用户指南

亚马逊弹性 VMware 服务

亚马逊弹性 VMware 服务: 用户指南

Table of Contents

什么是 Amazon 弹性 VMware 服务？

> **Note**
>
> Amazon EVS 处于公开预览版，可能会发生变化。

您可以使用亚马逊弹性 VMware 服务 (Amazon EVS) 直接在 (VPC) 中的 EC2 裸机实例上部署和运行 VMware 云基础 (Amazon Virtual Private Cloud VCF) 环境。

主题

亚马逊 EVS 的特点

以下是 Amazon EVS 的主要功能：

简化并加快迁移到 AWS

通过订阅可移植性和 VMware 云端云端 (VCF) 的自动部署，消除迁移摩擦并确保运营一致性。无需更改 IP 地址、重新培训员工或重新编写操作手册，即可扩展本地网络并迁移工作负载。

保持对云端 VMware 架构的控制权

完全控制您的 VMware 架构，并优化满足应用程序独特需求的虚拟化堆栈，包括插件和第三方解决方案。

自行管理或利用 AWS 合作伙伴提供托管体验

您可以自由选择和灵活地进行自我管理，或者利用 AWS 合作伙伴的专业知识来管理和运营您的 VCF环境， AWS 以实现您在人才、时间和成本方面的业务目标。

扩大业务规模，保护您的业务免受中断影响

在最安全、可扩展和最具弹性的云上增强可扩展性，以迁移和操作 VMware基于您的工作负载。

拥抱 AWS 创新，转变您的应用程序和基础架构

作为一项 AWS原生服务，Amazon EVS 通过 200 多种服务（包括托管数据库、分析、无服务器和容器以及生成式 AI）来简化 VMware 环境的扩展和扩展，从而实现业务转型。

开始使用 Amazon EVS

要创建您的第一个 Amazon EVS 环境，请参阅入门。通常，开始使用 Amazon EVS 需要完成以下步骤。

1. 完成 必备任务。有关更多信息，请参阅 设置 Amazon 弹性 VMware 服务。
2. 创建 Amazon EVS 环境。在创建环境期间，Amazon EVS 使用您指定的 CIDR 范围创建所需的 VLAN 子网，并将主机添加到环境中。
3. 自定义 VCF。根据需要在 vSphere 用户界面中配置您的环境。这可能包括设置登录、策略、监控等。
4. Connect 并迁移。将您的环境连接到本地数据中心，并将您的 VCF 工作负载迁移到 Amazon EVS。

访问亚马逊 EVS

您可以使用以下接口定义和配置您的 Amazon EVS 部署：

- Amazon EVS 控制台-提供用于创建亚马逊 EVS 环境的 Web 界面。
- AWS CLI -提供适用于各种各样的命令 AWS 服务 并在 Windows、macOS 和 Linux 上受支持。有关更多信息，请参阅 AWS Command Line Interface。
- AWS CloudFormation -为每种资源类型提供规范，例如`AWS::EVS::Environment`。您可以使用资源规范创建模板，并 CloudFormation 负责为您配置和配置资源。

Amazon EVS 的概念和组成部分

> **Note**
>
> Amazon EVS 处于公开预览版，可能会发生变化。

本节介绍了 Amazon EVS 的一些关键概念和组件。

亚马逊 EVS 环境

Amazon EVS 环境是 VMware 云基础 (VCF) 资源的逻辑容器，例如 vSphere 主机、vSAN、NSX 和 SDDC Manager。环境包含一个整合的 VCF 域，其中包含一个 vSphere 群集，该群集托管用于管理、监控和实例化 VCF 软件堆栈的组件。每个环境都直接映射到 SDDC 管理器设备。有关更多信息，请参阅 the section called “架构”。

亚马逊 EVS 主机

Amazon EVS VMware ESXi 主机是在 Amazon EC2 裸机实例上运行的主机。

服务访问子网

服务访问子网是一个标准 VPC 子网，允许 Amazon EVS 访问 VCF 部署。在创建 Amazon EVS 环境期间，您可以指定 Amazon EVS 用于访问服务的 VPC 和子网。

当您创建 Amazon EVS 环境时，Amazon EVS 会在服务访问子网中配置弹性网络接口，以促进与 VCF 设备和主机的管理连接。 ESXi Amazon EVS 需要这种连接才能部署、管理和监控 VCF 部署。

Amazon EVS VLAN 子网

亚马逊 EVS VLAN 子网是由亚马逊 EVS 管理的亚马逊 VPC 子网。VLAN 子网为 Amazon EVS 主机以及 VMware NSX、HCX 和 vCenter Server 等 VCF 设备提供 VPC 连接。 VMware VMware 每个 VLAN 子网都有一个 VLAN 标记，允许对 VLAN 网络流量进行逻辑分段。

Amazon EVS 会创建该服务在创建 Amazon EVS 环境时使用的所有 VLAN 子网。您提供 VLAN 子网使用的 CIDR 块输入。考虑到未来的扩展需求，您应确保根据要配置的主机数量正确调整您的 VLAN 子网 CIDR 块的大小。有关更多信息，请参阅 the section called “Amazon EVS 联网注意事项”。

> **Important**
>
> Amazon EVS VLAN 子网只能在创建 Amazon EVS 环境的过程中创建，并且在创建环境后无法修改。在创建环境之前，必须确保正确调整 VLAN 子网 CIDR 块的大小。部署环境后，您将无法添加 VLAN 子网。

> **Important**
>
> EC2 安全组规则不会在连接到 VLAN 子网的 Amazon EVS 弹性网络接口上强制执行。要控制进出 VLAN 子网的流量，必须使用网络访问控制列表。

> **Note**
>
> Amazon EVS IPv6 目前不支持。

主机 VMkernel 管理 VLAN 子网

主机 VMkernel 管理 VLAN 子网将管理流量与用户流量分开，并允许远程管理主机。EVS 主机管理 vmkernel 网络接口连接到该子网。

vMotion VLAN 子网

v Motion VLAN 子网在逻辑上分段 VMware vMotion 流量，并在 vMotion 过程中用于在主机之间移动虚拟机。

vSAN VLAN 子网

vSAN 使用 vSAN VLAN 子网将与 VMware vSAN 存储操作相关的流量与其他网络流量分开。

VTEP VLAN 子网

VTEP VLAN 子网使用 VMware NSX 虚拟隧道终端节点 (VTEP) 来封装和解封 Amazon EVS 主机的覆盖网络流量。 ESXi

边缘 VTEP VLAN 子网

Edge VTEP VLAN 子网是一个专门用于 NSX Edge 设备覆盖流量的专用 VTEP VLAN 子网。此 VLAN 用于 NSX 边缘和 ESXi 主机之间的重叠通信。

虚拟机管理 VLAN 子网

虚拟机管理 VLAN 子网用于管理虚拟设备，包括 NSX Manager、vCenter Server 和 SDDC Manager。

HCX 上行链路 VLAN 子网

HCX 上行链路 VLAN 子网用于 HCX Interconnect (HCX-IX) 和 HCX 网络扩展 (HCX-NE) 设备之间的通信，并支持创建 HCX 服务网格上行链路。

NSX 上行链路 VLAN 子网

NSX 上行链路 VLAN 子网用于将您的 NSX 覆盖网络连接到您的 VPC 的其余部分以及您配置的任何其他外部网络。NSX 上行链路 VLAN 子网是在 NSX Edge 节点上行链路上配置的。

扩展 VLAN 子网

扩展 VLAN 子网可用于启用其他 VCF 支持的功能，例如 NSX 联合。Amazon EVS 在创建环境期间会创建两个扩展 VLAN 子网。

VMware NSX

VMware NSX 是一个支持网络虚拟化的软件定义网络 (SDN) 平台。Amazon EVS 使用 VMware NSX 来创建和管理运行 VMware 云基础 (VCF) 设备和工作负载的覆盖网络。Amazon EVS 部署了一对 active/standby NSX Edge 节点和一个 NSX 覆盖网络。作为部署的一部分，Amazon EVS 会自动代表您配置所有 NSX 路由和上行链路。有关常见 NSX 概念的更多信息，请参阅《VMware NSX 安装指南》中的关键概念。

VMware 混合云扩展 (HCX)

VMware 混合云扩展 (VMware HCX) 是一个应用程序移动平台，旨在简化应用程序迁移、重新平衡工作负载以及优化跨数据中心和云的灾难恢复。您可以使用 HCX 将 VMware基于您的工作负载迁移到 Amazon EVS。

您可以使用关联的传输网关或使用 AWS Direct Connect 与传输网关的 AWS Site-to-Site VPN 连接来配置 VMware HCX 的连接。有关更多信息，请参阅 迁移。

亚马逊 EVS 架构

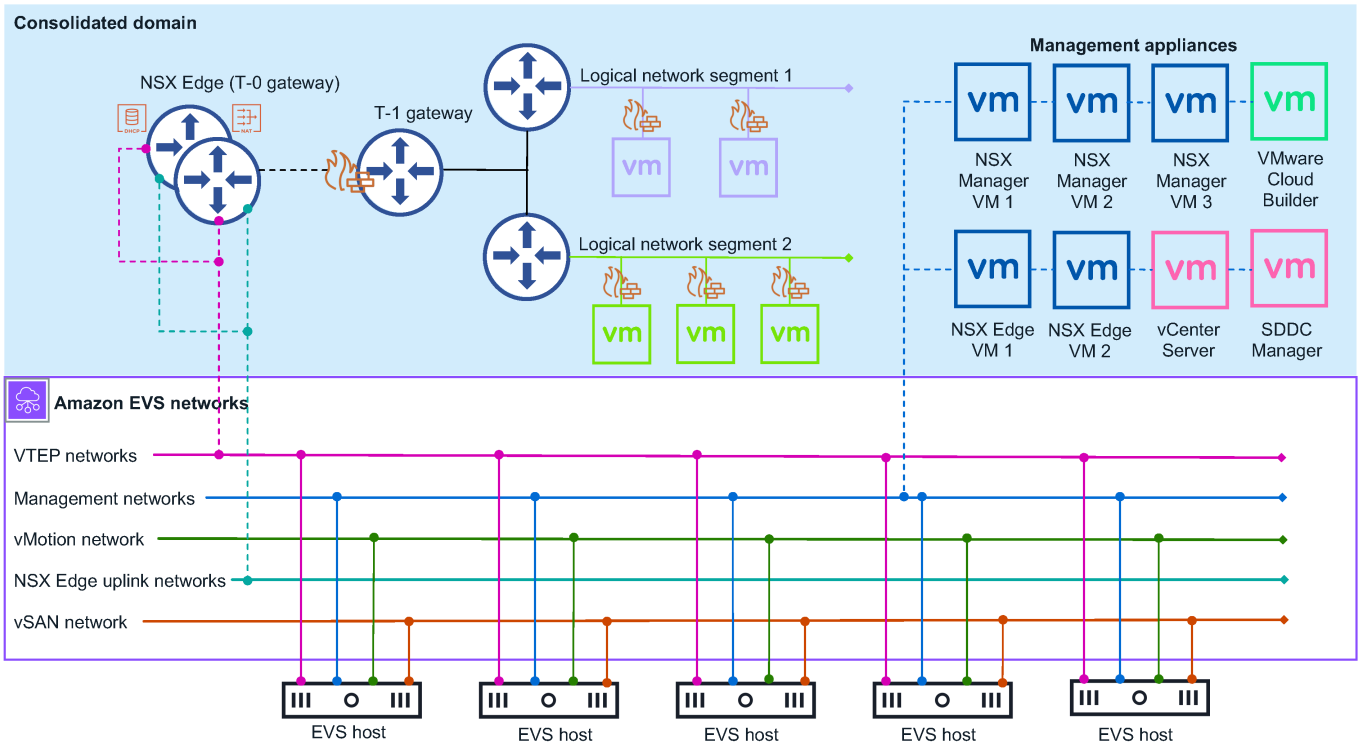
> **Note**
>
> Amazon EVS 处于公开预览版，可能会发生变化。

Amazon EVS 实施了 VMware 云基础 (VCF) 整合架构模型。在此模型中，VCF 管理组件和客户工作负载在整合的域上一起运行。Amazon EVS 环境通过单个 vCenter 服务器进行管理，该服务器具有 vSphere 资源池，可在管理工作负载和客户工作负载之间提供隔离。

Amazon EVS 部署的合并域包含以下 VCF 管理组件：

- ESXi 主机
- vCenter Server 实例
- SDDC 管理器
- vSAN 数据存储库
- 三节点 NSX Manager 群集
- vSphere 集群
- NSX Edge 群集

下图显示了在 Amazon EVS 环境中部署的 Amazon EVS 架构示例，并显示了环境中的组件是如何连接的。在图中，具有整合域架构的 Amazon EVS 环境以蓝色阴影显示。底层的 Amazon EVS 网络拓扑如紫色实线所示。



网络拓扑

Amazon EVS 环境有两个独立的管理网络层：

Amazon VPC

创建环境期间在 VPC 中创建的 Amazon VPC 和 Amazon EVS VLAN 子网构成了 VCF 部署的底层网络。此基础架构为 NSX 覆盖网络、主机管理、vMotion 和 VSAN 提供连接。Amazon VPC 路由服务器支持底层网络和覆盖网络之间的动态路由。有关更多信息，请参阅 the section called “概念和组件”。

> **Note**
>
> Amazon EVS VLAN 子网仅用于促进 VCF 底层通信。运行客户工作负载的来宾虚拟机必须部署在 NSX 叠加网络上。不支持在 Amazon EVS VLAN 子网底层网络上部署访客虚拟机。

VMware NSX 覆盖网络

作为部署的一部分，Amazon EVS 会代表您配置 NSX 覆盖网络。您可以配置其他 NSX 覆盖网络，以实现 Amazon EVS 环境中不同工作负载或应用程序之间的网络隔离。有关更多信息，请参阅 VMware Cloud Foundation 产品文档中的 VMware 云基础叠加设计。

> **Note**
>
> 对于具有两个 NSX Edge 节点的 Active/Standby NSX Edge 集群，Amazon EVS 仅支持一个 Tier-0 网关。此 Tier-0 网关连接并通告您配置为与 Amazon EVS 配合使用的所有覆盖网络。

两个网络层通过带有两个 NSX Edge 节点的 Active/Standby NSX Edge 群集相连。NSX Edge 节点允许中的虚拟机之间通过 VPC 进行通信 VLANs、互联网连接以及使用 AWS Direct Connect 或带有传输网关的 AWS Site-to-Site VPN 进行私有连接。

Amazon EVS 联网注意事项

管理网络需要以下网络资源配置。您在创建 Amazon EVS 环境时提供这些输入。有关更多信息，请参阅 the section called “概念和组件”。

- 亚马逊 VPC。确保您的 VPC IPv4 CIDR 块大小适当，以适应所需的 VPC 子网和 Amazon EVS 在创建环境时预置的 Amazon EVS VLAN 子网。有关更多信息，请参阅 the section called “Amazon EVS VLAN 子网”。

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

- 您的 VPC 中的服务访问子网。Amazon EVS 使用此子网来保持与您的 SDDC Manager 设备的永久连接。有关更多信息，请参阅服务访问子网。

  > **Note**
  >
  > Amazon EVS 目前仅支持单可用区部署。Amazon EVS 使用的所有 VPC 子网都必须存在于服务可用区域的单个可用区中。

