVS VLAN 子網路流量 41
擷取 VCF 登入資料並存取 VCF 管理設備 41
設定 EC2 序列主控台 41
連線至 EC2 序列主控台 42
設定對 EC2 序列主控台的存取 42
清除 43
刪除 Amazon EVS 主機和環境 43
刪除 VPC Route Server 元件 45
刪除網路存取控制清單 (ACL) 46
刪除彈性網路介面 46
取消關聯和刪除子網路路由表 46
刪除子網路 46
刪除 VPC 46
後續步驟 46
遷移 47
先決條件 47
檢查 HCX VLAN 子網路的狀態 48
檢查 HCX VLAN 子網路是否與網路 ACL 相關聯 49
使用 HCX 公有上行 VLAN ID 建立分散式連接埠群組 50
（選用） 設定 HCX WAN 最佳化 50
（選用） 啟用 HCX 行動性最佳化網路 50
驗證 HCX 連線 51
安全 52
身分與存取管理 52
目標對象 53
使用身分驗證 53

使用政策管理存取權 56
Amazon Elastic VMware Service 如何搭配 使用 IAM 58
Amazon EVS 身分型政策範例 64
對 Amazon Elastic VMware Service 身分和存取進行故障診斷 76
AWS 受管政策 77
使用服務連結角色 79
使用其他 服務 82
AWS CloudFormation 82
Amazon EVS 和 AWS CloudFormation 範本 82
進一步了解 AWS CloudFormation 83
Amazon FSx for NetApp ONTAP 83
將 設定為 NFS 資料存放區 83
將 設定為 iSCSI 資料存放區 85
疑難排解 89
故障診斷失敗的環境狀態檢查 89
檢閱環境狀態檢查資訊 89
連線能力檢查失敗 89
主機計數檢查失敗 89
金鑰重複使用檢查失敗 90
金鑰涵蓋範圍檢查失敗 90
此主機上的 vSphere HA 代理程式無法到達隔離地址 91
ESXi 主機叢集的 VSAN 升級預先檢查失敗 91
端點和配額 92
服務端點 92
Service Quotas 93
文件歷史紀錄 95
..... xcvi

什麼是 Amazon Elastic VMware Service？

> **Note**
>
> Amazon EVS 目前為公開預覽版本，可能會有所變更。

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
- 開始使用 Amazon EVS
- 存取 Amazon EVS
- Amazon EVS 的概念和元件
- Amazon EVS 架構

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

> **Note**
>
> Amazon EVS 目前為公開預覽版本，可能會有所變更。

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。環境包含具有 vSphere 叢集的合併 VCF 網域，該叢集託管用於管理、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 “架構”。

Amazon EVS 主機

Amazon EVS 主機是在 Amazon EC2 裸機執行個體上執行的 VMware ESXi 主機。

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 設備和 ESXi 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。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。

Note

Amazon EVS 目前不支援 IPv6。

主機 VMkernel 管理 VLAN 子網路

主機 VMkernel 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 網路界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 ESXi 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 ESXi 主機之間的浮水印通訊。

VM 管理 VLAN 子網路

VM 管理 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 的其餘部分和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 AWS 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。如需詳細資訊，請參閱遷移。

