VMware Cloud on Dell EMC Horizon Deployment Guide

VMware Cloud on Dell EMC
You can find the most up-to-date technical documentation on the VMware website at:
https://docs.vmware.com/
Contents

1 Introduction 4

2 Prerequisites 5

3 VMware Cloud on Dell EMC Configurations 6
   Create Network Segments 6
   Configure DNS Services 7
      Add Default Zone 7
      Add FQDN Zone 8
   Network and Security Configurations 8
      Add Management Groups 8
      Add Compute Groups 9
   Setting Gateway Firewall Rules 10

4 Horizon Deployment and Configuration 13
   Create Resource Pools 14
   Install Horizon Connection Server 14
   Configure Horizon Connection Server 15
   Deploy Unified Access Gateway Appliance 17
   Configure Unified Access Gateway Appliance 21
   Configure Edge Service Settings 23

5 Configuring Load Balancer 29
   Deploy AVI Controller 29
   Configure AVI Controller 31
   Deploy Avi Service Engine 36
   Configure Avi Service Engine 39
      Create an IP Group 40
      Create a Custom Health Monitor Profile 41
      Create L7 Pools 42
   Install the SSL Certificate Required for VIP 43
   Create L7 Virtual Service 43
   Create a Static Route 45

6 Preparing a Virtual Machine for Cloning 46
   Create Instant-Clone Desktop Pools 46
   Install Horizon Agent 48
Introduction

The VMware Cloud on Dell EMC Horizon Deployment Guide provides a brief overview of the tasks involved in deploying Horizon on VMware Cloud on Dell EMC. This document should be read in conjunction with the following documentation: VMware Horizon, Horizon on VMware Cloud on Dell EMC Reference Architecture, and VMware Cloud on Dell EMC.

The information is intended for anyone who wants to deploy and configure Horizon to run remote desktops and applications on the on-premises infrastructure managed by VMware Cloud on Dell EMC. The information in this document is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and data center operations.
Prerequisites

Fulfill the following prerequisites before you start the Horizon deployment:

- To connect VMware Cloud on Dell EMC with your upstream network or vice versa, you must configure appropriate firewall and security groups on the VMware Cloud on Dell EMC portal.
- You must have an active directory domain controller that can be used for the Horizon environment.
- Ensure that the DNS server is available and appropriate DNS records are configured for all the Horizon management components.
- Configure the layer 3 networking and appropriate routing to reach the VMware Cloud on Dell EMC resources.
- If you want to use certificates for your Horizon environment, ensure that the certificates are available.
To deploy Horizon on VMware Cloud on Dell EMC, you must configure the network segments, DNS settings, and security groups on the VMware Cloud on Dell EMC portal.

This chapter includes the following topics:

- Create Network Segments
- Configure DNS Services
- Network and Security Configurations

Create Network Segments

Create network segments to configure the following networks:

- **DMZ network:** An intermediate network between VMware Cloud on Dell EMC and the Internet. It connects the incoming interfaces, Unified Access Gateway, and DMZ load balancer.
- **Horizon management network:** A dedicated network for Horizon components. All Horizon virtual machines (VMs) except Unified Access Gateway are hosted on this network.
- **Horizon user workload network:** A dedicated network for Horizon virtual desktops and published applications.

Procedure

2. Click the **VMware Cloud on Dell EMC** service.
3. Click the required SDDC name.
4. Click **Network > Network & Security > Segments**.
5. Click **Add Segment**.
6. Add the following network segments:
   - Enter the DMZ network segment name.
     For example, enter `sddc-cgw-dmz`. 
Enter the Horizon management network segment name. For example, enter `sddc-cgw-horizon-mgmt`.

Enter the Horizon user workload network segment name. For example, enter `sddc-cgw-horizon-user-workload`.

7. Click **Save**.

### Configure DNS Services

Configure the following DNS zones to use your existing DNS servers with VMware Cloud on Dell EMC.

- **Add Default Zone**
- **Add FQDN Zone**

#### Add Default Zone

Configure the default DNS zone details, such as zone name, domain, and DNS servers.