  > **Note**
  >
  > 所有 VPC 子网都需要关联的路由表，这些路由表是根据贵组织的网络要求配置的。

- VPC 的 DHCP 选项集中的主 DNS 服务器 IP 地址和辅助 DNS 服务器 IP 地址，用于解析主机 IP 地址。Amazon EVS 还要求您为部署中的每个 VCF 管理设备和 Amazon EVS 主机创建一个包含 A 记录的 DNS 正向查找区域和一个包含 PTR 记录的反向查找区域。有关更多信息，请参阅 the section called “DNS 服务器配置”。
- Amazon EVS VLAN 子网 CIDR 块用于在创建环境期间 Amazon EVS 为您配置的每个 VLAN 子网。CIDR 块的最小大小必须为 /28 网络掩码，最大大小必须为 /24 网络掩码。CIDR 块必须不重叠。
- 启用了 Amazon VPC 路由服务器传播的路由服务器实例。
- 服务访问子网中的两个路由服务器端点。
- 两个路由服务器对等体，它们与 Amazon EVS 配置的 NSX Edge 节点与路由服务器终端节点对等。

0 级网关

Tier-0 网关处理逻辑网络和物理网络之间的所有南北向流量，并且是在 NSX 重叠网络上创建的。此 Tier-0 网关是作为 Amazon EVS 部署的一部分创建的。

> **Note**
>
> 对于具有两个 NSX Edge 节点的 Active/Standby NSX Edge 集群，Amazon EVS 仅支持一个 Tier-0 网关。

1 级网关

Tier-1 网关在 NSX 重叠网络上创建，处理环境内路由网段之间的东西向流量。Tier-1 网关具有到分段的下行链路连接和到 Tier-0 网关的上行链路连接。如果需要，您可以创建和配置其他 Tier-1 网关。

NSX Edge 群集

Amazon EVS 使用 NSX Manager 界面部署包含两个在模式下运行的 NSX Edge 节点的 NSX Edge 集群。 Active/Standby 此 NSX Edge 集群提供了运行 Tier-0 和 Tier-1 网关的平台，以及 IPsec VPN 连接及其 BGP 路由机制。

亚马逊 EVS 资源

Amazon EVS 在创建环境时会预配置以下 AWS 资源。这些资源显示在您允许 Amazon EVS 访问的 VPC 中，并且在创建 AWS CLI 后显示在 AWS Management Console 和中。

> **Important**
>
> 在 Amazon EVS 控制台和 API 之外修改这些资源可能会影响您的 Amazon EVS 环境的可用性和稳定性。

- Amazon EVS 弹性网络接口，可连接您的 VCF 设备和主机。
- 在 Amazon EC2 裸机实例上运行的 Amazon EVS ESXi 主机。有关更多信息，请参阅 the section called “亚马逊 EVS 主机”。

  > **Important**
  >
  > 您的 Amazon EVS 环境必须至少有 4 台主机，且不超过 16 台主机。Amazon EVS 仅支持 4-16 台主机的环境。

- 将您的 VPC 连接到 VCF 设备的 Amazon EVS VLAN 子网。有关更多信息，请参阅 the section called “Amazon EVS VLAN 子网”。

设置 Amazon 弹性 VMware 服务

> **Note**
>
> Amazon EVS 处于公开预览版，可能会发生变化。

要使用 Amazon EVS，您需要配置其他 AWS 服务，并设置您的环境以满足 VMware 云基础 (VCF) 的要求。

主题

报名参加 AWS

如果您没有 AWS 账户，请完成以下步骤来创建一个。

1. 打开https://portal.aws.amazon.com/billing/注册。
2. 按照屏幕上的说明操作。

创建 IAM 用户

1. 选择根用户并输入您的 AWS 账户电子邮件地址，以账户所有者的身份登录 IA M 控制台。在下一页上，输入您的密码。

> **Note**
>
> 强烈建议您遵守以下使用 Administrator IAM 用户的最佳实践，妥善保存根用户凭证。只在执行少数账户和服务管理任务时才作为根用户登录。

2. 在导航窗格中，选择用户，然后选择创建用户。
3. 对于用户名，输入 Administrator。
4. 选中 AWS 管理控制台访问旁边的复选框。然后选择自定义密码，并在文本框中输入新密码。
5. （可选）默认情况下，AWS 要求新用户在首次登录时创建新密码。您可以清除 User must create a new password at next sign-in（用户必须在下次登录时创建新密码）旁边的复选框以允许新用户在登录后重置其密码。
6. 选择下一步: 权限。
7. 在设置权限下，选择将用户添加到组。
8. 选择创建组。
9. 在 Create group（创建组）对话框中，对于 Group name（组名称），输入 Administrators。
10. 选择 “筛选策略”，然后选择 AWS 托管任务函数来筛选表格内容。
11. 在策略列表中，选中对应的复选框AdministratorAccess。然后选择 Create group（创建组）。

> **Note**
>
> 您必须先激活 IAM 用户和角色对账单的访问权限，然后才能使用这些AdministratorAccess权限访问 AWS Billing and Cost Management 控制台。为此，请按照“向账单控制台委派访问权限”教程第 1 步中的说明进行操作。

12. 返回到组列表中，选中您的新组所对应的复选框。如有必要，选择 Refresh（刷新）以在列表中查看该组。
13. 选择下一步: 标签。
14. （可选）通过以键值对的形式附加标签来向用户添加元数据。有关在 IAM 中使用标签的更多信息，请参阅《IAM 用户指南》中的标记 IAM 实体。

15选择 Next: Review（下一步：审核）以查看要添加到新用户的组成员资格的列表。如果您已准备好继续，请选择 Create user（创建用户）。

您可以使用相同的流程来创建更多群组和用户，并允许您的用户访问您的 AWS 账户资源。要了解如何使用限制用户对特定 AWS 资源的权限的策略，请参阅访问管理和示例策略。

创建 IAM 角色以向 IAM 用户委托 Amazon EVS 权限

您可以使用角色来委托对 AWS 资源的访问权限。借助 IAM 角色，您可以在您的信任账户与其他可信账户之间建立 AWS 信任关系。信任账户拥有要访问的资源，可信账户包含需要访问资源的用户。

创建信任关系后，IAM 用户或来自可信账户的应用程序可以使用 AWS Security Token Service (AWS STS) `AssumeRole` API 操作。此操作提供临时安全证书，允许访问您账户中的 AWS 资源。有关更多信息，请参阅用户指南中的创建向 IAM 用户委派权限的 AWS Identity and Access Management 角色。

按照以下步骤创建一个 IAM 角色，该角色的权限策略允许访问 Amazon EVS 操作。

> **Note**
>
> Amazon EVS 不支持使用实例配置文件将 IAM 角色传递给 EC2 实例。

Example

IAM console

1. 前往 I AM 控制台。
2. 在左侧菜单中，选择政策。
3. 选择创建策略。
4. 在策略编辑器中，创建启用 Amazon EVS 操作的权限策略。有关策略示例，请参阅 the section called “创建和管理 Amazon EVS 环境”。要查看所有可用的 Amazon EVS 操作、资源和条件密钥，请参阅服务授权参考中的操作。
5. 选择下一步。
6. 在策略名称下，输入一个有意义的策略名称来标识此策略。
7. 查看此策略中定义的权限。

8. （可选）添加标签以帮助识别、组织或搜索此资源。
9. 选择创建策略。
10. 在左侧菜单中，选择角色。
11. 选择创建角色。
12. 对于“可信实体类型”，选择 AWS 账户。
13. 在“是”下 AWS 账户 ，指定您要执行 Amazon EVS 操作的账户，然后选择下一步。
14. 在添加权限页面上，选择您之前创建的权限策略，然后选择下一步。
15. 在“角色名称”下，输入一个有意义的名称来标识此角色。
16. 查看信任政策，并确保将正确的委托人列 AWS 账户 为委托人。
17. （可选）添加标签以帮助识别、组织或搜索此资源。
18. 选择创建角色。

AWS CLI

1. 将以下内容复制到信任策略 JSON 文件中。对于委托人 ARN，请将示例 AWS 账户 ID 和`service-user`名称替换为您自己的 AWS 账户 ID 和 IAM 用户名。

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

2. 创建角色。`evs-environment-role-trust-policy.json`替换为您的信任策略文件名。

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

3. 创建启用 Amazon EVS 操作的权限策略并将该策略附加到该角色。将 `myAmazonEVSEnvironmentRole` 替换为您的角色名称。有关策略示例，请参阅 the section

called “创建和管理 Amazon EVS 环境”。要查看所有可用的 Amazon EVS 操作、资源和条件密钥，请参阅服务授权参考中的操作。

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

注册商 AWS 业、 AWS 企业入门计划或 AWS 企业支持计划

Amazon EVS 要求客户注册 AWS 商业、 AWS 企业入口或企业 AWS 支持计划，才能持续获得 Amazon EVS 技术支持和架构指导。如果您有业务关键型工作负载，我们建议您注册 Enterprise O AWS n-Ramp 或 Enterprise Su AWS pport 计划。有关更多信息，请参阅比较 Supp AWS ort 计划。

> **Important**
>
> 如果您未注册企业版、企业版入口计划或 AWS 企业 AWS 支持计划，Amazon EVS 环境创建将失败。 AWS

检查 配额

要启用 Amazon EVS 环境创建，请确保您的账户具有所需的最低账户级别配额。有关更多信息，请参阅 the section called “服务配额”。

> **Important**
>
> 如果每个 EVS 环境配额值的主机数量不低于 4，则创建 Amazon EVS 环境会失败。

规划 VPC CIDR 大小并配置 VPC 组件

要启用 Amazon EVS 环境创建，您必须为 Amazon EVS 提供包含子网和足够的 IP 地址空间的 VPC，以便 Amazon EVS 创建连接到您的 VCF 设备的 VLAN 子网。有关 VPC 创建要求的更多信息，请参阅the section called “创建包含子网和路由表的 VPC”。

主路由表

Amazon EVS 子网在创建时会隐式关联到您的 VPC 的主路由表。要启用与 DNS 或本地系统等依赖服务的连接以成功部署环境，您必须配置 VPC 的主路由表以允许流量流向这些系统。有关 Amazon EVS 主路由表配置的更多信息，请参阅the section called “配置 VPC 主路由表”。

DHCP 选项集

Amazon EVS 使用您的 VPC 的 DHCP 选项集来检索以下内容：

- 用于解析主机 IP 地址的域名系统 (DNS) 服务器。
- 网络时间协议 (NTP) 服务器，用于避免 SDDC 中的时间同步问题。

要成功部署 Amazon EVS 环境，您的 VPC 的 DHCP 选项集必须具有以下 DNS 设置：

- DHCP 选项集中的主 DNS 服务器 IP 地址和辅助 DNS 服务器 IP 地址。
- 一个 DNS 正向查找区域，其中包含部署中每个 VCF 管理设备和 Amazon EVS 主机的 A 记录，详情请参见。the section called “创建 Amazon EVS 环境”
- 一个反向查找区域，其中包含部署中每个 VCF 管理设备和 Amazon EVS 主机的 PTR 记录，详情请参见。the section called “创建 Amazon EVS 环境”

对于 NTP 配置，您可以使用默认 Amazon NTP 地址`169.254.169.123`或您喜欢的其他 IPv4 地址。

有关 Amazon EVS 支持的 DNS 和 NTP 服务器配置选项的更多信息，请参阅。the section called “使用 VPC DHCP 选项集配置 DNS 和 NTP 服务器”

创建 VPC 路由服务器基础架构

Amazon EVS 使用亚马逊 VPC 路由服务器为您的 VPC 底层网络启用基于 BGP 的动态路由。有关为使用 Amazon EVS 设置路由服务器的信息，请参阅the section called “使用终端节点和对等体设置一个 VPC 路由服务器实例”。

为本地连接创建公交网关

您可以使用关联的中转网关或使用传输网关的 AWS Site-to-Site VPN 连接来配置本地数据中心 AWS Direct Connect 与 AWS 基础设施的连接。有关更多信息，请参阅 the section called “（可选）配置本地网络连接”。

创建 Amazon EC2 容量预留

亚马逊 EVS 启动亚马逊 EC2 i4i.metal 实例，这些实例代表您的亚马逊 EVS ESXi 环境中的主机。为确保在需要时有足够的 i4i.metal 实例容量可用，我们建议您申请 Ama EC2 zon 容量预留。您能够随时创建容量预留，并且可以选择何时启动。您可以申请容量预留以便立即使用，也可以申请容量预留以备将来的某个日期使用。有关更多信息，请参阅 Amazon Elastic Cloud 用户指南中的通过 EC2 按需容量预留来预留计算容量。

设置 AWS CLI

AWS CLI 是一款用于使用的命令行工具 AWS 服务，包括 Amazon EVS。它还用于对从本地计算机访问 Amazon EVS 虚拟化环境和其他 AWS 资源的 IAM 用户或角色进行身份验证。要从命令行配置 AWS 资源，您需要获取 AWS 访问密钥 ID 和密钥，以便在命令行中使用。然后，您需要在 AWS CLI 中配置这些凭证。有关更多信息，请参阅版本 2 AWS Command Line Interface 用户指南 AWS CLI中的设置。

创建密 Amazon EC2 钥对

Amazon EVS 使用您在创建环境时提供的 Amazon EC2 密钥对来连接您的主机。要创建密钥对，请按照 Amazon Elastic Compute Cloud 用户指南中为您的 Amazon EC2 实例创建密钥对中的步骤进行操作。

为 VMware 云基础 (VCF) 做好环境准备

在部署 Amazon EVS 环境之前，您的环境必须满足 VMware 云基础 (VCF) 基础设施要求。有关详细的 VCF 先决条件，请参阅 Cloud F VMware oundation 产品文档中的规划和准备工作手册。

您还应该熟悉 VCF 5.2.1 的要求。有关更多信息，请参阅 VCF 5.2.1 发行说明

> **Note**
>
> 亚马逊 EVS 目前仅支持 VCF 版本 5.2.1.x。

获取 VCF 许可证密钥

要使用 Amazon EVS，您需要提供 VCF 解决方案密钥和 vSAN 许可密钥。VCF 解决方案密钥必须至少有 256 个内核。vSAN 许可密钥必须至少有 110 TiB 的 vSAN 容量。有关 VCF 许可证的更多信息，请参阅 Cloud Fou ndation 管理指南中的在 C VMware loud Foun VMware dation 中管理许可证密钥。

> **Note**
>
> 您的 VCF 许可证将适用于所有 AWS 地区的 Amazon EVS，以确保许可证合规。Amazon EVS 不验证许可证密钥。要验证许可证密钥，请访问 Broadcom 支持部门。

> **Note**
>
> 使用 SDDC 管理器用户界面管理 VCF 解决方案和 vSAN 许可密钥。Amazon EVS 要求您在 SDDC 管理器中保留有效的 VCF 解决方案和 vSAN 许可密钥，服务才能正常运行。如果您使用 vSphere Client 管理这些密钥，则必须确保这些密钥也显示在 SDDC Manager 用户界面的许可屏幕上。

VMware HCX 先决条件

您可以使用 VMware HCX 将 VMware基于现有的工作负载迁移到 Amazon EVS。在将 VMware HCX 与 Amazon EVS 配合使用之前，请确保已完成以下先决任务。