Amazon EVS 架構

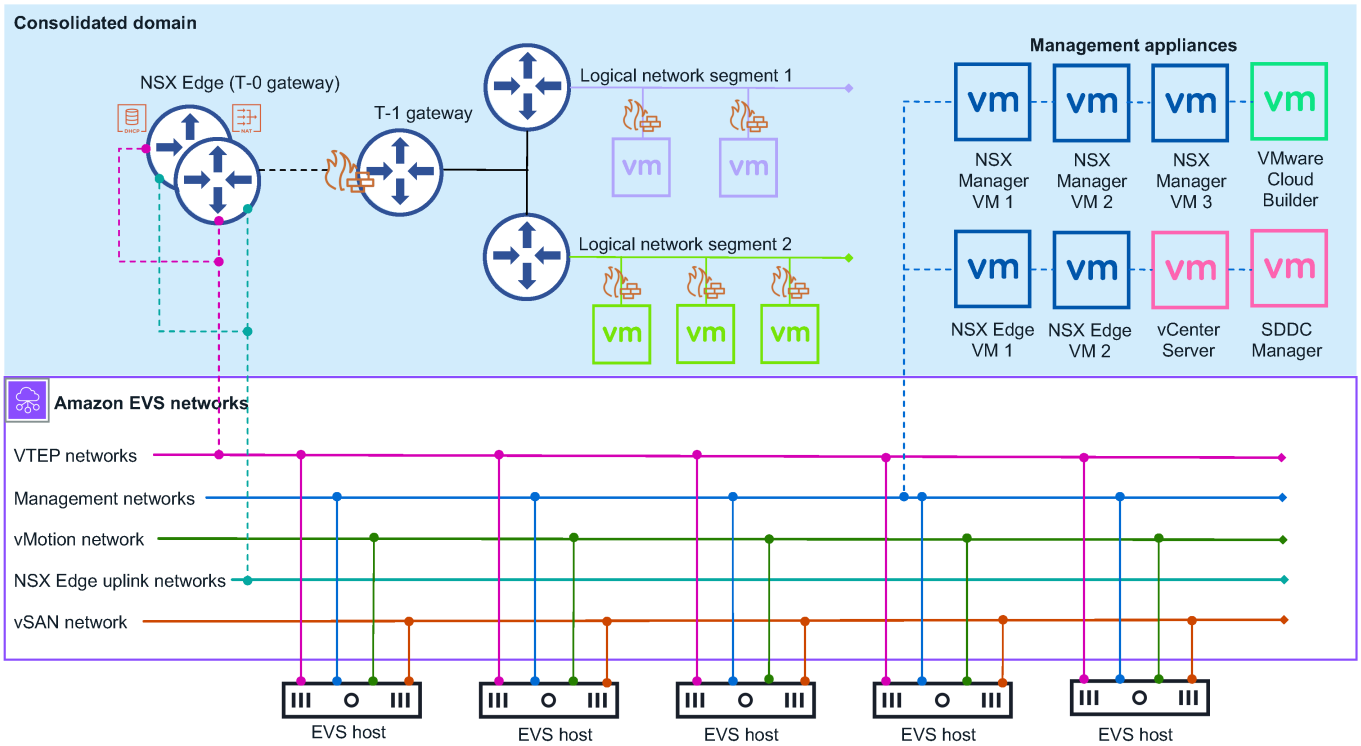
> **Note**
>
> Amazon EVS 目前為公開預覽版本，可能會有所變更。

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：

- ESXi 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。基礎 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 會在部署過程中代表您設定 NSX 覆蓋網路。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 中的虛擬機器與網際網路連線之間透過 VPC 進行通訊，並使用具有傳輸閘道的 AWS 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 “DNS 伺服器組態”。
- 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 Management Console 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 ESXi 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

> **Note**
>
> Amazon EVS 目前為公開預覽版本，可能會有所變更。

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。

主題

- 註冊 AWS
- 建立 IAM 使用者
- 建立 IAM 角色以將 Amazon EVS 許可委派給 IAM 使用者
- 註冊 AWS 商業、 AWS Enterprise On-Ramp 或 AWS 企業支援計劃
- 檢查配額
- 規劃 VPC CIDR 大小並設定 VPC 元件
- 建立 VPC Route Server 基礎設施
- 為內部部署連線建立傳輸閘道
- 建立 Amazon EC2 容量保留
- 設定 AWS CLI
- 建立 Amazon EC2 金鑰對
- 為 VMware Cloud Foundation (VCF) 準備您的環境
- 取得 VCF 授權金鑰
- VMware HCX 先決條件

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您的 AWS 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 Management Console access (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 會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 Filter policies (篩選政策)，然後選取 AWS managed -job function (AWS 受管工作職能) 以篩選表格內容。
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**
>
> 您必須先啟用 IAM 使用者和角色對帳單的存取權，才能使用 AdministratorAccess 許可存取 AWS 帳單和成本管理主控台。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建立更多群組和使用者，以及讓使用者能夠存取您的 AWS 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。此操作提供臨時安全登入資料，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. 在左側選單中，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，才能持續存取 Amazon EVS 技術支援和架構指導。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 計劃，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the section called “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 大小並設定 VPC 元件

若要啟用 Amazon EVS 環境建立，您必須為 Amazon EVS 提供包含子網路和足夠 IP 地址空間的 VPC，以便 Amazon EVS 建立連線至 VCF 設備的 VLAN 子網路。如需 VPC 建立需求的詳細資訊，請參閱 the section called “使用子網路和路由表建立 VPC”。

主路由表

Amazon EVS 子網路會在建立時隱含地與您 VPC 的主要路由表相關聯。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 VPC 的主要路由表，以允許這些系統的流量。如需 Amazon EVS 主要路由表組態的詳細資訊，請參閱 the section called “設定 VPC 主要路由表”。

DHCP 選項集

Amazon EVS 使用您 VPC 的 DHCP 選項集來擷取下列項目：

- 用於解析主機 IP 地址的網域名稱系統 (DNS) 伺服器。
- 網路時間通訊協定 (NTP) 伺服器，用於避免 SDDC 中的時間同步問題。

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 主機的 DNS 轉送查詢區域，如 中所述the section called “建立 Amazon EVS 環境”。
- 部署中每個 VCF 管理設備與 Amazon EVS 主機 PTR 記錄的反向查詢區域，如 中所述the section called “建立 Amazon EVS 環境”。

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 DNS 和 NTP 伺服器組態的 Amazon EVS 支援選項的詳細資訊，請參閱 the section called “使用 VPC DHCP 選項集設定 DNS 和 NTP 伺服器”。

