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

# 什么是亚马逊弹性 VMware 服务？

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

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，请参阅开始使用。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 设置亚马逊弹性 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

本节介绍了 Amazon EVS 的一些关键概念和组件。

## Amazon 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 域以及一个 vSphere 集群，该集群托管用于管理、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 主机是在 Amazon EC2 裸机实例上运行的 VMware ESX 主机。Amazon EVS 主机使用本地 NVMe 实例存储卷来存储 vSAN 数据存储，用于存储您的管理和工作负载虚拟机。

> **Warning**
>
> 实例存储卷是临时性的。如果底层 EC2 实例停止或终止，存储在这些卷上的数据将不会保留。停止或终止 Amazon EVS 使用的 Amazon EC2 实例而不在 VCF 中进行退役可能会导致数据丢失。
> 有关主机维护的更多信息，请参见the section called “主机维护”。

## 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 ESX 主机的管理连接。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。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 块不得与与 VPC 关联的任何现有 CIDR 块重叠。

创建后，VLAN 子网会隐式关联您的 VPC 的主路由表。部署后，您可以将 VLAN 子网与自定义路由表显式关联。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 安全组规则不适用于连接到 VLAN 子网的 Amazon EVS 弹性网络接口。要控制进出 VLAN 子网的流量，必须使用网络访问控制列表。

## 主机管理 VLAN 子网

主机管理 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 ESX 主机的覆盖网络流量。

## 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 ESX 主机之间的重叠通信。

## 管理虚拟机 VLAN 子网

管理虚拟机 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 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。

# Amazon EVS 架构

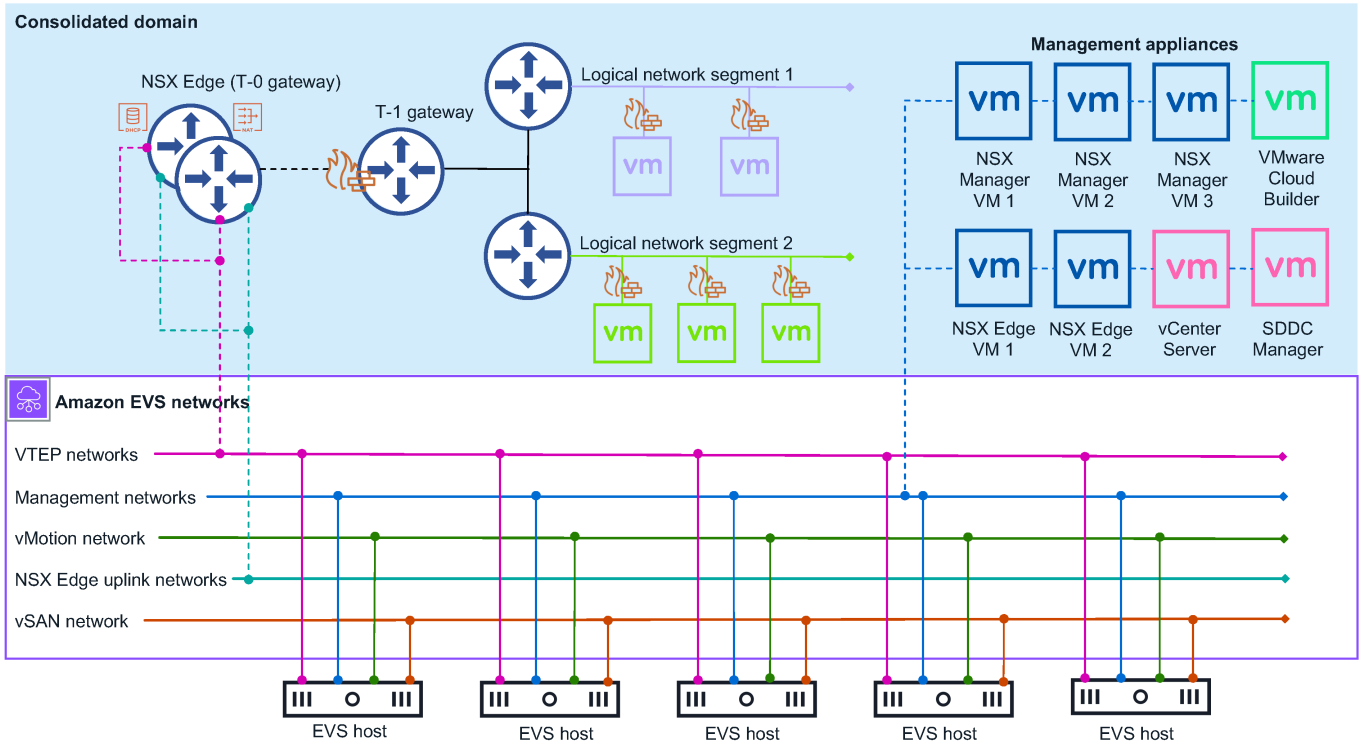
Amazon EVS 实施了 VMware 云基础 (VCF) 整合架构模型。在此模型中，VCF 管理组件和客户工作负载在整合的域上一起运行。Amazon EVS 环境通过单个 vCenter 服务器进行管理，该服务器具有 vSphere 资源池，可在管理工作负载和客户工作负载之间提供隔离。

Amazon EVS 部署的合并域包含以下 VCF 管理组件：

- ESX 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 边缘群集

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 覆盖网络上。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 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 在创建环境时配置的 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 the section called “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 “配置 DNS 服务器”。
- 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流量，并在 NSX 覆盖网络上创建。此 0 层网关是作为 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 边缘群集

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 管理控制台 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 ESX 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”。

# 设置亚马逊弹性 VMware 服务

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。有关部署先决条件的摘要清单，请参阅the section called “部署清单”。

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 IAM 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 管理控制台访问权限旁边的复选框。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 man  AWS aged-job 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AdministratorAccess权限，然后才能使用这些权限访问 AWS 账单和成本管理控制台。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）。

您可以使用相同的过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

您可以使用角色委派对 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 企业入门计划或企业 AWS 支持计划，才能持续获得技术支持和架构指导。 AWS Business Support 是满足亚马逊 EVS 要求的最低 AWS 支持级别。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 服务配额。

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

## 规划 VPC 网段大小

在创建 Amazon EVS 环境时，您需要指定 VPC CIDR 块。创建环境后无法更改 VPC CIDR 块，并且需要预留足够的空间来容纳 Amazon EVS 在环境部署期间创建的所需的 EVS 子网和主机。因此，在部署之前，务必仔细规划 CIDR 块大小，同时考虑 Amazon EVS 要求和您未来的扩展需求。Amazon EVS 需要一个最小大小为 /22 网络掩码的 VPC CIDR 块，以便为所需的 EVS 子网和主机留出足够的空间。有关更多信息，请参阅 the section called “Amazon EVS 联网注意事项”。

> **Important**
>
> 确保您的 VPC 子网和 Amazon EVS 为 VCF 设备创建的 VLAN 子网都有足够的 IP 地址空间。VPC CIDR 块的最小大小必须为 /22 网络掩码，以便为所需的 EVS 子网和主机留出足够的空间。

> **Note**
>
> Amazon EVS IPv6 目前不支持。

# 创建带有子网的 VPC

Amazon EVS 将您的环境部署到您提供的 VPC 中。此 VPC 必须包含用于访问 Amazon EVS 服务的子网 (the section called “服务访问子网”)。有关为 Amazon EVS 创建带有子网的 VPC 的步骤，请参阅。the section called “创建包含子网和路由表的 VPC”

# 配置 VPC 主路由表

Amazon EVS VLAN 子网隐式关联到 VPC 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”。

> **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。

## 网关路由要求

根据您的连接要求为以下网关类型配置路由：

- NAT 网关 (NGW)
  - 仅限出站互联网接入可选。
  - 必须位于具有互联网网关访问权限的公有子网中。

- 将来自私有子网和 EVS VLAN 子网的路由添加到 NAT 网关。
- 有关更多信息，请参阅 A mazon VPC 用户指南中的使用 NAT 网关。

- 公交网关 (TGW)
  - 需要通过 Di AWS rect Connect 和 AWS Site-to-Site VPN 进行本地连接。
  - 为本地网络范围添加路由。
  - 如果使用 BGP，请配置路由传播。
  - 有关更多信息，请参阅 Amazon VPC 用户指南中的 Amazon VPC 传输网关中的中转网关。

## 最佳实践

- 记录所有路由表配置。
- 使用一致的命名约定。
- 定期审核您的路由表。
- 进行更改后测试连通性。
- 备份路由表配置。
- 监控路由的运行状况和传播。

有关使用路由表的更多信息，请参阅 Amazon VPC 用户指南中的配置路由表。

# 配置您的 VPC 的 DHCP 选项集

**Important**

如果您不满足以下 Amazon EVS 要求，则您的环境部署将失败：

- 在 DHCP 选项集中包括主 DNS 服务器 IP 地址和辅助 DNS 服务器 IP 地址。
- 在部署中包括每个 VCF 管理设备和 Amazon EVS 主机的 A 记录的 DNS 正向查找区域。
- 包括一个 DNS 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。
- 配置 VPC 的主路由表，确保存在通往您的 DNS 服务器的路由。
- 确保您的域名注册有效且未过期，并且不存在重复的主机名或 IP 地址。
- 配置您的安全组和网络访问控制列表 (ACLs)，以允许 Amazon EVS 与以下人员通信：
  - TCP/UDP 端口 53 上的 DNS 服务器。

- 通过 HTTPS 和 SSH 进行主机管理 VLAN 子网。
- 通过 HTTPS 和 SSH 管理 VLAN 子网。

有关更多信息，请参阅 the section called “使用 VPC DHCP 选项集配置 DNS 和 NTP 服务器”。

# 创建和配置 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。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。在路由服务器对等方上配置的对等 ASN 必须匹配，并且对等 IP 地址必须是唯一的。

**Important**

如果您不满足 Amazon EVS 对 VPC 路由服务器配置的以下要求，则您的环境部署将失败：

- 您必须在服务访问子网中配置至少两个路由服务器端点。
- 为 Tier-0 网关配置边界网关协议 (BGP) 时，VPC 路由服务器对等 ASN 值必须与 NSX Edge 对等体 ASN 值匹配。
- 创建两个路由服务器对等体时，必须为每个端点使用来自 NSX 上行链路 VLAN 的唯一 IP 地址。在部署 Amazon EVS 环境期间，这两个 IP 地址将分配给 NSX 边缘。
- 启用路由服务器传播时，必须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。如果传播的路由表没有明确的子网关联，BGP 路由通告就会失败。

**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)。

## 先决条件

在开始之前，您需要：

- 您的路由服务器的 VPC 子网。

- 管理 VPC 路由服务器资源的 IAM 权限。
- 路由服务器的 BGP ASN 值（亚马逊端 ASN）。该值必须在 1 到 4294967295 的范围内。
- 一个对等 ASN，用于将您的路由服务器与 NSX Tier-0 网关对等。在路由服务器和 NSX Tier-0 网关中输入的对等 ASN 值必须匹配。NSX Edge 设备的默认 ASN 为 65000。

### Steps

有关设置 VPC 路由服务器的步骤，请参阅路由服务器入门教程。

> **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。

> **Note**
>
> 我们建议您为路径服务器实例启用持久路由，持续时间介于 1-5 分钟之间。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。

> **Note**
>
> 在 Amazon EVS 环境部署并投入运行之前，BGP 连接状态将处于关闭状态。

## 为本地连接创建传输网关

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 Direct Connect 与 AWS 基础设施的连接。有关更多信息，请参阅 the section called “配置本地网络连接（可选）”。

## 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 环境中的 ESX 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.x 的要求。有关相关版本信息，请参阅 VCF 5.2.x 发行说明。

> **Note**
>
> 有关 Amazon EVS 提供的 VCF 版本的信息，请参阅。the section called “VCF 版本和实例 EC2 ”

## 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。

> **Important**
>
> 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。

> **Note**
>
> 您的 VCF 许可证将适用于所有 AWS 地区的 Amazon EVS，以满足许可证合规性要求。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。

# 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 EVS 环境中默认不安装 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
- 如果您需要 HCX 互联网连接，则必须完成以下先决任务：
  - 确保亚马逊提供的连续公有 CID IPv4 R 块网络掩码长度的 IPAM 配额为 /28 或更大。

    > **Important**
    >
    > 对于 HCX 互联网连接，Amazon EVS 要求使用来自公共 IPAM 池的 IPv4 CIDR 块，网络掩码长度等于 /28 或更大。使用任何网络掩码长度小于 /28 的 CIDR 块都将导致 HCX 连接问题。有关增加 IPAM 配额的更多信息，请参阅 IPAM 配额。

- 使用 CIDR 创建一个 IPAM 和一个最小 IPv4 网络掩码长度为 /28 的公共 IPAM 池。
- 从 IPAM 池中为 HCX Manager 和 HCX Interconnect (HCX-IXEIPs) 设备分配至少两个弹性 IP 地址 ()。为需要部署的每台 HCX 网络设备分配额外的弹性 IP 地址。
- 将公有 IPv4 CIDR 块作为其他 CIDR 添加到您的 VPC。

有关 HCX 设置的更多信息，请参阅the section called “选择您的 HCX 连接选项”和。the section called “HCX 连接选项”

# Amazon EVS 部署先决条件清单

本部分包含成功部署 Amazon EVS 环境必须完成的先决条件列表。

VCF 许可证密钥信息

| 组件 | 说明 | 最低要求 | 示例值 |
| --- | --- | --- | --- |
| 站点 ID | 博通提供的用于访问博通支持门户的站点 ID。 | 必须在 EVS 环境创建请求中提供 Broadcom 提供的站点 ID。 | 01234567 |
| VCF 解决方案密钥 | 单个 VCF 许可密钥，用于解锁整个 VCF 堆栈的功能，包括 vSphere、NSX、SDDC Manager 和 vCenter Server。 | 必须在 EVS 环境创建请求中提供有效的有效 VCF 解决方案密钥。现有 EVS 环境不能使用密钥。 | ABCDE-FGHIJ-KLMNO-PQRSTU-VWXYZ |
| vSAN 许可证密钥 | vSAN 许可密钥允许您在 VCF 环境中激活和使用 vSAN 软件。 | 必须在 EVS 环境创建请求中提供有效的有效 vSAN 许可密钥。现有 EVS 环境不能使用密钥。 | ABCDE-FGHIJ-KLMNO-PQRSTU-VWXYZ |

AWS 账户和地区信息

| 组件 | 说明 | 最低要求 | 示例值 |
| --- | --- | --- | --- |
| AWS 账户 ID 号 | 该 AWS 账户允许您创建和管理 AWS 资源以及访问 AWS 服务。 | 必须有 AWS 账户访问权限。 | 99999999999999 |
| AWS 区域 | 一个物理地理区域，用于 AWS 维护多个隔离的数据中心，称为可用区。 | 必须指定要部署 Amazon EVS 的 AWS 区域。有关目前可用 Amazon EVS 的区域列表，请参阅《 AWS 通用参考指南》中的亚马逊弹性 VMware 服务终端节点和配额。 | 美国西部（俄勒冈州） |

AWS 用于本地数据中心连接的 Transit Gateway

| 组件 | 说明 | 最低要求 | 示例值 |
| --- | --- | --- | --- |
| 中转网关 ID | 传输网关充当区域虚拟路由器，用于传输您的 VPC 和本地网络之间的流量。 | 必须使用传输网关将 Amazon EVS 环境连接到您的本地网络。 | tgw-0262a0e521示例 |
| 连接方法 | 要将您的本地网络连接到 Amazon EVS 环境，您必须使用带有 Di AWS rect Connect 或 AWS Site-to-Site VPN 的传输网关。 | 确定您将使用 AWS Direct Connect、AWS Site-to-Site VPN 还是两者的组合。有关在 Direct Connect 中使用 Site-to-Site VPN 的更多信息，请参阅带有 Direct Connect 的 AWS 私有 | AWS Site-to-Site 使用 AWS Direct Connect |

| 组件 | 说明 | 最低要求 | 示例值 |
| --- | --- | --- | --- |
| | | IP AWS Site-to-Site VPN。 | |

适用于亚马逊 EVS 环境的 VPC

| 组件 | 说明 | 最低要求 | 示例值 |
| --- | --- | --- | --- |
| - VPC ID | VPC 是一种虚拟网络，与您在自己的数据中心中运行的传统网络非常相似。 | 任何 Amazon VPC 都可用于环境部署。 | vpc-0abcdef1234567890 |
| VPC 网段 | 在 Amazon VPC 中，CIDR 块定义了您的 VPC 中可用的 IP 地址范围。 | 一个最小大小为 /22 网络掩码的 RFC 1918 CIDR 块。VPC CIDR 块的大小必须适当，以适应您的 VPC 中要部署的所有 EVS 子网和主机。这个 CIDR 块在您的环境中应该是唯一的。 | 10.1.0.0/20 |

EVS 环境的 VPC 子网

| 组件 | 说明 | 最低要求 | 示例值 |
| --- | --- | --- | --- |
| 服务访问子网 ID | 服务访问子网是支持 Amazon EVS 服务访问的标准 VPC 子网。有关更多信息，请参阅 the section called “服务访问子网”。 | 可以使用任何 VPC 子网，前提是该子网在 VPC 内大小合适。我们建议指定网络掩码为 /24 的 VPC 子网 CIDR 块。 | subnet-abcdef1234567890e |
| 服务访问子网 CIDR | VPC 子网 CIDR 块是使用 CIDR 表示法定 | 必须适当调整服务访问子网的大小，以适 | 10.1.0.0/24 |

| 组件 | 说明 | 最低要求 | 示例值 |
| --- | --- | --- | --- |
| | 义的 IP 地址范围，分配给 VPC 内的特定子网。 | 应要在您的 VPC 中部署的其他 EVS 子网和主机。我们建议指定网络掩码为 /24 的 VPC 子网 CIDR 块。 | |
| AWS 该区域内的可用区 ID | 一个 AWS 区域内的一个不同位置，旨在与其他区域的故障隔离开来 AZs，由一个或多个数据中心组成。 | 在创建子网期间，您可以指定 VPC 子网部署到的可用区。有关更多信息，请参阅 Amazon VPC 用户指南中的创建子网。 | us-west-2a |