> **Note**
>
> VMware 默认情况下，EVS 环境中未安装 HCX。

- 在将 VMware HCX 与 Amazon EVS 搭配使用之前，必须满足最低网络底层要求。有关更多信息，请参阅 VMware HCX 用户指南中的网络底层最低要求。
- 确认已在环境中安装和配置 VMware NSX。有关更多信息，请参阅《VMware NSX 安装指南》。
- 确保 VMware HCX 已激活并安装在环境中。有关激活和安装 VMware HCX 的更多信息，请参阅《HCX 入门指南》中的 VMware HCX 入门指南。 VMware

亚马逊弹性 VMware 服务入门

> **Note**
>
> Amazon EVS 处于公开预览版，可能会发生变化。

使用本指南开始使用亚马逊弹性 VMware 服务 (Amazon EVS)。您将学习如何使用自己的亚马逊虚拟私有云 (VPC) 中的主机创建亚马逊 EVS 环境。

完成后，您将拥有一个 Amazon EVS 环境，您可以使用该环境将 VMware 基于 vSphere 的工作负载迁移到。 AWS Cloud

> **Important**
>
> 为了尽可能简单快速地入门，本主题包括创建 VPC 的步骤，并指定了 DNS 服务器配置和 Amazon EVS 环境创建的最低要求。在创建这些资源之前，我们建议您规划符合要求的 IP 地址空间和 DNS 记录设置。您还应该熟悉 VCF 5.2.1 的要求。有关更多信息，请参阅 VCF 5.2.1 发行说明。

> **Important**
>
> 亚马逊 EVS 目前仅支持 VCF 版本 5.2.1.x。

主题

- 将 Amazon EVS VLAN 子网明确关联到 VPC 路由表
- （可选）为本地连接配置中转网关路由表和 Direct Connect 前缀
- 创建网络 ACL 来控制 Amazon EVS VLAN 子网流量
- 检索 VCF 凭证并访问 VCF 管理设备
- 配置 EC2 串行控制台
- 清理
- 后续步骤

先决条件

在开始之前，您必须完成 Amazon EVS 的先决任务。有关更多信息，请参阅 设置 Amazon 弹性 VMware 服务。

创建包含子网和路由表的 VPC

> **Note**
>
> VPC、子网和 Amazon EVS 环境都必须在同一个账户中创建。Amazon EVS 不支持 VPC 子网或 Amazon EVS 环境的跨账户共享。

1. 打开 Amazon VPC 管理控制台。
2. 在 VPC 控制面板上，选择创建 VPC。
3. 对于要创建的资源，选择 VPC 等。
4. 保持选中自动生成名称标签以为 VPC 资源创建名称标签，或者清除此选项以为 VPC 资源提供您自己的名称标签。
5. 对于 IPv4 CIDR 块，请输入 IPv4 CIDR 块。VPC 必须有 IPv4 CIDR 块。确保您创建的 VPC 大小足以容纳 Amazon EVS 子网。有关更多信息，请参阅 the section called “Amazon EVS 联网注意事项”。

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

6. 将租赁保持为. `Default` 选中此选项后，在此 VPC 中启动的 EC2 实例将使用启动实例时指定的租期属性。Amazon EVS 代表您启动裸机 EC2 实例。
7. 对于可用区数量 (AZs)，请选择 1。

> **Note**
>
> Amazon EVS 目前仅支持单可用区部署。

8. 展开自定义 AZs，然后为您的子网选择可用区。

> **Note**
>
> 您必须在支持 Amazon EVS 的 AWS 地区进行部署。有关 Amazon EVS 区域可用性的更多信息，请参阅端点和限额。

9. （可选）如果您需要互联网连接，请在“公有子网数量”中选择 1。
10. 在“私有子网数量”中，选择 1。
11. 要选择子网的 IP 地址范围，请展开自定义子网 CIDR 块。

> **Note**
>
> 还需要从这个 VPC CIDR 空间创建 Amazon EVS VLAN 子网。确保在 VPC CIDR 块中为服务所需的 VLAN 子网留出足够的空间。有关更多信息，请参阅 the section called “Amazon EVS 联网注意事项”。

12. （可选）要向资源授予互联网访问权限，对于 NAT 网关，请选择在 1 个可用区中。 IPv4 请注意，使用 NAT 网关会产生成本。有关更多信息，请参阅 NAT 网关定价。

> **Note**
>
> Amazon EVS 需要使用 NAT 网关来启用出站互联网连接。

13. 对于 VPC endpoints（VPC 端点），选择 None（无）。

> **Note**
>
> Amazon EVS Amazon S3 目前不支持网关 VPC 终端节点。要启用 Amazon S3 连接，必须使用 AWS PrivateLink 设置接口 VPC 终端节点 Amazon S3。有关更多信息，AWS PrivateLink 请参阅《Amazon 简单存储服务用户指南》 Amazon S3中的。

14对于 DNS 选项，请保持选中默认值。Amazon EVS 要求您的 VPC 具有所有 VCF 组件的 DNS 解析功能。

15.（可选）要向 VPC 添加标签，请展开其他标签，选择添加新标签，然后输入标签键和标签值。

16选择创建 VPC。

> **Note**
>
> 在创建 VPC 期间， Amazon VPC 会自动创建主路由表并默认将其隐式关联子网。

配置 VPC 主路由表

Amazon EVS 子网在创建时会隐式关联到您的 VPC 的主路由表。要启用与 DNS 或本地系统等依赖服务的连接以成功部署环境，您必须配置主路由表以允许流向这些系统。有关管理子网路由表的更多信息，请参阅《 Amazon VPC 用户指南》中的管理子网路由表。

部署 Amazon EVS 环境后，您可以配置显式路由表关联以启用通过自定义路由表的连接。有关更多信息，请参阅《 Amazon VPC 用户指南》中的替换主路由表。

> **Important**
>
> 只有在创建 Amazon EVS 环境之后，Amazon EVS 才支持使用自定义路由表。在创建 Amazon EVS 环境期间，不应使用自定义路由表，因为这可能会导致连接问题。

使用 VPC DHCP 选项集配置 DNS 和 NTP 服务器

Amazon EVS 使用您的 VPC 的 DHCP 选项集来检索以下内容：

- 用于解析主机 IP 地址的域名系统 (DNS) 服务器。

- 网络时间协议 (NTP) 服务器，用于避免 SDDC 中的时间同步问题。

您可以使用 Amazon VPC 控制台或创建 DHCP 选项集 AWS CLI。有关更多信息，请参阅《 Amazon VPC 用户指南》中的创建 DHCP 选项集。

要启用 DNS 连接以成功部署环境，必须先将 VPC 的主路由表配置为允许 DNS 流量。有关更多信息，请参阅 the section called “配置 VPC 主路由表”。

DNS 服务器配置

您最多可以输入四个域名系统 (DNS) 服务器 IPv4 的地址。您可以用 Route 53 作 DNS 服务器提供商，也可以提供自己的自定义 DNS 服务器。有关将 Route 53 配置为现有域的 DNS 服务的更多信息，请参阅将 Route 53 设置为正在使用的域的 DNS 服务。

> **Note**
>
> 同时使用 Route 53 和自定义域名系统 (DNS) 服务器可能会导致意外行为。

> **Note**
>
> Amazon EVS IPv6 目前不支持。

要成功部署环境，您的 VPC 的 DHCP 选项集必须具有以下 DNS 设置：

- DHCP 选项集中的主 DNS 服务器 IP 地址和辅助 DNS 服务器 IP 地址。
- 一个 DNS 正向查找区域，其中包含部署中每个 VCF 管理设备和 Amazon EVS 主机的 A 记录，详情请参见。the section called “创建 Amazon EVS 环境”
- 一个反向查找区域，其中包含部署中每个 VCF 管理设备和 Amazon EVS 主机的 PTR 记录，详情请参见。the section called “创建 Amazon EVS 环境”

有关在 DHCP 选项集中配置 DNS 服务器的更多信息，请参阅创建 DHCP 选项集。

> **Note**
>
> 如果您使用在的私有托管区域中定义的自定义 DNS 域名 Route 53，或者将私有 DNS 与接口 VPC 终端节点 (AWS PrivateLink) 一起使用，则必须

将enableDnsHostnames和enableDnsSupport属性都设置为true。有关更多信息，请参阅您的 VPC 的 DNS 属性。

NTP 服务器配置

NTP 服务器为您的网络提供时间。您最多可以输入四个网络时间协议 (NTP) 服务器 IPv4 的地址。有关在 DHCP 选项集中配置 NTP 服务器的更多信息，请参阅创建 DHCP 选项集。

> **Note**
>
> Amazon EVS IPv6 目前不支持。

您可以通过 IPv4 地址指定 Amazon 时间同步服务169.254.169.123。默认情况下，Amazon EVS 部署的亚马逊 EC2 实例在 IPv4 地址使用亚马逊时间同步服务。169.254.169.123

有关 NTP 服务器的更多信息，请参阅 RFC 2123。有关亚马逊时间同步服务的更多信息，请参阅亚马逊 EC2 用户指南中的设置实例时间。

（可选）配置本地网络连接

您可以使用关联的中转网关或使用传输网关的 AWS Site-to-Site VPN 连接来配置本地数据中心 AWS Direct Connect 与 AWS 基础设施的连接。 AWS Site-to-Site VPN 通过互联网创建与传输网关的 IPsec VPN 连接。 AWS Direct Connect 通过私有 IPsec 专用连接创建与传输网关的 VPN 连接。创建 Amazon EVS 环境后，您可以使用任一选项将本地数据中心防火墙连接到 VMware NSX 环境。

要启用与本地系统的连接以成功部署环境，您必须配置 VPC 的主路由表以允许流向这些系统。有关更多信息，请参阅 the section called “配置 VPC 主路由表”。

创建 Amazon EVS 环境后，您必须使用在 Amazon EVS 环境中 CIDRs 创建的 VPC 更新传输网关路由表。有关更多信息，请参阅 the section called “（可选）为本地连接配置中转网关路由表和 Direct Connect 前缀”。

有关设置 AWS Direct Connect 连接的更多信息，请参阅AWS Direct Connect 网关和公交网关关联。有关将 AWS Site-to-Site VPN 与 Tr AWS ansit Gateway 配合使用的更多信息，请参阅 T Amazon VPC ransit Gateway 用户指南中 Amazon VPC 传输网关中的AWS Site-to-Site VPN 附件。

> **Note**
>
> Amazon EVS 不支持通过 Di AWS rect Connect 私有虚拟接口 (VIF) 或直接终止到底层 VPC 的 AWS Site-to-Site VPN 连接进行连接。

使用终端节点和对等体设置一个 VPC 路由服务器实例

Amazon EVS 使用亚马逊 VPC 路由服务器为您的 VPC 底层网络启用基于 BGP 的动态路由。您必须指定一个路由服务器，该服务器共享到服务访问子网中至少两个路由服务器端点的路由。在路由服务器对等体上配置的对等 ASN 必须匹配，并且对等 IP 地址必须是唯一的。

> **Important**
>
> 启用路由服务器传播时，请确保所有正在传播的路由表都至少有一个明确的子网关联。如果路由表确实存在明确的子网关联，BGP 路由通告就会失败。

有关设置 VPC 路由服务器的更多信息，请参阅路由服务器入门教程。

> **Note**
>
> 对于路由服务器对等体活性检测，Amazon EVS 仅支持默认 BGP keepalive 机制。Amazon EVS 不支持多跳双向转发检测 (BFD)。

> **Note**
>
> 我们建议您为路径服务器实例启用持续时间在 1-5 分钟之间的永久路由。如果启用，则即使所有 BGP 会话都已结束，路由也将保留在路由服务器的路由数据库中。有关更多信息，请参阅《Amazon VPC 用户指南》中的创建路由服务器。

> **Note**
>
> 如果您使用的是 NAT 网关或传输网关，请确保您的路由服务器配置正确，可以将 NSX 路由传播到 VPC 路由表。

创建 Amazon EVS 环境

> **Important**
>
> 为了尽可能简单快速地入门，本主题包括使用默认设置创建 Amazon EVS 环境的步骤。在创建环境之前，我们建议您熟悉所有设置，并使用符合您要求的设置部署环境。只能在初始环境创建期间配置环境。创建环境后，就无法对其进行修改。有关所有可能的亚马逊 EVS 环境设置的概述，请参阅亚马逊 EVS API 参考指南。

> **Note**
>
> 您的环境 ID 将提供给所有 AWS 地区的 Amazon EVS，以满足 VCF 许可合规需求。

> **Note**
>
> Amazon EVS 环境必须部署到与 VPC 和 VPC 子网相同的区域和可用区。

完成此步骤即可创建包含主机和 VLAN 子网的 Amazon EVS 环境。

Example

Amazon EVS console

1. 前往 Amazon EVS 控制台。

   > **Note**
   >
   > 确保控制台右上角显示的 AWS 区域是您要在其中创建环境的区域。 AWS 如果不是，请选择 AWS 区域名称旁边的下拉列表并选择要使用的 AWS 区域。

   > **Note**
   >
   > 从亚马逊 EVS 控制台触发的 Amazon EVS 操作不会生成 CloudTrail 事件。

2. 在导航窗格中，选择环境。
3. 选择创建环境。
4. 在验证 Amazon EVS 要求页面上，执行以下操作。
   a. 检查是否满足 Su AWS pport 要求和服务配额要求。有关 Amazon EVS 支持要求的更多信息，请参阅the section called “注册商 AWS 业、 AWS 企业入门计划或 AWS 企业支持计划”。有关 Amazon EVS 配额要求的更多信息，请参阅the section called “服务配额”。
   b. （可选）在“名称”中，输入环境名称。
   c. 对于环境版本，请选择您的 VCF 版本。亚马逊 EVS 目前仅支持 5.2.1.x 版本。
   d. 对于站点 ID，请输入您的博通网站 ID。
   e. 对于 VCF 解决方案密钥，请输入 VCF 解决方案密钥。现有环境无法使用此许可证密钥。

> **Note**
>
> VCF 解决方案密钥必须至少有 256 个内核。

> **Note**
>
> 您的 VCF 许可证将适用于所有 AWS 地区的 Amazon EVS，以确保许可证合规。Amazon EVS 不验证许可证密钥。要验证许可证密钥，请访问 Broadcom 支持部门。

> **Note**
>
> Amazon EVS 要求您在 SDDC 管理器中保留有效的 VCF 解决方案密钥，服务才能正常运行。如果您在部署后使用 vSphere Client 管理 VCF 解决方案密钥，则必须确保密钥也显示在 SDDC Manager 用户界面的许可屏幕上。

   f. 对于 vSAN 许可密钥，请输入 vSAN 许可密钥。现有环境无法使用此许可证密钥。

> **Note**
>
> vSAN 许可密钥必须至少有 110 TiB 的 vSAN 容量。

> **Note**
>
> 您的 VCF 许可证将适用于所有 AWS 地区的 Amazon EVS，以确保许可证合规。Amazon EVS 不验证许可证密钥。要验证许可证密钥，请访问 Broadcom 支持部门。