建立 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。如需設定 Route Server for Amazon EVS 用量的詳細資訊，請參閱 the section called “使用端點和對等設定 VPC Route Server 執行個體”。

為內部部署連線建立傳輸閘道

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

建立 Amazon EC2 容量保留

Amazon EVS 會在您的 Amazon EVS 環境中啟動代表 ESXi 主機的 Amazon EC2 i4i.metal 執行個體。ESXi 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 AWS 存取金鑰 ID 和私密金鑰，以便在命令列中使用。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 5.2.1 要求。如需詳細資訊，請參閱 VCF 5.2.1 版本備註

> **Note**
>
> Amazon EVS 目前僅支援 VCF 5.2.1.x 版。

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

> **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**
>
> 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。如果您使用 vSphere 用戶端管理這些金鑰，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。

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 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。
- 確保 VMware HCX 已啟用並安裝在環境中。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。

Amazon Elastic VMware Service 入門

> **Note**
>
> Amazon EVS 目前為公開預覽版本，可能會有所變更。

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 5.2.1 要求。如需詳細資訊，請參閱 VCF 5.2.1 版本備註。

> **Important**
>
> Amazon EVS 目前僅支援 VCF 5.2.1.x 版。

主題

- 先決條件
- 使用子網路和路由表建立 VPC
- 設定 VPC 主要路由表
- 使用 VPC DHCP 選項集設定 DNS 和 NTP 伺服器
- （選用）設定內部部署網路連線
- 使用端點和對等設定 VPC Route Server 執行個體
- 建立 Amazon EVS 環境
- 驗證 Amazon EVS 環境建立
- 將 Amazon EVS VLAN 子網路明確關聯至 VPC 路由表

- （選用）設定傳輸閘道路由表和 Direct Connect 字首以進行內部部署連線
- 建立網路 ACL 以控制 Amazon EVS VLAN 子網路流量
- 擷取 VCF 登入資料並存取 VCF 管理設備
- 設定 EC2 序列主控台
- 清除
- 後續步驟

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。

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 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。

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。

設定 VPC 主要路由表

建立 VPC 的主要路由表時，Amazon EVS 子網路會隱含關聯。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，您必須設定主路由表，以允許這些系統的流量。如需管理子網路路由表的詳細資訊，請參閱 Amazon VPC 《 使用者指南》中的管理子網路路由表。

部署 Amazon EVS 環境之後，您可以設定明確的路由表關聯，以透過自訂路由表啟用連線。如需詳細資訊，請參閱 Amazon VPC 《 使用者指南》中的取代主路由表。

> **Important**
>
> Amazon EVS 僅在建立 Amazon EVS 環境後，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

Amazon EVS 使用您 VPC 的 DHCP 選項集來擷取下列項目：

- 用於解析主機 IP 地址的網域名稱系統 (DNS) 伺服器。
- 網路時間通訊協定 (NTP) 伺服器，用於避免 SDDC 中的時間同步問題。

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。

若要啟用 DNS 連線以成功部署環境，您必須先設定 VPC 的主要路由表，以允許 DNS 流量。如需詳細資訊，請參閱the section called “設定 VPC 主要路由表”。

DNS 伺服器組態

您可以輸入最多四個網域名稱系統 (DNS) 伺服器的 IPv4 地址。您可以使用 Route 53 做為 DNS 伺服器提供者，也可以提供自己的自訂 DNS 伺服器。如需將 Route 53 設定為現有網域之 DNS 服務的詳細資訊，請參閱將 Route 53 設為使用中網域的 DNS 服務。

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

若要成功部署環境，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 主機的 DNS 轉送查詢區域，如 中所述the section called “建立 Amazon EVS 環境”。
- 部署中每個 VCF 管理設備與 Amazon EVS 主機 PTR 記錄的反向查詢區域，如 中所述the section called “建立 Amazon EVS 環境”。

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。

> **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。

NTP 伺服器組態

NTP 伺服器向網路提供時間。您可以輸入最多四個網路時間通訊協定 (NTP) 伺服器的 IPv4 地址。如需在 DHCP 選項集中設定 NTP 伺服器的詳細資訊，請參閱建立 DHCP 選項集。

> **Note**
>
> Amazon EVS 目前不支援 IPv6。

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。如需有關 Amazon Time Sync Service 的詳細資訊，請參閱《Amazon EC2 使用者指南》中的設定執行個體的時間。

（選用）設定內部部署網路連線

您可以使用 AWS Direct Connect 搭配相關聯的傳輸閘道，或使用連至傳輸閘道的 AWS Site-to-Site VPN 連接，來設定現場部署資料中心與 AWS 基礎設施的連線。 AWS Site-to-Site VPN 會透過網際網路建立連至傳輸閘道的 IPsec VPN 連線。 會透過私有專用連線 AWS Direct Connect 建立連至傳輸閘道的 IPsec VPN 連線。建立 Amazon EVS 環境後，您可以使用任一選項將內部部署資料中心防火牆連線至 VMware NSX 環境。