适用于 EVS 环境的 EVS VLAN 子网

| 组件 | 说明 | 最低要求 | 示例值 |
| --- | --- | --- | --- |
| 主机管理 VLAN CIDR | 主机管理 VLAN 子网的 CIDR 块。有关更多信息，请参阅 the section called “主机管理 VLAN 子网”。 | 网络掩码的最小大小必须为 /28，网络掩码的最大大小必须为 /24。不得与与 VPC 关联的任何现有 CIDR 块重叠。 | 10.1.1.0/24 |
| vMotion VLAN CIDR | vMotion VLAN 子网的 CIDR 块。有关更多信息，请参阅 the section called “vMotion VLAN 子网”。 | 必须与主机管理 VLAN 的大小相同。 | 10.1.2.0/24 |
| vSAN VLAN CIDR | vSAN VLAN 子网的 CIDR 块。有关更多信息，请参阅 the | 必须与主机管理 VLAN 的大小相同。 | 10.1.3.0/24 |

| 组件 | 说明 | 最低要求 | 示例值 |
| --- | --- | --- | --- |
| | section called “vSAN VLAN 子网”。 | | |
| VTEP VLAN CIDR | VTEP VLAN 子网的 CIDR 块。有关更多信息，请参阅 the section called “VTEP VLAN 子网”。 | 必须与主机管理 VLAN 的大小相同。 | 10.1.4.0/24 |
| 边缘 VTEP VLAN CIDR | 边缘 VTEP VLAN 子网的 CIDR 块。有关更多信息，请参阅 the section called “边缘 VTEP VLAN 子网”。 | 网络掩码的最小大小必须为 /28，网络掩码的最大大小必须为 /24。不得与与 VPC 关联的任何现有 CIDR 块重叠。 | 10.1.5.0/24 |
| 管理虚拟机 VLAN CIDR | 管理虚拟机 VLAN 子网的 CIDR 块。有关更多信息，请参阅 the section called “管理虚拟机 VLAN 子网”。 | 网络掩码的最小大小必须为 /28，网络掩码的最大大小必须为 /24。不得与与 VPC 关联的任何现有 CIDR 块重叠。 | 10.1.6.0/24 |
| HCX 上行链路 VLAN CIDR | HCX 上行链路 VLAN 子网的 CIDR 块。有关更多信息，请参阅 the section called “HCX 上行链路 VLAN 子网”。 | 网络掩码的最小大小必须为 /28，网络掩码的最大大小必须为 /24。不得与与 VPC 关联的任何现有 CIDR 块重叠。 | 10.1.7.0/24 |
| NSX 上行链路 VLAN CIDR | NSX 上行链路 VLAN 子网的 CIDR 块。有关更多信息，请参阅 the section called “NSX 上行链路 VLAN 子网”。 | 网络掩码的最小大小必须为 /28，网络掩码的最大大小必须为 /24。不得与与 VPC 关联的任何现有 CIDR 块重叠。 | 10.1.8.0/24 |

| 组件 | 说明 | 最低要求 | 示例值 |
| --- | --- | --- | --- |
| 扩展 VLAN 1 CIDR | 扩展 VLAN 子网的 CIDR 块。有关更多信息，请参阅 the section called “扩展 VLAN 子网”。 | 网络掩码的最小大小必须为 /28，网络掩码的最大大小必须为 /24。不得与与 VPC 关联的任何现有 CIDR 块重叠。 | 10.1.9.0/24 |
| 扩展 VLAN 2 CIDR | 扩展 VLAN 子网的 CIDR 块。有关更多信息，请参阅 the section called “扩展 VLAN 子网”。 | 网络掩码的最小大小必须为 /28，网络掩码的最大大小必须为 /24。不得与与 VPC 关联的任何现有 CIDR 块重叠。 | 10.1.10.0/24 |

DNS 和 NTP 基础架构

| 组件 | 说明 | 最低要求 | 示例值 |
| --- | --- | --- | --- |
| 主 DNS 服务器的 IP 地址 | 主域名系统 (DNS) 服务器用作该域所有 DNS 记录的真实来源。 | 您可以使用可用主机范围内的任何有效的、未使用 IPv4 的地址。 | 10.1.1.10 |
| 辅助 DNS 服务器 IP 地址 | 域名 DNS 记录的备份 DNS 服务器。 | 您可以使用可用主机范围内的任何有效的、未使用 IPv4 的地址。 | 10.1.5.25 |
| NTP 服务器 IP 地址 | 网络时间协议 (NTP) 服务器是一种使用 NTP 标准在网络中同步时钟的设备或应用程序。 | 您可以将默认 Amazon 时间同步服务与本地 `169.254.169.123` IP 地址或其他 NTP 服务器 IP 地址一起使用。 | 169.254.169.123（亚马逊时间同步服务） |

| 组件 | 说明 | 最低要求 | 示例值 |
| --- | --- | --- | --- |
| 用于 VCF 部署的 FQDN | 完全限定域名 (FQDN) 是网络上设备的绝对名称。FQDN 由主机名和域名组成。 | FQDN 只能包含字母数字字符、减号 (-) 和用作标签之间分隔符的句点。必须是有效且未过期的唯一 FQDN。 | evs.local |

VPC DHCP 选项集

| 组件 | 说明 | 最低要求 | 示例值 |
| --- | --- | --- | --- |
| DHCP 选项集 ID | DHCP 选项集是 VPC 中的资源（例如 EC2 实例）使用的一组网络设置，用于通过您的虚拟网络进行通信。 | 必须包含至少 2 个 DNS 服务器。您可以使用 Route 53 或自定义 DNS 服务器。还必须包含您的 DNS 域名和 NTP 服务器。 | dopt-0a1b2c3D |

EC2 key pair

| 组件 | 说明 | 最低要求 | 示例值 |
| --- | --- | --- | --- |
| EC2 key pair 名称 | EC2 key pair 是一组用于安全连接到 Amazon EC2 实例的安全证书。 | 密钥对名称必须是唯一的。 | `my-ec2-key-pair` |

VPC 路由表

| 组件 | 说明 | 最低要求 | 示例值 |
| --- | --- | --- | --- |
| 主路由表 ID | 在 Amazon VPC 中，主路由表是使用 VPC 自动创建的默认路由 | 要成功部署环境，必须配置为启用与 DNS | rtb-0123456789abcdef0 |

| 组件 | 说明 | 最低要求 | 示例值 |
| --- | --- | --- | --- |
| | 表，它控制未与其他路由表明确关联的任何 VPC 子网的流量。当 Amazon EVS 创建 EVS VLAN 子网时，这些子网会隐式关联到您的 VPC 的主路由表。 | 或本地系统等相关服务的连接。 | |

网络访问控制列表 (ACL)

| 组件 | 说明 | 最低要求 | 示例值 |
| --- | --- | --- | --- |
| 网络 ACL ID | 网络访问控制列表 (ACL) 允许或拒绝子网级别的入站或出站流量。 | 必须允许 Amazon EVS 与以下人员通信：<br>• TCP/UDP 端口 53 上的 DNS 服务器。<br>• 通过 HTTPS 和 SSH 进行主机管理 VLAN 子网。<br>• 通过 HTTPS 和 SSH 管理虚拟机 VLAN 子网。 | acl-0f62c640e793a38a3 |

VCF 组件的 DNS 记录

| 组件 | 说明 | 最低要求 | IP 地址示例 | 主机名示例 |
| --- | --- | --- | --- | --- |
| ESX 主机 1 | 在 ESX 主机 1 的 A 记录和 PTR 记录中定义的 IP 地址和主机名。 | Amazon EVS 需要一个带有 A 记录的 DNS 正向查找区域和一个反向查找区域，该 | 10.1.0.10 | esxi01 |

| 组件 | 说明 | 最低要求 | IP 地址示例 | 主机名示例 |
| --- | --- | --- | --- | --- |
| | | 区域包含为每个 EVS 部署中的每个 ESX 主机创建 PTR 记录。 | | |
| ESX 主机 2 | 在 ESX 主机 2 的 A 记录和 PTR 记录中定义的 IP 地址和主机名。 | Amazon EVS 需要一个带有 A 记录的 DNS 正向查找区域和一个反向查找区域，该区域包含为每个 EVS 部署中的每个 ESX 主机创建 PTR 记录。 | 10.1.0.11 | esxi02 |
| ESX 主机 3 | 在 ESX 主机 3 的 A 记录和 PTR 记录中定义的 IP 地址和主机名。 | Amazon EVS 需要一个带有 A 记录的 DNS 正向查找区域和一个反向查找区域，该区域包含为每个 EVS 部署中的每个 ESX 主机创建 PTR 记录。 | 10.1.0.12 | esxi03 |
| ESX 主机 4 | 在 ESX 主机 4 的 A 记录和 PTR 记录中定义的 IP 地址和主机名。 | Amazon EVS 需要一个带有 A 记录的 DNS 正向查找区域和一个反向查找区域，该区域包含为每个 EVS 部署中的每个 ESX 主机创建 PTR 记录。 | 10.1.0.13 | esxi04 |

| 组件 | 说明 | 最低要求 | IP 地址示例 | 主机名示例 |
| --- | --- | --- | --- | --- |
| vCenter Server 设备 | vCenter Server 设备的 A 记录和 PTR 记录中定义的 IP 地址和主机名。 | Amazon EVS 需要一个带有 A 记录的 DNS 正向查找区域和一个反向查找区域，其中包含为每个 EVS 部署中的每个 VCF 管理设备创建 PTR 记录。 | 10.1.5.10 | vc01 |
| NSX Manager 群集 | 在 NSX Manager 群集的 A 记录和 PTR 记录中定义的 IP 地址和主机名。 | Amazon EVS 需要一个带有 A 记录的 DNS 正向查找区域和一个反向查找区域，其中包含为每个 EVS 部署中的每个 VCF 管理设备创建 PTR 记录。 | 10.1.5.11 | nsx |
| SDDC 管理器设备 | 在 SDDC Manager 设备的 A 记录和 PTR 记录中定义的 IP 地址和主机名。 | Amazon EVS 需要一个带有 A 记录的 DNS 正向查找区域和一个反向查找区域，其中包含为每个 EVS 部署中的每个 VCF 管理设备创建 PTR 记录。 | 10.1.5.12 | sddcm01 |

| 组件 | 说明 | 最低要求 | IP 地址示例 | 主机名示例 |
| --- | --- | --- | --- | --- |
| 云构建器设备 | 在云构建器设备的 A 记录和 PTR 记录中定义的 IP 地址和主机名。 | Amazon EVS 需要一个带有 A 记录的 DNS 正向查找区域和一个反向查找区域，其中包含为每个 EVS 部署中的每个 VCF 管理设备创建 PTR 记录。 | 10.1.5.13 | cb01 |
| NSX Edge 1 设备 | 在 NSX Edge 1 设备的 A 记录和 PTR 记录中定义的 IP 地址和主机名。 | Amazon EVS 需要一个带有 A 记录的 DNS 正向查找区域和一个反向查找区域，其中包含为每个 EVS 部署中的每个 VCF 管理设备创建 PTR 记录。 | 10.1.5.14 | edge01 |
| NSX Edge 2 设备 | 在 NSX Edge 2 设备的 A 记录和 PTR 记录中定义的 IP 地址和主机名。 | Amazon EVS 需要一个带有 A 记录的 DNS 正向查找区域和一个反向查找区域，其中包含为每个 EVS 部署中的每个 VCF 管理设备创建 PTR 记录。 | 10.1.5.15 | edge02 |

| 组件 | 说明 | 最低要求 | IP 地址示例 | 主机名示例 |
| --- | --- | --- | --- | --- |
| NSX Manager 1 设备 | 在 NSX Manager 1 设备的 A 记录和 PTR 记录中定义的 IP 地址和主机名。 | Amazon EVS 需要一个带有 A 记录的 DNS 正向查找区域和一个反向查找区域，其中包含为每个 EVS 部署中的每个 VCF 管理设备创建 PTR 记录。 | 10.1.5.16 | nsx01 |
| NSX Manager 2 设备 | 在 NSX Manager 2 设备的 A 记录和 PTR 记录中定义的 IP 地址和主机名。 | Amazon EVS 需要一个带有 A 记录的 DNS 正向查找区域和一个反向查找区域，其中包含为每个 EVS 部署中的每个 VCF 管理设备创建 PTR 记录。 | 10.1.5.17 | nsx02 |
| NSX Manager 3 设备 | 在 NSX Manager 3 设备的 A 记录和 PTR 记录中定义的 IP 地址和主机名。 | Amazon EVS 需要一个带有 A 记录的 DNS 正向查找区域和一个反向查找区域，其中包含为每个 EVS 部署中的每个 VCF 管理设备创建 PTR 记录。 | 10.1.5.18 | nsx03 |

VPC 路由服务器基础架构

| 组件 | 说明 | 最低要求 | 示例值 |
| --- | --- | --- | --- |
| 路由服务器 ID | 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。在路由服务器和 NSX Edge 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。 | rs-0a1b2c3d4e5f67890 |
| 路由服务器关联 | 路由服务器和 VPC 之间的连接。 | 您的路由服务器必须与您的 VPC 关联。 | `{ "RouteServerAssociation": { "RouteServerId": "rs-0a1b2c3d4e5f67890", "VpcId": "vpc-1", "State": "associating" } }` |
| VPC 路由服务器端的 BGP ASN（亚马逊端 ASN） | 亚马逊端 ASN 代表 VPC 路由服务器和 NS AWS X Edge 对等体之间的 BGP 会话的一端。您在创建路由服务器时指定此 BGP ASN。有关更多信息，请参阅 Amazon | 此值必须是唯一的，并且在 1-4294967295 的范围内。 AWS 建议使用 64512—65534（16 位 ASN）或 4200000000—4294967294（32 位 ASN）范围内的私有 ASN。 | 65001 |

| 组件 | 说明 | 最低要求 | 示例值 |
| --- | --- | --- | --- |
| | VPC 用户指南中的创建路由服务器。 | | |
| 路由服务器端点 1 ID | 路由服务器端点是AWS子网内的托管组件，用于促进路由服务器与 BGP 对等体之间的 BGP（边界网关协议）连接。 | 必须将路由服务器端点部署到服务访问子网中。 | rse-0123456789abcdef0 |
| 路由服务器对等体 1 ID | 路由服务器对等体是路由服务器端点与部署在 AWS (NSX Edge) 中的设备之间的 BGP 对等会话。 | 在路由服务器对等体中指定的对等 ASN 值必须与用于 NSX Edge Tier-0 网关的对等 ASN 值相匹配。 | rsp-0123456789abcdef0 |
| 路由服务器对等体 1 IP 地址（EVS NSX Edge 1 端） | 路由服务器对等体的 IP 地址 (`PeerAddress`)。 | 必须使用 NSX 上行链路 VLAN 中唯一未使用的 IP 地址。作为部署的一部分，Amazon EVS 会将此 IP 地址应用于 NSX Edge 1，并与路由服务器终端节点对等对等。 | 10.1.7.10 |
| 路由服务器对等体 1 端点 ENI 地址 | 路由服务器对等体的端点 ENI IP 地址 (`EndpointEniAddress`)。 | 路由服务器在创建对等体时自动生成。 | 10.1.7.11 |
| 路由服务器端点 2 ID | 路由服务器端点是AWS子网内的托管组件，用于促进路由服务器与 BGP 对等体之间的 BGP（边界网关协议）连接。 | 必须将路由服务器端点部署到服务访问子网中。 | rse-fedcba9876543210f |

| 组件 | 说明 | 最低要求 | 示例值 |
| --- | --- | --- | --- |
| 路由服务器对等体 2 ID（EVS NSX Edge 2 端） | 路由服务器对等体是路由服务器端点与部署在 AWS (NSX Edge) 中的设备之间的 BGP 对等会话。 | 在路由服务器对等体中指定的对等 ASN 值必须与用于 NSX Edge Tier-0 网关的对等 ASN 值相匹配。 | rsp-fedcba9876543210f |
| 路由服务器对等体 2 IP 地址 | 路由服务器对等体的 IP 地址 (`PeerAddress`)。 | 必须使用来自 NSX 上行链路 VLAN 的唯一 IP 地址。作为部署的一部分，Amazon EVS 会将此 IP 地址应用于 NSX Edge 2，并与路由服务器终端节点对等对等。 | 10.1.7.200 |
| 路由服务器对等体 2 端点 ENI 地址 | 路由服务器对等体的端点 ENI IP 地址 (`EndpointEniAddress`)。 | 路由服务器在创建对等体时自动生成。 | 10.1.7.201 |
| 路由服务器传播 | 路由服务器传播将 FIB 中的路由安装到您指定的路由表上。 | 必须指定与您的服务访问子网关联的路由表。Amazon EVS 目前仅支持 IPv4 联网。 | `{ "RouteServerEndpoint": { "RouteServerId": "rs-1", "RouteServerEndpointId": "rse-1", "VpcId": "vpc-1", "SubnetId": "subnet-1", "State": "pending" } }` |

| 组件 | 说明 | 最低要求 | 示例值 |
| --- | --- | --- | --- |
| NSX 对等端的 BGP ASN | 连接的 NSX 端的 BGP ASN。 | 建议使用 NSX 的默认 ASN 65000 | 65000 |

HCX 互联网接入资源（可选）

| 组件 | 说明 | 最低要求 | 示例值 |
| --- | --- | --- | --- |
| IPAM ID | 亚马逊 VPC IP 地址管理器 (IPAM) 用于管理 HCX 互联网访问的 IP 地址。 | 必须配置为提供公用 IPv4 地址。仅在 HCX 互联网接入配置中需要。 | ipam-0123456789abcdef0 |
| IPAM 池 ID | 亚马逊拥有的公有 IPv4 IPAM 池，为 HCX 组件提供地址。 | 必须配置为公共 IPv4 池。仅在 HCX 互联网接入配置中需要。 | ipam-pool-0123456789abcdef0 |
| HCX 公共 VLAN CIDR 块 | 从 IPAM 池中为 H IPv4 CX 公有 VLAN 子网分配的辅助公有 CIDR 块。 | 必须具有 /28 网络掩码，并且必须从亚马逊拥有的 IPAM 公共池中分配。仅在 HCX 互联网接入配置中需要。 | 18.97.137.0/28 |
| 弹性 IP 地址 | 从 IPAM 池中为 HCX 组件分配的顺序弹性 IP 地址。 | HCX Manager、HCX Interconnect Appliance (HCX-IX) 和 HCX 网络扩展 (HCX-NE) 的同一 IPAM 池中至少 3 EIPs 个。仅在 HCX 互联网接入配置中需要。 | eipalloc-0123456789abcdef0、eipalloc-0123456789abcdef1、eipalloc-0123456789abcdef2、eipalloc-0123456789abcdef2 |

# 亚马逊弹性 VMware 服务入门

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.x 的要求。有关相关版本信息，请参阅 VCF 5.2.x 发行说明。

> **Important**
>
> 有关 Amazon EVS 提供的 VCF 版本的信息，请参阅。the section called “VCF 版本和实例 EC2 ”

主题

- 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 设置亚马逊弹性 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。

Example

Amazon VPC console

1. 打开 Amazon VPC 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《 AWS 通用参考指南》中的亚马逊弹性 VMware 服务终端节点和配额。

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. 对于私有子网数量，请选择 1。此私有子网将用作您在环境创建步骤中提供给 Amazon EVS 的服务访问子网。有关更多信息，请参阅 the section called “服务访问子网”。
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子网隐式关联到主路由表。

AWS CLI

1. 打开终端会话。
2. 在单个可用区中创建具有私有子网和可选公有子网的 VPC。

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

VPC_ID=$ (aws ec2 describe-vpcs\--filters name=tag: Name，values=evs-vpc\--query 'Vpcs [0]。 VpcId'\--输出文本)---

3. 启用 DNS 主机名和 DNS 支持。

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

4. 在 VPC 中创建私有子网。

```
aws ec2 create-subnet \
```

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

5. 存储私有子网 ID，以便在后续命令中使用。

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

6. （可选）如果需要互联网连接，请创建公有子网。

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

7. （可选）存储公有子网 ID，以便在后续命令中使用。

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

8. （可选）如果已创建公有子网，则创建并连接互联网网关。

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

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

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

```
  --internet-gateway-id $IGW_ID
```

9. （可选）如果需要互联网连接，请创建 NAT 网关。

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

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

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

10.创建和配置必要的路由表。

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

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

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

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

11.向路由表中添加必要的路由。

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

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

12.将路由表与您的子网关联。

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

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

> **Note**
>
> 在创建 VPC 期间，Amazon VPC 会自动创建主路由表并默认将子网隐式关联到主路由表。

# 选择您的 HCX 连接选项

为您的 Amazon EVS 环境选择一个连接选项：

- 私有连接：为 HCX 提供高性能网络路径，优化可靠性和一致性。需要使用 AWS Direct Connect 或 Site-to-Site VPN 进行外部网络连接。
- 互联网连接：使用公共互联网建立可快速设置的灵活迁移路径。需要使用 VPC IP 地址管理器 (IPAM) 和弹性 IP 地址。

有关详细分析，请参阅the section called “HCX 连接选项”。

选择您的选项：

- 选项 A：仅限私有连接 → 继续the section called “配置 VPC 主路由表”。
- 选项 B：互联网连接 → 继续the section called “HCX 互联网连接设置”。

## HCX 互联网连接设置

> **Note**
>
> 如果您选择了 HCX 私有连接，请跳过本节并继续。the section called “配置 VPC 主路由表”