**Procedure**

2. Click the **VMware Cloud on Dell EMC** service.
3. Search for your SDDC and click the SDDC name.
4. Click **Network > Network & Security > DNS**.
5. Click **Add DNS Zone > Add Default Zone**.
6. Enter the zone name, domain, and DNS servers.

7. Click **Save**.
Add FQDN Zone

Configure the default FQDN zone details, such as zone name, domain, and DNS servers.

Procedure

2. Click the VMware Cloud on Dell EMC service.
3. Search for your SDDC and click the SDDC name.
4. Click Network > Network & Security > DNS.
5. Click Add DNS Zone > Add FQDN Zone.
6. Enter the zone name, domain, and DNS servers.
7. Click Save.

Network and Security Configurations

Use the VMware Cloud on Dell EMC Networking & Security inventory to create groups of network services that you can use when you create firewall rules.

Create the following network groups and firewall rules:

- Add Management Groups
- Add Compute Groups
- Add Management Gateway Firewall Rules
- Add Compute Gateway Firewall Rules

Add Management Groups

Management inventory groups contain SDDC infrastructure components. Use these groups in managing gateway firewall rules.
Procedure

1 Log in to the VMware Cloud Services Console at https://console.cloud.vmware.com/csp/gateway/discovery.

2 Click the VMware Cloud on Dell EMC service.

3 Click the required SDDC name.

4 Click Network > Network & Security > Groups.

5 Click Management Groups > Add Groups.

6 Create the following groups:
   - Jumphost: You can configure the group members with jump server IP addresses, specific subnets from where you want to access the vCenter Server, or set specific IP address to allow inbound access to VMware Cloud on Dell EMC.
   - Connection Server: You can configure the group members with Horizon connection server IP addresses or subnets to allow inbound access to the vCenter Server.

7 Click Set Members to open the Select Members page.

   Management groups contain VMs on the Management Network. Management group members must be specified by IP address. Therefore, Provide one or more IP addresses of management VMs in CIDR format.

8 Click SAVE to create the group.

Add Compute Groups

Compute inventory groups categorize compute VMs using criteria such as names, IP addresses, and tags.

Procedure

1 Log in to the VMware Cloud Services Console at https://console.cloud.vmware.com/csp/gateway/discovery.

2 Click the VMware Cloud on Dell EMC service.

3 Click the required SDDC name.
Click **Network > Network & Security > Groups.**

Click **Compute Groups > Add Groups.**

Create the following groups:

- **Jump host:** Create this group to manage and configure the Horizon Management components. Add the respective IP address or subnet to allow inbound connection to the Horizon Connection Server.
- **Connection Server:** Create this group and configure the group members with IP addresses of the Connection Server.
- **VDI user subnet:** Create this group and configure the group members with IP subnets to allow inbound traffic to Avi load balancer.
- **AVI Load Balancer:** Create this group and configure the group members with virtual IP address of the Avi Load balancer.

Click **Set Members** to open the **Select Members** page.

Compute groups contain VMs or network objects such as segments in the Compute network. There are several ways to designate membership in a compute group.

- **IP/MAC address:** Enter an IP address, MAC addresses, CIDR block, or a range of IP addresses in the form `ip-ip`.

For example, `192.168.1.1–192.168.1.100`.

Tag the group.

Click **SAVE** to create the group.

**Setting Gateway Firewall Rules**

A firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined firewall rules.

**Add Management Gateway Firewall Rules**

By default, the management gateway blocks traffic to all destinations from all sources. Add Management Gateway firewall rules to allow traffic as needed.
Procedure


2. Click the **VMware Cloud on Dell EMC** service.

3. Click the required SDDC name.

4. Click **Network > Network & Security > Gateway Firewall**.

5. On the **Gateway Firewall** card, click **Management Gateway**.

6. To add a rule, click **ADD RULE** and give the new rule a **Name**.

7. Enter the parameters for the new rule.

   Parameters are initialized to their default values (for example, **All** for **Sources** and **Destinations**). To edit a parameter, move the mouse pointer over the parameter value and click the pencil icon (✏️) to open a parameter-specific editor.