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 “（選用）設定傳輸閘道路由表和 Direct Connect 字首以進行內部部署連線”。

如需設定 AWS Direct Connect 連線的詳細資訊，請參閱AWS Direct Connect 閘道和傳輸閘道關聯。如需搭配使用 AWS Site-to-Site與 AWS 傳輸閘道的詳細資訊，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。在路由伺服器對等上設定的對等 ASN 必須相符，且對等 IP 地址必須是唯一的。

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。

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

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)。

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。

   > **Note**
   >
   > 從 Amazon EVS 主控台觸發的 Amazon EVS 操作不會產生 CloudTrail 事件。

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，執行下列動作。
   a. 檢查是否符合 AWS 支援要求和服務配額要求。如需 Amazon EVS 支援需求的詳細資訊，請參閱 the section called “註冊 AWS 商業、 AWS Enterprise On-Ramp 或 AWS 企業支援計劃”。如需 Amazon EVS 配額需求的詳細資訊，請參閱 the section called “Service Quotas”。
   b. （選用）針對名稱，輸入環境名稱。
   c. 針對環境版本，選擇您的 VCF 版本。Amazon EVS 目前僅支援 5.2.1.x 版。
   d. 針對網站 ID，輸入您的 Broadcom 網站 ID。
   e. 針對 VCF 解決方案金鑰，輸入 VCF 解決方案金鑰。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。

   f. 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 會要求您在 SDDC Manager 中維護有效的 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 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。

g. 對於 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。

h. 選擇下一步。

5. 在指定主機詳細資訊頁面上，完成下列步驟 4 次，將 4 個主機新增至環境。Amazon EVS 環境需要 4 個主機才能進行初始部署。

   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。

   > **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。

   d. 針對 SSH 金鑰對，選擇 SSH 金鑰對以存取主機。

   e. 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 VPC，選擇您先前建立的 VPC。

b. 針對服務存取子網路，選擇您建立 VPC 時建立的私有子網路。

c. 對於安全群組 - 選用 ，您可以選擇最多 2 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。

d. 在管理連線下，輸入要用於 Amazon EVS VLAN 子網路的 CIDR 區塊。

> **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”。

e. 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。

> **Note**
>
> 請確定您提供的 VLAN CIDR 區塊在 VPC 中大小正確。如需詳細資訊，請參閱the section called “Amazon EVS 網路考量事項”。

f. 在工作負載/VCF 連線下，輸入 NSX 上行 VLAN 的 CIDR 區塊，然後選擇 2 個透過 NSX 上行對等至 Route Server 端點的 VPC Route Server 對等 IDs。

> **Note**
>
> Amazon EVS 需要與 2 個 Route Server 端點和 2 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”。

g. 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 VMware Cloud Foundation 的最新套件版本，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**
>
> 建立環境可能需要幾個小時。

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 Amazon EVS 支援需求的詳細資訊，請參閱 the section called “註冊 AWS 商業、 AWS Enterprise On-Ramp 或 AWS 企業支援計劃”。如需 Amazon EVS 配額需求的詳細資訊，請參閱 the section called “Service Quotas”。

> **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 VMware Cloud Foundation 的最新套件版本，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`，指定您先前建立的 VPC，最低 IPv4 CIDR 範圍為 /22。
- 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`，Amazon EVS 目前僅支援 VCF 5.2.1.x。
- 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 Client 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。

> **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”。

- 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。

> **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**
>
> Amazon EVS 需要與 2 個 Route Server 端點和 2 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。此 ID 允許存取 Broadcom 入口網站，並在軟體合約或合約續約結束時由 Broadcom 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-5.2.1 \
--terms-accepted \
--license-info "{
      \"solutionKey\": \"00000-00000-00000-abcde-11111\",
      \"vsanKey\": \"00000-00000-00000-abcde-22222\"
    }" \
   --initial-vlans "{
      \"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\"
    },
    {
      \"hostName\": \"esx02\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\"
    },
    {
      \"hostName\": \"esx03\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\"
    },
    {
      \"hostName\": \"esx04\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\"
    }
  ]" \
--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-5.2.1",
        "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-5.2.1",
        "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。