要为 Amazon EVS 启用 HCX 互联网连接，您必须：

- 确保亚马逊提供的连续公有 IPv4 CIDR 块网络掩码长度的 VPC IP 地址管理器 (IPAM) 配额为 /28 或更大。

  > **Important**
  >
  > 如果使用亚马逊提供的任何网络掩码长度小于 /28 的连续公有 IPv4 CIDR 块，则会导致 HCX 连接问题。有关增加 IPAM 配额的更多信息，请参阅 IPAM 配额。

- 使用最小网络掩码长度为 /28 的 CIDR 创建 IPv4 IPAM 和公共 IPAM 池。
- 从 IPAM 池中为 HCX Manager 和 HCX Interconnect (HCX-IXEIPs) 设备分配至少两个弹性 IP 地址 ()。为需要部署的每台 HCX 网络设备分配额外的弹性 IP 地址。
- 将公有 IPv4 CIDR 块作为其他 CIDR 添加到您的 VPC。

有关在创建环境后管理 HCX 互联网连接的更多信息，请参阅the section called “HCX 公共连接”。

创建 IPAM

按照以下步骤创建 IPAM。

> **Note**
>
> 您可以使用 IPAM 免费套餐创建用于亚马逊 EVS 的 IPAM 资源。虽然 IPAM 本身在免费套餐中是免费的，但与 IPAM 结合使用的其他 AWS 服务（例如 NAT 网关和任何超出免费套餐限制的公有 IPv4 地址）的费用由您承担。有关 IPAM 定价的更多信息，请参阅定Amazon VPC 价页面。

> **Note**
>
> Amazon EVS CIDRs 目前不支持私有 IPv6 全球单播地址 (GUA)。

### 创建公共 IPv4 IPAM 池

按照以下步骤创建公共 IPv4 池。

#### IPAM console

1. 打开 IAM 控制台。
2. 在导航窗格中，选择池。
3. 选择公有范围。有关作用域的更多信息，请参阅 IPAM 的工作原理。
4. 选择创建池。
5. （可选）添加池的名称标签和池的描述。
6. 在 “地址系列” 下，选择IPv4。
7. 在资源规划下，保持选中在范围内规划 IP 空间。
8. 在 Locale（区域设置）下，选择池的区域设置。 AWS 区域是您希望此 IPAM 池可用于分配的区域。您选择的区域必须与您的 VPC 部署到的 AWS 区域相匹配。
9. 在服务下，选择 EC2 (EIP/VPC)。这将宣传从该池中 CIDRs 分配给 Amazon EC2 服务（用于弹性 IP 地址）。
10. 在公有 IP 来源下，选择 Amazon 拥有。
11. 在 “配置” 下CIDRs ，选择 “添加亚马逊拥有的公有 CIDR”。
12. 在 “网络掩码” 下，选择 CIDR 网络掩码长度。/28 是所需的最小网络掩码长度。
13. 选择创建池。

#### AWS CLI

1. 打开终端会话。
2. 从 IPAM 获取公共范围 ID。

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

```
  --output text)
```

3. 在公共范围内创建 IPAM 池。

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

4. 存储池 ID，以便在后续命令中使用。

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

5. 从池中配置一个 CIDR 块，网络掩码的最小长度为 /28。

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

从 IPAM 池中分配弹性 IP 地址

按照以下步骤从 IPAM 池中为 HCX Service Mesh 设备分配弹性 IP 地址 (EIPs)。

Amazon VPC console

1. 打开 Amazon VPC 控制台。
2. 在导航窗格中，选择弹性 IPs。
3. 选择 Allocate Elastic IP address (分配弹性 IP 地址)。
4. 选择 “使用 IPv4 IPAM 池分配”。
5. 选择您之前配置的亚马逊拥有的公共 IPv4 池。
6. 在 “分配 IPAM 方法” 下，选择 “在 IPAM 池中手动输入地址”。

> **Important**
>
> 您无法将公有 IPAM CIDR 块中的前两个 EIPs 或最后一个 EIP 关联到 VLAN 子网。EIPs 这些地址保留为网络、默认网关和广播地址。如果您尝试将其与 VLAN 子网关联，Amazon EVS 会引 EIPs 发验证错误。

> **Important**
>
> 在 IPAM 池中手动输入地址，确保不会分配该 EIPs Amazon EVS 储备。如果您允许 IPAM 选择 EIP，IPAM 可能会分配一个 Amazon EVS 保留的 EIP，从而导致在与 VLAN 子网关联的 EIP 期间失败。

7. 指定要从 IPAM 池中分配的 EIP。
8. 选择 Allocate。
9. 重复此过程以分配所需的剩余 EIPs 部分。您需要 EIPs 从 IPAM 池中为 HCX Manager 和 HCX Interconnect (HCX-IX) 设备分配至少两个。为需要部署的每个 HCX 网络设备分配额外的 EIP。

AWS CLI

1. 打开终端会话。
2. 获取您之前创建的 IPAM 池 ID。

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

3. 从 IPAM 池中分配弹性 IP 地址。您需要 EIPs 从 IPAM 池中为 HCX Manager 和 HCX Interconnect (HCX-IX) 设备分配至少两个。为需要部署的每个 HCX 网络设备分配额外的 EIP。

> **Important**
>
> 您不能将公有 IPAM CIDR 块中的前两个 EIPs 或最后一个 EIP 与 VLAN 子网关联。EIPs 这些地址保留为网络、默认网关和广播地址。如果您尝试将其与 VLAN 子网关联，Amazon EVS 会引 EIPs 发验证错误。

> **Important**
>
> 在 IPAM 池中手动输入地址，确保不会分配该 EIPs Amazon EVS 储备。如果您允许 IPAM 选择 EIP，IPAM 可能会分配一个 Amazon EVS 保留的 EIP，从而导致在与 VLAN 子网关联的 EIP 期间失败。

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

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

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

将公有 IPv4 CIDR 块从 IPAM 池添加到 VPC 以实现 HCX 互联网连接

要启用 HCX 互联网连接，您必须将 IPAM 池中的公有 IPv4 CIDR 块作为额外 CIDR 添加到您的 VPC。Amazon EVS 使用此 CIDR 区块将 VMware HCX 连接到您的网络。按照以下步骤将 CIDR 块添加到您的 VPC。

> **Important**
>
> 您必须手动输入添加到您的 VPC 的 IPv4 CIDR 块。Amazon EVS 目前不支持使用 IPAM 分配的 CIDR 块。使用 IPAM 分配的 CIDR 块可能会导致 EIP 关联失败。

Amazon VPC console

1. 打开 Amazon VPC 控制台。
2. 在导航窗格中，选择您的 VPCs。
3. 选择您之前创建的 VPC，然后选择操作、编辑 CIDRs。
4. 选择添加新 IPV4 CIDR。
5. 选择 IPV4 CIDR 手动输入。
6. 从您之前创建的公共 IPAM 池中指定 CIDR 块。

AWS CLI

1. 打开终端会话。
2. 获取 IPAM 池 ID 和已配置的 CIDR 块。

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

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

3. 将 CIDR 块添加到您的 VPC。

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

# 配置 VPC 主路由表

Amazon EVS VLAN 子网隐式关联到 VPC 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。主路由表必须包含 VPC 的 CIDR 的路由。只有在初始部署 Amazon EVS 环境时才需要使用主路由表。部署环境后，您可以将环境配置为使用自定义路由表。有关更多信息，请参阅 the section called “配置自定义路由表”。

部署环境后，您必须将每个 Amazon EVS VLAN 子网与您的 VPC 中的路由表明确关联。如果您的 VLAN 子网未与 VPC 路由表明确关联，NSX 连接就会失败。我们强烈建议您在部署环境后将子网与自定义路由表明确关联。有关更多信息，请参阅 the section called “配置 VPC 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

> **Important**
>
> 如果您不满足以下 Amazon EVS 要求，则您的环境部署将失败：
>
> - 在 DHCP 选项集中包括主 DNS 服务器 IP 地址和辅助 DNS 服务器 IP 地址。
> - 在部署中包括每个 VCF 管理设备和 Amazon EVS 主机的 A 记录的 DNS 正向查找区域。
> - 包括一个 DNS 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。
> - 配置 VPC 的主路由表，确保存在通往 DNS 服务器的路由。
> - 确保您的域名注册有效且未过期，并且不存在重复的主机名或 IP 地址。
> - 配置您的安全组和网络访问控制列表 (ACLs)，以允许 Amazon EVS 与以下人员通信：
>   - TCP/UDP 端口 53 上的 DNS 服务器。
>   - 通过 HTTPS 和 SSH 进行主机管理 VLAN 子网。
>   - 通过 HTTPS 和 SSH 管理 VLAN 子网。

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

- 用于主机 IP 地址解析的域名系统 (DNS) 服务器。
- 用于 DNS 解析的域名。
- 用于时间同步的网络时间协议 (NTP) 服务器。

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。

## 配置 DNS 服务器

DNS 配置可在您的 Amazon EVS 环境中启用主机名解析。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。
- 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。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。

### 配置 DNS 以实现本地连接

对于本地连接，我们建议使用带有入站解析器的 Route 53 私有托管区域。此设置支持混合 DNS 解析，在这种解析中，您可以将 Route 53 用于您的 VPC 内的内部 DNS，并将其与您现有的本地 DNS 基础设施集成。这使您的 VPC 中的资源无需复杂配置即可解析本地网络上托管的域名，反之亦然。如果需要，您也可以将自己的 DNS 服务器与 Route 53 出站解析器配合使用。有关配置步骤，请参阅 Amazon Route 53 开发者指南中的创建私有托管区域和将入站 DNS 查询转发到您的 VPC。

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

> **Note**
>
> 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。

### 解决 DNS 可访问性问题

Amazon EVS 需要与 SDDC Manager 和 VPC 的 DHCP 选项集中的 DNS 服务器建立持久连接，才能访问 DNS 记录。如果与 SDDC Manager 的永久连接不可用，Amazon EVS 将无法再验证环境状态，并且您可能会失去对环境的访问权限。有关解决此问题的步骤，请参阅the section called “可接通性检查失败”。

## 配置 NTP 服务器

NTP 服务器为您的网络提供时间。在您的 Amazon EC2 实例上提供一致且准确的时间参考对于许多 VCF 环境任务和流程至关重要。时间同步对于以下方面至关重要：

- 系统日志和审计
- 安全运营
- 分布式系统管理
- 问题排查

您最多可以在 VPC 的 DHCP 选项集中输入四台 NTP 服务器 IPv4 的地址。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 Amazon Time Sync 服务的更多信息，请参阅 Cloud Foundation 文档中的 EC2 实例中的精确时钟和时间同步和在 VMware Cloud Foundation 主机上配置 NTP。 VMware

#### 配置 NTP 设置

1. 选择你的 NTP 来源：
   - Amazon 时间同步服务（推荐）
   - 自定义 NTP 服务器
2. 将 NTP 服务器添加到您的 DHCP 选项集中。有关更多信息，请参阅 Amazon VPC 用户指南中的创建 DHCP 选项集。

3. 验证时间同步。有关 DHCP 选项集配置的更多信息，请参见the section called “配置您的 VPC 的 DHCP 选项集”。

配置本地网络连接（可选）

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 Direct Connect 与 AWS 基础设施的连接。

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 “为本地连接配置中转网关路由表和 Direct Connect 前缀（可选）”。

有关设置 Direct Connect 连接的更多信息，请参阅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。在路由服务器对等方上配置的对等 ASN 必须匹配，并且对等 IP 地址必须是唯一的。

如果要为 HCX Internet 连接配置路由服务器，则必须为在此过程的第一步中创建的服务访问子网和公有子网配置路由服务器传播。

> **Important**
>
> 如果您不满足 Amazon EVS 对 VPC 路由服务器配置的以下要求，则您的环境部署将失败：
>
> - 您必须在服务访问子网中配置至少两个路由服务器端点。

- 为 Tier-0 网关配置边界网关协议 (BGP) 时，VPC 路由服务器对等 ASN 值必须与 NSX Edge 对等体 ASN 值匹配。
- 创建两个路由服务器对等体时，必须为每个端点使用来自 NSX 上行链路 VLAN 的唯一 IP 地址。在部署 Amazon EVS 环境期间，这两个 IP 地址将分配给 NSX 边缘。
- 启用路由服务器传播时，必须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。如果传播的路由表没有明确的子网关联，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。

**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。

**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久路由，持续时间介于 1-5 分钟之间。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。

## 问题排查

如果您遇到问题：

- 确认每个路由表都有明确的子网关联。
- 检查为路由服务器和 NSX Tier-0 网关输入的对等 ASN 值是否匹配。
- 确认路由服务器端点 IP 地址是唯一的。
- 查看路由表中的路由传播状态。
- 使用 VPC 路由服务器对等日志来监控 BGP 会话运行状况并对连接问题进行故障排除。有关更多信息，请参阅 Amazon VPC 用户指南中的路由服务器对等登录。

# 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。

如果您计划配置 HCX 互联网连接，请确保您配置的网络 ACL 规则允许 HCX 组件所需的入站和出站连接。有关 HCX 端口要求的更多信息，请参阅 VMware HCX 用户指南。

> **Important**
>
> 如果您通过互联网连接，则将弹性 IP 地址与 VLAN 关联可直接访问该 VLAN 子网上的所有资源。确保您配置了适当的网络访问控制列表，以根据您的安全要求限制访问。

> **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。

# 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 区域的 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。

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，检查是否满足了服务要求。有关更多信息，请参阅 设置亚马逊弹性 VMware 服务。
   a. （可选）在“名称”中，输入环境名称。

b. 对于环境版本，请选择您的 VCF 版本。有关 Amazon EVS 提供的 VCF 版本的信息，请参阅。the section called “VCF 版本和实例 EC2 ”

c. 对于站点 ID，请输入您的博通网站 ID。

d. 对于 VCF 解决方案密钥，输入 VCF 解决方案密钥（适用于 VCF 的 VMware vSphere 8 Enterprise Plus）。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，以满足许可证合规性要求。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。

e. 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，以满足许可证合规性要求。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，以便选择服务才能正常运行。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。

f. 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。

g. 选择下一步。

5. 在 “指定主机详细信息” 页面上，完成以下步骤四次，向环境中添加四台主机。Amazon EVS 环境需要四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。

d. 对于 ESX 主机版本，在创建环境期间，将使用所选 VCF 版本的默认 ESX 版本。请参阅the section called “VCF 版本和实例 EC2 ”了解更多信息。

> **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。

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

f. 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 HCX 连接要求，请选择是要通过私有连接使用 HCX 还是通过互联网使用 HCX。

b. 对于 VPC，请选择您之前创建的 VPC。

c. （仅适用于 HCX 互联网连接）对于 HCX 网络 ACL，请选择您的 HCX VLAN 将与哪个网络 ACL 关联。

> **Important**
>
> 我们强烈建议您创建专用 HCX VLAN 的自定义网络 ACL。有关更多信息，请参阅 the section called “配置网络 ACL”。

d. 对于服务访问子网，请选择在创建 VPC 时创建的私有子网。

e. 对于安全组-可选，您最多可以选择两个安全组来控制 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。

f. 在 “管理连接” 下，输入要用于 Amazon EVS VLAN 子网的 CIDR 块。对于 HCX 上行链路 VLAN CIDR 块，如果配置公用 HCX VLAN，则必须指定网络掩码长度恰好为 /28 的 CIDR 块。如果为公共 HCX VLAN 指定了任何其他 CIDR 块大小，Amazon EVS 将引发验证错误。对于私有 HCX VLAN 和所有其他 VLANs CIDR 块，您可以使用的最小网络掩码长度为 /28，最大值为 /24。

> **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”。

g. 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。

h. 在 “工作负载/vCF 连接” 下，输入 NSX 上行链路 VLAN 的 CIDR 块，然后选择两个通过 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**
>
> 在部署 EVS 之前，Amazon EVS 需要一个与两个路由服务器终端节点和两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”。

i. 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，输入用于托管 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**
>
> 在此环境中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。有关更多信息，请参阅 设置亚马逊弹性 VMware 服务。

> **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。
- 有关`--vcf-version`，the section called “VCF 版本和实例 EC2 ”请参阅 Amazon EVS 提供的 VCF 版本，
- 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（适用于 VCF 的 v VMware Sphere 8 Enterprise Plus）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。如果配置公用 HCX VLAN，则必须指定网络掩码长度恰好为 /28 的 CIDR 块。如果为公共 HCX VLAN 指定了任何其他 CIDR 块大小，Amazon EVS 将引发验证错误。对于私有 HCX VLAN 和所有其他 VLANs CIDR 块，您可以使用的最小网络掩码长度为 /28，最大值为 /24。
- `hcxNetworkAclId`用于配置 HCX 互联网连接。为公共 HCX VLAN 指定自定义网络 ACL。

> **Important**
>
> 我们强烈建议您创建专用 HCX VLAN 的自定义网络 ACL。有关更多信息，请参阅 the section called “配置网络 ACL”。

> **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。专用主机 ID 是可选的。

> **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**
>
> 在部署 EVS 之前，Amazon EVS 需要一个与两个路由服务器终端节点和两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，请输入您唯一的 Broadcom 网站 ID。此 ID 支持访问 Broadcom 门户，由 Broadcom 在软件合同结束或合同续订时提供给您。
- （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-5.2.2 \
--terms-accepted \
--license-info "{
      \"solutionKey\": \"00000-00000-00000-abcde-11111\",
      \"vsanKey\": \"00000-00000-00000-abcde-22222\"
    }" \
   --initial-vlans "{
      \"isHcxPublic\": true,
      \"hcxNetworkAclId\": \"nacl-abcd1234\",
      \"vmkManagement\": {
        \"cidr\": \"10.10.0.0/24\"
      },
      \"vmManagement\": {
        \"cidr\": \"10.10.1.0/24\"
      },
      \"vMotion\": {
        \"cidr\": \"10.10.2.0/24\"
      },
      \"vSan\": {
        \"cidr\": \"10.10.3.0/24\"
```

```
      },
      \"vTep\": {
        \"cidr\": \"10.10.4.0/24\"
      },
      \"edgeVTep\": {
        \"cidr\": \"10.10.5.0/24\"
      },
      \"nsxUplink\": {
        \"cidr\": \"10.10.6.0/24\"
      },
      \"hcx\": {
        \"cidr\": \"10.10.7.0/24\"
      },
      \"expansionVlan1\": {
        \"cidr\": \"10.10.8.0/24\"
      },
      \"expansionVlan2\": {
          \"cidr\": \"10.10.9.0/24\"
      }
    }" \
--hosts "[
    {
      \"hostName\": \"esx01\",
      \"keyName\": \"sshKey-04-05-45\”,
      \"instanceType\": \"i4i.metal\",
      \"dedicatedHostId\": \"h-07879acf49EXAMPLE\"
    },
    {
      \"hostName\": \"esx02\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\",
      \"dedicatedHostId\": \"h-07878bde50EXAMPLE\"
    },
    {
      \"hostName\": \"esx03\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\",
      \"dedicatedHostId\": \"h-07877eio51EXAMPLE\"
    },
    {
      \"hostName\": \"esx04\",
      \"keyName\": \"sshKey-04-05-45\",
      \"instanceType\": \"i4i.metal\",
      \"dedicatedHostId\": \"h-07863ghi52EXAMPLE\"
```

```
    }
  ]" \
--connectivity-info "{
    \"privateRouteServerPeerings\": [\"rsp-1234567890abcdef0\",\"rsp-
abcdef01234567890\"]
  }" \
  --vcf-hostnames "{
    \"vCenter\": \"vcf-vc01\",
    \"nsx\": \"vcf-nsx\",
    \"nsxManager1\": \"vcf-nsxm01\",
    \"nsxManager2\": \"vcf-nsxm02\",
    \"nsxManager3\": \"vcf-nsxm03\",
    \"nsxEdge1\": \"vcf-edge01\",
    \"nsxEdge2\": \"vcf-edge02\",
    \"sddcManager\": \"vcf-sddcm01\",
    \"cloudBuilder\": \"vcf-cb01\"
  }" \
--site-id my-site-id \
--region us-east-2
```

以下为示例响应。