   - **Sources**: Do the following:
     a. Select **Any** to allow traffic from any source address or address range.
     b. Select **System Defined Groups** and select **vCenter** to allow traffic from your SDDC's vCenter Server.

   - **Destinations**: Do the following:
     a. Select **Any** to allow traffic to any destination address or address range.
     b. Select **System Defined Groups** and select **vCenter** to allow traffic from your SDDC's vCenter Server.

   The new rule is enabled by default.

8. Click **PUBLISH** to create the rule.

   The system gives the new rule an integer **ID** value, which is used in log entries generated by the rule.

   Firewall rules are applied in order from top to bottom. Because there is a default **Drop** rule at the bottom and the rules above are always **Allow** rules, management gateway firewall rule order has no impact on traffic flow.
Add Compute Gateway Firewall Rules

By default, the Compute Gateway blocks traffic to all uplinks. Add Compute Gateway firewall rules to allow traffic as needed.

Procedure

2. Click the VMware Cloud on Dell EMC service.
3. Click the required SDDC name.
5. On the GATEWAY FIREWALL card, click Compute Gateway.
6. To add a rule, click ADD RULE and give the new rule a Name.
7. Enter the parameters for the new rule.
   Parameters are initialized to their default values (for example, All for Sources and Destinations). To edit a parameter, move the mouse pointer over the parameter value and click the pencil icon (✏️) to open a parameter-specific editor.

8. Create two firewall rules, one for managing the connection server inbound rule and another for managing the load balancer inbound rule.
   For example, create the firewall rules, Connection Server Inbound and Load Balancer Inbound, and provide the details as captured in the following table.

<table>
<thead>
<tr>
<th>Name</th>
<th>Sources</th>
<th>Destinations</th>
<th>Applied To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Server Inbound</td>
<td>Jumpshot</td>
<td>Connection Servers</td>
<td>All Uplinks</td>
</tr>
<tr>
<td>Load Balancer Inbound</td>
<td>VDI-User-Desktop</td>
<td>Load Balancer VIP</td>
<td>All Uplinks</td>
</tr>
</tbody>
</table>

9. Click PUBLISH to create the rule.
   The system gives the new rule an integer ID value, which is used in log entries generated by the rule.
Horizon Deployment and Configuration

You use the Horizon Standard Server to install the Horizon Connection Server as a single server, or as the first instance in a group of replicated Connection Server instances. If you want to replicate the existing connection server instances, you use the Horizon Replica Server.

Procedure

1. **Create Resource Pools**
   You use resource pools to compartmentalize all resources in a cluster.

2. **Install Horizon Connection Server**
   The Horizon Connection Server standard installation creates a new, local View LDAP configuration. The installation loads the schema definitions, Directory Information Tree (DIT) definition, access Control Lists (ACL), and initializes the data.

3. **Configure Horizon Connection Server**
   You configure the Horizon Connection Server by:

4. **Deploy Unified Access Gateway Appliance**
   Unified Access Gateway is an appliance that is normally installed in a demilitarized zone (DMZ). Unified Access Gateway is used to ensure that the only traffic entering the corporate data center is traffic on behalf of an authenticated remote user. Unified Access Gateway directs authentication requests to the appropriate server and discards any unauthenticated request. Users can access only the resources that they are authorized to access.

5. **Configure Unified Access Gateway Appliance**
   You can configure the security protocols and cryptographic algorithms that are used to encrypt communications between clients and the Unified Access Gateway appliance from the admin configuration pages.

6. **Configure Edge Service Settings**
   You can deploy Unified Access Gateway with Horizon Cloud with On-Premises Infrastructure and Horizon Air cloud infrastructure. For the Horizon deployment, the Unified Access Gateway appliance replaces Horizon security server.
Create Resource Pools

You use resource pools to compartmentalize all resources in a cluster.

After you order an SDDC using the VMware Cloud on Dell EMC portal, two resource pools are available:

- Compute Resource Pool: You create child resource pools and manage them.