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
```

（選用）設定傳輸閘道路由表和 Direct Connect 字首以進行內部部署連線

如果您使用具有傳輸閘道的 AWS 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，您可能還需要更新您的 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。

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，也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。

> **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。

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。如需擷取秘密的詳細資訊，請參閱從 AWS Secrets Manager 取得秘密。

> **Note**
>
> Amazon EVS 不提供秘密的受管輪換。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。

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

根據預設，Amazon EVS 會在新部署的 Amazon EVS 主機上啟用 ESXi Shell。此組態允許透過 ECAmazon EC2EC2 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 ESXi 主機互動。

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

連線至 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

SDDC UI and Amazon EVS console

1. 前往 SDDC Manager 使用者介面。
2. 從 vSphere 叢集移除主機。這將從 SDDC 網域取消指派主機。針對叢集中的每個主機重複此步驟。如需詳細資訊，請參閱 VCF 產品文件中的從工作負載網域中的 vSphere 叢集移除主機。
3. 停用未指派的主機。如需詳細資訊，請參閱 VCF 產品文件中的停用主機。
4. 前往 Amazon EVS 主控台。

   > **Note**
   >
   > 從 Amazon EVS 主控台觸發的 Amazon EVS 操作不會產生 CloudTrail 事件。

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。
9. 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。

10. 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》中的取消容量保留。

SDDC UI and 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-5.2.1",
            "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-5.2.1",
            "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. 前往 SDDC Manager 使用者介面。
4. 從 vSphere 叢集移除主機。這將從 SDDC 網域取消指派主機。針對叢集中的每個主機重複此步驟。如需詳細資訊，請參閱 VCF 產品文件中的從工作負載網域中的 vSphere 叢集移除主機。
5. 停用未指派的主機。如需詳細資訊，請參閱 VCF 產品文件中的停用主機。
6. 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
```

7. 重複上述步驟，刪除您環境中剩餘的主機。
8. 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。

9. 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》中的取消容量保留。

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。

刪除彈性網路介面

如需刪除彈性網路介面的步驟，請參閱《Amazon EC2 使用者指南》中的刪除網路介面。

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，請參閱遷移。

使用 VMware Hybrid Cloud Extension (VMware HCX) 將工作負載遷移至 Amazon EVS

> **Note**
>
> Amazon EVS 目前為公開預覽版本，可能會有所變更。

建立 Amazon EVS 環境之後，您可以使用 VMware Hybrid Cloud Extension (VMware HCX) 將現有的 VMware 型工作負載遷移至 Amazon Elastic VMware Service (Amazon EVS)。如需 VMware HCX 遷移的詳細資訊，請參閱 VMware HCX 使用者指南中的 VMware HCX 遷移類型。 VMware

下列教學課程說明如何使用 VMware HCX 將 VMware 工作負載遷移至 Amazon EVS。

您可以使用 VMware HCX 透過私有連線，使用 AWS Direct Connect 搭配相關聯的傳輸閘道，或使用 AWS Site-to-Site VPN 連接至傳輸閘道來遷移工作負載。

> **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。

如需設定 AWS Direct Connect 連線的詳細資訊，請參閱 AWS Direct Connect 《 使用者指南》中的AWS 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。

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，並且已使用 AWS Direct Connect 具有傳輸閘道的傳輸閘道或具有傳輸閘道 AWS Site-to-Site VPN 建立並連線至您的內部部署網路。如需建立 Amazon EVS 環境的步驟，請參閱 開始使用。如需 VMware HCX 先決條件的詳細資訊，請參閱 the section called “VMware HCX 先決條件”。

檢查 HCX VLAN 子網路的狀態

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。
6. 複製 HCX `vlan` ID 以供日後使用。

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
```

以下是範例回應。

```
{
 "environmentVlans": [
        {
            "vlan": 80,
            "cidr": "10.10.7.0/24",
            "availabilityZone": "us-east-2c",
            "functionName": "hcx",
            "createdAt": "2025-04-13T13:39:58.845000+00:00",
            "modifiedAt": "2025-04-13T13:47:57.067000+00:00",
            "vlanState": "CREATED",
            "stateDetails": ""
        },
        {
            "vlan": 20,
            "cidr": "10.10.1.0/24",
```

