Getting started with Amazon Elastic VMware Service

Author's Note for Portfolio Review: *This sample focuses on network architecture and security boundary configurations. I selected it to show how I defined cross-service constraints (for example, BGP dependencies on VPC Route Server) and documented security limitations—specifically regarding security groups and boot volume encryption support. In the published customer documentation, the boot volume encryption limitation is documented on the data protection page. In this portfolio excerpt, I've also included it as a getting started prerequisite to illustrate my core recommendation: constraints that affect compliance or service fit should appear before customers provision resources.*

Important

To get started as simply and quickly as possible, this topic specifies the minimum requirements for Amazon EVS environment creation. Before creating these resources, review the following prerequisites and architectural constraints:

Network Planning: Plan out your IP address space and DNS record setup. You cannot change the IP addressing scheme after deployment.

VCF Version: Amazon EVS only supports VCF version 5.2.1.x at this time. You should familiarize yourself with VCF 5.2.1 requirements. For more information, see the VCF 5.2.1 release notes.

Boot Volume Encryption: Amazon EVS hosts do not support encryption for the Amazon EBS boot volume at this time. Ensure this limitation meets your data residency and compliance requirements before creating an environment.

Prerequisites

Before getting started, you must complete the Amazon EVS prerequisite tasks. For more information, see *Setting up Amazon Elastic VMware Service*.

Network infrastructure: dynamic routing

Set up a VPC Route Server instance with endpoints and peers

Amazon EVS uses Amazon VPC Route Server to enable BGP-based dynamic routing to your VPC underlay network. You must specify a route server that shares routes to at least two route server endpoints in the service access subnet. The peer ASN configured on the route server peers must match, and the peer IP addresses must be unique.

Important

Your environment deployment fails if you don't meet these Amazon EVS requirements for VPC Route Server configuration:

- You must configure at least two route server endpoints in the service access subnet.
- When configuring Border Gateway Protocol (BGP) for the Tier-0 gateway, the VPC Route Server peer ASN value must match the NSX Edge peer ASN value.
- When creating the two route server peers, you must use a unique IP address from the NSX uplink VLAN for each endpoint. These two IP addresses will be assigned to the NSX edges during Amazon EVS environment deployment.
- When enabling Route Server propagation, you must ensure that all route tables being propagated have at least one explicit subnet association. BGP route advertisement fails if propagated route tables do not have an explicit subnet association.

For more information about setting up VPC Route Server, see the Route Server get started tutorial.

Security architecture: layer 2 isolation

Create a network ACL to control Amazon EVS VLAN subnet traffic

Amazon EVS uses a network access control list (ACL) to control traffic to and from Amazon EVS VLAN subnets. For more information, see Create a network ACL for your VPC in the Amazon VPC User Guide.

If you plan to configure HCX internet connectivity, ensure that the network ACL rules that you configure allow the necessary inbound and outbound connections for HCX components. For more information about HCX port requirements, see the VMware HCX User Guide.

Important

EC2 security groups do not function on elastic network interfaces that are attached to Amazon EVS VLAN subnets. To control traffic to and from Amazon EVS VLAN subnets, you must use a network access control list.

Service implementation: environment configuration

Create an Amazon EVS environment

Author's note for portfolio review: *Steps 1–5 (licensing & host configuration) omitted for brevity.*

6. On the **Configure networks and connectivity** page, do the following.
   a. For **HCX connectivity requirements**, select whether you want to use HCX with private connectivity or over the internet.
   b. For **VPC**, choose the VPC that you previously created.
   c. (For HCX internet connectivy only) For **HCX network ACL**, choose which network ACL your HCX VLAN will be associated with.

> **Important**
>
> We strongly recommend that you create a custom network ACL dedicated to the HCX VLAN. For more information, see the section called “Configure network ACL”.

   d. For **Service access subnet**, choose the private subnet that was created when you created the VPC.
   e. For **Security group -*optional*** , you can choose up to two security groups that control communication between the Amazon EVS control plane and VPC. Amazon EVS uses the default security group if no security group is chosen.

> **Note**
>
> Ensure that the security groups that you choose provide connectivity to your DNS servers and Amazon EVS VLAN subnets.

   f. Under **Management connectivity**, enter the CIDR blocks to be used for the Amazon EVS VLAN subnets. For **HCX uplink VLAN CIDR block**, if configuring a public HCX VLAN, you must specify a CIDR block with a netmask length of exactly /28. Amazon EVS throws a validation error if any other CIDR block size is specified for the public HCX VLAN. For a private HCX VLAN and all other VLANs CIDR blocks, the minimum netmask length that you can use is /28 and the maximum is /24.

> **Important**
>
> Amazon EVS VLAN subnets can only be created during Amazon EVS environment creation, and cannot be modified after the environment is created. You must ensure that the VLAN subnet CIDR blocks are properly sized before creating the environment. You will not be able to add VLAN subnets after the environment is deployed. For more information, see the section called “Amazon EVS networking considerations”.

g. Under **Expansion VLANs**, enter the CIDR blocks for additional Amazon EVS VLAN subnets that can be used to expand VCF capabilities within Amazon EVS, such as enabling NSX Federation.

h. Under **Workload/VCF connectivity**, enter the CIDR block for the NSX uplink VLAN, and choose two VPC Route Server peer IDs that peer to Route Server endpoints over the NSX uplink.

i. Choose **Next**.