When deploying both management and user resources in the same SDDC, create the following child resource pools within the compute resource pool to manage your Horizon deployments:

- Management resource pool: Manages Horizon deployments and connection servers.
- User resource pool: Horizon users to manage the desktop pools and published applications.

Procedure

1. Use the vSphere Web Client to log in to a vCenter Server instance.
3. Create management and user resource pools.
   - For example, create the management and user resource pools, Horizon Management Resource Pool and Horizon User Resource Pool, respectively.
4. Enter other required information and click OK.

Results

The resource pools you created are listed under SDDC Datacenter > Compute-ResourcePool.

Install Horizon Connection Server

The Horizon Connection Server standard installation creates a new, local View LDAP configuration. The installation loads the schema definitions, Directory Information Tree (DIT) definition, access Control Lists (ACL), and initializes the data.

Prerequisites

- Create a virtual machine and install the Windows Server operating system.
- Ensure that the virtual machine is on sddc-cgw-horizon-mgmt network with a static IP and domain assigned to the network.

Procedure

1. Download VMware Horizon and save the installer to your Windows VM.
To start the installation process, right-click the installer file and select Run as Administrator.

In the Welcome to Installation Wizard for VMware Horizon Connection Server window, click Next.

Accept the license agreement and click Next.

Select the installation folder and click Next.

In the Installation Options window, perform the following steps and then click Next.

- Select the type of Horizon server as Horizon Standard Server.
  
  **Note** When you are installing a replicated instance of the connection server, you must select Horizon Replica Server.

- Select the Install HTML Access check box.

Enter the Data Recovery password and click Next.

Select Configure Windows Firewall automatically and click Next.

Select a domain user or a user group that can access the Horizon administrative console and click Next.

Select Join the VMware Customer Experience Improvement Program and click Next.

Select Dell EMC as the deployment type and click Install.

  **Note** You cannot change the deployment location of the Horizon Connection Server after the installation is completed.

In the Installer Completed window, click Finish.

  **Note** Install the second Horizon Connection Server by following the steps described in this procedure. However, you must select Horizon Replica Server as the Horizon server type.

**Configure Horizon Connection Server**

You configure the Horizon Connection Server by:

- Providing a valid license key
- Adding vCenter Server instances to Horizon to create and manage the VMs.
- Adding an instant-clone domain administrator to create instant desktop pools.

**Procedure**

1. Log in to your Horizon Connection Server host at, https://cs1.vx.dts.locale\admin.

2. To enter the licensing information:
   
   a. Click **Settings > Product Licensing and Usage**
   
   b. Enter the license number.
3. To add a vCenter Server instance:
   a. Navigate to **Settings > Servers > Add**
   b. Enter the following information:
      - Server address, user name, and password
      - Port number as **443**.

c. In the **Advanced Settings** section, specify the concurrent operation limits.
d Read the certification information and click **Accept**.
   Skip the **View Composer** configuration as you use instant clones for deployment.

e Configure the storage settings and click **Next**.

f Review the configurations and click **Finish**.

4 To add an instant-clone domain administrator:
   - Click **Settings > Instant Clone Domain Accounts > Add**.
   - Enter the user name and password for the instant-clone domain administrator.

5 Disable the tunnel settings for the Horizon Connection Server:
   - Navigate to **Settings > Servers > Connection Servers**.
   - Select the first Connection Server, for example CS1, and click **Edit**.
   - In the **HTTP(S) Secure Tunnel** section, clear the **Use Secure Tunnel connection to machine** check box.
     - You must clear this check box to disable the Connection Server URL and use the virtual IP address.

6 Click **Ok**.

## Deploy Unified Access Gateway Appliance

Unified Access Gateway is an appliance that is normally installed in a demilitarized zone (DMZ). Unified Access Gateway is used to ensure that the only traffic entering the corporate data center is traffic on behalf of an authenticated remote user. Unified Access Gateway directs authentication requests to the appropriate server and discards any unauthenticated request. Users can access only the resources that they are authorized to access.

**Prerequisites**
- Download the UAG OVF appliance using the My VMware account.
- Create DNS record mapping for UAG1 and UAG2 in the Active Directory for both internal and external IPs.