```
{
    "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-5.2.2",
        "termsAccepted": true,
        "licenseInfo": [
            {
                "solutionKey": "00000-00000-00000-abcde-11111",
                "vsanKey": "00000-00000-00000-abcde-22222"
            }
        ],
```

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

# 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-5.2.2",
        "termsAccepted": true,
        "licenseInfo": [
            {
                "solutionKey": "00000-00000-00000-abcde-11111",
                "vsanKey": "00000-00000-00000-abcde-22222"
            }
        ],
        "siteId": "my-site-id",
        "checks": [],
        "connectivityInfo": {
            "privateRouteServerPeerings": [
                "rsp-056b2b1727a51e956",
                "rsp-07f636c5150f171c3"
```

```
            ]
        },
        "vcfHostnames": {
            "vCenter": "vcf-vc01",
            "nsx": "vcf-nsx",
            "nsxManager1": "vcf-nsxm01",
            "nsxManager2": "vcf-nsxm02",
            "nsxManager3": "vcf-nsxm03",
            "nsxEdge1": "vcf-edge01",
            "nsxEdge2": "vcf-edge02",
            "sddcManager": "vcf-sddcm01",
            "cloudBuilder": "vcf-cb01"
        },
        "credentials": []
    }
}
```

# 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。如果您创建了公有 HCX VLAN，请务必将公有 HCX VLAN 子网与您的 VPC 中路由到互联网网关的公共路由表明确关联。

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
```

## 关联 EIPs 到 HCX 公有 VLAN 子网（用于 HCX 互联网连接）

按照以下步骤将弹性 IP 地址 (EIPs) 从 IPAM 池关联到 HCX 公共 VLAN，以实现 HCX 互联网连接。您需要为 HCX Manager 和 HCX Interconnect (HCX-IX) 设备关联至少两个 EIPs 设备。为需要部署的每个 HCX 网络设备关联一个额外的 EIP。在 IPAM 池中，您最多可以有 13 EIPs 个与 HCX 公共 VLAN 相关联。

**Important**

如果您没有将 IPAM 池中的至少两个 EIPs 与 HCX 公有 VLAN 子网关联，HCX 公共互联网连接就会失败。

**Note**

Amazon EVS 目前仅支持与 HCX VLAN 关联 EIPs 。

**Note**

您无法将公有 IPAM CIDR 块中的前两个 EIPs 或最后一个 EIP 与 VLAN 子网关联。 EIPs 这些地址保留为网络、默认网关和广播地址。如果您尝试将其与 VLAN 子网关联，Amazon EVS 会引 EIPs 发验证错误。

Amazon EVS console

1. 前往 Amazon EVS 控制台。

2. 在导航菜单上，选择环境。
3. 选择环境。
4. 在 “网络和连接” 选项卡下，选择 HCX 公共 VLAN。
5. 选择将 EIP 关联到 VLAN。
6. 选择要与 HCX 公共 VLAN 关联的弹性 IP 地址。
7. 选择关联 EIPs。
8. 检查 EIP 关联以确认它们 EIPs 已与 HCX 公用 VLAN 关联。

AWS CLI

1. 要将弹性 IP 地址与 VLAN 相关联，请使用示例`associate-eip-to-vlan`命令。
   - `environment-id`-您的亚马逊 EVS 环境的 ID。
   - `vlan-name`-要与弹性 IP 地址关联的 VLAN 的名称。
   - `allocation-id`-弹性 IP 地址的分配 ID。

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

   该命令返回有关 VLAN 的详细信息，包括新的 EIP 关联：

   ```
   {
       "vlan": {
           "vlanId": 80,
           "cidr": "18.97.137.0/28",
           "availabilityZone": "us-east-2c",
           "functionName": "hcx",
           "subnetId": "subnet-02f9a4ee9e1208cfc",
           "createdAt": "2025-08-22T23:42:16.200000+00:00",
           "modifiedAt": "2025-08-23T13:42:28.155000+00:00",
           "vlanState": "CREATED",
           "stateDetails": "VLAN successfully created",
           "eipAssociations": [
               {
                   "associationId": "eipassoc-09e966faad7ecc58a",
                   "allocationId": "eipalloc-0429268f30c4a34f7",
                   "ipAddress": "18.97.137.2"
   ```

```
            }
        ],
        "isPublic": true,
        "networkAclId": "acl-02fa8ab4ad3ddfb00"
    }
}
```

该eipAssociations数组显示了新的关联，包括：

- associationId-此 EIP 关联的唯一 ID，用于取消关联。
- allocationId-关联弹性 IP 地址的分配 ID。
- ipAddress-分配给 VLAN 的 IP 地址。

2. 重复该步骤以关联其他 EIPs。

### 为本地连接配置中转网关路由表和 Direct Connect 前缀（可选）

如果您使用传输网关 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。

## 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 凭据以及 ESX 根密码。有关检索密钥的更多信息，请参阅 Secrets Manager 用户指南中的从 S AWS ecrets Manager 获取 AWS 密钥。

> **Note**
>
> Amazon EVS 不提供密钥的托管式轮换。我们建议您在设定的轮换时段内定期轮换密钥，以确保密钥不会长期有效。

从 S AWS ecrets Manager 检索 VCF 凭据后，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（可选）

默认情况下，Amazon EVS 在新部署的亚马逊 EVS 主机上启用 ESX Shell。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 ESX 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 ESX 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 ESX Shell 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

Amazon EVS console

1. 前往 Amazon EVS 控制台。
2. 在导航窗格中，选择环境。
3. 选择包含要删除的主机的环境。
4. 选择 “主机” 选项卡。
5. 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。
6. 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。

7. 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。

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

3. 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
```

4. 重复前面的步骤，删除环境中剩余的主机。
5. 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。

6. 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 IPAM 资源（用于 HCX 互联网连接）

如果您已配置 HCX 互联网连接，请按照以下步骤删除您的 IPAM 资源。

1. 从公共 IPAM 池中释放 EIP 分配。有关更多信息，请参阅《VPC IP 地址管理器用户指南》中的释放分配。
2. 从 IPAM 池中取消配置公共 IPv4 CIDR。有关更多信息，请参阅《VPC IP 地址管理器用户指南》中的 CIDRs 从池中取消配置。
3. 删除公共 IPAM 池。有关更多信息，请参阅《VPC IP 地址管理器用户指南》中的删除池。
4. 删除 IPAM。有关更多信息，请参阅 V P C IP 地址管理器用户指南中的删除 IP AM。

## 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。

## 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 HCX 将工作负载迁移到 Amazon EVS VMware

部署 Amazon EVS 后，您可以通过私有或公共互联网连接部署 VMware HCX，以便于将工作负载迁移到 Amazon EVS。有关更多信息，请参阅 HC VMware X 用户指南中的 VMware HCX 入门。

**Important**

通常不建议在以下情况下进行基于 HCX 互联网的迁移：

- 对网络抖动或延迟敏感的应用程序。
- 时间紧迫的 vMotion 操作。
- 具有严格性能要求的大规模迁移。

对于这些场景，我们建议使用 HCX 私有连接。与基于互联网的连接相比，私有专用连接可提供更可靠的性能。

## HCX 连接选项

您可以使用带有 Di AWS rect Connect 或 Site-to-Site VPN 连接的私有连接，或者使用公共连接，将工作负载迁移到 Amazon EVS。

根据您的情况和连接选项，您可能更喜欢在 HCX 上使用公共或私有连接。例如，某些站点可能具有私有连接，性能一致性更高，但由于 VPN 加密或链路速度有限，吞吐量会降低。同样，您可能拥有高吞吐量的公共互联网连接，其性能差异更大。借助 Amazon EVS，您可以选择使用最适合自己的连接选项。

下表比较了 HCX 私有连接和公有连接之间的区别。

| 私有连接 | 公有连接 |
| --- | --- |
| 概述 | 概述 |
| 仅使用 VPC 内的私有连接。您可以选择将 Di AWS rect Connect 或 Site-to-Site VPN 与传输网关一起使用，以实现外部网络连接。 | 使用带有弹性 IP 地址的公共互联网连接，无需专用的私有连接即可进行迁移。 |

| 私有连接 | 公有连接 |
| --- | --- |
| 最适合 | 最适合 |
| • 对时间敏感的 vMotion 操作。<br>• 大规模迁移。<br>• 对延迟/抖动敏感的应用程序。<br>• 大容量数据传输。<br>• 已有 AWS 直接连接/VPN AWS Site-to-Site 的组织。 | • 没有 AWS 直接连接/VPN AWS Site-to-Site 的地点。<br>• 成本敏感型项目。 |
| 主要优势 | 主要优势 |
| • 一致的低延迟连接。<br>• 专用带宽分配。<br>• 更可靠的网络性能。<br>• 可以为私有环境禁用默认 HCX 加密以优化性能。<br>• 无需管理公有 IP。 | • 设置速度比私有连接更快。<br>• 对于较小的迁移来说，成本效益高。 |
| 重要注意事项 | 重要注意事项 |
| • 更复杂的初始设置。<br>• 更高的前期基础架构成本。<br>• 更长的实施时间表。<br>• 任何 HCX 组件都没有直接的互联网连接。 | • 网络性能变化更大。<br>• 可能存在带宽限制。<br>• 延迟高于私有连接。<br>• 每个组件都需要一个从公共 IPAM 池中分配的专用弹性 IP 地址。<br>• EIP 关联可为每个 HCX 组件提供直接的互联网连接。 |

# HCX 私有连接架构

HCX 私有连接解决方案集成了多个组件：

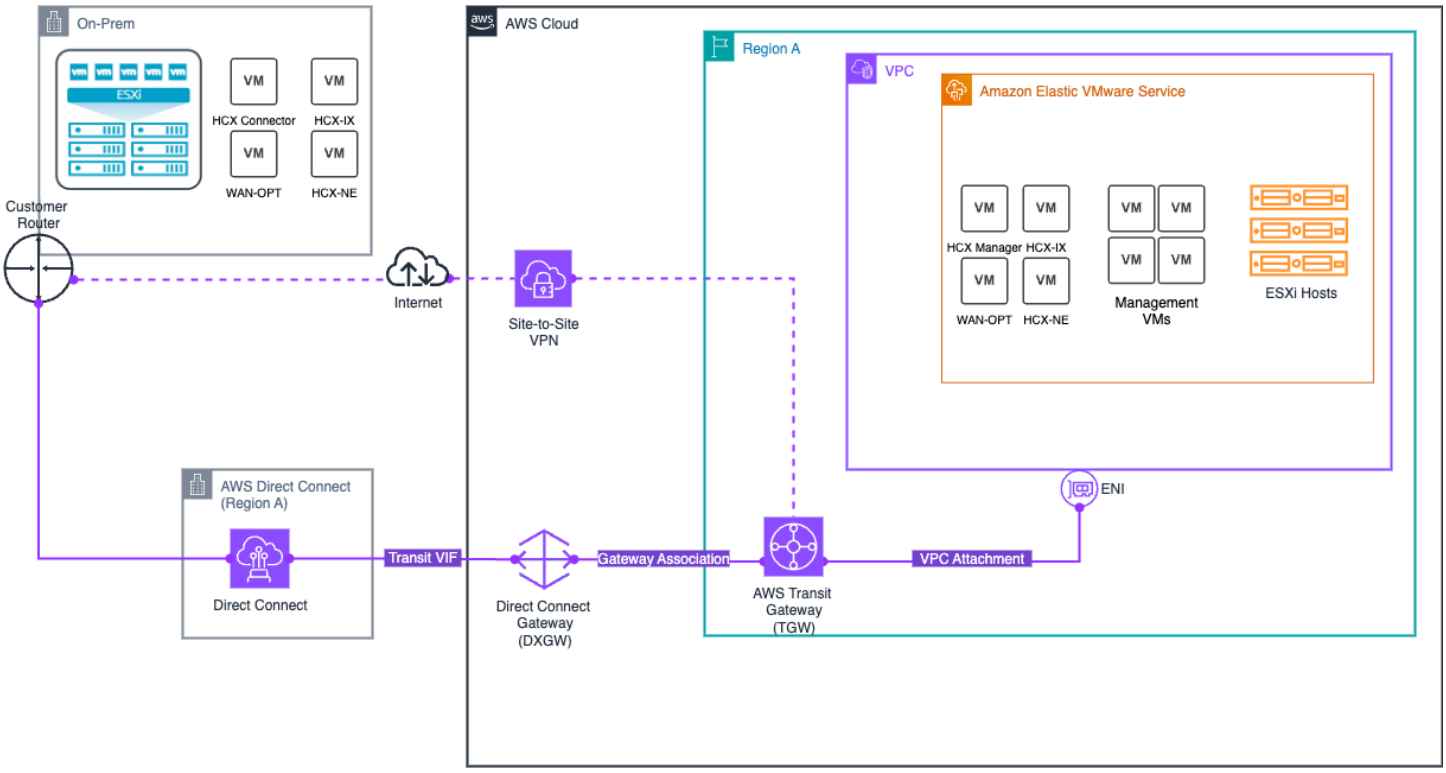
- 亚马逊 EVS 网络组件

- 仅使用专用 VLAN 子网进行安全通信，包括专用 HCX VLAN。
- 支持网络 ACLs 进行流量控制。
- 支持通过私有 VPC 路由服务器对路由进行动态 BGP 传播。

- AWS 用于本地连接的托管网络传输选项
  - AWS Direct Connect + Tr AWS ansit Gateway 使您能够通过私有专用连接将本地网络连接到亚马逊 EVS。有关更多信息，请参阅 AWS Direct Connect + T AWS ransit Gateway。
  - AWS Site-to-Site VPN + T AWS ransit Gateway 提供了通过互联网在远程网络和传输网关之间创建 IPsec VPN 连接的选项。有关更多信息，请参阅 T AWS ransit Gateway + AWS Site-to-Site VPN。

> **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。

下图说明了 HCX 私有连接架构，显示了如何将 Di AWS rect Connect 和 Site-to-Site VPN 与传输网关配合使用，通过私有专用连接实现安全的工作负载迁移。



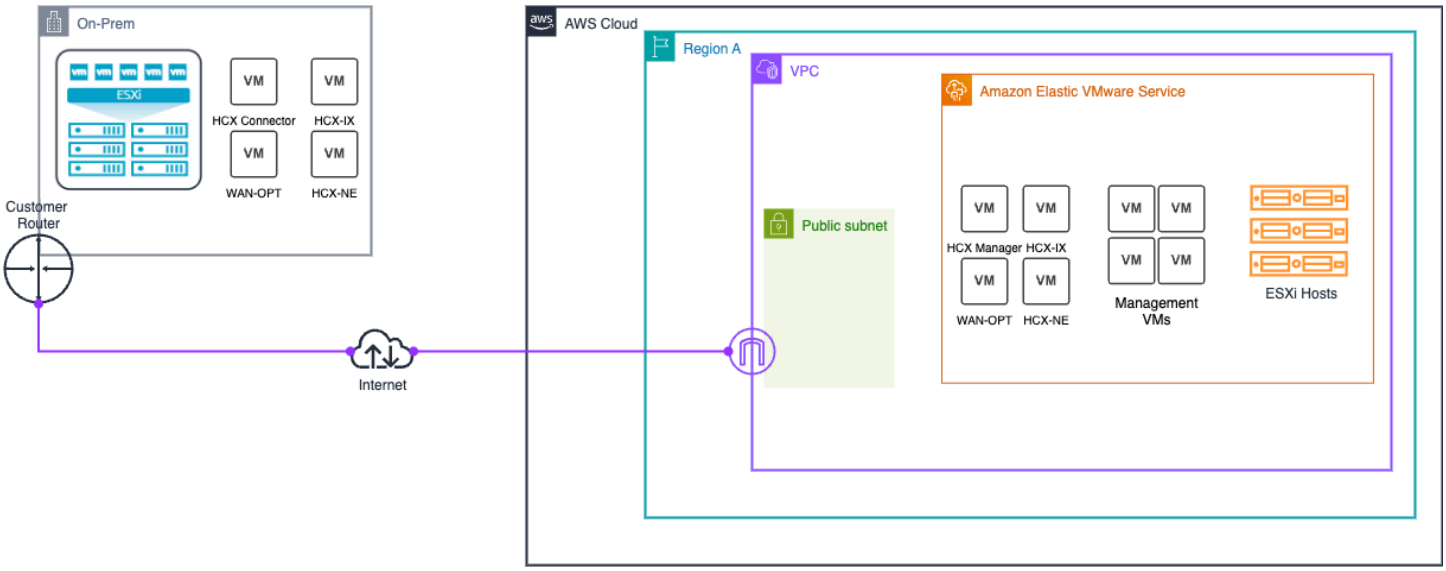
# HCX 互联网连接架构

HCX 互联网连接解决方案由几个协同工作的组件组成：

- 亚马逊 EVS 网络组件
  - 使用隔离的公有 HCX VLAN 子网在 Amazon EVS 和您的本地 HCX 设备之间实现互联网连接。
  - 支持网络 ACLs 进行流量控制。
  - 支持通过公共 VPC 路由服务器对路由进行动态 BGP 传播。
- IPAM 和公共知识产权管理
  - 亚马逊 VPC IP 地址管理器 (IPAM) 管理亚马逊拥有的公有 IPAM 池中的公共 IPv4 地址分配。
  - 辅助 VPC CIDR 块 (/28) 从 IPAM 池中分配，从而创建一个与主 VPC CIDR 分开的隔离公有子网。

有关更多信息，请参阅 the section called “HCX 公共连接”。

下图说明了 HCX 互联网连接架构。




# HCX 迁移设置

本教程介绍如何配置 VMware HCX 以将您的工作负载迁移到 Amazon EVS。

## 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。有关更多信息，请参阅 the section called “VMware HCX 先决条件”。

> **Important**
>
> Amazon EVS 对 HCX 公共互联网连接有独特的要求。
> 如果您需要 HCX 公共连接，则必须满足以下要求：
>
> - 使用 CIDR 创建一个 IPAM 和一个最小 IPv4 网络掩码长度为 /28 的公共 IPAM 池。
> - 从 IPAM 池中为 HCX Manager 和 HCX Interconnect (HCX-IXEIPs) 设备分配至少两个弹性 IP 地址 ()。为需要部署的每台 HCX 网络设备分配额外的弹性 IP 地址。
> - 将公有 IPv4 CIDR 块作为其他 CIDR 添加到您的 VPC。
>
> 有关更多信息，请参阅 the section called “HCX 互联网连接设置”。

## 检查 HCX VLAN 子网的状态

作为标准 Amazon EVS 部署的一部分，将为 HCX 创建一个 VLAN。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 并检查状态是否为 “已创建”，“公用” 是否为真。

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
```

2. 在响应输出中，标识为functionNamevlanState的 VLAN，hcxCREATED并检查是否设置isPublic为true。以下为示例响应。

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