```
            "availabilityZone": "us-east-2c",
            "functionName": "vmManagement",
            "createdAt": "2025-04-13T13:39:58.456000+00:00",
            "modifiedAt": "2025-04-13T13:47:57.524000+00:00",
            "vlanState": "CREATED",
            "stateDetails": ""
        }
 ]
}
```

2. 識別具有 functionName的 VLAN，hcx並檢查 vlanState是否為 CREATED。
3. 複製 HCX vlan ID 以供日後使用。

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”。

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。

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

HCX WAN 最佳化服務 (HCX-WAN-OPT) 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-WAN-IX) 一起部署。HCX-WAN-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 行動性最佳化網路 (MON) 是 HCX 網路延伸服務的一項功能。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 可讓您設定將工作負載流量遷移至 Amazon EVS 的最佳路徑，避免透過來源閘道進行長往返網路路徑。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
> 行動性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

Amazon Elastic VMware Service 的安全性

> **Note**
>
> Amazon EVS 目前為公開預覽版本，可能會有所變更。

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 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 Elastic VMware Service 時套用共同責任模型。它說明如何設定 Amazon Elastic VMware Service 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 Elastic VMware Service 資源。

目錄

- Amazon Elastic VMware Service 的身分和存取管理

Amazon Elastic VMware Service 的身分和存取管理

> **Note**
>
> Amazon EVS 目前為公開預覽版本，可能會有所變更。

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 資源。 IAM 是您可以免費使用 AWS 服務 的 。

主題

- 目標對象
- 使用身分驗證
- 使用政策管理存取權
- Amazon Elastic VMware Service 如何搭配 使用 IAM
- Amazon EVS 身分型政策範例
- 對 Amazon Elastic VMware Service 身分和存取進行故障診斷
- AWS Amazon EVS 的 受管政策
- 使用 Amazon EVS 的服務連結角色

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 Elastic VMware Service 中執行的工作。

服務使用者 – 如果您使用 Amazon Elastic VMware Service 執行任務，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 Elastic VMware Service 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。

服務管理員 - 如果您在公司負責 Amazon Elastic VMware Service 資源，您可能擁有 Amazon Elastic VMware Service 的完整存取權。您的任務是判斷服務使用者應存取哪些 Amazon Elastic VMware Service 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 Elastic VMware Service 使用 ，請參閱 the section called “Amazon Elastic VMware Service 如何搭配 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 Elastic VMware Service 存取權的詳細資訊。若要檢視您可以在其中使用的 Amazon Elastic VMware Service 身分型政策範例 IAM，請參閱 Amazon Elastic VMware Service 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。您必須擔任 IAM 角色，以 AWS 帳戶根使用者、 IAM 使用者或 身分進行身分驗證 （ 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 Management Console 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 憑證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 Single Sign-On 的後續產品 ） 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

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」，是藉由您用來建立帳戶的電子郵件地址和密碼以登入並存取。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

最佳實務是， 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 目錄或任何使用透過身分來源提供的登入資料 AWS 服務 存取的使用者。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 IAM Identity Center 的相關資訊，請參閱《AWS IAM Identity Center (AWS Single Sign-On 的後續版本 ） 使用者指南》中的什麼是 IAM Identity Center？。 AWS Single Sign-On

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》中的建立 IAM 使用者 （ 而非角色 ） 的時機。

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。您可以透過 AWS Management Console 切換 IAM 角色暫時在 中擔任 角色。 https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-console.html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。如需許可集的資訊，請參閱《AWS IAM Identity Center (AWS Single Sign-On 的後續版本） 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 – 服務連結角色是一種連結至 的服務角色類型 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，當與身分或資源相關聯時， AWS 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，使用者無法執行任何作業，甚至也無法變更他們自己的密碼。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。管理員將許可給予群組時，該群組中的所有使用者都會獲得那些許可。

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 Management Console 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。內嵌政策會直接內嵌到單一使用者、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。所有這類政策中的明確拒絕都會覆寫該允許。如需許可界限的詳細資訊，請參閱《IAM 使用者指南》中的IAM 實體的許可界限。
- 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 是一種用於分組和集中管理您企業擁有 AWS 帳戶 的多個 的服務。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 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，請參閱 IAM 使用者指南中的工作階段政策。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。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 Elastic VMware Service 如何搭配 使用 IAM

> **Note**
>
> Amazon EVS 目前為公開預覽版本，可能會有所變更。

使用 IAM 管理 Amazon Elastic VMware Service 的存取權之前，請先了解哪些 IAM 功能可與 Amazon Elastic VMware Service 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
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

IAM 功能	Amazon EVS 支援
the section called “搭配 Amazon EVS 使用臨時登入資料”	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