**Procedure**

1 Use the vSphere Web Client to log in to a vCenter Server instance.

2 Right click the Horizon management resource pool that you previously created and select **Deploy OVF Template**.

3 Select an OVF template and click **Next**.
   - You can select an OVF template by browsing the .ova file you downloaded or by entering a URL.
4 Enter a name for the virtual machine and select the location as SDDC-Datacenter and click Next.

5 Select the Horizon management resource pool that you previously created and click Next.

6 Verify the details and click Next.

7 Select the deployment configuration as Two Nic and click Next.

8 Select WorkloadDatastore and click Next.

9 Select appropriate networks and click Next.

For example, select networks as shown in the following figure, where:

- sddc-cgw-dmz is a DMZ network.
- sddc-cgw-horizon-mgmt is a Horizon management network.
- sddc-cgw-horizon-user-workload is a Horizon desktop network.

Deploy OVF Template

<table>
<thead>
<tr>
<th>Select an OVF template</th>
<th>Select a name and folder</th>
<th>Select a compute resource</th>
<th>Review details</th>
<th>Configuration</th>
<th>Select storage</th>
<th>Select networks</th>
<th>Source Network</th>
<th>Destination Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Internet</td>
<td>sddc-cgw-dmz</td>
</tr>
<tr>
<td>ManagementNetwork</td>
<td>sddc-cgw-horizon-mgmt</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BackendNetwork</td>
<td>sddc-cgw-horizon-user-workload</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

10 In the Customize Template window, do the following:

a IPMode for NIC 1 (eth0): Select STATICV4.

c  Configure the NIC 1 details.

- **NIC 1 (eth0) IPv4 address**: Enter the IPv4 address for NIC 1 to be used as an Internet network interface.
- **DNS server address**: Enter the IP addresses of the domain name server.
- **DNS Search Domain**: Enter the DNS search list.
- **NIC 1 (eth0) IPv4 netmask**: Enter the IP4 netmask for the Internet network interface.
- **IPv4 Default Gateway**: Enter the default gateway address.
d Configure the NIC 2 details.

- **NIC 2 (eth1) IPv4 address**: Enter the IPv4 address for NIC 2 to be used as a management network interface.
- **List of IPv4 custom routes for NIC 2 (eth1)**: Enter the list of IPv4 custom routes.
- **NIC 2 (eth1) IPv4 netmask**: Enter the IP4 netmask for the management network interface.
- **Unified Access Gateway Appliance Name**: Enter the name of the Unified Access Gateway.

e Select **Join the VMware Customer Experience Improvement Program to join CEIP** check box and enter the password.

This is required for root and REST API access for the Unified Access Gateway appliance.

f Select the **Enable SSH** check box and click **Next**.

11 Verify the details and click **Finish**.

**Note** Deploy the second Unified Access Gateway appliance by following the steps described in this procedure.

**Results**

The Unified Access Gateway appliance is deployed and starts automatically.
Configure Unified Access Gateway Appliance

You can configure the security protocols and cryptographic algorithms that are used to encrypt communications between clients and the Unified Access Gateway appliance from the admin configuration pages.

Procedure

1. Open the admin User Interface (UI) by entering the URL
   \[https://<mycoUnifiedGatewayAppliance>.com:9443/admin/index.html\]
   in a web browser.
   In this URL, FQDN-of-UAG1-appliance is DNS-resolvable, fully qualified domain name of the Unified Access Gateway appliance.

2. Log in by entering an admin user name and password.
   Enter the same password that you used when deploying the Unified Access Gateway.

3. Select **Configure Manually** to configure the settings manually.
   You can also import the settings by using the JSON file.
On the **Advanced Settings > System Configuration** page:

a. Verify the Unified Access Gateway name and other settings.