```
        }
    ]
}
```

## 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”。

**Important**

如果您通过互联网连接，则将弹性 IP 地址与 VLAN 关联可直接访问该 VLAN 上的所有资源。确保配置了适当的网络访问控制列表，以根据您的安全要求限制访问。

**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 (ACL)。

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。

## 检查 EVS VLAN 子网是否与路由表显式关联

Amazon EVS 要求所有 EVS VLAN 子网都必须与您的 VPC 中的路由表显式关联。对于 HCX 互联网连接，您的 HCX 公有 VLAN 子网必须与您的 VPC 中路由到互联网网关的公共路由表显式关联。按照以下步骤检查显式路由表关联。

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. 选择您的 EVS VLAN 子网应与之明确关联的路由表。
4. 选择子网关联选项卡。
5. 在 “显式子网关联” 下，检查是否列出了所有 EVS VLAN 子网。如果此处未列出 VLAN 子网，则该 VLAN 子网与主路由表隐式关联。要让 Amazon EVS 正常运行，您必须将所有 VLAN 子网与路由表明确关联。对于 HCX 公有 VLAN 子网，必须有一个以互联网网关为目标的关联公共路由表。要解决此问题，请选择编辑子网关联并添加缺少的 VLAN 子网。

AWS CLI

1. 打开终端会话。
2. 运行以下示例命令以检索所有 EVS VLAN 子网的详细信息，包括路由表关联。如果此处未列出 VLAN 子网，则该 VLAN 子网与主路由表隐式关联。要让 Amazon EVS 正常运行，您必须将所有 VLAN 子网与路由表明确关联。对于 HCX 公有 VLAN 子网，必须有一个以互联网网关为目标的关联公共路由表。

```
aws ec2 describe-subnets
```

3. 显式关联您的 EVS VLAN 子网与您的 VPC 中的路由表。以下是一个命令示例。

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

# （对于 HCX 互联网连接）检查 EIPs 是否与 HCX VLAN 子网相关联

对于您部署的每个 HCX 网络设备，您都必须拥有一个来自 IPAM 池的 EIP，与 HCX 公有 VLAN 子网相关联。您需要将至少两个 EIPs 与 HCX Manager 和 HCX Interconnect (HCX-IX) 设备的 HCX 公有 VLAN 子网关联。按照以下步骤检查是否存在必要的 EIP 关联。

**Important**

如果您没有将 IPAM 池中的至少两个 EIPs 与 HCX 公有 VLAN 子网关联，HCX 公共互联网连接就会失败。

**Note**

您不能将公有 IPAM CIDR 块中的前两个 EIPs 或最后一个 EIP 与 VLAN 子网关联。 EIPs 这些地址保留为网络、默认网关和广播地址。如果您尝试将其与 VLAN 子网关联，Amazon EVS 会引 EIPs 发验证错误。

Example

Amazon EVS console

1. 前往 Amazon EVS 控制台。
2. 在导航菜单上，选择环境。
3. 选择环境。
4. 在 “网络和连接” 选项卡下，选择 HCX 公共 VLAN。
5. 检查 EIP 关联选项卡，确认 EIPs 已与 HCX 公共 VLAN 关联。

AWS CLI

1. 要检查 EIPs 哪些与 HCX VLAN 子网关联，请使用`list-environment-vlans`命令。对于`environment-id`，请使用包含 HCX VLAN 的 EVS 环境的唯一 ID。

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

该命令会返回有关您的详细信息 VLANs，包括 EIP 关联：

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

该eipAssociations数组显示 EIP 关联，包括：

- associationId-此 EIP 关联的唯一 ID。
- allocationId-关联弹性 IP 地址的分配 ID。

- ipAddress-分配给 VLAN 的 IP 地址。

## 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

> **Note**
>
> HCX 4.11.3 中不再提供广域网优化功能。有关更多信息，请参阅 HCX 4.11.3 发行说明。

HCX 广域网优化服务 (HCX-WO) 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-IX) 一起部署。HCX-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 允许您在扩展第 2 层网络时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 包括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。

# 配置 HCX 公共互联网连接

您可以通过将弹性 IP 地址与 VLAN 关联来为 HCX 公共 VLAN 配置公共互联网接入。这为需要互联网访问才能进行迁移操作的 VMware HCX 设备和工作负载提供了直接的互联网连接。

## 相关主题

本主题介绍管理 HCX 公共 VLAN 的互联网接入。要完成实施，请执行以下操作：

1. 完成中的先决条件设置亚马逊弹性 VMware 服务。
2. 在中配置初始设置开始使用。
3. 配置互联网接入（本主题）。

## 关于 HCX VLAN 互联网接入

您可以为 VMware HCX 设备配置互联网接入，从而允许您通过互联网将工作负载迁移到 Amazon EVS 的 HCX。

这种方法：

- 无需专用的专用连接即可实现虚拟机迁移。

- 提供灵活、经济实惠的迁移解决方案。

> **Important**
>
> 通常不建议在以下情况下进行基于 HCX 互联网的迁移：
>
> - 对网络抖动或延迟敏感的应用程序。
> - 时间紧迫的 vMotion 操作。
> - 具有严格性能要求的大规模迁移。
>
> 对于这些场景，我们建议使用 HCX 私有连接。与基于互联网的连接相比，私有专用连接可提供更可靠的性能。

## 互联网连接概述

请查看以下注意事项。

### HCX 网络要求和 DNAT

HCX 有特定的网络限制，会影响您设置公共互联网接入的方式。

HCX 不支持目标网络地址转换 (DNAT)。相反，HCX 要求上行链路网络可使用默认网关 IP 地址进行路由。

与其他 VPC 子网一样，Amazon EVS VLAN 子网包含默认网关 IP 地址。但是，即使您使用地址范围之外的 CIDR 块，这些子网也始终是私有子网。 RFC1918

启用 HCX 互联网连接

为了在没有 DNAT 的情况下启用互联网连接，Amazon EVS 使用了特定的 CIDR 配置方法：

- 互联网可路由 CIDR 要求：Amazon EVS 需要与您的 HCX VLAN 子网 CIDR 匹配的可互联网路由 CIDR。
- IPAM 分配：Amazon EVS 使用最小网络掩码长度为 /28 的公有 IPAM 分配的 CIDR 作为互联网可路由的 CIDR。
- VPC 配置：您必须手动将 IPAM 分配的公有 CIDR 作为辅助 VPC CIDR 添加到您的 VPC。

- VLAN 子网部署：配置 IPAM 和 VPC 后，您可以在 Amazon EVS 部署期间在 HCX VLAN 子网中使用公有 IPAM 分配的 CIDR。
- 弹性 IP 配置：Amazon EVS 需要以下配置：
  - 分配弹性 IPs：您可以 IPs 从 IPAM 分配的 CIDR 中分配弹性。您必须从 IPAM 池中为 HCX Manager 和 HCX Interconnect (HCX-IXEIPs) 设备分配至少两个弹性 IP 地址 ()。为需要部署的每台 HCX 网络设备分配额外的弹性 IP 地址。
  - 与 VLAN 关联：将要与 HCX 设备一起使用的每个弹性 IP 关联到 HCX VLAN 子网。使用 Amazon EVS 控制台或 AWS CLI 进行此关联。
  - 配置网关地址：来自 CIDR 的第一个可用地址将成为您在 HCX 设备中配置的网关地址。
  - 流量路由：每个关联的弹性 IP 的流量直接路由到具有相同 IP 地址的目标 HCX 设备，无需使用 DNAT。

有关为 Amazon EVS 环境部署配置 HCX 的互联网连接的步骤，请参阅设置亚马逊弹性 VMware 服务和。开始使用

## 操作注意事项

- HCX 公共 VLAN CIDR 块的网络掩码长度必须为 /28。
- EIPs 使用 Amazon EVS 控制台部署后可以与 HCX 公用 VLAN 关联或取消关联 AWS CLI，但它们必须来自同一 IPAM 池。
- 每个 EIP 关联都有自己唯一的关联 ID。
- 公共 IPAM 池 EIPs 中最多可以有 13 个与 /28 HCX 公共 VLAN 相关联。您无法将公有 IPAM 分配的 CIDR 块中的前两个 EIPs 或最后一个 EIP 与 HCX 公有 VLAN 子网关联。 EIPs 这些地址保留为网络、默认网关和广播地址。如果您尝试将其与 VLAN 关联，Amazon EVS 会引发 EIPs 验证错误。

## 安全注意事项

- 网络访问控制列表 (ACLs) 仍然适用于流经 HCX 公有 VLAN 子网的流量。
- 安全组规则不适用于 HCX 公有 VLAN 子网上的流量。使用网络 ACLs 进行流量控制。

> **Important**
>
> 如果您通过互联网连接，则将弹性 IP 地址与 VLAN 关联可直接访问该 VLAN 上的所有资源。确保您配置了适当的网络访问控制列表，以根据您的安全要求限制访问。

# 管理弹性 IP 地址 VLANs

您可以使用 Amazon EVS 控制台或，将弹性 IP 地址与 HCX 公共 VLAN 关联和取消关联。 AWS CLI

> **Note**
>
> 目前，Amazon EVS 仅支持将弹性 IP 地址与 HCX 公有 VLAN 关联和取消关联。

## 将弹性 IP 地址与 VLAN 相关联

### 先决条件

请确保您具备以下条件：

- 弹性 IP 地址是从亚马逊拥有的公有 IPAM 池中分配的。
- 亚马逊 EVS 环境已经创建。

### Example

Amazon EVS console

1. 前往 Amazon EVS 控制台。
2. 在导航菜单上，选择环境。
3. 选择环境。
4. 在 “网络和连接” 选项卡下，选择 HCX 公共 VLAN。

   > **Note**
   >
   > Amazon EVS 目前仅支持与 HCX VLAN 关联 EIPs 。

5. 选择将 EIP 关联到 VLAN。
6. 选择要与 HCX 公共 VLAN 关联的弹性 IP 地址。
7. 选择关联 EIPs。您最多可以有 13 个 EIPs 与 HCX 公共 VLAN 相关联。

> **Note**
>
> 您无法将公有 IPAM CIDR 块 EIPs 中的前两个与 VLAN 子网相关联。 EIPs 这些地址保留为网络地址和默认网关地址。

8. 检查 EIP 关联以确认它们 EIPs 已与 HCX 公用 VLAN 关联。

AWS CLI

1. 要将弹性 IP 地址与 VLAN 相关联，请使用示例`associate-eip-to-vlan`命令。
   - `environment-id`-您的亚马逊 EVS 环境的 ID。
   - `vlan-name`-一定是`hcx`。Amazon EVS 目前仅支持与 HCX VLAN 的 EIP 关联。
   - `allocation-id`-弹性 IP 地址的分配 ID。

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

   该命令返回有关 VLAN 的详细信息，包括新的 EIP 关联：

```
{
    "vlan": {
        "vlanId": 80,
        "cidr": "18.97.137.0/28",
        "availabilityZone": "us-east-2c",
        "functionName": "hcx",
        "subnetId": "subnet-02f9a4ee9e1208cfc",
        "createdAt": "2025-08-22T23:42:16.200000+00:00",
        "modifiedAt": "2025-08-23T13:42:28.155000+00:00",
        "vlanState": "CREATED",
        "stateDetails": "VLAN successfully created",
        "eipAssociations": [
            {
                "associationId": "eipassoc-09e966faad7ecc58a",
                "allocationId": "eipalloc-0429268f30c4a34f7",
                "ipAddress": "18.97.137.2"
            }
        ],
```

```
        "isPublic": true,
        "networkAclId": "acl-02fa8ab4ad3ddfb00"
    }
}
```

该eipAssociations数组显示了新的关联，包括：

- associationId-此 EIP 关联的唯一 ID，用于取消关联。
- allocationId-关联弹性 IP 地址的分配 ID。
- ipAddress-分配给 VLAN 的 IP 地址。

2. 重复该步骤以关联其他 EIPs。您最多可以有 13 个 EIPs 与 HCX 公共 VLAN 相关联。

## 取消弹性 IP 地址与 VLAN 的关联

### 先决条件

请确保您具备以下条件：

- 亚马逊 EVS 环境已经创建。
- EIP 与 Amazon EVS 环境相关联。

### Example

Amazon EVS console

1. 前往 Amazon EVS 控制台。
2. 在导航菜单上，选择环境。
3. 选择环境。
4. 在 “网络和连接” 选项卡下，选择 HCX 公共 VLAN。
5. 选择解除 EIP 与 VLAN 的关联。
6. 选择要取消与 HCX 公共 VLAN 关联的弹性 IP 地址。

> **Important**
> 取消关联 EIPs 可能会导致使用公共 VLAN 子网的设备断开互联网连接。

7. 选择取消关联 EIPs。

8. 检查 EIP 关联以确认 EIPs 已取消与 HCX 公共 VLAN 的关联。

AWS CLI

要取消弹性 IP 地址与 VLAN 的关联，请使用示例`disassociate-eip-from-vlan`命令。

- `environment-id`-您的亚马逊 EVS 环境的 ID。
- `vlan-name`-一定是`hcx`。Amazon EVS 目前仅支持与 HCX VLAN 的 EIP 关联。
- `association-id`-要删除的 EIP 关联的关联 ID。

> **Important**
>
> 取消关联 EIPs 可能会导致使用公共 VLAN 子网的设备断开互联网连接。

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

该命令返回有关已删除 EIP 关联的 VLAN 的详细信息：