若要全面了解 Amazon Elastic VMware Service 和其他 AWS 服務 的運作方式 IAM，請參閱《IAM 使用者指南》中的 AWS 服務 。 IAM

主題

- Amazon EVS 的身分型政策
- Amazon EVS 中的存取控制清單 (ACLs)
- 使用 Amazon EVS 的屬性型存取控制 (ABAC)
- 搭配 Amazon EVS 使用臨時登入資料
- 轉送 Amazon EVS 的存取工作階段
- Amazon EVS 的服務角色
- Amazon EVS 的服務連結角色

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 Elastic VMware Service 身分型政策的範例，請參閱 Amazon Elastic VMware Service 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位置時 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哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

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 Elastic VMware Service 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 Elastic VMware Service 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 Elastic VMware Service 動作的清單，請參閱《服務授權參考》中的 Amazon Elastic VMware Service 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哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

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

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

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

若要查看 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，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哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素（或Condition區塊）可讓您指定陳述式生效的條件。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，只有在資源以其 IAM 使用者 名稱加上標籤時，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 Elastic VMware Service 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條件索引鍵。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 Elastic VMware Service 條件金鑰清單，請參閱《服務授權參考》中的 Amazon Elastic VMware Service 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 Elastic VMware Service 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。您可以將標籤連接到 IAM 實體 （使用者或角色） 和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。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 Elastic VMware Service 資源，或在請求中將標籤傳遞至 Amazon Elastic VMware Service。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 使用臨時登入資料

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。

如果您 AWS Management Console 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權給 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 Elastic VMware Service 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

> **Note**
>
> Amazon EVS 目前為公開預覽版本，可能會有所變更。

根據預設， IAM 使用者 和 角色沒有建立或修改 Amazon Elastic VMware Service 資源的許可。他們也無法使用 AWS Management Console 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 Elastic VMware Service 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 Elastic VMware Service 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低權限許可 – 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 – 您可以在政策中新增條件，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 AWS CloudFormation。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證您的 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 Elastic VMware Service 主控台

若要存取 Amazon Elastic VMware Service 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 Elastic VMware Service 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，主控台對於附加該政策的主體將無法如預期運作。

為了確保您的 IAM 主體仍然可以使用 Amazon Elastic VMware Service 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。相反地，只允許存取與您嘗試執行之 API 操作相符的動作。

允許使用者檢視他們自己的許可

此範例說明如何建立政策， 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。如果您已在帳戶中建立 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"
            ],
            "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 Elastic VMware Service 身分和存取進行故障診斷

> **Note**
>
> Amazon EVS 目前為公開預覽版本，可能會有所變更。

使用以下資訊來協助您診斷和修正使用 Amazon Elastic VMware Service 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 Elastic VMware Service 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 Elastic VMware Service 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 Elastic VMware Service 是否支援這些功能，請參閱 the section called “Amazon Elastic VMware Service 如何搭配 使用 IAM”。
- 若要了解如何提供您擁有之 資源 AWS 帳戶 的存取權，請參閱《IAM 使用者指南》IAM 使用者 中的在您擁有 AWS 帳戶 的另一個 中提供 的存取權。
- 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

> **Note**
>
> Amazon EVS 目前為公開預覽版本，可能會有所變更。

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。我們建議您定義使用案例專屬的客戶管理政策，以便進一步減少許可。

您無法變更 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

您無法`AmazonEVSServiceRolePolicy`連接至 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` - 建立、修改、標記和刪除彈性網路界面，用於在 Amazon EVS 和客戶 VPC 子網路中的 VMware Virtual Cloud Foundation (VCF) SDDC Manager 設備之間建立持久性連線。Amazon EVS 需要此連線才能部署、管理和監控 VCF 部署。

若要檢視 JSON 政策文件的最新版本，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	日期
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	2025 年 6 月 9 日

變更	描述	日期
	參閱 the section called “AWS 受管政策：AmazonEVSServiceRolePolicy”。	
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

> **Note**
>
> Amazon EVS 目前為公開預覽版本，可能會有所變更。

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。已定義的許可包括信任政策和許可政策。許可原則無法附加到其他任何 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資訊，請參閱《可搭配 IAM 運作的AWS 服務》，尋找 Service-linked roles (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 子網路和 VPCs。