> **Note**
>
> Amazon EVS 要求您在 SDDC Manager 中保留有效的 vSAN 许可密钥，服务才能正常运行。如果您在部署后使用 vSphere Client 管理 vSAN 许可密钥，则必须确保密钥也显示在 SDDC Manager 用户界面的许可屏幕上。

g. 对于 VCF 许可条款，请选中复选框以确认您已购买并将继续保持所需数量的 VCF 软件许可，以涵盖 Amazon EVS 环境中的所有物理处理器内核。有关您在亚马逊 EVS 中的 VCF 软件的信息将与 Broadcom 共享，以验证许可证合规性。

h. 选择下一步。

5. 在指定主机详细信息页面上，完成以下步骤 4 次，向环境中添加 4 个主机。Amazon EVS 环境需要 4 台主机进行初始部署。

a. 选择添加主机详细信息。

b. 对于 DNS 主机名，输入主机的主机名。

c. 对于实例类型，请选择 EC2 实例类型。

> **Important**
>
> 请勿停止或终止 Amazon EVS 部署的 EC2 实例。此操作会导致数据丢失。

> **Note**
>
> 亚马逊 EVS 目前仅支持 i4i.metal EC2 实例。

d. 对于 SSH 密钥对，请选择一个 SSH 密钥对，以便通过 SSH 访问主机。

e. 选择添加主机。

6. 在 “配置网络和连接” 页面上，执行以下操作。

   a. 对于 VPC，请选择您之前创建的 VPC。

   b. 对于服务访问子网，请选择在创建 VPC 时创建的私有子网。

   c. 对于安全组-可选，您最多可以选择 2 个安全组来控制 Amazon EVS 控制平面和 VPC 之间的通信。如果未选择任何安全组，Amazon EVS 将使用默认安全组。

   > **Note**
   >
   > 确保您选择的安全组提供与您的 DNS 服务器和 Amazon EVS VLAN 子网的连接。

   d. 在 “管理连接” 下，输入要用于 Amazon EVS VLAN 子网的 CIDR 块。

   > **Important**
   >
   > Amazon EVS VLAN 子网只能在创建 Amazon EVS 环境的过程中创建，并且在创建环境后无法修改。在创建环境之前，必须确保正确调整 VLAN 子网 CIDR 块的大小。部署环境后，您将无法添加 VLAN 子网。有关更多信息，请参阅 the section called “Amazon EVS 联网注意事项”。

   e. 在 “扩展” 下 VLANs，输入其他 Amazon EVS VLAN 子网的 CIDR 块，这些子网可用于扩展 Amazon EVS 中的 VCF 功能，例如启用 NSX Federation。

   > **Note**
   >
   > 确保您提供的 VLAN CIDR 块在 VPC 内大小正确。有关更多信息，请参阅 the section called “Amazon EVS 联网注意事项”。

   f. 在 “工作负载/vCF 连接” 下，输入 NSX 上行链路 VLAN 的 CIDR 块，然后选择 2 个通过 NSX 上行链路与路由服务器端点对等 IDs 的 VPC 路由服务器对等体。

   > **Note**
   >
   > Amazon EVS 需要一个与 2 个路由服务器终端节点和 2 个路由服务器对等体关联的 VPC 路由服务器实例。此配置支持通过 NSX 上行链路进行基于 BGP 的动态路由。有关更多信息，请参阅 the section called “使用终端节点和对等体设置一个 VPC 路由服务器实例”。

   g. 选择下一步。

7. 在 “指定管理 DNS 主机名” 页面上，执行以下操作。
   a. 在管理设备 DNS 主机名下，输入托管 VCF 管理设备的虚拟机的 DNS 主机名。如果使用 Route 53 作为 DNS 提供商，还要选择包含您的 DNS 记录的托管区域。
   b. 在 “凭证” 下，选择是要使用 Secrets Manager 的 AWS 托管 KMS 密钥还是要使用您提供的客户托管 KMS 密钥。此密钥用于加密使用 SDDC Manager、NSX Manager 和 vCenter 设备所需的 VCF 凭据。

      > **Note**
      > 客户托管的 KMS 密钥会产生使用成本。有关更多信息，请参阅 AWS KMS 定价页面。

   c. 选择下一步。
8. （可选）在添加标签页面上，添加要分配给此环境的所有标签，然后选择下一步。

   > **Note**
   > 作为该环境的一部分创建的主机将收到以下标记：`DoNotDelete-EVS-environmentid-hostname`。

   > **Note**
   > 与 Amazon EVS 环境关联的标签不会传播到底层 AWS 资源，例如 EC2 实例。您可以使用相应的服务控制台或在底层 AWS 资源上创建标签 AWS CLI。

9. 在查看并创建页面上，查看您的配置并选择创建环境。

   > **Important**
   > 在环境部署期间，Amazon EVS 会创建 EVS VLAN 子网并将其隐式关联到主路由表。部署完成后，您必须明确将 Amazon EVS VLAN 子网与路由表关联，以便 NSX 连接。有关更多信息，请参阅 the section called “将 Amazon EVS VLAN 子网明确关联到 VPC 路由表”。

> **Note**
>
> Amazon EVS 部署了最新捆绑版本的 VMware Cloud Foundation，其中可能不包括单个产品更新，即异步补丁。部署完成后，我们强烈建议您使用 Broadcom 的异步补丁工具 (AP 工具) 或 SDDC Manager 产品内 LCM 自动化来检查和更新各个产品。NSX 升级必须在 SDDC 管理器之外完成。

> **Note**
>
> 创建环境可能需要几个小时。

AWS CLI

1. 打开终端会话。
2. 创建 Amazon EVS 环境。以下是`aws evs create-environment`请求示例。

> **Important**
>
> 在运行`aws evs create-environment`命令之前，请检查是否已满足所有 Amazon EVS 先决条件。如果未满足先决条件，则环境部署将失败。有关 Amazon EVS 支持要求的更多信息，请参阅the section called “注册商 AWS 业、 AWS 企业入门计划或 AWS 企业支持计划”。有关 Amazon EVS 配额要求的更多信息，请参阅the section called “服务配额”。

> **Important**
>
> 在环境部署期间，Amazon EVS 会创建 EVS VLAN 子网并将其隐式关联到主路由表。部署完成后，您必须明确将 Amazon EVS VLAN 子网与路由表关联，以便 NSX 连接。有关更多信息，请参阅 the section called “将 Amazon EVS VLAN 子网明确关联到 VPC 路由表”。

> **Note**
>
> Amazon EVS 部署了最新捆绑版本的 VMware Cloud Foundation，其中可能不包括单个产品更新，即异步补丁。部署完成后，我们强烈建议您使用 Broadcom 的异步补丁工具（AP 工具）或 SDDC Manager 产品内 LCM 自动化来检查和更新各个产品。NSX 升级必须在 SDDC 管理器之外完成。

> **Note**
>
> 环境部署可能需要几个小时。

- 对于`--vpc-id`，请指定您之前创建的 VPC，其最小 IPv4 CIDR 范围为 /22。
- 对于`--service-access-subnet-id`，请指定在创建 VPC 时创建的私有子网的唯一 ID。
- 对于`--vcf-version`，亚马逊 EVS 目前仅支持 VCF 5.2.1.x。
- 使用`--terms-accepted`，您确认已购买并将继续保持所需数量的 VCF 软件许可证，以涵盖 Amazon EVS 环境中的所有物理处理器内核。有关您在亚马逊 EVS 中的 VCF 软件的信息将与 Broadcom 共享，以验证许可证合规性。
- 对于`--license-info`，请输入您的 VCF 解决方案密钥和 vSAN 许可密钥。

  > **Note**
  >
  > VCF 解决方案密钥必须至少有 256 个内核。vSAN 许可密钥必须至少有 110 TiB 的 vSAN 容量。

  > **Note**
  >
  > Amazon EVS 要求您在 SDDC 管理器中保留有效的 VCF 解决方案密钥和 vSAN 许可密钥，服务才能正常运行。如果您在部署后使用 vSphere Client 管理这些许可密钥，则必须确保它们也显示在 SDDC Manager 用户界面的许可屏幕上。

> **Note**
>
> 现有的 Amazon EVS 环境无法使用 VCF 解决方案密钥和 vSAN 许可密钥。

- 有关`--initial-vlans`指定 Amazon EVS 代表您创建的 Amazon EVS VLAN 子网的 CIDR 范围。 VLANs 它们用于部署 VCF 管理设备。

> **Important**
>
> Amazon EVS VLAN 子网只能在创建 Amazon EVS 环境的过程中创建，并且在创建环境后无法修改。在创建环境之前，必须确保正确调整 VLAN 子网 CIDR 块的大小。部署环境后，您将无法添加 VLAN 子网。有关更多信息，请参阅 the section called “Amazon EVS 联网注意事项”。

- 对于`--hosts`，指定 Amazon EVS 部署环境所需的主机的主机详细信息。包括每台主机的 DNS 主机名、 EC2 SSH 密钥名称和 EC2 实例类型。

> **Important**
>
> 请勿停止或终止 Amazon EVS 部署的 EC2 实例。此操作会导致数据丢失。

> **Note**
>
> 亚马逊 EVS 目前仅支持 i4i.metal EC2 实例。

- 对于`--connectivity-info`，请指定您在上一步中创建的 2 个 VPC 路由服务器对等体 IDs 。

> **Note**
>
> Amazon EVS 需要一个与 2 个路由服务器终端节点和 2 个路由服务器对等体关联的 VPC 路由服务器实例。此配置支持通过 NSX 上行链路进行基于 BGP 的动态路由。有关更多信息，请参阅 the section called “使用终端节点和对等体设置一个 VPC 路由服务器实例”。

- 对于`--vcf-hostnames`，输入用于托管 VCF 管理设备的虚拟机的 DNS 主机名。

- 对于--site-id，请输入您的唯一博通网站 ID。此 ID 允许访问 Broadcom 门户，由博通在您的软件合同或合同续订期满时提供给您。
- （可选）对于--region，请输入您的环境将部署到的区域。如果未指定区域，则使用您的默认区域。

```
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
```

以下为示例响应。

```
{
    "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"
        }
```

```
    }
}
```

验证 Amazon EVS 环境的创建

Example

Amazon EVS console

1. 前往 Amazon EVS 控制台。
2. 在导航窗格中，选择环境。
3. 选择环境。
4. 选择 “详细信息” 选项卡。
5. 检查环境状态是否为 “已通过”，环境状态是否为 “已创建”。这可以让你知道环境已准备就绪。

> **Note**
>
> 创建环境可能需要几个小时。如果 “环境” 状态仍显示 “正在创建”，请刷新页面。

AWS CLI

1. 打开终端会话。
2. 使用您的环境的环境 ID 和包含您的资源的区域名称运行以下命令。当环境处于可用状态时，`environmentState`即可使用`CREATED`。

> **Note**
>
> 创建环境可能需要几个小时。如果`environmentState`仍然显示`CREATING`，请再次运行命令以刷新输出。

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

以下为示例响应。

```
{
    "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": []
    }
}
```

将 Amazon EVS VLAN 子网明确关联到 VPC 路由表

将每个 Amazon EVS VLAN 子网与您的 VPC 中的路由表明确关联。此路由表用于允许 AWS 资源与运行 Amazon EVS 的 NSX 网段上的虚拟机进行通信。

Example

Amazon VPC console

1. 前往 VPC 控制台。
2. 在导航窗格中，选择 Route tables（路由表）。
3. 选择要与 Amazon EVS VLAN 子网关联的路由表。
4. 选择子网关联选项卡。
5. 在 “显式子网关联” 下，选择 “编辑子网关联”。
6. 选择所有 Amazon EVS VLAN 子网。
7. 选择 Save associations (保存关联)。

AWS CLI

1. 打开终端会话。
2. 识别 Amazon EVS VLAN 子网 IDs。

```
aws ec2 describe-subnets
```

3. 将您的 Amazon EVS VLAN 子网与您的 VPC 中的路由表相关联。

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

（可选）为本地连接配置中转网关路由表和 Direct Connect 前缀

如果您使用传输网关 AWS Direct Connect 或 AWS Site-to-Site VPN 配置本地网络连接，则必须使用在 Amazon EVS 环境中 CIDRs 创建的 VPC 更新传输网关路由表。有关更多信息，请参阅 Amazon VPC 传输网关中的公交网关路由表。

如果您使用的是 AWS Direct Connect，则可能还需要更新 Direct Connect 前缀，以便从 VPC 发送和接收更新的路由。有关更多信息，请参阅允许 Dire AWS ct Connect 网关进行前缀交互。

创建网络 ACL 来控制 Amazon EVS VLAN 子网流量

Amazon EVS 使用网络访问控制列表 (ACL) 来控制进出亚马逊 EVS VLAN 子网的流量。您可以为自己的 VPC 使用默认网络 ACL，也可以使用与安全组规则相似的规则为您的 VPC 创建自定义网络 ACL，从而为您的 VPC 添加一层安全保护。有关更多信息，请参阅 Amazon VPC 用户指南中的为您的 VPC 创建网络 ACL。

> **Important**
>
> EC2 安全组在连接到 Amazon EVS VLAN 子网的弹性网络接口上不起作用。要控制进出 Amazon EVS VLAN 子网的流量，您必须使用网络访问控制列表。

检索 VCF 凭证并访问 VCF 管理设备

Amazon EVS 使用 S AWS ecrets Manager 在您的账户中创建、加密和存储托管密钥。这些密钥包含安装和访问 vCenter Server、NSX 和 SDDC Manager 等 VCF 管理设备所需的 VCF 凭据。有关检索密钥的更多信息，请参阅从 Secrets Manager 获取 AWS 密钥。

> **Note**
>
> Amazon EVS 不提供对您的密钥的托管轮换。我们建议您在设定的轮换窗口中定期轮换密钥，以确保密钥不会持续很长时间。

从 S AWS ecrets Manager 检索 VCF 凭证后，您可以使用它们登录您的 VCF 管理设备。有关更多信息，请参阅产品文档中的登录 SDDC Manager 用户界面以及如何使用和配置 vSphere 客户端。VMware

配置 EC2 串行控制台

默认情况下，Amazon EVS 在新部署的 Amazon EVS 主机上启用 ESXi 命令行管理程序。此配置允许通过串行控制台访问 Amazon EC2 实例的 EC2 串行端口，您可以使用串行控制台对启动、网络配置和其他问题进行故障排除。串行控制台不要求您的实例拥有任何联网功能。使用串行控制台，您可以向正在运行的 EC2 实例输入命令，就像键盘和显示器直接连接到实例的串行端口一样。

可以使用控制台或控制台访问 EC2 串行 EC2 控制台 AWS CLI。有关更多信息，请参阅 Amazon EC2 用户指南中的实例EC2 串行控制台。

> **Note**
>
> EC2 串行控制台是 Amazon EVS 支持的唯一一种访问直接控制台用户界面 (DCUI) 以在本地与 ESXi 主机交互的机制。

> **Note**
>
> 默认情况下，Amazon EVS 会禁用远程 SSH。有关启用 SSH 访问远程 ESXi 命令行管理程序的更多信息，请参阅 VMware vSphere 产品文档中的使用 SSH 进行远程 ESXi 外壳访问。

Connect 连接到 EC2 串行控制台

要连接到 EC2 串行控制台并使用您选择的工具进行故障排除，必须完成某些先决任务。有关更多信息，请参阅 Amazon EC2 用户指南中的 EC2 串行控制台和连接到 EC2 串行控制台的先决条件。

> **Note**
>
> 要连接到 EC2 串行控制台，您的 EC2 实例状态必须为`running`。如果实例处于、、、或`terminated`状态 `pending` `stopping` `stopped`shutting-down，则无法连接到串行控制台。有关实例状态变化的更多信息，请参阅亚马逊 EC2 用户指南中的亚马逊 EC2 实例状态更改。