System Configuration

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>UAG Name</td>
<td>UAG1.vx.dts.local</td>
</tr>
<tr>
<td>Locale</td>
<td>en_US</td>
</tr>
<tr>
<td>Password Age</td>
<td>90</td>
</tr>
<tr>
<td>Cipher Suites</td>
<td>TLS_AES_128_GCM_SHA256,TLS_AES_256_GCM_SHA384</td>
</tr>
<tr>
<td>Enable TLS 1.0</td>
<td>NO</td>
</tr>
<tr>
<td>Enable TLS 1.1</td>
<td>NO</td>
</tr>
<tr>
<td>Enable TLS 1.2</td>
<td>YES</td>
</tr>
<tr>
<td>Enable TLS 1.3</td>
<td>YES</td>
</tr>
<tr>
<td>Syslog Type</td>
<td>UDP</td>
</tr>
<tr>
<td>Syslog URL</td>
<td></td>
</tr>
<tr>
<td>Syslog Audit URL</td>
<td></td>
</tr>
<tr>
<td>Health Check URL</td>
<td>/favicon.ico</td>
</tr>
<tr>
<td>Cookies To Be Cached</td>
<td>none</td>
</tr>
<tr>
<td>Quiesce Mode</td>
<td>NO</td>
</tr>
<tr>
<td>Monitor Interval</td>
<td>60</td>
</tr>
<tr>
<td>Authentication Timeout</td>
<td>300000</td>
</tr>
<tr>
<td>Body Receive Timeout</td>
<td>15000</td>
</tr>
</tbody>
</table>

b. Verify the DNS server details, NTP server details, and other settings.

Body Receive Timeout: 15000

Maximum Connections per Session: 16

Client Connection Idle Timeout: 360
5  Click **Save**.

6  On the **Network Settings** page, verify the default gateway details and other settings.

   **Network Settings**

<table>
<thead>
<tr>
<th>IPv4 Default Gateway</th>
<th>192.168.3.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Default Gateway</td>
<td>Not Available</td>
</tr>
</tbody>
</table>

   **NIC 1: Internet facing interface**

   - IP Mode: IPv4
   - IP Allocation Mode: STATICv4
   - IPv4 Address: 192.168.3.28
   - IPv4 Netmask: 255.255.255.0
   - IPv4 Static Routes: 
   - IPv6 Address: Not Available
   - IPv6 Prefix: Not Available

   **NIC 2: Management network interface**

   - IP Mode: IPv4
   - IP Allocation Mode: STATICv4
   - IPv4 Address: 192.168.2.28
   - IPv4 Netmask: 255.255.255.0
   - IPv4 Static Routes: 
   - IPv6 Address: Not Available
   - IPv6 Prefix: Not Available

   ![Close button](image)

7  Click **Close**.

**What to do next**

Configure the edge service settings for the components that Unified Access Gateway is deployed with. After the edge settings are configured, configure the authentication settings.

**Configure Edge Service Settings**

You can deploy Unified Access Gateway with Horizon Cloud with On-Premises Infrastructure and Horizon Air cloud infrastructure. For the Horizon deployment, the Unified Access Gateway appliance replaces Horizon security server.
Procedure

1. Open the admin UI by entering the URL

2. Log in by entering an admin user name and password.
   Enter the same password that you used when deploying the Unified Access Gateway.

3. In the Configure Manually section, click Select.

4. In the General Settings > Edge Service Settings, click Show.

5. Click the Horizon Settings gearbox icon.

6. On the Horizon Settings page, toggle Enable Horizon to YES.
7 Configure the edge service settings for Horizon.

### Horizon Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Horizon</td>
<td>YES</td>
</tr>
<tr>
<td>Connection Server URL *</td>
<td><a href="https://cs1.vx.dts.local:443">https://cs1.vx.dts.local:443</a></td>
</tr>
<tr>
<td>Connection Server URL Thumbprint</td>
<td>sha1-4a8c06eb45a51bde10e320043352bb6018b1</td>
</tr>
<tr>
<td>Connection Server IP mode</td>
<td>IPv4</td>
</tr>
<tr>
<td>Re-Write Origin Header</td>
<td>NO</td>
</tr>
<tr>
<td>Enable PCOIP</td>
<td>YES</td>
</tr>
<tr>
<td>Disable PCOIP Legacy Certificate</td>
<td>NO</td>
</tr>
<tr>
<td>PCOIP External URL</td>
<td></td>
</tr>
<tr>
<td>Enable Blast</td>
<td>YES</td>
</tr>
<tr>
<td>Blast External URL</td>
<td></td>
</tr>
<tr>
<td>Enable UDP Tunnel Server</td>
<td>NO</td>
</tr>
<tr>
<td>Blast Proxy Certificate</td>
<td>Select</td>
</tr>
<tr>
<td>Enable Tunnel</td>
<td>NO</td>
</tr>
</tbody>
</table>