```
{
    "vlan": {
        "vlanId": 80,
        "cidr": "18.97.137.0/28",
        "availabilityZone": "us-east-2c",
        "functionName": "hcx",
        "subnetId": "subnet-02f9a4ee9e1208cfc",
        "createdAt": "2025-08-22T23:42:16.200000+00:00",
        "modifiedAt": "2025-08-23T13:48:49.846000+00:00",
        "vlanState": "CREATED",
        "stateDetails": "VLAN successfully created",
        "eipAssociations": [],
        "isPublic": true,
        "networkAclId": "acl-02fa8ab4ad3ddfb00"
    }
}
```

空eipAssociations数组确认弹性 IP 地址已成功解除与 VLAN 的关联。

## 关于基于互联网的迁移的 HCX 广域网优化

> **Note**
>
> HCX 4.11.3 中不再提供广域网优化功能。有关更多信息，请参阅 HCX 4.11.3 发行说明。

通过互联网执行迁移时，HCX 广域网优化 (HCX-WO) 可以提高迁移性能。该服务与 HCX 互连设备 (HCX-IX) 配合使用，可以：

- 应用数据减少技术以最大限度地减少带宽使用量。
- 实施 WAN 路径调节以优化网络性能。
- 通过高延迟互联网连接提高迁移速度。
- 增强基于互联网的迁移的可靠性。

HCX 广域网优化对于基于互联网的迁移特别有用，其中：

- 网络延迟可能高于私有连接选项。
- 可用带宽可能有限或可变。
- 网络状况可能会因互联网流量模式而波动。

有关在配置互联网连接后设置 HCX WAN 优化的详细说明，请参阅the section called “（可选）设置 HCX 广域网优化”。

> **Note**
>
> 尽管广域网优化可以显著提高基于互联网的迁移性能，但在具有专用 10Gbit、低延迟连接的环境中，它可能无法提供额外的好处。在决定是否启用此功能时，请考虑您的网络特征。

# 管理 Amazon EVS 环境

本章包括以下主题，可帮助您管理环境。

- the section called “VCF 订阅”-描述 VCF 订阅如何与 Amazon EVS 配合使用，以及客户对 VCF 订阅管理的责任。
- the section called “VCF 版本和实例 EC2 ”-描述支持的 VCF 和 ESX 版本以及如何在 Amazon EVS 中查看版本可用性。
- the section called “生命周期管理”-描述 Amazon EVS 环境中的生命周期管理职责，包括底层基础设施管理、VCF 升级管理、ESX 主机生命周期管理。
- the section called “环境维护”-介绍如何为您的 Amazon EVS 环境执行常见维护任务，包括网络配置、ESX 主机维护、检查环境状态以及管理 VCF 凭证的密钥轮换计划。
- the section called “创建主机”-介绍如何在部署环境后创建 Amazon EVS 主机并将该主机添加到集群。
- the section called “删除主机”-介绍如何删除 Amazon EVS 主机并将其从集群中移除。

## VCF 订阅

> **Note**
>
> Amazon EVS 不支持永久的 vSphere 许可。您必须拥有有效且有效的 VMware 云基础订阅才能使用 Amazon EVS。

Amazon EVS 使用 VMware 云基金会 (VCF) 订阅以及您带给 AWS (BYOS) 的许可可移植性权利。要成功部署 Amazon EVS 环境，您需要在环境创建请求中提供有效的 VCF 解决方案密钥和 vSAN 许可密钥。vSphere 许可密钥用作 VCF 的解决方案密钥。每个 VCF 许可密钥只能用于一个 Amazon EVS 环境。如果您尝试使用已在其他环境中使用的 VCF 许可证密钥，则环境创建将失败。

您的 VCF 解决方案密钥必须至少有 256 个内核，才能为 Amazon EVS 在创建环境时部署的四个初始 EC2 i4i.metal 主机提供足够的核心容量。每台 i4i.metal 主机需要 64 个内核。vSAN 许可密钥必须至少有 110 TiB 的 vSAN 容量。如果您尝试使用大小过小的许可证密钥，则环境创建将失败。

> **Note**
>
> 您的 VCF 订阅将适用于所有 AWS 地区的 Amazon EVS，以满足许可证合规要求。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**
>
> 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。

## 订阅管理

您负责管理您的 VCF 订阅。您的 VCF 订阅必须在 SDDC 管理器中进行管理。从 SDDC Manager 中删除您的许可证密钥或将其替换为正在使用的许可密钥将导致环境状态检查失败，从而使您无法向 Amazon EVS 环境中添加主机。有关环境状态检查的更多信息，the section called “监控环境状态”以及the section called “对失败的环境状态检查进行故障排除”。有关 VCF 许可证密钥的更多信息，请参阅 Cloud Foundation 文档中的管理 VMware VMware 云基础中的许可证密钥。

> **Important**
>
> 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。虽然必须使用 vSphere Client 将密钥分配给您的主机和 vSAN 集群，但您必须确保这些密钥也显示在 SDDC Manager 用户界面的许可屏幕上。

## 添加 VCF 许可证密钥

在 Broadcom 支持门户中，您可以购买额外的 VCF 许可证密钥，如果您已经有大密钥，则可以拆分许可证密钥，或者合并多个许可证密钥。这允许您许可在初始部署后添加到环境中的主机，或许可其他环境。确保将购买的许可证密钥添加到 vCenter Sever 和 SDDC Manager 清单中。如果要添加主机，请确保将许可证分配给 vSphere 中的正确主机，并且有足够的内核和 vSAN 存储容量。Amazon EVS 不支持未经许可的主机。有关更多信息，请参阅文档中的在 vSphere Client 中为资产配置许可设置。VMware

在许可证密钥的评估期到期之前，必须将新的未过期许可密钥分配给 vCenter Server 才能保持有效状态。成功设置 Amazon EVS 环境需要有效的许可密钥。如果提供的许可证密钥已过期，则您的环境将

无法部署。有关创建 VCF 许可证密钥的更多信息，请参阅 VMware 文档中的创建新许可证。如果您在添加的许可证密钥时遇到问题，请参阅the section called “密钥覆盖率检查失败”。

## 正在删除 VCF 许可证密钥

删除环境中的主机后，您可以从 SDDC Manager 清单中删除 VCF 许可密钥以减少核心和 vSAN 容量。要符合与 vSphere 一起使用的产品的许可模式，必须从清单中移除所有未分配的许可密钥。如果您在 Broadcom Support Portal 中拆分、合并或升级了许可证密钥，则必须移除旧的许可密钥。有关更多信息，请参阅 VMware 文档中的移除许可证。

# Amazon EVS 提供的 VCF 版本和 EC2 实例类型

Amazon EVS 提供 VMware 云基础 (VCF)、ESX 和 EC2 实例类型的多个版本，您可以在创建环境和创建主机时选择这些版本。

## 正在检查提供的 VCF 版本、ESX 版本和实例类型 EC2

AWS 控制台在创建环境向导中显示 Amazon EVS 提供的 VCF 版本列表。当您在向现有环境中添加主机时选择实例类型时，可以看到可用的 ESX 版本。您还可以使用 CLI 查看 VCF 版本、ESX 版本和 EC2 实例类型。

Example

Amazon EVS console

1. 前往 Amazon EVS 控制台。
2. 在导航菜单上，选择环境。
3. 请执行以下操作之一：

   要检查 VCF 版本，请执行以下操作：

   a. 选择 “创建环境”。

   b. 在 “验证 Amazon EVS” 要求下，选择您的 VCF 版本，以查看该状态对您来说是可用还是受限。

   要检查 ESX 版本，请执行以下操作：

   a. 选择现有环境。

   b. 选择 Create host (创建主机)。

   c. 选择实例类型以查看可用的 ESX 版本。

AWS CLI

运行以下命令以检索有关 VCF 和 ESX 版本的信息：

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

示例响应：

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

> **Note**
>
> 如果您需要的版本已显示RESTRICTED，并且您有特殊需求，the section called “请求访问受限的 VCF 版本”请参阅，了解有关如何访问该版本的更多信息。

## 亚马逊 EVS 中的当前 VCF 版本

Amazon EVS 目前提供以下 VCF 版本用于创建环境：

| VCF 版本 | 默认 ESX 版本 | Status | EC2 实例类型 |
|---|---|---|---|
| VCF-5.2.2 | ESXi-8.0u3g-24859861 | AVAILABLE | i4i.metal |
| VCF-5.2.1 | ESXi-8.0u3b-24280767 | 限制 | i4i.metal |

> **Note**
>
> 创建新的 Amazon EVS 环境时，必须指定 VCF 版本。

## ESX 版本注意事项

每个 VCF 版本都有一个基于博通 VCF 物料清单 (BOM) 的默认 ESX 版本。创建新环境时，不能选择特定的 ESX 版本。所选 VCF 版本的默认 ESX 版本会自动应用。

但是，在向您的环境中添加主机时，您可以为所选的实例类型选择可用的 ESX 版本。如果您未指定，Amazon EVS 将使用与您的环境的 VCF 版本关联的默认 ESX 版本。

添加主机后，只能使用 vCenter 生命周期管理器升级其 ESX 版本。

> **Note**
>
> Amazon EVS 不提供博通发布的所有版本的 VCF 和 ESX。有关软件互操作性信息，请参阅 Broadcom 互操作性表。要了解与 AWS EC2 实例的完全硬件兼容性，请参阅 Broadcom 兼容性指南。

## 请求访问受限的 VCF 版本

如果您需要访问带有RESTRICTED状态的 VCF 版本，请联系 Su AWS pport 并提供以下信息：

- 你的 AWS 账户 ID
- 该 AWS 地区
- 你需要的具体 VCF 版本

- 您的用例和业务理由（例如security/compliance, compatibility/dependency、和其他）

AWS Support 将审核您的请求并批准或请求更多信息。批准后， AWS 控制台或 `get-versions` API 响应`AVAILABLE`中的版本状态将更改为。

# Amazon EVS 环境生命周期管理

本页描述了您在 Amazon EVS 环境中的生命周期管理职责。

Amazon EVS 的一个主要优势是，您可以完全控制自己的云端 VMware 架构。您可以优化 C VMware loud Foundation (VCF) 软件堆栈，以满足应用程序的独特需求。由于 Amazon EVS 是一项自我管理服务，因此您需要负责亚马逊云硬盘环境中使用的 VMware 软件（例如 ESX、vSphere、vSAN、NSX 和 SDDC Manager）的生命周期管理和维护。您还负责维护任何第三方集成，例如您集成到 Amazon EVS 主机中的数据保护解决方案。

您负责配置 Amazon EVS 使用的底层 AWS 网络组件，包括 VPC 路由表、安全组和网络访问控制列表 (ACL) 规则、VPC 路由服务器配置、互联网网关、NAT 网关和传输网关（用于本地连接）。

AWS 负责使用您提供的联网配置部署 Amazon EVS 环境。环境部署包括以下内容：

- 引导您的 Amazon EVS 环境的网络配置。
- 使用您提供的 VPC 路由服务器实例启用南北路由。
- 部署所需的 EVS VLAN 子网、弹性网络接口和四台初始 ESX 主机。
- 使用 Tier-0 网关和 Tier-1 网关配置 NSX 覆盖网络。
- 部署一个有两个 NSX Edge 节点处于模式的 NSX Edge 群集。 Active/Standby
- 创建和配置初始 vSAN 群集并装载数据存储。

您负责 VMware NSX 的配置，包括网段、分布式防火墙规则和负载均衡器。在 EVS 环境部署后，您还负责配置您通过 Amazon EVS 实施的任何集成解决方案，包括 VMware HCX 配置和其他 NSX Tier-1 网关。

有关客户责任 AWS 的更多信息，请参阅责任AWS 共担模型。

> **Note**
>
> 在 Amazon EVS 环境部署中，创建并配置了 Tier-0 网关和第 1 层网关。Amazon EVS 目前仅支持单个 Tier-0 网关。对这些逻辑路由器或 NSX Edge 节点的任何修改都 VMs 可能影响连接，因此应予以避免。

## VMware 软件更新

> **Warning**
>
> 如果您在部署 Amazon EVS 环境后更新了 ESX 版本，则在 “委托主机” 步骤中验证 VCF 主机期间，SDDC 管理器可能会失败。有关解决此问题的步骤，请参阅the section called “SDDC 管理器在主机调试期间无法验证 VCF 主机”。

有关 Amazon EVS 提供的 VCF 版本的信息，请参阅。the section called “VCF 版本和实例 EC2 ”根据责任AWS 共担模式，您负责在 EVS 环境中对 VCF 软件（包括 ESX、vCenter Server、vSAN、NSX、SDDC Manager 和其他集成解决方案）应用任何补丁、更新或升级。部署后，我们建议您查看 Amazon EVS 部署的 VCF 软件版本并根据需要进行更新。您可以通过 B roadcom 支持门户获取 VCF 更新。我们还建议您制定并遵守更新和补丁的定期维护计划。

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

> **Note**
>
> Amazon EVS 不提供博通发布的所有版本的 VCF 和 ESX。有关软件互操作性信息，请参阅 Broadcom 互操作性表。要了解与 AWS EC2 实例的完全硬件兼容性，请参阅 Broadcom 兼容性指南。

某些补丁、更新或升级可能会对您的环境中运行的工作负载产生影响。在修补、更新或升级 VCF 软件之前，我们建议您查看《VCF 生命周期管理指南》，以了解这些更改将如何影响您的环境。我们还建议您在部署到生产环境之前，先在暂存环境中测试更改。您可以查看 VCF 5.2.x 发行说明，了解最新的 VCF 5.2.x 更新。

# ESX 主机的生命周期和维护

您负责管理和维护 Amazon EVS 环境中的 ESX 主机生命周期，包括监控主机运行状况和修复主机问题。有关更多信息，请参阅 the section called “环境维护”。

AWS 对底层 i4i.metal EC2 实例执行定期维护，以确保基础架构的可靠性、可用性和性能。有关更多信息，请参阅 the section called “关于 EC2 实例的 AWS 定期维护”。

# 对您的环境进行维护

本节介绍如何为您的 Amazon EVS 环境执行常见维护任务。

主题

- 监控环境的状态和资源
- AMI 维护
- 亚马逊 EVS 主机维护
- 为 Amazon EVS 子网配置自定义路由表
- 配置网络访问控制列表以控制 Amazon EVS VLAN 子网流量
- 密钥管理生命周期

## 监控环境的状态和资源

您可以使用 Amazon EVS 控制台或监控您的 Amazon EVS 环境和底层 AWS 资源的各个方面。 AWS CLI

> **Note**
>
> VMware 云基础 (VCF) 组件在 SDDC 管理器中进行监控。您无法使用 Amazon EVS 控制台或监控 VCF 组件。 AWS CLI有关使用 SDDC 管理器监控 Cloud F VMware oundation (VCF) 组件的信息，请参阅 SDDC 管理器入门。

### 查看环境状态和资源

环境状态可帮助您确定您的环境是否遇到需要注意的问题。按照此过程检查环境的状态并查看底层资源。

Example

Amazon EVS console

1. 打开 Amazon EVS 控制台。
2. 在导航窗格中，选择环境。
3. 选择您的环境 ID 以打开环境详细信息页面。
4. 在 “详细信息” 下，查看环境状态。

   如果您的环境正常，则状态将显示为 “已通过”。如果存在问题，则状态将显示为 “失败”。当状态为 Fail e d 时，您可以查看弹出窗口，其中显示了四项环境状态检查的结果：

   - 密钥重复使用-显示 “已通过” 或 “失败”，以指示 VCF 许可证密钥是否有效。
   - 主机计数-显示 “未知”、“已通过” 或 “失败” 以指示主机连接状态。
   - 密钥覆盖率-显示 “已通过” 或 “失败”，以指示 VCF 许可证密钥是否涵盖所有主机。
   - 可接通性-显示 “通过” 或 “失败” 以指示 SDDC 管理器的可访问性。

   有关对环境状态检查失败进行故障排除的信息，请参阅问题排查。

   查看您环境中的资源

   选择以下选项卡之一：

   - 主机-显示您环境中的主机。
   - 网络和连接-显示与您的环境关联的 VPC、EVS 子网和 VPC 路由服务器资源。
   - 管理设备-显示您环境中的 VCF 管理设备及其的 DNS 主机名和相关凭据。
   - 标签-显示与您的环境关联的标签。

AWS CLI

您可以使用 AWS CLI 来检查您的环境状态和资源。

列出所有环境及其状态