配置对 EC2 串行控制台的访问权限

要配置对 EC2 串行控制台的访问权限，您或您的管理员必须在账户级别授予串行控制台访问权限，然后配置 IAM 策略以向您的用户授予访问权限。对于 Linux 实例，您还必须在每个实例上配置一个基于密码的用户，以便您的用户可以使用串行控制台进行故障排除。有关更多信息，请参阅 Amazon EC2 用户指南中的配置 EC2 串行控制台访问权限。

清理

按照以下步骤删除已创建的 AWS 资源。

删除 Amazon EVS 主机和环境

按照以下步骤删除 Amazon EVS 主机和环境。此操作将删除在您的 Amazon E VMware VS 环境中运行的 VCF 安装。

> **Note**
>
> 要删除 Amazon EVS 环境，必须先删除该环境中的所有主机。如果存在与环境关联的主机，则无法删除该环境。

Example

SDDC UI and Amazon EVS console

1. 转到 SDDC 管理器用户界面。
2. 从 vSphere 集群中移除主机。这将取消分配给 SDDC 域的主机。对群集中的每台主机重复此步骤。有关更多信息，请参阅 VCF 产品文档中的从工作负载域的 vSphere 集群中移除主机。
3. 停用未分配的主机。有关更多信息，请参阅 VCF 产品文档中的停用主机。
4. 前往 Amazon EVS 控制台。

   > **Note**
   >
   > 从亚马逊 EVS 控制台触发的 Amazon EVS 操作不会生成 CloudTrail 事件。

5. 在导航窗格中，选择环境。
6. 选择包含要删除的主机的环境。
7. 选择 “主机” 选项卡。
8. 选择主机，然后在 “主机” 选项卡中选择 “删除”。对环境中的每台主机重复此步骤。
9. 在 “环境” 页面的顶部，选择删除，然后选择删除环境。

   > **Note**
   >
   > 删除环境还会删除亚马逊 EVS 创建的 Amazon EVS VLAN 子网和 Secrets Manager AWS 密钥。 AWS 您创建的资源不会被删除。这些资源可能会继续产生费用。

10如果您已有不再需要的 Amazon EC2 容量预留，请确保已将其取消。有关更多信息，请参阅 Amazon EC2 用户指南中的取消容量预留。

SDDC UI and AWS CLI

1. 打开终端会话。
2. 确定包含要删除的主机的环境。

```
aws evs list-environments
```

以下为示例响应。

```
{
    "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. 转到 SDDC 管理器用户界面。
4. 从 vSphere 集群中移除主机。这将取消分配给 SDDC 域的主机。对群集中的每台主机重复此步骤。有关更多信息，请参阅 VCF 产品文档中的从工作负载域的 vSphere 集群中移除主机。

5. 停用未分配的主机。有关更多信息，请参阅 VCF 产品文档中的停用主机。
6. 从环境中删除主机。以下是`aws evs delete-environment-host`请求示例。

> **Note**
>
> 要删除环境，必须先删除该环境中包含的所有主机。

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

7. 重复前面的步骤，删除环境中剩余的主机。
8. 删除环境。

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

> **Note**
>
> 删除环境还会删除亚马逊 EVS 创建的 Amazon EVS VLAN 子网和 Secrets Manager AWS 密钥。您创建的其他 AWS 资源不会被删除。这些资源可能会继续产生费用。

9. 如果您已有不再需要的 Amazon EC2 容量预留，请确保已将其取消。有关更多信息，请参阅 Amazon EC2 用户指南中的取消容量预留。

删除 VPC 路由服务器组件

有关删除您创建的 Amazon VPC 路由服务器组件的步骤，请参阅 Amazon VPC 用户指南中的路由服务器清理。

删除网络访问控制列表 (ACL)

有关删除网络访问控制列表的步骤，请参阅 Amazon VPC 用户指南中的删除 VPC 的网络 ACL。

删除弹性网络接口

有关删除弹性网络接口的步骤，请参阅 Amazon EC2 用户指南中的删除网络接口。

取消关联并删除子网路由表

有关取消关联和删除子网路由表的步骤，请参阅 Amazon VPC 用户指南中的子网路由表。

删除子网

删除 VPC 子网，包括服务访问子网。有关删除 VPC 子网的步骤，请参阅 Amazon VPC 用户指南中的删除子网。

> **Note**
>
> 如果您将 Route 53 用于 DNS，请在尝试删除服务访问子网之前移除入站终端节点。否则，您将无法删除服务访问子网。

> **Note**
>
> 删除环境后，Amazon EVS 会代表您删除 VLAN 子网。只有删除环境后，才能删除 Amazon EVS VLAN 子网。

删除 VPC

有关删除 VPC 的步骤，请参阅 Amazon VPC 用户指南中的删除您的 VPC。

后续步骤

使用 VMware 混合云扩展 (VMware HCX) 将您的工作负载迁移到 Amazon EVS。有关更多信息，请参阅 迁移。

使用 VMware 混合云扩展 (VMware HCX) 将工作负载迁移到 Amazon EVS

> **Note**
>
> Amazon EVS 处于公开预览版，可能会发生变化。

创建亚马逊 EVS 环境后，您可以使用 VMware 混合云扩展 (VMware HCX) 将 VMware基于现有的工作负载迁移到亚马逊弹性 VMware 服务 (Amazon EVS)。有关 VMware HCX 迁移的更多信息，请参阅 VMware HCX 用户指南中的 VMware HCX 迁移类型。

以下教程介绍如何使用 VMware HCX 将 VMware 工作负载迁移到 Amazon EVS。

您可以使用 VMware HCX 通过私有连接迁移工作负载，将工作负载 AWS Direct Connect 与关联的中转网关一起使用，也可以使用 AWS Site-to-Site VPN 连接迁移到传输网关。

> **Note**
>
> Amazon EVS 不支持通过 Di AWS rect Connect 私有虚拟接口 (VIF) 或直接终止到底层 VPC 的 AWS Site-to-Site VPN 连接进行连接。

有关设置 AWS Direct Connect 连接的更多信息，请参阅《 AWS Direct Connect 用户指南》中的AWS Direct Connect 网关和公交网关关联。有关将 AWS Site-to-Site VPN 与 Tr AWS ansit Gateway 配合使用的更多信息，请参阅 T Amazon VPC ransit Gateway 用户指南中 Amazon VPC 传输网关中的AWS Site-to-Site VPN 附件。

先决条件

在将 VMware HCX 与 Amazon EVS 配合使用之前，请确保已满足 HCX 先决条件，并且已创建一个 Amazon EVS 环境，并使用传输网关或 AWS Direct Connect 带有传输网关的 AWS Site-to-Site VPN 连接到您的本地网络。有关创建 Amazon EVS 环境的步骤，请参阅入门。有关 VMware HCX 先决条件的更多信息，请参阅the section called “VMware HCX 先决条件”。

检查 HCX VLAN 子网的状态

按照以下步骤检查 HCX VLAN 子网的配置是否正确。

Example

Amazon EVS console

1. 前往 Amazon EVS 控制台。
2. 在导航窗格中，选择环境。
3. 选择 Amazon EVS 环境。
4. 选择 “网络和连接” 选项卡。
5. 在下方 VLANs，识别 HCX VLAN 并检查状态是否已创建。
6. 复制 HCX `vlan` ID 以备日后使用。

AWS CLI

1. 使用您的环境的环境 ID 和包含您的资源的区域名称运行以下命令。

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

以下为示例响应。

```
{
 "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. 识别带有 of `functionName` 的 VLAN `hcx` 并检查是否`vlanState`为`CREATED`。
3. 复制 HCX `vlan` ID 以备日后使用。

检查 HCX VLAN 子网是否与网络 ACL 关联

按照以下步骤检查 HCX VLAN 子网是否与网络 ACL 关联。有关网络 ACL 关联的更多信息，请参阅the section called “创建网络 ACL 来控制 Amazon EVS VLAN 子网流量”。

Example

Amazon VPC console

1. 转到 Amazon VPC 控制台。
2. 在导航窗格中，选择 “网络” ACLs。
3. 选择与您的 VLAN 子网关联的网络 ACL。
4. 选择子网关联选项卡。
5. 检查 HCX VLAN 子网是否列在关联的子网中。

AWS CLI

1. 使用`Values`过滤器中的 HCX VLAN 子网 ID 运行以下命令。

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

2. 检查响应中是否返回了正确的网络 ACL。

使用 HCX 公共上行链路 VLAN ID 创建分布式端口组

转到 vSphere Client 界面，按照添加分布式端口组中的步骤将分布式端口组添加到 vSphere 分布式交换机。

在 vSphere Client 界面中配置故障恢复时，请确保 uplink1 为活动上行链路，uplink2 为备用上行链路，以启用故障切换。 Active/Standby 对于 vSphere Client 界面中的 VLAN 设置，请输入您之前识别的 HCX VLAN ID。

（可选）设置 HCX 广域网优化

HCX 广域网优化服务 (HCX-WAN-OPT) 通过应用数据缩减和广域网路径调节等广域网优化技术，改善了专线或互联网路径的性能特征。对于无法使用专用 10Gbit 路径进行迁移的部署，建议使用 HCX 广域网优化服务。在 10Gbit 中，低延迟部署中，使用 WAN 优化可能无法提高迁移性能。有关更多信息，请参阅 VMware HCX 部署注意事项和最佳实践。

HCX 广域网优化服务与 HCX 广域网互连服务设备 (HCX-WAN-IX) 一起部署。 HCX-WAN-IX 负责企业环境和 Amazon EVS 环境之间的数据复制。

要将 HCX 广域网优化服务与 Amazon EVS 配合使用，您需要在 HCX VLAN 子网中使用分布式端口组。使用在前面的步骤中创建的分布式端口组。

（可选）启用 HCX 移动优化联网

HCX 移动优化网络 (MON) 是 HCX 网络扩展服务的一项功能。支持 MON 的网络扩展通过在 Amazon EVS 环境中启用选择性路由，改善已迁移虚拟机的流量。MON 允许您配置将工作负载流量迁移到 Amazon EVS 的最佳路径，从而避免通过源网关的漫长往返网络路径。此功能适用于所有 Amazon EVS 部署。有关更多信息，请参阅 VMware HCX 用户指南中的配置移动优化网络。

> **Important**
>
> 在启用 HCX MON 之前，请阅读以下 HCX 网络扩展的限制和不支持的配置。
> 网络扩展的限制和限制
> 移动优化网络拓扑的限制和限制

> **Important**
>
> 在启用 HCX MON 之前，请确保在 NSX 接口中为目标网络 CIDR 配置了路由再分配。有关更多信息，请参阅 VMware NSX 文档中的配置 BGP 和路由重新分发。

验证 HCX 连接

VMware HCX 包含可用于测试连接的内置诊断工具。有关更多信息，请参阅 VMware HCX 用户指南中的 VMware HCX 故障排除。

Amazon 弹性 VMware 服务中的安全

> **Note**
>
> Amazon EVS 处于公开预览版，可能会发生变化。

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方共同承担 AWS 的责任。责任共担模型将其描述为云的安全性和云中的安全性：

- 云安全 — AWS 负责保护在云 AWS 服务 中运行的基础架构 AWS Cloud。 AWS 还为您提供可以安全使用的服务。作为 AWS 合规性计划的一部分，第三方审核人员将定期测试和验证安全性的有效性。要了解适用于 Amazon Elastic VMware 服务的合规计划，请参阅AWS 服务 按合规计划划分的范围。
- 云端安全 — 您的责任由您 AWS 服务 使用的内容决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

本文档可帮助您了解在使用 Amazon Elastic VMware 服务时如何应用分担责任模型。它向您展示了如何配置 Amazon Elastic VMware 服务以满足您的安全与合规目标。您还将学习如何使用其他方法来帮助您监控和保护您 AWS 服务 的 Amazon Elastic S VMware ervice 资源。

内容

Amazon 弹性 VMware 服务的身份和访问管理

> **Note**
>
> Amazon EVS 处于公开预览版，可能会发生变化。

AWS Identity and Access Management (IAM) AWS 服务 可以帮助管理员安全地控制对 AWS 资源的访问权限。 IAM 管理员控制谁可以通过身份验证（登录）和授权（拥有权限）来使用 Amazon 弹性 VMware 服务资源。 IAM 无需支付额外费用即可使用。 AWS 服务

主题

受众

您使用 AWS Identity and Access Management (IAM) 的方式会有所不同，具体取决于您在亚马逊弹性 VMware 服务中所做的工作。

服务用户 — 如果您使用 Amazon Elastic Service VMware 服务完成工作，则您的管理员会为您提供所需的凭证和权限。当您使用更多的 Amazon Elastic VMware 服务功能来完成工作时，您可能需要额外的权限。了解如何管理访问权限有助于您向管理员请求适合的权限。

服务管理员-如果您负责公司的亚马逊弹性 VMware 服务资源，则可能拥有对亚马逊弹性 VMware 服务的完全访问权限。您的工作是确定您的 VMware 服务用户应访问哪些亚马逊弹性服务功能和资源。然后，您必须向 IAM 管理员提交更改服务用户权限的请求。查看此页面上的信息以了解的基本概念 IAM。要详细了解贵公司如何使用 IAM Amazon Elastic VMware 服务，请参阅the section called “亚马逊弹性 VMware 服务是如何使用的 IAM”。

IAM 管理员-如果您是 IAM 管理员，则可能需要详细了解如何编写策略来管理 Amazon Elastic S VMware ervice 的访问权限。要查看您可以在中 IAM使用的亚马逊弹性 VMware 服务基于身份的策略示例，请参阅亚马逊弹性 VMware 服务基于身份的策略示例。

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 AWS 账户根用户身份进行身份验证（登录 AWS） IAM 用户，或者通过担任 IAM 角色进行身份验证。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 AWS IAM Identity Center (IAM Identity Center) 用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。

当您以联合身份登录时，您的管理员之前使用 IAM 角色设置了联合身份。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅 AWS 登录用户指南 AWS 账户中的如何登录到您的。

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅 AWS 一般参考中的签名版本 4 签名流程。

无论使用何种身份验证方法，您可能还需要提供其它安全信息。例如， AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅 AWS IAM 身份中心（AWS Single Sign-On 的继任者）用户指南中的多重身份验证和 IA M 用户指南 AWS中的使用多重身份验证 (MFA)。

亚马逊云科技账户根用户

首次创建时 AWS 账户，您首先需要一个单一登录身份，该身份可以完全访问账户中的所有资源 AWS 服务 和资源。此身份称为 AWS 账户根用户，使用您创建账户时使用的电子邮件地址和密码登录即可访问。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关需要您以 root 用户身份登录的任务的完整列表，请参阅《账户管理参考指南》中的 “需要根用户凭证的任务”。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）使用与身份提供商的联合身份验证 AWS 服务 通过临时证书进行访问。

联合身份是指您的企业用户目录、Web 身份提供商、Identity Center 目录中的用户，或者任何使用 AWS 服务 通过身份源提供的凭据进行访问的用户。 AWS Directory Service当联合身份访问时 AWS 账户，他们将扮演角色，角色提供临时证书。