### Notes

a **Connection Server URL**: Enter the address of the first Horizon Connection Server. For example, enter https://<first connection server>.

b Do the following to obtain the thumbprint:

1. Log in to the Horizon Connection Server by entering the Horizon Connection Server URL in a web browser.
2 Click Not secure.

Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

You have chosen to disable security warnings for this site. Re-enable warnings

- Certificate (Invalid)
- Cookies (3 in use)
- Site settings
3 Click **Certificate > Details > Thumbprint.**

![Certificate Thumbprint](image)

4 Copy the Thumbprint.

c **Connection Server URL Thumbprint:** Paste the thumbprint in the text box by suffixing it with `sha1=`.

For example, enter `sha1=4a8c06eb45a51bde10e320043352bb6018b1ee47`.

d **Connection Server IP mode:** Select **IPv4**.

The connection server IP mode indicates the IP mode of a Horizon Connection Server.

e Toggle **Enable PCOIP** to **Yes**.

f Toggle **Enable Blast** to **Yes**.

All other details on the **Horizon Settings** page are populated by default.

8 Click **Save**.
Results

The edge server establishes connection with the Unified Access Gateway appliance. The successful connections are displayed in green as shown in the following figure.

Unified Access Gateway Appliance v3.10

Note  Configure the second Unified Access Gateway by following the steps described in this procedure.
Configuring Load Balancer

Software load balancing is required to route network traffic to different servers.

This chapter includes the following topics:
- Deploy AVI Controller
- Configure AVI Controller
- Deploy Avi Service Engine
- Configure Avi Service Engine

Deploy AVI Controller

Avi controllers exchange information securely with the service engines. The health of servers, client-connection statistics, and client-request logs collected by the service engines are regularly uploaded to the controllers. The controllers and service engines together process logs and aggregate analytics.

Procedure

1. Download the AVI controller appliance.
   - Contact your sales representative to get the Avi controller installer.
2. Use the vSphere Web Client to log in to a vCenter Server instance.
3. Right-click the Horizon management resource pool and select Deploy OVF template.
4. On the Select an OVF template page, select Local file, click the button to upload files, and navigate to the Avi controller file on your local machine.
5. On the Select a name and folder page, enter a unique name for the virtual machine and select a deployment location.
7. On the Review details page, verify the details.
8. On the Select storage page, select WorkloadDatastore.
On the **Select networks** page, select the management network as the destination network. For example, select `sddc-cgw-horizon-mgmt`.

### Deploy OVF Template

- **Select networks**
  - Select a destination network for each source network.

<table>
<thead>
<tr>
<th>Source Network</th>
<th>Destination Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>sddc-cgw-horizon-mgmt</td>
</tr>
</tbody>
</table>

### IP Allocation Settings

- **IP allocation:** Static - Manual
- **IP protocol:** IPv4
10 On the **Customize template** page, enter the management IP address, subnet mask, default gateway, and sysadmin login authentication key.

Sysadmin login authentication key is used when you are deploying the service engine. Therefore, save the authentication key.

**Deploy OVF Template**

<table>
<thead>
<tr>
<th>7 Customize template</th>
<th>Customize template</th>
<th>Customize the deployment properties of this software solution.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Application</td>
<td>4 settings</td>
</tr>
<tr>
<td>Management Interface IP Address</td>
<td>IP address for the Management Interface. Leave blank if using DHCP. Example: 192.168.10.4, 192.168.2.30</td>
<td></td>
</tr>
<tr>
<td>Management Interface Subnet Mask</td>
<td>Subnet mask for the Management Interface. Leave blank if using DHCP. Example: 24 or 255.255.255.0, 255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Optional default gateway for the Management Network. Leave blank if using DHCP.</td>
<td>192.168.2.1</td>
</tr>
<tr>
<td>Sysadmin login authentication key</td>
<td>Sysadmin login authentication key</td>
<td>VMware:</td>
</tr>
</tbody>
</table>

11 On the **Ready to complete** page, review the details and click **Finish** to deploy the Avi controller.

**Configure AVI Controller**

Configure the Avi Controller to manage your service engines.