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

您不需要手動建立服務連結角色。當您在 AWS Management Console、 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」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，請參閱端點和配額。

將 Amazon EVS 與其他 AWS 服務搭配使用

> **Note**
>
> Amazon EVS 目前為公開預覽版本，可能會有所變更。

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

> **Note**
>
> Amazon EVS 目前為公開預覽版本，可能會有所變更。

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

> **Note**
>
> Amazon EVS 目前為公開預覽版本，可能會有所變更。

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，可提供廣泛採用的一組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

> **Note**
>
> Amazon EVS 目前為公開預覽版本，可能會有所變更。

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. 對於交界路徑，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

> **Note**
>
> Amazon EVS 目前為公開預覽版本，可能會有所變更。

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 ESXi 主機儲存體設定軟體 iSCSI 轉接器

對於每個 ESXi 主機，您必須設定軟體 iSCSI 轉接器，以便 ESXi 主機可以使用它來存取 iSCSI 儲存。如需在 vSphere 中為 ESXi 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 ESXi 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 ESXi 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 ESXi 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

> **Note**
>
> Amazon EVS 目前為公開預覽版本，可能會有所變更。

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，以識別特定且可偵測的問題。

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 無法連線到環境，則此檢查會失敗。

如果此檢查失敗，Amazon EVS 就無法再連線 SDDC Manager 來驗證環境狀態，而且無法再將主機新增至環境。連線能力失敗也會導致授權金鑰重複使用和金鑰涵蓋範圍檢查失敗，以及主機計數檢查傳回未知回應。

Reachabilty 失敗表示 SDDC Manager、防火牆組態或缺少憑證可能有問題。您可以嘗試解決這些問題，或聯絡 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 5.2.1 的需求。

如果此檢查失敗，您將需要新增主機，讓您的環境符合此最低需求。Amazon EVS 僅支援具有 4 到 16 個主機的環境。

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 授權只能用於一個 Amazon EVS 環境。如果已使用的授權新增至環境，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 中檢閱您的授權設定，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 元件授權金鑰。Amazon EVS 會要求您在 SDDC Manager 中維護有效的元件授權金鑰，服務才能正常運作。如果您使用 vSphere 用戶端管理元件授權金鑰，您必須確保這些金鑰也會出現在 SDDC Manager 使用者介面的授權畫面中，以防止授權金鑰檢查失敗。

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 環境或無法將 Amazon EVS 主機新增至環境的錯誤回應。金鑰涵蓋範圍失敗可能表示下列其中一個問題：

- 您已超過 Amazon EVS 支援的主機計數。Amazon EVS 支援每個環境 4 到 16 個主機。如果此問題發生，請移除或新增主機，直到您的環境位於支援的主機範圍。
- VCF 授權未正確指派給 vCenter 伺服器。您必須在 vCenter Server 的評估期間到期或目前指派的授權到期之前，將授權指派給 vCenter Server。如果此問題發生，請在 SDDC Manager 中檢閱授權指派。
- 目前的 VCF 授權不包含 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。如果此問題發生，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 元件授權金鑰。Amazon EVS 會要求您在 SDDC Manager 中維護有效的元件授權金鑰，服務才能正常運作。如果您使用 vSphere 用戶端管理元件授權金鑰，您必須確保這些金鑰也會出現在 SDDC Manager 使用者介面的授權畫面中，以防止授權金鑰檢查失敗。

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 ESXi 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。

若要移除 vSphere HA 錯誤訊息，您必須停用 vSphere HA。如需在 vSphere 用戶端中停用 vSphere HA 的步驟，請參閱停用和啟用 VMware 高可用性 (HA) 一文。

ESXi 主機叢集的 VSAN 升級預先檢查失敗

嘗試使用 SDDC Manager 升級 ESXi 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。

Amazon Elastic VMware Service 端點和配額

> **Note**
>
> Amazon EVS 目前為公開預覽版本，可能會有所變更。

以下是此服務的服務端點和服務配額。若要以程式設計方式連線至 AWS 服務，您可以使用 端點。除了標準 AWS 端點之外，有些 會在選取的區域中 AWS 服務 提供 FIPS 端點。如需詳細資訊，請參閱 AWS 服務端點。服務配額 (也稱為限制) 是 AWS 帳戶的服務資源或操作的最大數量。如需更多相關資訊，請參閱 AWS Service Quotas。

服務端點

Amazon EVS API 提供區域和雙堆疊端點，以及美國區域的 FIPS 端點。若要搭配 使用雙堆疊端點 AWS CLI，請參閱 SDK AWS SDKs 和工具參考指南中的雙堆疊和 FIPS 端點組態。

區域名稱	區域	端點	通訊協定
美國東部 （維吉尼亞北部）	us-east-1	evs.us-east-1.amazonaws.com evs-fips.us-east-1.amazonaws.com evs.us-east-1.api.aws evs-fips.us-east-1.api.aws	HTTPS
美國東部 (俄亥俄)	us-east-2	evs.us-east-2.amazonaws.com evs-fips.us-east-2.amazonaws.com evs.us-east-2.api.aws evs-fips.us-east-2.api.aws	HTTPS
美國西部 (奧勒岡)	us-west-2	evs.us-west-2.amazonaws.com evs-fips.us-west-2.amazonaws.com	HTTPS

區域名稱	區域	端點	通訊協定
		evs.us-west-2.api.aws evs-fips.us-west-2.api.aws	
亞太區域 (東京)	ap-northeast-1	evs.ap-northeast-1.amazonaws.com evs.ap-northeast-1.api.aws	HTTPS
歐洲 (法蘭克福)	eu-central-1	evs.eu-central-1.amazonaws.com evs.eu-central-1.api.aws	HTTPS
歐洲 (愛爾蘭)	eu-west-1	evs.eu-west-1.amazonaws.com evs.eu-west-1.api.aws	HTTPS

Service Quotas

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 Management Console 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。

> **Important**
>
> 若要啟用 Amazon EVS 環境建立，每個 EVS 環境配額的主機計數必須至少為 4。預設配額為 0。若要增加此配額，請前往 Service Quotas 主控台並請求增加配額。

> **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**
>
> 如果您打算將 EC2 專用主機用於 Amazon EVS 環境，請確定您的 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。

名稱	預設	可調整	描述
每個 EVS 環境的主機計數	0	是	可在單一 Amazon EVS 環境中佈建的主機數量上限。
每個 AWS 帳戶的環境計數	1	是	目前區域中可在此帳戶中建立的 EVS 環境數目上限。

Amazon Elastic VMware Service 使用者指南的文件歷史記錄

> **Note**
>
> Amazon EVS 目前為公開預覽版本，可能會有所變更。

下表說明 Amazon Elastic VMware Service 的文件版本。

變更	描述	日期
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 AmazonEVS ServiceRolePolicy	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。