要集中管理访问权限，建议您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中创建用户和群组，也可以连接并同步到您自己的身份源中的一组用户和群组，以便在您的所有 AWS 账户 和应用程序中使用。有关 IAM 身份中心的信息，请参阅什么是 IAM 身份中心？ 在 AWS IAM 身份中心（AWS Single Sign-On 的继任者）用户指南中。

IAM 用户 和群组

IAM 用户是指您内部 AWS 账户 对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时证书，而不是创建 IAM 用户 谁拥有长期证书，例如密码和访问密钥。但是，如果您有需要长

期凭证的特定用例 IAM 用户，我们建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的用例，应在需要时更新访问密钥。

IAM 群组是指定集合的身份 IAM 用户。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可以拥有一个名为的群组，IAMAdmins并授予该群组管理 IAM 资源的权限。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅 IAM 用户指南中的何时创建 IAM 用户（而不是角色）。

IAM 角色

IAM 角色是您内部具有特定权限 AWS 账户 的身份。它类似于 IAM 用户，但与特定的人无关。您可以 AWS Management Console 通过切换 IAM 角色在中临时扮演角色。您可以通过调用 AWS CLI 或 AWS API 操作或使用自定义 URL 来代入角色。有关使用角色的方法的更多信息，请参阅 IAM 用户指南中的使用 IAM 角色。

IAM 具有临时证书的角色在以下情况下很有用：

- 联合用户访问：要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色的信息，请参阅《IAM 用户指南》中的为第三方身份提供者创建角色。如果您使用 IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 会将权限集与IAM中的角色相关联。有关权限集的信息，请参阅 AWS IAM 身份中心（AWS Single Sign-On 的继任者）用户指南中的权限集。
- 临时 IAM 用户 权限- IAM 用户 可以代入一个 IAM 角色来临时获得特定任务的不同权限。
- 跨账户访问-您可以使用 IAM 角色允许其他账户中的某人（受信任的委托人）访问您账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些资源 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解角色和基于资源的跨账户访问策略之间的区别，请参阅 IAM 用户指南中的 IAM 角色与基于资源的策略的区别。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在服务中进行调用时，该服务通常会在其中运行应用程序 Amazon EC2 或在其中存储对象 Amazon S3。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 委托人权限-当您使用 IAM 用户 或角色在中执行操作时 AWS，您被视为委托人。策略向主体授予权限。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中触发另一个操作。在这种情况下，您必须具有执行这两个操作的权限。

  - 服务角色-服务 IAM 角色是服务代替您执行操作的角色。 IAM 管理员可以在内部创建、修改和删除服务角色 IAM。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。
  - 服务相关角色-服务相关角色是一种与服务相关联的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。 IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 上运行的应用程序 Amazon EC2 -您可以使用 IAM 角色管理在 Amazon EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时证书。这比在 Amazon EC2 实例中存储访问密钥更可取。要为 Amazon EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建一个附加到该实例的实例配置文件。实例配置文件包含该角色，并允许在 Amazon EC2 实例上运行的程序获得临时证书。有关更多信息，请参阅 IAM 用户指南中的使用 IAM 角色向在 Amazon EC2 实例上运行的应用程序授予权限。

要了解是否使用 IAM 角色，请参阅 IAM 用户指南中的何时创建 IAM 角色（而不是用户）。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。 AWS 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的结构和内容的更多信息，请参阅 IAM 用户指南中的 JSON 策略概览。

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

每个 IAM 实体（用户或角色）一开始都没有权限。原定设置情况下，用户什么都不能做，甚至不能更改他们自己的密码。要为用户授予执行某些操作的权限，管理员必须将权限策略附加到用户。或者，管理员可以将用户添加到具有预期权限的组中。当管理员为某个组授予访问权限时，该组内的全部用户都会获得这些访问权限。

IAM 无论您使用何种方法执行操作，策略都会定义该操作的权限。例如，假设您有一个允许 `iam:GetRole` 操作的策略。拥有该策略的用户可以从 AWS Management Console AWS CLI、或 AWS API 获取角色信息。

基于身份的策略

基于身份的策略是您可以附加到身份（例如、角色或群组）的 JSON 权限策略文档。 IAM 用户这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅 IAM 用户 IAM 指南中的创建策略。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 AWS 账户。托管策略包括 AWS 托管策略和客户托管策略。要了解如何在托管式策略和内联策略之间进行选择，请参阅 IAM 用户指南中的在托管式策略与内联策略之间进行选择。

基于资源的策略

基于资源的策略是您附加到资源（例如 Amazon S3 存储桶）的 JSON 策略文档。服务管理员可以使用这些策略来定义指定的委托人（账户成员、用户或角色）可以对该资源以及在什么条件执行哪些操作。基于资源的策略是内联策略。没有基于托管资源的策略。

访问控制列表 (ACLs)

访问控制列表 (ACLs) 是一种控制哪些委托人（账户成员、用户或角色）有权访问资源的策略。 ACLs 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。 Amazon S3 AWS WAF、和 Amazon VPC 都是支持的服务示例 ACLs。要了解更多信息 ACLs，请参阅《亚马逊简单存储服务开发者指南》中的访问控制列表 (ACL) 概述。

其他策略类型

AWS 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界-权限边界是一项高级功能，您可以在其中设置基于身份的策略可以向 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅 IAM 用户指南中的IAM 实体的权限边界。
- 服务控制策略 (SCPs)- SCPs 是指定组织或组织单位 (OU) 的最大权限的 JSON 策略 AWS Organizations。 AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果您启用组织中的所有功能，则可以将服务控制策略 (SCPs) 应用于您的任何或所有帐户。SCP 限制成员账户中实体的权限，包括每个亚马逊云科技账户根用户。有关组织和的更多信息 SCPs，请参阅 AWS Org anizations 用户指南中的 SCPs 工作原理。

- 会话策略：会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅 IAM 用户指南中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

亚马逊弹性 VMware 服务是如何使用的 IAM

> **Note**
>
> Amazon EVS 处于公开预览版，可能会发生变化。

在使用 IAM 管理亚马逊弹性 VMware 服务的访问权限之前，请先了解亚马逊弹性 VMware 服务可以使用哪些 IAM 功能。

IAM 功能	亚马逊 EVS 支持
the section called “Amazon EVS 基于身份的政策”	是
the section called “Amazon EVS 中基于资源的政策”	否
the section called “亚马逊 EVS 的政策行动”	是
the section called “Amazon EVS 的政策资源”	部分
the section called “亚马逊 EVS 的政策条件密钥”	是
the section called “亚马逊 EVS 中的访问控制列表 (ACLs)”	否
the section called “使用 Amazon EVS 进行基于属性的访问控制 (ABAC)”	是

IAM 功能	亚马逊 EVS 支持
the section called “在 Amazon EVS 中使用临时证书”	是
the section called “Amazon EVS 的转发访问会话”	是
the section called “亚马逊 EVS 的服务角色”	否
the section called “Amazon EVS 的服务相关角色”	是

要全面了解 Amazon Elastic Service 和其他 VMware AWS 服务 服务是如何使用 IAM的 IAMAWS 服务 ，请参阅 IAM 用户指南。

主题

- Amazon EVS 基于身份的政策
- 亚马逊 EVS 中的访问控制列表 (ACLs)
- 使用 Amazon EVS 进行基于属性的访问控制 (ABAC)
- 在 Amazon EVS 中使用临时证书
- Amazon EVS 的转发访问会话
- 亚马逊 EVS 的服务角色
- Amazon EVS 的服务相关角色

Amazon EVS 基于身份的政策

支持基于身份的策略：是

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户托管策略定义自定义 IAM 权限。

使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源，以及允许或拒绝操作的条件。您无法在基于身份的策略中指定委托人，因为它适用于该策略所关联的用户或角色。要了解您在 JSON 策略中使用的所有元素，请参阅 IAM 用户指南中的 IAM JSON 策略元素参考。

Amazon EVS 基于身份的政策示例

要查看亚马逊弹性 VMware 服务基于身份的策略示例，请参阅亚马逊弹性 VMware 服务基于身份的策略示例。

Amazon EVS 中基于资源的政策

支持基于资源的策略：否

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户访问，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当委托人和资源处于不同位置时 AWS 账户，可信账户中的 IAM 管理员还必须向委托人实体（用户或角色）授予访问资源的权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅 IAM 用户指南中的跨账户在 IAM 中访问资源。

亚马逊 EVS 的政策行动

支持动作是

管理员可以使用亚马逊云科技 JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

IAM 基于身份的策略的`Action`元素描述了该策略允许或拒绝的一个或多个具体操作。策略操作通常与关联的 AWS API 操作同名。此策略用于策略中以授予执行关联操作的权限。

Amazon Elastic S VMware ervice 中的策略操作在操作前使用以下前缀：`evs:`。例如，要授予某人使用 Amazon EVS `CreateEnvironment` API 操作创建环境的权限，您需要将该`evs:CreateEnvironment`操作包含在他们的策略中。策略语句必须包含 `Action` 或 `NotAction` 元素。Amazon Elastic S VMware ervice 定义了自己的一组操作，这些操作描述了您可以使用该服务执行的任务。

要在单个语句中指定多项操作，请使用逗号将它们隔开，如下所示：

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

```
      "evs:action2"
```

您也可以使用通配符（*）指定多个操作。例如，要指定以单词 List 开头的所有操作，包括以下操作：

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

要查看亚马逊弹性 VMware 服务操作列表，请参阅服务授权参考中的亚马逊弹性 VMware 服务定义的操作。

Amazon EVS 的政策资源

支持策略资源：部分

管理员可以使用亚马逊云科技 JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

Resource JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符 (*) 指示语句应用于所有资源。

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

要查看 Amazon EVS 资源类型及其列表 ARNs，请参阅《VMware 服务授权参考》中的 Amazon Elastic Service 定义的资源。要了解您可以使用哪些操作来指定每种资源的 ARN，请参阅 A mazon Elast VMware ic Service 定义的操作。

某些 Amazon EVS API 操作支持多种资源。例如，在调用 ListEnvironments API 操作时可以引用多个环境。要在单个语句中指定多个资源，请 ARNs 用逗号分隔。

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

例如，Amazon EVS 环境资源具有以下 ARN：

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

要my-environment-2在您的语句中指定环境my-environment-1，请使用以下示例 ARNs：

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

要指定属于特定账户的所有环境，请使用通配符 (*)：

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

亚马逊 EVS 的政策条件密钥

支持特定于服务的策略条件键：是

管理员可以使用亚马逊云科技 JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

Condition元素（或Condition块）允许您指定语句生效的条件。Condition 元素是可选的。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 AWS 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 AWS 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有当资源标有 IAM 用户 名称时，您才能授予访问该资源的 IAM 用户 权限。有关更多信息，请参阅 IAM 用户指南中的IAM 策略元素：变量和标签。

Amazon Elastic S VMware ervice 定义了自己的条件键集，还支持使用一些全局条件键。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

所有 Amazon EC2 操作都支持aws:RequestedRegion和ec2:Region条件键。有关更多信息，请参阅示例：限制对特定区域的访问。

要查看亚马逊弹性 VMware 服务条件密钥列表，请参阅 VMware 服务授权参考中的亚马逊弹性服务的条件密钥。要了解您可以使用条件键的操作和资源，请参阅 Amazon Elastic S VMware ervice 定义的操作。

亚马逊 EVS 中的访问控制列表 (ACLs)

支持 ACLs：否

访问控制列表 (ACLs) 控制哪些委托人（账户成员、用户或角色）有权访问资源。 ACLs 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

使用 Amazon EVS 进行基于属性的访问控制 (ABAC)

支持 ABAC（策略中的标签）：是

基于属性的访问控制（ABAC）是一种授权策略，该策略基于属性来定义权限。在中 AWS，这些属性称为标签。您可以向 IAM 实体（用户或角色）和许多 AWS 资源附加标签。标记实体和资源是 ABAC 的第一步。然后，您可以设计 ABAC 策略以允许在委托人的标签与他们尝试访问的资源上的标签匹配时进行操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

您可以将标签附加到亚马逊弹性 VMware 服务资源，也可以在请求中将标签传递给亚马逊弹性 VMware 服务。要基于标签控制访问，您需要使用 `aws:ResourceTag/<key-name>`、`aws:RequestTag/<key-name>` 或 `aws:TagKeys` 条件键在策略的条件元素中提供标签信息。有关可以在条件键中使用标签的操作的更多信息，请参阅《服务授权参考》中的 Amazon EVS 定义的操作。

在 Amazon EVS 中使用临时证书

支持临时凭证：是

当你使用临时证书登录时，有些 AWS 服务 不起作用。有关更多信息，包括哪些 AWS 服务 适用于临时证书，请参阅 IAM 用户指南中的AWS 服务 与 IA M 配合使用的信息。

如果您使用除用户名和密码之外的任何方法登录，则 AWS Management Console 使用的是临时证书。例如，当您 AWS 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的从用户切换到 IAM 角色（控制台）。

您可以使用 AWS CLI 或 AWS API 手动创建临时证书。然后，您可以使用这些临时证书进行访问 AWS。 AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 中的临时安全凭证。

Amazon EVS 的转发访问会话

支持转发访问会话（FAS）：是

当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两项操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

亚马逊 EVS 的服务角色

支持服务角色：否

服务角色是由一项服务担任、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。

Amazon EVS 的服务相关角色

支持服务相关角色：是

服务相关角色是一种链接到的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

有关创建或管理 Amazon Elastic Service VMware 服务相关角色的详细信息，请参阅the section called “使用服务相关角色”。

Amazon EVS 基于身份的策略示例

> **Note**
>
> Amazon EVS 处于公开预览版，可能会发生变化。

默认情况下 IAM 用户 ，角色无权创建或修改 Amazon 弹性 VMware 服务资源。他们也无法使用 AWS Management Console AWS CLI、或 AWS API 执行任务。 IAM 管理员必须创建 IAM 策略，授予用户和角色对其所需的指定资源执行特定 API 操作的权限。然后，管理员必须将这些策略附加到需要这些权限的 IAM 用户 或群组。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅 IAM 用户指南中的使用 JSON 编辑器创建策略。

主题

- 策略最佳实践
- 使用亚马逊弹性 VMware 服务控制台
- 允许用户查看他们自己的权限
- 创建和管理 Amazon EVS 环境
- 获取并列出 Amazon EVS 环境、主机和 VLANs

策略最佳实践

基于身份的策略决定了是否有人可以在您的账户中创建、访问或删除亚马逊弹性 VMware 服务资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的 AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的AWS 托管式策略或工作职能的AWS 托管式策略。
- 应用最低权限权限-使用 IAM 策略设置权限时，仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用应用权限 IAM 的更多信息，请参阅 IAM 用户指南 IAM中的策略和权限。
- 使用 IAM 策略中的条件进一步限制访问权限-您可以在策略中添加条件以限制对操作和资源的访问权限。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定 AWS 服务的（例如）使用的，则也可以使用条件来授予对服务操作的访问权限 AWS CloudFormation。有关更多信息，请参阅 IAM 用户指南中的 IAM JSON 策略元素：条件。
- 用于 IAM Access Analyzer 验证您的 IAM 策略以确保权限的安全性和功能性 — IAM Access Analyzer 验证新的和现有的策略，使策略符合 IAM 策略语言 (JSON) 和 IAM 最佳实践。 IAM Access Analyzer 提供 100 多项政策检查和切实可行的建议，以帮助您制定安全和实用的策略。有关更多信息，请参阅 IAM 用户指南中的IAM Access Analyzer 策略验证。
- 需要多重身份验证 (MFA)-如果您的账户中有 IAM 用户 需要root用户的情况，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的配置受 MFA 保护的 API 访问。