```
aws evs list-environments
```

> **Tip**
>
> 使用--query参数筛选输出。例如：

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

列出环境主机

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

列出环境 VLANs

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

有关 API 操作的更多信息，请参阅 Amazon EVS API 参考指南中的以下内容：

- ListEnvironments
- ListEnvironmentHosts
- ListEnvironmentVlans

## AMI 维护

Amazon EVS 使用自定义 EVS Amazon 系统映像 (AMI) 部署 ESX 主机。AMI 包含一个自定义供应商插件，其中包含在亚马逊 EC2上运行 ESX 所需的软件包。

### 解决由于集群映像不兼容而导致的添加主机失败的问题

向环境中添加主机时，该主机将安装最新版本的 EVS 自定义供应商插件。如果您的环境使用带有较旧附加版本的主机，则添加新主机会失败，并显示新主机与您的集群映像不兼容的错误。有关修复此问题的详细步骤，请参阅the section called “添加由于集群映像不兼容而导致的主机故障”。

## 亚马逊 EVS 主机维护

由于 Amazon EVS 是一项自我管理服务，因此您负责维护在主机上运行的 C VMware loud Foundation (VCF) 软件、监控主机运行状况和修复主机问题，包括在主机出现故障时更换主机。有关在 Cloud F

VMware oundation (VCF) 中管理 ESX 主机的更多信息，请参阅 Cloud F VMware oundation 文档中的主机管理。

## 检查底层 EC2 实例的运行状况

Ama EC2 zon 会自动检查每个正在运行的 EC2 实例，以识别硬件和软件问题。您可以在 EC2 控制台中查看这些状态检查的结果，也可以确定可检测 AWS CLI 到的具体问题。有关更多信息，请参阅《亚马逊 EC2 用户指南》和《 AWS CLI 命令行参考》describe-instance-status中的 “查看亚马逊 EC2 实例的状态检查”。

您可以创建 CloudWatch 警报，以便在特定实例的状态检查失败时向您发出警报。有关更多信息，请参阅《亚马逊 EC2 用户指南》中的为状态检查失败的亚马逊 EC2 实例创建 CloudWatch 警报。

## 关于 EC2 实例的 AWS 定期维护

AWS 对底层 EC2 实例执行定期维护，以确保可靠性、可用性和性能。 EC2 裸机实例与其他 EC2 实例一样受到相同类型的计划事件的影响。 AWS 由于底层硬件问题或定期维护，可以安排事件以重启、停止和停用您的实例。这些事件不会频繁发生。有关更多信息，请参阅 Amazon EC2 用户指南中的计划事件类型。

> **Note**
>
> 在发生任何预定重启事件之前，应在 vSphere Client 中将主机置于维护模式。

如果您的一个实例将受到计划事件的影响，请使用与您的 AWS 账户关联的电子邮件地址提前通过电子邮件 AWS 通知您。 AWS 还会发送一个 AWS Health 事件，您可以使用 Amazon 对其进行监控和管理 EventBridge。有关更多信息，请参阅亚马逊 EC2 用户指南中的使用 Amazon 监控 He AWS al th 中的事件 EventBridge和亚马逊 EC2 实例的计划事件。

您可以随时重新安排活动，使其在适合您的特定日期和时间举行。可以将事件重新计划到事件截止日期之前的日期。有关更多信息，请参阅 A mazon EC2 用户指南中的重新安排 EC2 实例的预定事件。

## 使用 EC2 按需容量预留

您可以使用 EC2 按需容量预留来确保您的集群在维护期间有足够的容量。您可以在特定可用区域中预留任意持续时间的容量。有关更多信息，请参阅 Amazon EC2 用户指南中的使用 EC2 按需容量预留来预留计算容量。

有关创建容量预留的步骤，请参阅 Amazon EC2 用户指南中的创建容量预留。

> **Note**
>
> 如果您使用 EC2 按需容量预留或 EC2 专用主机，我们建议您为任务关键型工作负载保留一台备用主机。虽然容量预留可确保您访问给定可用区域中特定数量的 EC2 实例容量，但拥有备用主机可以提供额外的冗余层，这对于任务关键型工作负载至关重要。对于专用主机，即使主主机需要维护或遇到问题，备用主机也能确保您维护任务关键型工作负载的环境。

## 为 AWS 日程安排**system-maintenance**和**instance-retirement**活动做准备

AWS 安排两种类型system-maintenance的事件：网络维护和电源维护。

- 在网络维护期间，计划的实例会在短时间内失去网络连接。在维护完成后，将恢复与实例的正常网络连接。
- 在电源维护期间，计划的实例将短时间脱机，然后重启。在 EC2 裸机实例上执行重启时，不会保留实例存储卷数据。

AWS 在检测到托管您的 EC2 实例的底层硬件性能下降时安排 EC2 instance-retirement事件。

要修复system-maintenance和instance-retirement事件，请在维护事件发生之前使用 Amazon EVS 控制台或 AWS CLI 和 SDDC Manager 将故障主机替换为新主机。如果您等待维护事件发生并且需要重启 EC2 实例，则存储在实例存储卷上的 vSAN 数据将丢失。有关详细步骤，请参阅the section called “更换 Amazon EVS 主机”。

> **Important**
>
> EC2 控制台不应用于管理您的 Amazon EVS 主机的状态，包括停止、启动和终止。请勿尝试启动、停止或终止 Amazon EVS 部署的 EC2 实例。此操作会导致 vSAN 数据丢失。

### 更换 Amazon EVS 主机

按照以下步骤更换 Amazon EVS 主机。

> **Warning**
>
> Amazon EVS 主机使用自定义供应商插件来提供重要的主机功能。当您在环境中添加主机时，该主机将具有最新版本的 Amazon EVS 定制插件。如果您的环境使用带有较旧插件版本的

主机，则向 vSphere 集群添加主机将导致集群映像修复失败。有关解决此问题的步骤，请参阅the section called “解决由于集群映像不兼容而导致的添加主机失败的问题”。

**Warning**

如果您在部署后更新了 ESX 版本，则在 “委托主机” 步骤中验证 VCF 主机期间，SDDC 管理器可能会失败。有关解决此问题的步骤，请参阅the section called “SDDC 管理器在主机调试期间无法验证 VCF 主机”。

**Note**

确保正确设置每个 EVS 环境配额的 Amazon EVS 主机数量，以确保成功创建主机。如果此配额值小于您尝试在单个 Amazon EVS 环境中预置的主机数量，则主机创建失败。对于需要更换主机的维护操作，您可能需要申请增加配额。有关更多信息，请参阅 服务配额。

Example

Amazon EVS console and SDDC Managuer UI

1. 前往 Amazon EVS 控制台。
2. 在导航窗格中，选择环境。
3. 选择包含要替换的主机的环境。
4. 选择 “主机” 选项卡。
5. 选择 Create host (创建主机)。
6. 指定主机详细信息并选择创建主机。
7. 要验证是否完成，请检查主机状态是否已更改为 “已创建”。
8. 从 Secrets Manager 中检索 ESX 根密码的 AWS 凭证。有关检索密钥的更多信息，请参阅 Secrets Manager 用户指南中的从 S AWS ecrets Manager 获取 AWS 密钥。
9. 前往 SDDC 管理器。
10. 使用您在上一步中检索到的 ESX 根证书，在 SDDC 管理器中调试新主机。有关更多信息，请参阅 VMware Cloud Foundation 文档中的佣金主持人。

11.将新主机添加到集群。有关更多信息，请参阅《vSphere》文档中的如何使用快速入门工作流程将 ESX 主机添加到 vSphere 集群。

12.在 SDDC 管理器中停用要从 SDDC 管理器中移除的旧主机。有关更多信息，请参阅 VMware Cloud Fou ndation 文档中的停用主机。

13返回亚马逊 EVS 控制台。

14.在主机选项卡下，选择故障主机，然后选择删除 > 删除主机。

AWS CLI and SDDC Manager UI

1. 打开一个新的终端会话。
2. 创建新主机。参见下面的示例命令以供参考。

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

3. 从 Secrets Manager 中检索 ESX 根密码的 AWS 凭证。有关检索密钥的更多信息，请参阅 Secrets Manager 用户指南中的从 S AWS ecrets Manager 获取 AWS 密钥。
4. 前往 SDDC 管理器。
5. 使用您在上一步中检索到的 ESX 根证书，在 SDDC 管理器中调试新主机。有关更多信息，请参阅 VMware Cloud Foundation 文档中的佣金主持人。
6. 将新主机添加到包含受损主机的群集中。
7. 在 SDDC 管理器中停用受损主机。有关更多信息，请参阅 VMware Cloud Fou ndation 文档中的停用主机。
8. 返回航站楼。
9. 删除故障主机。参见下面的示例命令以供参考。

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

问题排查

有关故障排除指导，请参阅问题排查。如果您在查看故障排除指南后仍然遇到问题，请联系 Supp AWS ort 寻求进一步帮助。

## 为 Amazon EVS 子网配置自定义路由表

只有在创建 Amazon EVS 环境之后，Amazon EVS 才支持使用自定义路由表。要成功创建环境，必须将主路由表配置为允许流向依赖服务（例如 DNS 和本地系统）的流量。这是因为在环境部署期间，Amazon EVS VLAN 子网隐式关联到我们 VPC 的主路由表。

部署环境后，您必须将每个 Amazon EVS VLAN 子网与您的 VPC 中的路由表明确关联。如果您的 VLAN 子网未与 VPC 路由表明确关联，NSX 连接就会失败。我们强烈建议您将子网与自定义路由表明确关联。自定义路由表可以更精细地控制您的 VPC 内的网络流量路由，从而允许为特定的子网或网关量身定制路由规则。有关创建自定义路由表的更多信息，请参阅 Amazon VPC 用户指南中的为您的 VPC 创建路由表。

## 配置网络访问控制列表以控制 Amazon EVS VLAN 子网流量

网络访问控制列表 (ACL) 在子网级别允许或拒绝特定的入站或出站流量。您可以使用网络 ACLs 来控制 Amazon EVS VLAN 子网的入站和出站流量。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。

**Warning**

Amazon EVS 需要访问您的 VCF 部署。您必须配置您的安全组和网络访问控制列表 (ACLs)，以允许 Amazon EVS 与以下人员通信：

- TCP/UDP 端口 53 上的 DNS 服务器。
- 通过 HTTPS 和 SSH 进行主机管理 VLAN 子网。
- 通过 HTTPS 和 SSH 管理虚拟机 VLAN 子网。

如果您的安全组和网络 ACLs 不允许这种访问，Amazon EVS 环境部署将失败，现有环境的合规状态可能会降低。

## 密钥管理生命周期

在初始环境部署时，Amazon EVS 使用 S AWS ecrets Manager 在您的账户中创建、加密和存储密钥。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 凭据以及 ESX 主机的根密码。删除 EVS 环境后，Amazon EVS 还会代表您删除托管密钥。

您负责秘密生命周期管理，包括密钥轮换。Amazon EVS 不提供密钥的托管式轮换。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。有关更多信息，请参阅 S AWS ecrets Manager 用户指南中的轮换计划。

# 创建 Amazon EVS 主机

部署 Amazon EVS 环境后，您可以添加主机以提高容量和工作负载弹性。Amazon EVS 在每个环境中支持 4-16 台主机。此操作只能在部署 Amazon EVS 环境后使用。

Note

您必须在 SDDC 管理器用户界面中分配和调试主机。

创建 Amazon EVS 主机

按照以下步骤创建 Amazon EVS 主机。

Warning

Amazon EVS 主机使用自定义供应商插件来提供重要的主机功能。当您在环境中添加主机时，该主机将具有最新版本的 Amazon EVS 定制插件。如果您的环境使用带有较旧插件版本的主机，则向 vSphere 集群添加主机将导致集群映像修复失败。有关解决此问题的步骤，请参阅the section called “解决由于集群映像不兼容而导致的添加主机失败的问题”。

**Warning**

如果您在 Amazon EVS 环境部署后更新了 ESX 版本，则在 “委托主机” 步骤中验证 VCF 主机期间，SDDC 管理器可能会失败。有关解决此问题的步骤，请参阅the section called “SDDC 管理器在主机调试期间无法验证 VCF 主机”。

**Note**

确保正确设置每个 EVS 环境配额的 Amazon EVS 主机数量，以确保成功创建主机。如果此配额值小于您尝试在单个 Amazon EVS 环境中预置的主机数量，则主机创建失败。要提高配额，您可以申请增加配额。有关更多信息，请参阅 服务配额。

**Note**

如果您在向环境中添加主机时未指定 ESX 版本，Amazon EVS 会自动使用与您的环境的 VCF 版本关联的默认 ESX 版本。请参阅the section called “VCF 版本和实例 EC2 ”了解更多信息。

**Important**

添加 ESX 主机时，请选择与您的目标 vSphere 集群匹配的 ESX 版本。如果相同版本不可用，请部署旧版本并使用 vSphere 生命周期管理器进行升级。有关更多信息，请参阅 the section called “SDDC 管理器在主机调试期间无法验证 VCF 主机”。升级可能需要重新启动主机，并增加调试主机所需的时间。

ESX 版本比 vSphere 集群映像 ESX 版本更新的主机无法降级。您需要删除主机，然后使用正确的 ESX 版本重新创建主机。

Example

Amazon EVS console and SDDC Managuer UI

1. 前往 Amazon EVS 控制台。
2. 在导航窗格中，选择环境。
3. 选择要在其中创建主机的环境。

4. 选择 “主机” 选项卡。
5. 选择 Create host (创建主机)。
6. 指定主机详细信息并选择创建主机。
7. 要验证是否完成，请检查主机状态是否已更改为 “已创建”。
8. 前往 SDDC 管理器。
9. 在 SDDC 管理器中调试新主机。有关更多信息，请参阅 VMware Cloud Foundation 文档中的佣金主持人。
10. 使用 SDDC 管理器将新主机添加到群集。有关更多信息，请参阅《vSphere》文档中的如何使用快速入门工作流程将 ESX 主机添加到 vSphere 集群。

AWS CLI and SDDC Manager UI

1. 打开一个新的终端会话。
2. 创建新主机。参见下面的示例命令以供参考。

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

3. 前往 SDDC 管理器。
4. 在 SDDC 管理器中调试新主机。有关更多信息，请参阅 VMware Cloud Foundation 文档中的佣金主持人。
5. 使用 SDDC 管理器将新主机添加到群集。有关更多信息，请参阅《vSphere》文档中的如何使用快速入门工作流程将 ESX 主机添加到 vSphere 集群。

# 删除 Amazon EVS 主机

当不再需要 Amazon EVS 主机时，您可以从您的环境中删除该主机。Amazon EVS 要求您的环境至少有四台主机。Amazon EVS 不支持主机少于四台的环境。

> **Warning**
>
> 在不停用的情况下删除主机会在 vCenter 和 SDDC Manager 中留下陈旧的数据，可能需要付出额外的努力才能清理。在 Amazon EVS 控制台或 API 中删除主机之前，请确保您的主机已停用。

> **Warning**
>
> 请务必使用亚马逊 EVS 控制台或 API 移除您的亚马逊 EVS 主机。从控制台中删除 EC2 主机可能会使您的环境处于不一致的状态。

### 删除 Amazon EVS 主机

按照以下步骤删除 Amazon EVS 主机。

Example

SDDC Managuer UI and Amazon EVS console

1. 前往 SDDC 管理器。
2. 从 SDDC 管理器中移除群集。
3. 在 SDDC 管理器中停用主机。有关更多信息，请参阅 VMware Cloud Fou ndation 文档中的停用主机。
4. 前往 Amazon EVS 控制台。
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. 选择删除主机。
9. 选择主机，然后在 “主机” 选项卡中选择 “删除”。对要删除的每台主机重复此步骤。

SDDC Manager UI and AWS CLI

1. 前往 SDDC 管理器。
2. 从 SDDC 管理器中移除群集。

3. 在 SDDC 管理器中停用主机。有关更多信息，请参阅 VMware Cloud Fou ndation 文档中的停用主机。
4. 打开一个新的终端会话。
5. 删除主机。参见下面的示例命令以供参考。

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

# Amazon 弹性 VMware 服务中的安全

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。要了解适用于亚马逊弹性 VMware 服务 (Amazon EVS) 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 EVS 时如何应用分担责任模型。它向您展示了如何配置 Amazon EVS 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 AWS 服务 来帮助您监控和保护您的 Amazon EVS 资源。

内容



## 亚马逊 EVS 中的数据保护

责任AWS 共担模式适用于亚马逊弹性 VMware 服务的数据保护。如本模型所述 AWS ，负责保护运行所有 AWS 云的全球基础架构。您有责任保持对托管在此基础架构上的内容的控制，包括 VMware 云基金会 (VCF) 组件。您还要负责所使用的安全配置和管理任务。 AWS 服务 有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS 安全博客上的责任AWS 共担模型和 GDPR 博客文章。

出于数据保护目的，我们建议您保护 AWS 账户 凭据并使用 AWS IAM Identity Center 或设置个人用户 AWS Identity and Access Management。这样，每个用户只获得履行其工作职责所需的权限。还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证（MFA）。

- 用于 SSL/TLS 与 AWS 资源通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。有关使用 CloudTrail 跟踪捕获 AWS 活动的信息，请参阅《 AWS CloudTrail 用户指南》中的使用跟 CloudTrail 踪。

> **Note**
>
> Amazon EVS 不会记录非AWS 组件的用户活动，例如您的 VCF 环境中的活动。这些活动记录在各种 VMware 控制台中，例如 vSphere 和 NSX Manager。如果需要集中式 VCF 日志，则可以配置 VCF 监控解决方案（例如 A VMware ria Operations 或 Tan VMware zu Observability）来实现此结果。有关更多信息，请参阅 VCF 文档中的 VMware Cloud Foundation 和 Cloud F VMware oundation 模式下的 VMware Aria S VMware u ite 生命周期。

- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务 Amazon Macie，例如，它有助于发现和保护存储在中的敏感数据 Amazon S3。
- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-3 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-3 版》https://aws.amazon.com/compliance/fips/。

我们强烈建议您切勿将敏感的识别信息（例如客户的电子邮件地址）放入标签或自由格式的文本字段（例如“姓名”字段）中。这包括您使用控制台、API 或 AWS 服务 使用其他方式使用 Amazon EVS 或 AWS SDKs其他。 AWS CLI在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供 URL，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

## 静态加密

Amazon EVS 部署 i4i.metal EC2 实例，默认情况下，这些实例对存储在实例存储卷上的数据使用透明的 AES-256 加密。Amazon EVS 目前不支持 EBS 启动卷加密。

### 亚马逊 EBS 启动音量

亚马逊 EVS i4i.metal 实例使用亚马逊 EBS 启动卷。启动卷包含 EC2 实例启动和运行所需的操作系统和其他必要文件。启动卷未加密。Amazon EVS 目前不支持启动卷加密。启动卷不包含来自虚拟机的用户数据。

### 实例存储卷

Amazon EVS i4i.metal EC2 实例带有本地 NVMe SSD 存储，这是实例硬件的一部分。Amazon EVS 使用 NVMe 实例存储卷作为 vSAN 数据存储的磁盘。在您部署 Amazon EVS 环境后，vSAN 数据存储将保存您的管理和工作负载虚拟机。

NVMe 实例存储卷上的数据使用 XTS-AES-256 密码进行加密，该密码在实例的硬件模块上实现。用于加密写入本地连接的 NVMe 存储设备的数据的密钥是按客户和卷计算的。有关更多信息，请参阅 Amazon EC2 用户指南中的静态加密。

部署 Amazon EVS 环境后，您可以为存储在 data-at-rest vSAN 数据存储中的所有数据、单个虚拟机 VMs () 或其中的单个文件启用 vSAN 加密。 VMs当有些 VMs 需要加密而另一些则不要求加密时，或者当虚拟机中的特定磁盘或文件需要加密时，这种精细控制可能很有用。有关更多信息，请参阅 vSAN 文档中的 v VMware SAN Data-At-Rest 加密的工作原理。

## 传输中加密

默认情况下，Amazon EVS 不会对您的传输流量进行加密。要对通过 Amazon EVS 传输的数据进行加密，您可以将应用程序层加密与传输层安全 (TLS) 等协议一起使用。要了解有关 EC2 实例流量加密的信息，请参阅 Amazon EC2 用户指南中的传输中加密。

> **Note**
>
> Nitro 网络加密不适用于 Amazon EVS 部署的 EC2 实例。Amazon EVS 不支持对主机间流量进行传输加密。

### 用于本地连接的传输加密选项

要加密本地数据中心与 Amazon EVS 之间的流量，您可以将 Di AWS rect Connect 和 AWS Site-To-Site VPN 与 T AWS ransit Gateway 结合使用。这种组合提供了 IPsec加密的私有连接，与基于互联网的 VPN 连接相比，还可以降低网络成本，增加带宽吞吐量，并提供更稳定的网络体验。有关更多信息，请参阅带有 Di AWS rect Connect 的私有 IP AWS Site-to-Site VPN。

> **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。Amazon E IPSec VS 确实支持在 NSX Edge Tier-0

或 Tier-1 网关上终止 VPN。有关更多信息，请参阅 NSX 文档中的添加 NSX IPSec VPN 服务。 VMware

MAC Security (MACsec) 是一项 IEEE 标准，可提供数据机密性、数据完整性和数据来源真实性。您可以使用支持 MACsec 加密从公司数据中心到 Di AWS rect Connect 位置的数据的 Di AWS rect Connect 连接。有关更多信息，请参阅 Di AWS rect Connect 用户指南中的 Dire AWS ct Connect 中的 MAC 安全。

### 对传输中的 VMware 网络数据进行加密

部署 Amazon EVS 环境后，您可以通过多种方式在 VMware VCF 层强制执行传输中数据加密：

- VMware vDefende 分布式防火墙-允许您实现精细的网络分段并在虚拟机之间强制 TLS/SSL 加密。有关更多信息，请参阅 VMware VCF 文档中的使用用户界面为分布式防火墙配置安全设置。
- vSAN data-in-transit 加密-可用于加密 vSAN 群集中主机之间的所有数据和元数据。有关更多信息，请参阅 vSAN 文档中的 v VMware SAN Data-In-Transit 加密。
- 加密 vSphere vMotion-确保通过 vSphere vMotion 传输的数据的机密性、完整性和真实性。有关更多信息，请参阅《vSphere》文档中的什么是加密 vSphere vMotion。

## 密钥和机密管理

在 Amazon EVS 环境部署期间，Amazon EVS 使用 S AWS ecrets Manager 创建、加密和存储包含安装和访问 VCF 管理设备所需的 VMware VCF 凭证以及 ESX 根密码的密钥。删除 EVS 环境后，Amazon EVS 还会代表您删除托管密钥。有关更多信息，请参阅 S ecrets Manager 用户指南中的 Secrets Manager AWS 密钥中的内容。

Secrets Manager 使用带有 AWS KMS 密钥和数据密钥的信封加密来保护每个密钥值。除非另有说明，否则将使用 Secrets Manager 的默认 AWS 托管密钥。或者，您可以在创建环境时指定客户托管密钥来加密您的密钥。有关更多信息，请参阅 S ecr AWS ets Manager 用户指南中的 Secrets Manager 中的 AWS 密钥加密和解密。

> **Note**
>
> 客户托管密钥需要支付额外的使用费。默认 AWS 托管密钥是免费提供的。有关更多信息，请参阅 S AWS ecrets Manager 用户指南中的定价。

部署后，Amazon EVS 不会在 S AWS ecrets Manager 和你的 VCF 软件之间同步证书。您有责任确保与您的 Amazon EVS 环境相关的机密与 SDDC 管理器中的凭证保持同步，以避免 VCF 密码过期和无法访问 VCF 软件。

Amazon EVS 不会代表您轮换机密。您负责轮换与您的环境相关的密钥。我们强烈建议您在创建环境后立即轮换您的密钥，并实施轮换计划以定期更新您的密钥。有关轮换 Secrets Manager AWS 密钥的更多信息，请参阅 Secret s Man ager 用户指南中的按 Lambda 函数轮换。 AWS 有关 VCF 密码管理的更多信息，请参阅 Cloud F VMware oundation 文档中的密码管理。

**Important**

部署后，Amazon EVS 不会在 S AWS ecrets Manager 和你的 VCF 软件之间同步证书。如果在部署后使用 S AWS ecrets Manager，则必须保持 S AWS ecrets Manager 和 SDDC Manager 之间的凭据同步，以避免 VCF 密码过期问题。如果 SDDC 管理员凭据未保持最新，则可能无法访问 VCF 软件。

**Note**

Amazon EVS 不提供密钥的托管轮换。

**Note**

使用 Lambda 函数进行 Secrets Manager AWS 密钥轮换需要付费。有关更多信息，请参阅 S AWS ecrets Manager 用户指南中的定价。

## 互联网络流量隐私

Amazon EVS 使用客户提供的 VPC 在 Amazon EVS 环境中的资源之间创建边界，并控制这些资源、您的本地网络和互联网之间的流量。有关 Amazon VPC 安全的更多信息，请参阅《 Amazon VPC 用户指南》 Amazon VPC中的 “确保网际流量隐私”。

默认情况下，Amazon EVS 会在创建环境时创建拒绝直接访问互联网的私有 VLAN 子网。要为您的 VPC 再增加一层安全保护，您可以为您的 VPC 创建自定义网络访问控制列表，其中包含进一步限制互联网连接的规则。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。

如果您是 NSX 管理员，则可以配置以下 NSX 功能来保护网络流量：

- VMware vDefende 网关防火墙-保护网络边界，防范外部威胁（南北流量）。有关更多信息，请参阅 VMware NSX 文档中的添加网关防火墙策略和规则。
- VMware vDefende 分布式防火墙-防范来自内部网络内部的攻击（东西向流量）。有关更多信息，请参阅 VMware NSX 文档中的添加分布式防火墙。

# Amazon 弹性 VMware 服务的身份和访问管理

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）使用亚马逊弹性 VMware 服务 (Amazon EVS) 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 Amazon EVS 中所做的工作。

服务用户 — 如果您使用 Amazon EVS 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 EVS 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。

如果您无法访问 Amazon EVS 中的某项功能，请参阅the section called “对 Amazon EVS 身份和访问进行故障排除”。

服务管理员-如果您负责公司的 Amazon EVS 资源，那么您可能拥有对 Amazon EVS 的完全访问权限。您的工作是确定您的服务用户应访问哪些 Amazon EVS 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 IAM 与 Amazon EVS 配合使用，请参阅the section called “亚马逊 EVS 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 EVS 的访问权限。要查看您可以在中使用的 Amazon EVS 基于身份的策略示例，请参阅。 IAMthe section called “Amazon EVS 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 root 用户身份进行身份验证（登录 AWS）IAM 用户，或者通过扮 IAM 演角色进行身份验证。

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 管理控制台 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《登录用户指南》中的如何 AWS 登录到您 AWS 账户的。

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 Identity Center（ AWS 单点登录的继任者）用户指南中的多重身份验证和 IAM 用户指南AWS中的使用多重身份验证 (MFA)。

### AWS 账户 root 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 root 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

可访问该身份。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 单点登录的继任者）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使用案例，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 管理控制台 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 Identity Center（ AWS 单点登录的继任者）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。
- 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。默认情况下，用户无法执行任何操作，甚至无法更改自己的密码。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。当管理员向群组授予权限时，该群组中的所有用户都将获得这些权限。

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 管理控制台 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 JSON 策略，用于指定中组织或组织单位 (OU) 的最大权限 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 AWS 账户的根用户。有关组织和的更多信息 SCPs，请参阅《 AWS 组织用户指南》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 EVS 是如何使用的 IAM

在使用 IAM 管理对 Amazon EVS 的访问权限之前，请先了解哪些 IAM 功能可用于 Amazon EVS。

| IAM 特征 | 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 “针对 Amazon EVS 的政策行动” | 是 |

| IAM 特征 | 亚马逊 EVS 支持 |
| --- | --- |
| the section called “Amazon EVS 的政策资源” | 部分 |
| the section called “Amazon EVS 的政策条件密钥” | 是 |
| the section called “Amazon 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 |
| 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 “Amazon 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 EVS 和其他 AWS 服务 产品的使用方式 IAM，请在 IAM 用户指南 IAM中查看AWS 服务 与之配合使用的内容。

## 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》中的使用客户管理型策略定义自定义 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主体，因为它适用于其附加的用户或角色。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 Amazon EVS 基于身份的政策示例，请参阅。the section called “Amazon EVS 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。

针对 Amazon EVS 的政策行动

支持动作是

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。

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 EVS 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 EVS 定义了自己的一组操作，这些操作描述了您可以使用此服务执行的任务。

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 Amazon EVS 操作列表，请参阅《服务授权参考》中的 Amazon EVS 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 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。

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/*"
```

Amazon 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 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。

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，只有当资源标有资源 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 EVS 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 Amazon EVS 条件密钥列表，请参阅《服务授权参考》中的 Amazon EVS 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 EVS 定义的操作。

## Amazon 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。您可以将标签附加到 IAM 实体（用户或角色）和许多 AWS 资源。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

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 Amazon EVS 资源，也可以在请求中将标签传递给 Amazon EVS。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

当你使用临时凭证登录时，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 管理控制台 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 AWS 服务，再加上 AWS 服务 向下游服务发出请求的请求。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。

## Amazon 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

支持服务关联角色：是

服务相关角色是一种与服务相关联的 AWS 服务服务角色。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关联角色的权限。

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

## Amazon EVS 基于身份的策略示例

默认情况下 IAM 用户 ，角色无权创建或修改 Amazon EVS 资源。他们也无法使用 AWS 管理控制台 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 EVS 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Amazon EVS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 托管策略或工作职能的AWS 托管策略。

- 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的方式使用的，则也可以使用条件来授予对服务操作的访问权限 AWS 服务，例如 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 EVS 控制台

要访问 Amazon EVS 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 AWS 账户的 Amazon EVS 资源的详细信息。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 EVS 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",
                "ec2:ModifyInstanceAttribute"
            ],
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonEVSManaged": "false"
                }
            }
        },
        {
            "Sid": "CreateSubnetWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSubnet"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*"
```

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

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

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

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

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

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

## 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 EVS 身份和访问进行故障排除

使用以下信息来帮助您诊断和修复在使用 Amazon EVS 和 IAM时可能遇到的常见问题。

主题

- AccessDeniedException
- 我想允许我以外的人访问我 AWS 账户 的 Amazon EVS 资源

## 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 AWS 账户 的 Amazon EVS 资源

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 EVS 是否支持这些功能，请参阅the section called “亚马逊 EVS 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

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使用案例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 “使用服务关联角色”。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AWSServiceRoleForAmazonEVS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-发现 VPC 网络组件，包括子网和。 VPCs创建、修改、标记和删除弹性网络接口，这些接口用于在您的 VPC 子网中的 Amazon EVS 和 VMware 虚拟云基金会 (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。
- ec2-删除 Amazon EVS 在您提出 EVS 主机删除请求时创建的 EC2 实例。描述和修改 EC2 实例属性，以便在需要时可以禁用默认 EC2 实例终止和停止保护，以支持 EVS 主机删除。
- ec2-管理 EBS 卷以安装和清理云构建器。在创建环境期间，云构建器会安装到其中一台 Amazon EVS 部署的主机上，以执行 VCF 配置更改。完成后，Amazon EVS 会通过分离和删除存储云构建器的 EC2 卷来移除云构建器。
- ec2-如果您请求删除环境，请代表您删除 EVS VLAN 子网。
- secretsmanager-删除 Amazon EVS 在创建环境期间创建并存储在 S AWS ecrets Manager 中的 VCF 密码。如果环境创建失败或您请求删除环境，Amazon EVS 会删除该服务在您的账户中创建的所有密钥。通过提供 AWS 密钥 ARN 来配置 vCenter 连接器时，从 Secrets Manager 检索 vCenter 凭证。该权限的范围以资源标签条件为限，EvsAccess=true以确保 Amazon EVS 仅访问明确标记为 Amazon EVS vCenter 访问的机密。
- kms-当存储在 Secrets Manager 中的 vCenter 凭据使用 KMS 密钥加密时，解密密密钥并描述 KMS 密钥。权限的范围以资源标签条件为限，EvsAccess=true以确保 Amazon EVS 仅访问明确标记为 vCenter 访问的 KMS 密钥。
- cloudwatch-发布有配额 CloudWatch 的 Amazon EVS 资源的 AWS 使用量指标。

要查看有关该政策的更多详细信息，包括最新版本的 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 -政策已更新 | Amazon EVS 更新了政策，允许该服务从 Secrets AWS | 2026 年 3 月 23 日 |

| 更改 | 描述 | 日期 |
| --- | --- | --- |
| | Manager 检索 vCenter 凭证并解密使用 KMS 密钥加密的机密。要了解更多信息，请参阅the section called “AWS 托管策略：Amazon EVSService RolePolicy”。 | |
| 亚马逊 EVSService RolePolicy -政策已更新 | Amazon EVS 更新了政策，增加了全面的资源管理功能，包括 EC2 实例管理、EBS 卷操作和 S AWS ecrets Manager 集成。要了解更多信息，请参阅the section called “AWS 托管策略：Amazon EVSService RolePolicy”。 | 2025 年 8 月 14 日 |
| 亚马逊 EVSService RolePolicy -政策已更新 | Amazon EVS 更新了政策，允许该服务删除 EVS VLAN 子网，并将亚马逊 EVS 使用率指标发布到。 CloudWatch 要了解更多信息，请参阅the section called “AWS 托管策略：Amazon EVSService RolePolicy”。 | 2025 年 7 月 14 日 |
| 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。要了解更多信息，请参阅the section called “AWS 托管策略：Amazon EVSService RolePolicy”。 | 2025 年 6 月 9 日 |
| 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

亚马逊弹性 VMware 服务使用 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。

服务相关角色可以更轻松地设置 Amazon EVS，因为您无需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，以及不能附加到任何其他 IAM 实体的权限策略。

只有在首先删除相关资源后，您才能删除服务关联角色。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，查看该服务的服务关联角色文档。

## 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、EVS 主机和指标。 VPCs CloudWatch

`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、编辑或删除服务关联角色。有关更多信息，请参阅《IAM 用户指南》中的服务关联角色权限。

## 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 管理控制台、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。

如果您删除该服务关联角色，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。创建服务关联角色后，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》中的编辑服务关联角色。

### 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关联角色的功能或服务，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》中的删除服务关联角色。

### 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《 AWS 通用参考指南》中的 Amazon 弹性 VMware 服务终端节点和配额。

## Amazon EVS 的弹性

AWS 全球基础设施是围绕 AWS 区域 可用区构建的。 AWS 区域 提供多个物理分隔和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络连接。利用可用区，您可以设计和操作在可用区之

间无中断地自动实现失效转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错能力和可扩展性。

Amazon EVS 环境可在单个 AWS 可用区域中使用。为了确保 Amazon EVS 单可用区基础设施的高可用性，Amazon EVS 提供了以下功能：

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

- Amazon EVS 支持使用 AWS 弹性灾难恢复来自动备份和恢复数据。
- 按照 VCF 要求，Amazon EVS 部署了一个包含两个 Active/Standby NSX Edge 节点的 NSX Edge 集群。NSX Edge 节点在不同的主机上运行，以确保高可用性，并允许在 NSX Edge 节点出现故障的极少数情况下进行快速故障转移。
- Amazon EVS 部署了由四台 ESX 主机组成的最低环境，这是 VCF 所要求的。部署后可以添加其他主机。这是一项 VMware 设计要求，旨在确保适当的 vSAN 法定人数，并在维护操作和主机故障期间保持可用性。有关更多信息，请参阅 Cloud Foundation 文档中的 VMware 云基础版 vSphere 集群设计。 VMware
- Amazon EVS 支持对 EC2 主机使用 EC2 分区置放群组或集群置放群组。分区放置组将您的 EC2 实例分布在逻辑分区中，这样一个分区中的实例组就不会与不同分区中的实例组共享底层硬件。此策略有助于降低大型分布式工作负载出现相关硬件故障的可能性。集群置放群组用于将您的 EC2 实例放在同一个物理机架中，以确保低延迟。有关更多信息，请参阅《 Amazon EC2 用户指南》中的对置放群组进行分区。

有关 AWS 区域和可用区的更多信息，请参阅AWS 全球基础设施。

## VMware 组件弹性

Amazon EVS 客户负责配置在 Amazon EVS 上运行的 VMware 组件，以确保虚拟机的高可用性 (VMs) 和工作负载弹性。

Amazon EVS 支持以下 VMware 云基础 (VCF) 弹性功能：

- vSphere 复制-提供基于主机的异步复制， VMs 用于灾难恢复和工作负载迁移。有关更多信息，请参阅《vSphere 复制》文档中的 VMware vSphere 复制的工作原理。
- vSAN 数据保护-使用本地存储在 vSAN 群集上的本机快照，使您能够 VMs 从勒索软件攻击的操作故障中快速恢复。有关更多信息，请参阅 vSAN 文档中的使用 vSAN 数据保护。

- vSphere HA- VMs 在主机出现故障时提供自动故障切换。有关更多信息，请参阅 VCF 文档中的 vCenter Ser ver for VMware Cloud Foundation 的高可用性设计。
- vSphere Fault Tolerance (FT)- VMs 通过创建和维护另一台相同且可在故障转移情况下持续更换的虚拟机，为关键任务提供持续可用性。有关更多信息，请参阅《vSphere》文档中的容错工作原理。
- vSAN 容忍故障 (FTT)-一种 vSAN 设置，用于确定虚拟机在无法访问之前可以承受多少主机故障。这定义了 vSAN 群集中虚拟机的冗余和容错级别。有关更多信息，请参阅 vSAN 文档中的容忍 vSAN 群集中的故障域出现其他故障。

# 将 Amazon EVS 与其他 AWS 服务一起使用

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

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

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

以下过程详细介绍了使用控制台和 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。 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 开始使用。
- 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

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 开始使用。
- 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 ESX 主机存储配置软件 iSCSI 适配器

对于每台 ESX 主机，您都必须配置软件 iSCSI 适配器，以便您的 ESX 主机可以使用它来访问 iSCSI 存储。有关在 vSphere 中为 ESX 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删除软件 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 ESX 主机提供共享块存储。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 ESX 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 v VMware Sphere 产品文档中的在 ESX 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。

# 问题排查

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，以确定具体和可检测的问题。

### 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，则此项检查将失败。

如果此项检查失败，Amazon EVS 将无法再访问 SDDC 管理器来验证环境状态，也无法再将主机添加到环境中。可访问性故障还将导致许可证密钥重复使用和密钥覆盖检查失败，而主机计数检查返回未知响应。

为确保可接通，请检查以下内容：

- 确保您的证书有效且未过期。可以使用 SDDC 管理器用户界面或 vSphere 客户端来管理 VCF 环境中的证书。部署后，建议您替换 VMware Cloud Foundation 管理域的所有证书。有关更多信息，请参阅 VMware Cloud Foundation 文档中的管理 VMware 云基础中的证书。
- 确保您的 DNS 服务器可以从服务访问子网访问，DNS 记录有效，并且不存在重复的主机名或 IP 地址。
- 如果您想创建自己的防火墙规则，请遵循以下准则：
  - 允许 TCP/UDP 访问 DNS 服务器。

- 允许 HTTPS/SSH 访问主机管理 VLAN 子网。
- 允许 HTTPS/SSH 访问管理虚拟机 VLAN 子网。

如果您在遵循本指南后仍无法解决问题，我们建议您联系 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.x 的要求。

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

## 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。如果您在环境创建请求中提供的 VCF 许可证密钥已被其他环境使用，则此检查将失败。

如果此项检查失败，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 管理器中审核许可证设置，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 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。虽然必须使用 vSphere Client 将密钥分配给您的主机和 vSAN 集群，但您必须确保这些密钥也显示在 SDDC Manager 用户界面的许可屏幕上。

## 密钥覆盖率检查失败

此项检查可验证分配给 vCenter 服务器的 VCF 许可证密钥是否为所有已部署的主机分配了足够的 vCPU 内核和 vSAN 存储容量（TiB）。

如果此项检查失败，您将收到错误响应，提示无法创建 Amazon EVS 环境。密钥覆盖失败可能表示存在以下问题之一：

- VCF 许可证未正确地分配给 vCenter 服务器。必须在 vCenter 服务器的评估期到期或当前分配的许可证到期之前，将许可证分配给该服务器。如果这是问题所在，请在 SDDC 管理器中审核许可证分配情况。

- 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。如果这是问题所在，请在 SDDC 管理器中添加 vSAN 许可证，直到满足使用需求为止。

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 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。虽然必须使用 vSphere Client 将密钥分配给您的主机和 vSAN 集群，但您必须确保这些密钥也显示在 SDDC Manager 用户界面的许可屏幕上。

# 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 ESX 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。

# ESX 主机群集的 vSAN 升级预检查失败

尝试使用 SDDC Manager 升级 ESX 主机群集时，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。

# 添加由于集群映像不兼容而导致的主机故障

问题

向环境中添加主机时，该主机具有最新版本的 EVS 自定义供应商插件。如果您的环境使用带有较旧附加版本的主机，则添加新主机会失败，并显示新主机与您的集群映像不兼容的错误。要修复此问题，必须使用 vSphere Lifecyle Manager 从新添加的主机中提取最新的可用插件版本。

解决方案

执行以下步骤。

1. 转到 vCenter VMware Server 中的主机和群集清单。
2. 通过创建一个临时的空集群，从新添加的主机中提取插件。
3. 在 “基础知识” 下，在 vCenter 清单中选择从 vCenter 清单中的现有主机导入映像并创建集群。将所有其他设置保留为默认设置。
4. 使用提取的映像创建此临时集群后，您可以删除该临时集群。该插件现在将在 vSphere 生命周期管理器库中提供。
5. 转到您的环境集群并选择更新选项卡。
6. 编辑您的集群映像并将插件版本更改为新提取的版本。
7. 选择保存。
8. 在 SDDC 管理器中，重试失败的添加主机任务。这将修复您的集群主机，将所有主机更新到最新的插件版本。集群映像修复需要重新启动主机。

# SDDC 管理器在主机调试期间无法验证 VCF 主机

问题

如果您在部署 Amazon EVS 环境后更新了 ESX 版本，则在 “委托主机” 步骤中验证 VCF 主机期间，SDDC 管理器可能会失败。要修复此问题，必须使用 vSphere Lifecyle Manager 在新添加的主机上升级 ESX。

解决方案

执行以下步骤。

> **Important**
>
> 这些步骤需要在 SDDC Manager 之外临时将主机添加到 vCenter。使用 vSphere Lifecyle Manager 执行除了 ESX 升级以外的任何操作都可能导致您的主机无法使用，因此需要您删除并创建新的 Amazon EVS 主机。

1. 转到 vCenter VMware Server 中的主机和群集清单。
2. 将主机临时添加到您的虚拟数据中心，确保选择使用映像管理主机。ESX 升级完成后，将在后续步骤中移除该主机。有关更多信息，请参阅《vSphere》文档中的如何将主机添加到 vSphere 数据中心或文件夹。

3. 将主机添加到 vSphere 后，升级主机上的 ESX 版本。这可以在房东的 “更新” 选项卡中完成。编辑主机映像以匹配集群的 ESX 版本。
4. 升级完成后，从 vCenter 清单中移除该主机。有关更多信息，请参阅《vSp here》文档中的如何从 vCenter 服务器实例中移除 ESX 主机。
5. 在 SDDC 管理器中调试您的主机。有关更多信息，请参阅 VMware Cloud Foundation 文档中的佣金主持人。
6. 主机调试完成后，使用 SDDC 管理器将主机添加到集群。

# 使用记录亚马逊 EVS API 调用 AWS CloudTrail

Amazon EVS 与 AWS CloudTrail一项服务集成，该服务提供了 IAM 用户、IAM 角色或 Amazon EVS 中的 AWS 服务所采取的操作的记录。 CloudTrail 将 Amazon EVS 的所有 AWS API 调用捕获为事件。捕获的调用包括来自亚马逊 EVS 控制台的调用和对 Amazon EVS API 操作的代码调用。如果您创建了跟踪，则可以允许将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括针对 Amazon EVS 的事件。如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的 “事件历史记录” 中查看最新的事件。使用收集的信息 CloudTrail，您可以确定向 Amazon EVS 发出的请求、发出请求的 IP 地址、谁提出了请求、何时提出请求以及其他详细信息。

要了解更多信息 CloudTrail，请参阅《AWS CloudTrail 用户指南》。

> **Note**
>
> Amazon EVS 不会记录非AWS 组件的用户活动，例如您的 VCF 环境中的活动。这些活动记录在各种 VMware 控制台中，例如 vSphere 和 NSX Manager。
> 如果需要集中式 VCF 日志记录，则可以配置 VCF 监控解决方案（例如 Cloud F VMware oundation Operations）来实现此结果。

## 亚马逊 EVS 信息位于 CloudTrail

CloudTrail 在您创建 AWS 账户时已在您的账户上启用。当 Amazon EVS 中发生活动时，该活动会与其他 AWS 服务 CloudTrail 事件一起记录在事件历史记录中。您可以在自己的 AWS 账户中查看、搜索和下载最近发生的事件。有关更多信息，请参阅使用事件历史记录查看 CloudTrail 事件。

要持续记录您的 AWS 账户中的事件，包括 Amazon EVS 的事件，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。默认情况下，当您在控制台中创建跟踪时，该跟踪将应用于所有 AWS 区域。跟踪记录 AWS 分区中所有区域的事件，并将日志文件传送到您指定的 Amazon S3 存储桶。此外，您可以配置其他 AWS 服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅下列内容：

- 创建跟踪记录概述
- CloudTrail 支持的服务和集成
- 配置 Amazon SNS 通知 CloudTrail
- 接收来自多个区域的 CloudTrail 日志文件

- 接收来自多个账户的 CloudTrail 日志文件

所有亚马逊 EVS 操作均由《亚马逊 EVS API 参考》记录 CloudTrail 并记录在案。例如，调用`GetEnvironment`和`DeleteEnvironment`操作会在 CloudTrail 日志文件中生成条目。`CreateEnvironment`

每个事件或日志条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是使用根用户证书还是 AWS 身份和访问管理 (IAM) 用户凭证发出。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务发出。

有关更多信息，请参阅 CloudTrail userIdentity 元素。

# 了解 Amazon EVS 日志文件条目

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 Amazon S3 存储桶。 CloudTrail 日志文件包含一个或多个日志条目。事件代表来自任何来源的单个请求，包括有关请求的操作、操作的日期和时间、请求参数等的信息。 CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此它们不会按任何特定的顺序出现。

# 亚马逊 EVS 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》中的什么是服务配额？。

通过集成 Service Quotas，您可以使用 AWS 管理控制台 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”。

有关 Amazon EVS 服务配额的更多信息，请参阅《 AWS 通用参考指南》中的 Amazon EVS 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。

**Note**

如果配置 HCX 互联网连接，则亚马逊提供的连续公有 CID IPv4 R 块网络掩码长度的 IPAM 配额必须为 /28 或更大。有关更多信息，请参阅 IPAM 的配额。

**Note**

亚马逊 CloudWatch 收集有配额的 Amazon EVS 资源（环境和主机）的 AWS 使用指标。有关更多信息，请参阅 Amazon CloudWatch 用户指南中的CloudWatch 使用量指标。

# 在中查看 Amazon EVS 服务配额 AWS 管理控制台

1. 打开服务配额控制台。
2. 在左侧导航窗格中，选择 AWS 服务。
3. 从 AWS 服务列表中，搜索并选择 Amazon 弹性 VMware 服务。
4. 选择查看配额。

   在服务配额列表中，您可以看到服务配额名称、应用的值（如果可用）、 AWS 默认配额以及配额值是否可调整。
5. 要查看有关服务配额的其他信息（如描述），请选择配额名称。
6. （可选）要申请增加配额，请选择要增加的配额，选择在账户级别申请增加配额，输入或选择所需信息，然后选择请求。

要使用更多地使用服务配额 AWS 管理控制台，请参阅 S ervice Quotas 用户指南。要请求提高配额，请参阅《Service Quotas 用户指南》中的请求提高配额。

# 使用 CLI 查看亚马逊 EVS 服务配额 AWS

运行以下命令查看您的 Amazon EVS 配额。

```
aws service-quotas list-aws-default-service-quotas \
    --query 'Quotas[*].
{Adjustable:Adjustable,Name:QuotaName,Value:Value,Code:QuotaCode}' \
    --service-code evs \
    --output table
```

> **Note**
>
> 返回的配额是可在当前 AWS 区域的此账户中创建的 Amazon EVS 环境或主机的数量。

要使用 AWS CLI 更多地处理服务配额，请参阅 CL AWS I 命令参考中的服务配额。要申请增加配额，请参阅《 AWS CLI request-service-quota-increase命令参考》中的命令。

# 《亚马逊弹性 VMware 服务用户指南》的文档历史记录

下表描述了 Amazon 弹性 VMware 服务的文档版本。

| 变更 | 说明 | 日期 |
| --- | --- | --- |
| 更新了亚马逊 EVSService RolePolicy | Amazon EVS 已更新托管策略，AmazonEVSServiceRolePolicy 允许该服务从 Secrets Manager 检索 vCent AWS er 凭证，并解密使用客户管理的 KMS 密钥加密的机密。 | 2026 年 3 月 23 日 |
| 更新了亚马逊 EVSService RolePolicy | Amazon EVS 更新了托管策略AmazonEVSServiceRolePolicy ，增加了全面的资源管理功能，包括 EC2 实例管理、EBS 卷操作和 S AWS ecrets Manager 集成。有关信息，请参阅 Amazon EVS 对 AWS 托管策略的更新。 | 2025 年 8 月 14 日 |
| 更新了亚马逊 EVSService RolePolicy | 更新了 AWS 托管政策 Amazon EVSService RolePolicy。 | 2025 年 8 月 4 日 |
| 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。<br><br>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 EVSServiceRolePolicy | 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。<br><br>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。