使用亚马逊弹性 VMware 服务控制台

要访问 Amazon Elastic S VMware ervice 控制台，IAM 委托人必须拥有一组最低权限。这些权限必须允许委托人列出和查看您的 Amazon Elastic S VMware ervice 资源的详细信息 AWS 账户。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的主体，控制台将无法按预期正常运行。

为确保您的 IAM 委托人仍然可以使用 Amazon Elastic S VMware ervice 控制台，请使用您自己的唯一名称创建策略，例如`AmazonEVSAdminPolicy`。将策略附加到主体。有关更多信息，请参阅 IAM 用户指南中的为用户添加权限：

```
{
    "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"
                }
            }
        }
    ]
}
```

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与您尝试执行的 API 操作相匹配的操作。

允许用户查看他们自己的权限

此示例说明如何创建允许查看附加 IAM 用户 到其用户身份的内联和托管策略的策略。此策略包括在控制台上或使用 AWS CLI 或 AWS API 以编程方式完成此操作的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
```

```
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

创建和管理 Amazon EVS 环境

此示例策略包括创建和删除 Amazon EVS 环境以及创建环境后添加或删除主机所需的权限。

您可以将 AWS 区域 替换为 AWS 区域 要在其中创建环境的。如果您的账户已经有 `AWSServiceRoleForAmazonEVS` 角色，您可以从策略中删除 `iam:CreateServiceLinkedRole` 操作。如果您曾经在自己的账户中创建过 Amazon EVS 环境，则具有这些权限的角色已经存在，除非您将其删除。

```
{
    "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": "*"
        }
    ]
```

```
}
```

获取并列出 Amazon EVS 环境、主机和 VLANs

此示例策略包括管理员在 us-east-2 中获取和列出给定账户中的所有 Amazon EVS 环境、主机以及 VLANs 该账户所需的最低权限。 AWS 区域

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

对 Amazon 弹性 VMware 服务身份和访问进行故障排除

> **Note**
>
> Amazon EVS 处于公开预览版，可能会发生变化。

使用以下信息来帮助您诊断和修复在使用 Amazon Elastic S VMware ervice 时可能遇到的常见问题，以及 IAM。

主题

- AccessDeniedException
- 我想允许我以外的人访问我的 Amazon Elastic S VMware ervice 资源 AWS 账户

AccessDeniedException

如果您`AccessDeniedException`在调用 AWS API 操作时收到，则表示您正在使用的 IAM 委托人证书没有进行该调用所需的权限。

```
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
```

在前面的示例消息中，用户无权调用 Amazon EVS `CreateEnvironment` API 操作。要向 IAM 委托人提供 Amazon EVS 管理员权限，请参阅the section called “Amazon EVS 基于身份的策略示例”。

有关 IAM 的更多一般信息，请参阅 IA M 用户指南中的使用策略控制对 AWS 资源的访问权限。

我想允许我以外的人访问我的 Amazon Elastic S VMware ervice 资源 AWS 账户

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以代入角色。对于支持基于资源的策略或访问控制列表 (ACLs) 的服务，您可以使用这些策略向人们授予访问您的资源的权限。

要了解更多信息，请参阅以下内容：

- 要了解 Amazon 弹性 VMware 服务是否支持这些功能，请参阅the section called “亚马逊弹性 VMware 服务是如何使用的 IAM”。
- 要了解如何提供对您拥有的资源的访问权限，请参阅 IAM 用户指南 IAM 用户 中的提供 AWS 账户对您拥有的其他资源的访问权限。 AWS 账户
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户
- 要了解如何通过联合身份验证提供访问权限，请参阅 IAM 用户指南中的向经过外部身份验证的用户提供访问权限（联合身份验证）。
- 要了解使用角色和基于资源的策略进行跨账户访问的区别，请参阅 IAM 用户指南中的 IAM 角色与基于资源的策略的区别。

AWS 亚马逊 EVS 的托管政策

> **Note**
>
> Amazon EVS 处于公开预览版，可能会发生变化。

AWS 托管策略是由创建和管理的独立策略 AWS。 AWS 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住，AWS 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 AWS 客户使用。我们建议通过定义特定于您的使用场景的客户管理型策略来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。AWS 最有可能在启动新的 API 或现有服务可以使用新 AWS 服务 的 API 操作时更新 AWS 托管策略。有关更多信息，请参阅《IAM 用户指南》中的AWS 托管策略。

AWS 托管策略：Amazon EVSService RolePolicy

您不能将 AmazonEVSServiceRolePolicy 附加到自己的 IAM 实体。本政策附属于服务相关角色，允许 Amazon EVS 代表您执行操作。有关更多信息，请参阅 the section called “使用服务相关角色”。当您使用具有iam:CreateServiceLinkedRole权限的 IAM 委托人创建环境时，系统会自动为您创建附有此策略的AWSServiceRoleforAmazonEVS服务相关角色。

此政策允许服务相关角色代表您 AWS 服务 进行呼叫。

权限详细信息

该策略包括以下权限，允许 Amazon EVS 完成以下任务。

- ec2-创建、修改、标记和删除弹性网络接口，该接口用于在客户 VPC 子网中的 Amazon EVS 和 VMware 虚拟云基础 (VCF) SDDC Manager 设备之间建立持久连接。Amazon EVS 需要这种连接才能部署、管理和监控 VCF 部署。

要查看最新版本的 JSON 策略文档，请参阅《AWS 托管策略参考指南》EVSServiceRolePolicy中的Amazon。

Amazon EVS 更新了托 AWS 管政策

查看自该服务开始跟踪这些更改以来，Amazon EVS AWS 托管政策更新的详细信息。要获得有关此页面更改的自动提示，请订阅 文档历史记录 页面上的 RSS 源。

更改	描述	日期
亚马逊 EVSService RolePolicy — 新增政策	Amazon EVS 添加了一项新政策，允许该服务连接到客户账户中的 VPC 子网。此连接是服务功能所必需的。要了解	2025年6月9日

更改	描述	日期
	更多信息，请参阅the section called “AWS 托管策略：Amazon EVSService RolePolicy”。	
亚马逊 EVS 开始追踪变更	Amazon EVS 开始跟踪其 AWS 托管政策的变更。	2025年6月9日

为 Amazon EVS 使用服务相关角色

> **Note**
>
> Amazon EVS 处于公开预览版，可能会发生变化。

Amazon Elast ic S VMware ervice 使用 AWS 身份和访问管理 (IAM) Access Management 服务相关角色。服务相关角色是一种独特的 IAM 角色，直接关联到 Amazon EVS。服务相关角色由 Amazon EVS 预定义，包括该服务代表您调用其他 AWS 服务所需的所有权限。

服务相关角色使设置 Amazon EVS 变得更加容易，因为您不必手动添加必要的权限。Amazon EVS 定义了其服务相关角色的权限，除非另有定义，否则只有 Amazon EVS 可以担任其角色。定义的权限包括信任策略和权限策略。不能将该权限策略附加到任何其他 IAM 实体。

只有在首先删除相关资源后，您才能删除服务相关角色。这样可以保护您的 Amazon EVS 资源，因为您不会无意中删除访问这些资源的权限。

有关支持服务相关角色的其他服务的信息，请参阅与 IAM 配合使用的AWS 服务，并查找 Service-linked role（服务相关角色）列中显示为 Yes（是）的服务。选择是和链接，查看该服务的服务相关角色文档。

Amazon EVS 的服务相关角色权限

Amazon EVS 使用名为的服务相关角色。AWSServiceRoleForAmazonEVS该角色允许 Amazon EVS 管理您账户中的环境。附加的策略允许该角色管理以下资源：EVS 弹性网络接口、EVS VLAN 子网和。 VPCs

AWSServiceRoleForAmazonEVS 服务相关角色信任以下服务代入该角色：

- evs.amazonaws.com

角色权限策略允许 Amazon EVS 对指定资源完成以下操作：

- AmazonEVSServiceRolePolicy

您必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的服务相关角色权限。

为 Amazon EVS 创建服务相关角色

您无需手动创建服务相关角色。当您在 AWS Management Console、CLI 或 AWS AP AWS I 中创建环境时，Amazon EVS 会为您创建服务相关角色。

如果您删除该服务相关角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。当您创建环境时，Amazon EVS 会再次为您创建服务相关角色。

编辑 Amazon EVS 的服务相关角色

Amazon EVS 不允许您编辑AWSServiceRoleForAmazonEVS服务相关角色。创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。但是可以使用 IAM 编辑角色描述。有关更多信息，请参阅《IAM 用户指南》中的编辑服务相关角色。

删除 Amazon EVS 的服务相关角色

如果不再需要使用某个需要服务相关角色的功能或服务，我们建议您删除该角色。这样就没有未被主动监控或维护的未使用实体。但是，您必须先清除您的服务相关角色，然后才能手动删除它。

清除服务相关角色

必须先删除服务相关角色使用的所有资源，然后才能使用 IAM 删除该角色。有关删除包含主机的 Amazon EVS 环境的步骤，请参阅the section called “删除 Amazon EVS 主机和环境”。

> **Note**
>
> 如果您尝试删除资源时 Amazon EVS 服务正在使用该角色，则删除可能会失败。如果发生这种情况，请等待几分钟后重试。

手动删除 服务相关角色

使用 IAM 控制台、 AWS CLI 或 AWS API 删除AWSServiceRoleForAmazonEVS服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的删除服务相关角色。

Amazon EVS 服务相关角色支持的区域

Amazon EVS 支持在提供服务的所有地区使用服务相关角色。有关更多信息，请参阅 端点和限额。

将 Amazon EVS 与其他 AWS 服务一起使用

> **Note**
>
> Amazon EVS 处于公开预览版，可能会发生变化。

Amazon EVS 与其他集成 AWS 服务 以提供其他解决方案。本主题介绍了 Amazon EVS 为添加功能而使用的一些服务。

主题

- 使用创建 Amazon EVS 资源 AWS CloudFormation
- 使用 Amazon FSx for NetApp ONTAP 运行高性能工作负载

使用创建 Amazon EVS 资源 AWS CloudFormation

> **Note**
>
> Amazon EVS 处于公开预览版，可能会发生变化。

Amazon EVS 与 AWS CloudFormation一项服务集成，可帮助您对 AWS 资源进行建模和设置，从而减少创建和管理资源和基础设施所花费的时间。您可以创建一个描述所需所有 AWS 资源的模板，例如 Amazon EVS 环境，并 AWS CloudFormation 负责为您配置和配置这些资源。

使用时 AWS CloudFormation，您可以重复使用模板来一致且重复地设置您的 Amazon EVS 资源。只需描述一次您的资源，然后在多个 AWS 账户 区域中一遍又一遍地配置相同的资源即可。

亚马逊 EVS 和模板 AWS CloudFormation

要为 Amazon EVS 和相关服务预置和配置资源，您必须了解AWS CloudFormation 模板。模板是 JSON 或 YAML 格式的文本文件。这些模板描述了您要在 AWS CloudFormation 堆栈中配置的资源。如果你不熟悉 JSON 或 YAML，可以使用 D AWS CloudFormation esigner 来帮助你开始使用 AWS CloudFormation 模板。有关更多信息，请参阅什么是 AWS CloudFormation 设计器？ 在《 AWS CloudFormation 用户指南》中。

Amazon EVS 支持在中创建环境。 AWS CloudFormation有关更多信息，包括适用于您的环境的 JSON 和 YAML 模板示例，请参阅 AWS CloudFormation 用户指南中的 Amazon EVS 资源类型参考。

了解更多关于 AWS CloudFormation

要了解更多信息 AWS CloudFormation，请参阅以下资源：

- AWS CloudFormation
- AWS CloudFormation 用户指南
- AWS CloudFormation 命令行界面用户指南

使用 Amazon FSx for NetApp ONTAP 运行高性能工作负载

> **Note**
>
> Amazon EVS 处于公开预览版，可能会发生变化。

Amazon FSx for NetApp ONTAP 是一项存储服务，允许您在云中启动和运行完全托管的 ONTAP 文件系统。ONTAP 是一种 NetApp文件系统技术，它提供了一组广泛采用的数据访问和数据管理功能。FSx for ONTAP 提供本地 NetApp 文件系统的功能、性能和 APIs 完全托管 AWS 服务的敏捷性、可扩展性和简单性。有关更多信息，请参阅《FSx 适用于 ONTAP 的用户指南》。

Amazon EVS 支持将 Amazon f FSx NetApp or ONTAP 用作在亚马逊 EVS 上运行的虚拟 VMware 机的 NFS/iSCSI 数据存储和访客连接存储。

将 NetApp ONTAP 配置 FSx 为 NFS 数据存储库

> **Note**
>
> Amazon EVS 处于公开预览版，可能会发生变化。

以下过程详细介绍了使用控制台 FSx 和在 Amazon EVS 上运行的 vSphere 客户端界面将 NetApp ONTAP 配置 FSx 为 Amazon EV VMware S 的 NFS 数据存储所需的最低步骤。

先决条件

在将 Amazon EVS 与 Amazon FSx f NetApp or ONTAP 配合使用之前，请确保已完成以下先决任务。

- Amazon EVS 环境已部署在您的虚拟私有云 (VPC) 中。有关更多信息，请参阅 入门。
- 您可以访问在亚马逊 EVS 上运行的 vSphere 客户端。
- 您或您的存储管理员必须拥有必要的权限才能在您的 VPC 中创建和管理 FSx ONTAP 文件系统。有关更多信息，请参阅 Amazon FSx for NetApp ONTAP 的身份和访问管理。

您的 IAM 委托人拥有在您的 VPC 中创建和管理 FSx ONTAP 文件系统的相应权限。有关更多信息，请参阅 the section called “创建和管理 Amazon EVS 环境”。

创建 FSx 适用于 NetApp ONTAP 的文件系统

1. 前往 Amazon FSx 控制台。
2. 选择创建文件系统。
3. FSx 为 NetApp ONTAP 选择亚马逊。
4. 选择下一步。
5. 选择标准创建。
6. 对于部署类型，选择单可用区部署选项。

> **Note**
>
> Amazon EVS 目前仅支持单可用区部署。

7. 对于固态硬盘存储容量，请指定 1024 GiB。
8. 对于吞吐容量，请选择指定吞吐容量。 MB/s 对于单可用区 1，至少选择 512，为单可用区 2 选择至少 768 MB/s 。
9. 选择可连接到您的亚马逊 EVS VLAN 子网的 Amazon EVS VPC。
10. 选择一个安全组，该组允许 ONTAP NFS 流量流向 Amazon EVS 主机 VMkernel 管理 VLAN 子网所需 FSx 的所有流量。
11. 选择您的文件系统将部署到的 Amazon EVS 服务访问子网。有关更多信息，请参阅 the section called “服务访问子网”。
12. 对于接合路径，请指定一个有意义的名称，例如在 v `/vol1` Sphere 中标识此卷。
13. 在 “默认卷配置” 中，将 “存储效率” 设置为 “已启用”。
14. 将其余设置保留为默认值，然后选择 “下一步”。
15. 查看文件系统属性并选择创建文件系统。

检索存储虚拟机的 NFS DNS 名称

1. 前往 Amazon FSx 控制台。
2. 在左侧菜单中，选择文件系统。
3. 选择新创建的文件系统。
4. 选择存储虚拟机选项卡。
5. 选择存储虚拟机。
6. 选择 “端点” 选项卡。
7. 复制网络文件系统 (NFS) DNS 名称以备以后在 VMware Vsphere 中使用。

使用适用于 ONTAP 的卷在 vSphere 中创建 NFS 数据存储库 FSx

按照在 vSphere 环境中创建 NFS 数据存储库中的说明，将 Amazon for NetApp ONTAP 配置为 vSphere FSx 的外部存储。 VMware 对于 vSphere 客户端界面中的服务器设置，请使用您在上一步中复制的存储虚拟机 (SVM) NFS DNS 名称。

将 NetApp ONTAP 配置 FSx FSx 为 iSCSI 数据存储库

> **Note**
>
> Amazon EVS 处于公开预览版，可能会发生变化。

以下过程详细介绍了使用在 Amazon EVS 上运行 FSx 的控制台和 vSphere 客户端界面将 NetApp ONTAP 配置为 Amazon EV VMware S 的 iSCSI 数据存储所需的最低步骤。 FSx

先决条件

在将 Amazon EVS 与 Amazon FSx f NetApp or ONTAP 配合使用之前，请确保已完成以下先决任务。

- Amazon EVS 环境已部署在您的虚拟私有云 (VPC) 中。有关更多信息，请参阅 入门。
- 您可以访问在亚马逊 EVS 上运行的 vSphere 客户端。
- 您或您的存储管理员必须拥有必要的权限才能在您的 VPC 中创建和管理 FSx ONTAP 文件系统。有关更多信息，请参阅 Amazon FSx for NetApp ONTAP 的身份和访问管理。

创建 FSx 适用于 NetApp ONTAP 的文件系统

1. 前往 Amazon FSx 控制台。
2. 选择创建文件系统。
3. FSx 为 NetApp ONTAP 选择亚马逊。
4. 选择下一步。
5. 选择标准创建。
6. 对于部署类型，选择单可用区部署选项。

> **Note**
>
> Amazon EVS 目前仅支持单可用区部署。

7. 对于固态硬盘存储容量，请指定 1024 GiB。
8. 对于吞吐容量，请选择指定吞吐容量。 MB/s 对于单可用区 1，至少选择 512，为单可用区 2 选择至少 768 MB/s 。
9. 选择可连接到您的亚马逊 EVS VLAN 子网的 Amazon EVS VPC。
10. 选择一个安全组，允许所有 ONTAP iSCSI 流量进入亚马逊 EVS 主机 VMkernel 管理 VLAN 子网。FSx
11. 选择您的文件系统将部署到的 Amazon EVS 服务访问子网。有关更多信息，请参阅 the section called “服务访问子网”。
12. 在 “默认卷配置” 中，将 “存储效率” 设置为 “启用”。
13. 将其余设置保留为默认值，然后选择 “下一步”。
14. 查看文件系统属性并选择创建文件系统。

在 vSphere 中为 ESXi 主机存储配置软件 iSCSI 适配器

对于每 ESXi 台主机，必须配置软件 iSCSI 适配器，以便您的 ESXi主机可以使用它来访问 iSCSI 存储。有关在 vSphere 中为 ESXi 主机配置软件 iSCSI 适配器的说明，请参阅 vSphere 产品文档中的添加或移除软件 iSCSI 适配器。 VMware

配置软件 iSCSI 适配器后，复制与 iSCSI 适配器关联的 iSCSI 限定名称 (IQN)。这些值将在以后使用。

创建 iSCSI LUN

FSx for ONTAP 允许您创建专门用于 iSCSI 访问的逻辑单元号 (LUNs)，从而为您的 ESXi 主机提供共享的数据块存储。您可以使用 NetApp ONTAP CLI 创建 LUN。

以下是命令示例。

> **Note**
>
> 建议将 LUN 大小配置为卷大小的 90%。

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

有关更多信息，请参阅《适用于 ONTAP 的用户指南》FSx 中的创建 iSCSI LUN。

配置启动器组并将其映射到 iSCSI LUN

现在，您已经创建了 iSCSI LUN，接下来该过程的下一步是创建一个启动器组 (igroup)，用于将卷连接到群集，并将该 LUN 映射到启动器组。您可以使用 NetApp ONTAP CLI 来执行这些操作。

1. 配置启动器组。

   以下是命令示例。对于--initiator，请使用您在上一步中复制 IQNs 的 iSCSI 适配器。

   ```
   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. 确认igroup存在。

   ```
   lun igroup show
   ```

3. 将 LUN 映射到启动器组。以下是命令示例。

   ```
   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`命令确认 LUN 已创建、联机并已映射。

```
lun show -path /vol/<vol_name>/<lun_name> -fields state,mapped,serial-hex
```

有关更多信息，请参阅《适用于 ONTAP 的用户指南》中的 “为 Linux 配置 iSCSI” 或FSx 为 Windows 配置 iSCSI。

在 vSphere 中配置 iSCSI LUN 的动态发现

要允许 ESXi 主机查看 iSCSI LUN，必须在 vSphere 客户端界面中为每台主机配置动态发现。在 iSCSI 服务器字段中，输入您在上一步中复制的 (NFS) DNS 名称。有关更多信息，请参阅 VMware vSphere 产品文档中的在 ESXi主机上为 iSCSI 和 iSER 配置动态或静态发现。

VMware 使用 iSCSI LUN 在 vSphere 中创建 VMFS 数据存储区

虚拟机文件系统 (VMFS) 数据存储库充当 VMware 虚拟机的存储库。按照创建 vSphere VMFS 数据存储中的说明，使用之前配置的 iSCSI LUN 在 vSphere 中设置 V VMware MFS 数据存储区。

故障排除

> **Note**
>
> Amazon EVS 处于公开预览版，可能会发生变化。

本章详细介绍了在创建或管理 Amazon EVS 环境时遇到的一些常见问题。

对失败的环境状态检查进行故障排除

Amazon EVS 会自动检查您的环境以发现问题。您可以查看环境的状态以确定具体且可检测到的问题。

查看环境状态检查信息

使用 Amazon EVS 控制台调查受损环境

1. 打开 Amazon EVS 控制台。
2. 在导航窗格中，选择环境，然后选择您的环境。
3. 选择 “详细信息” 选项卡可查看环境概览。
4. 检查环境状态。将鼠标悬停在该字段上可展开弹出窗口，其中包含每个环境状态检查的单独结果。

可接通性检查失败

可访问性检查可验证 Amazon EVS 与 SDDC Manager 的持续连接。如果 Amazon EVS 无法访问环境，则此检查将失败。

如果此检查失败，Amazon EVS 将无法再访问 SDDC Manager 来验证环境状态，也无法再将主机添加到环境中。可访问性失败还会导致许可证密钥重复使用和密钥覆盖率检查失败，并且主机计数检查会返回 “未知” 响应。

Reachabilty 故障表示 SDDC 管理器、防火墙配置可能存在问题或证书缺失。您可以尝试解决这些问题，也可以联系 Su AWS pport 寻求进一步帮助。

主机计数检查失败

此检查可验证您的环境是否至少有四台主机，这是 VCF 5.2.1 的要求。

如果此检查失败，则需要添加主机，以使您的环境满足此最低要求。Amazon EVS 仅支持 4 到 16 台主机的环境。

密钥重复使用检查失败

此检查可验证其他 Amazon EVS 环境是否未使用 VCF 许可密钥。VCF 许可证只能用于一个 Amazon EVS 环境。如果将使用过的许可证添加到环境中，则此检查将失败。

如果此检查失败，您将收到错误响应，提示无法创建 Amazon EVS 环境。要解决此问题，请在 SDDC Manager 中查看您的许可证设置，并将所有以前使用的许可证替换为未使用的许可证。

> **Important**
>
> 使用 SDDC 管理器用户界面管理 VCF 组件许可证密钥。Amazon EVS 要求您在 SDDC 管理器中保留有效的组件许可密钥，服务才能正常运行。如果使用 vSphere Client 管理组件许可密钥，则必须确保这些密钥也显示在 SDDC Manager 用户界面的许可屏幕上，以防止许可证密钥检查失败。

密钥覆盖率检查失败

此检查可验证分配给 vCenter Server 的 VCF 许可密钥是否为所有已部署的主机分配了足够的 vCPU 核心和 vSAN 存储容量 (TiB)。

如果此检查失败，您将收到错误响应，提示无法创建 Amazon EVS 环境，或者无法将 Amazon EVS 主机添加到环境中。密钥覆盖失败可能表示存在以下问题之一：

- 您已超出了 Amazon EVS 支持的主机数量。Amazon EVS 在每个环境中支持 4 到 16 台主机。如果是这个问题，请移除或添加主机，直到您的环境处于支持的主机范围内。
- VCF 许可证未正确分配给 vCenter 服务器。在 vCenter Server 的评估期到期或当前分配的许可证到期之前，您必须为其分配许可证。如果是这个问题，请在 SDDC 管理器中查看许可证分配。
- 当前的 VCF 许可证不涵盖 vCPU 核心和 vSAN 存储容量需求。VCF 解决方案密钥必须至少有 256 个内核。vSAN 许可密钥必须至少有 110 TiB 的 vSAN 容量。如果是这个问题，请在 SDDC Manager 中添加 vSAN 许可，直到您的使用需求得到满足。

如果上述操作无法解决问题，请联系 Su AWS pport 寻求进一步帮助。

> **Important**
>
> 使用 SDDC 管理器用户界面管理 VCF 组件许可证密钥。Amazon EVS 要求您在 SDDC 管理器中保留有效的组件许可密钥，服务才能正常运行。如果使用 vSphere Client 管理组件许可密钥，则必须确保这些密钥也显示在 SDDC Manager 用户界面的许可屏幕上，以防止许可证密钥检查失败。

此主机上的 vSphere HA 代理无法访问隔离地址

在 vCenter 用户界面中，选择 ESXi 主机后，您会看到消息 “此主机上的 vSphere HA 代理无法访问隔离地址 < 地址>”。IPv6

此错误消息表示主机上的 vSphere HA 代理无法到达 vSphere HA 用于心跳检查的默认 IPv6 隔离地址。该错误消息并不表示存在问题，只是因为 Amazon EVS IPv6 目前不支持。不 IPV6 支持 Amazon EVS 不会影响 vSphere HA 的核心功能。

要删除 vSphere HA 错误消息，必须禁用 vSphere HA。有关在 vSphere 客户端中禁用 vSphere HA 的步骤，请参阅博通的文章《禁用和启用 VMware 高可用性 (HA)》。

主机群集的 VSAN 升级预检查失败 ESXi

尝试使用 SDDC 管理器升级 ESXi 主机集群时，与 vSAN 磁盘相关的预检查可能会失败。这是因为 Amazon EVS 使用 vSAN Express 存储架构 (ESA)，升级预检查不适用于 vSAN ESA。有关更多信息，请参阅 Broadcom 知识库中关于此主题的文章。

Amazon 弹性 VMware 服务终端节点和配额

> **Note**
>
> Amazon EVS 处于公开预览版，可能会发生变化。

以下是该服务的服务端点和服务限额。要以编程方式连接到 AWS 服务，请使用终端节点。除标准 AWS 终端节点外，有些终端节点还在选定区域 AWS 服务 提供 FIPS 终端节点。有关更多信息，请参阅AWS 服务端点。服务限额（也称为限制）是 AWS 账户使用的服务资源或操作的最大数量。有关更多信息，请参阅AWS 服务配额。

服务端点

Amazon EVS API 提供区域和双堆栈终端节点，以及适用于美国区域的 FIPS 终端节点。要将双堆栈端点与一起使用 AWS CLI，请参阅和工具参考指南中的双堆栈和 FIPS 端点配置。 AWS SDKs

区域名称	区域	端点	协议
美国东部（北弗吉尼亚州）	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
美国东部（俄亥俄州）	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
美国西部（俄勒冈州）	us-west-2	evs.us-west-2.amazonaws.com evs-fips.us-west-2.amazonaws.com	HTTPS

区域名称	区域	端点	协议
		evs.us-west-2.api.aws evs-fips.us-west-2.api.aws	
亚太地区（东京）	ap-northeast-1	evs.ap-northeast-1.amazonaws.com evs.ap-northeast-1.api.aws	HTTPS
欧洲地区（法兰克福）	eu-central-1	evs.eu-central-1.amazonaws.com evs.eu-central-1.api.aws	HTTPS
欧洲地区（爱尔兰）	eu-west-1	evs.eu-west-1.amazonaws.com evs.eu-west-1.api.aws	HTTPS

服务配额

Amazon EVS 已与 Service Quotas 集成，您可以使用 AWS 服务 该配额从中心位置查看和管理您的配额。有关更多信息，请参阅《服务配额用户指南》中的 What Is Service Quotas?。

通过集成 Service Quotas，您可以使用 AWS Management Console 或 AWS CLI 来查看 Amazon EVS 配额的价值，并请求增加可调整配额的配额。有关更多信息，请参阅《S ervic e Quotas 用户指南》和《 AWS CLI 命令参考》request-service-quota-increase中的 “请求增加配额”。

Important

要启用 Amazon EVS 环境创建，每个 EVS 环境配额的主机数量必须至少为 4。默认配额为 0。要增加此配额，请前往 S ervice Quotas 控制台申请增加配额。

Important

确保您的 EC2 运行按需标准实例配额反映您将在 Amazon EVS 上使用的所有 EC2 实例所需的 v CPUs 数量。每个 i4i.metal 实例使用 128 v。CPUs 有关增加 EC2 服务配额的信息，请参阅 Amazon EC2 用户指南中的申请增加服务配额。

> **Note**
>
> 如果您计划在 Amazon EVS 环境中使用 EC2 EC2 专用主机，请确保您的专用 i4i 主机配额反映您打算在所需区域使用的专用主机的数量。有关增加 EC2 服务配额的信息，请参阅 Amazon EC2 用户指南中的申请增加服务配额。

名称	默认值	可调整	描述
每个 EVS 环境的主机数量	0	是	在单个 Amazon EVS 环境中可以配置的最大主机数量。
每个 AWS 账户的环境计数	1	是	该账户在当前区域中可以创建的最大 EVS 环境数量。

《亚马逊弹性 VMware 服务用户指南》的文档历史记录

> **Note**
>
> Amazon EVS 处于公开预览版，可能会发生变化。

下表描述了 Amazon 弹性 VMware 服务的文档版本。

变更	说明	日期
发布了每个 AWS 账户的环境计数配额	Amazon EVS 发布了每个 AWS 账户配额的环境数量。 每个 AWS 账户的环境数量配额表示在给定账户和地区中可以创建的最大 Amazon EVS 环境数量。	2025年7月8日
Amazon EVS 已在欧洲（爱尔兰）地区发布	Amazon EVS 已在欧洲（爱尔兰）地区发布。	2025 年 6 月 18 日
发布亚马逊 EVSService RolePolicy	亚马逊发布EVSServiceRolePolicy 了 AWS 托管政策。	2025 年 6 月 9 日
《用户指南》的初始版本	《亚马逊弹性 VMware 服务用户指南》已发布。 Amazon EVS 用户指南描述了所有 Amazon EVS 概念，并提供了在控制台和命令行界面中使用各种功能的说明。	2025 年 6 月 9 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。