**Procedure**

1 Open a web browser and enter the management IP of the controller.

For example, enter the management IP https:\192.168.2.30, which you assigned to the Avi controller when deploying it.
2 Enter the user name, assign a password, and then click Create Account.

3 Enter the following information and click **Next**:
   - DNS server IP address
   - DNS search domain name
   - Backup password
   - NTP server IP address
System Settings
Let’s get started with some basic setup questions.

DNS Resolver(s)
192.168.200.10

DNS Search Domain
vx.dts.local

Backup Configuration

Backup Passphrase
******

Confirm Backup Passphrase
******
4 Leave the SMTP Source and From Address as is and click Next.
5 Select **No Orchestrator**.

You must select **No Orchestrator** as you are creating the service engine appliance VMs manually. For an on-premises automated deployment of Avi on vCenter, appropriate read and write permissions to the vCenter API and access ESX management plane is required. The cloudadmin@vmc.local user does not have the required permissions.
6 Select **No** to **Support multiple Tenants**.

You are redirected to the Avi Vantage UI where you can download the service engine ova template.

**Deploy Avi Service Engine**

Avi Service Engines handle all the data plane operations within Vantage. The Service Engines host the virtual services and require either direct or routable access to the client and server networks. One or more Service Engines are grouped to share properties, such as network access and failover.

A typical Vantage deployment may have many Service Engines for various purposes, such as redundancy, scalability, and accommodating large numbers of applications being served.

**Procedure**

1. Log in to the Avi Controller console as an administrator.
2. Navigate to **Infrastructure > Clouds**.
3. Click the download icon (down arrow) and select **Ova**.
4 Click the key to generate a token.

An authentication token for Avi controller and controller cluster UUID for Avi controller is generated.

5 Use the vSphere Web Client to log in to a vCenter Server instance.

6 Right-click the Horizon management resource pool and select **Deploy OVF template**.

7 On the **Select an OVF template** page, select **Local file**, click the button to upload files, and navigate to the service engine OVA file on your local machine.

8 On the **Select a name and folder** page, enter a unique name for the virtual machine and select a deployment location.

9 On the **Select a compute resource** page, select **Horizon-Mgmt-ResourcePool**.

10 On the **Review details** page, verify the details.

11 On the **Select storage** page, select **WorkloadDatastore** to deploy the VM.

12 On the **Select networks** page, select the management network, Data Network 1.

   For example, select **sddc-cgw-dmz**.

   **Note** Only the management network and Data Network 1 interfaces are enabled.
13 On the **Customize template** page, enter details in all the text boxes as shown in the following figure.

14 On the **Ready to complete** page, review the details and click **Finish** to deploy the service engine.
15 Configure the IP address for Data Network 1:
   a From the Horizon Management Resource Pool, click the Service Engine VM.
   b Navigate to Summary > VM Hardware.
   c Expand Network adaptor 2 and copy the MAC address.
   d Log in to the Avi Controller console as an administrator.
   e Click Infrastructure > Service Engine.
   f Click the pencil icon to edit the interface.
   g In the MAC Address column, locate the MAC address that you copied.
   h Enter the IP address in the Static IPv4 text box corresponding to the Service Engine group where you located the MAC address.
   i Click Save.

**Note** Deploy the second Avi Service Engine by following the steps described in this procedure.

---

**Configure Avi Service Engine**

Configuring Avi service engine requires you to create an IP group, create a custom health monitor profile, create a pool, install the SSL certificate required for virtual IP (VIP), and create a virtual service.

**Prerequisites**

- Ensure that you have already deployed Unified Access Gateway.
- Ensure that Avi controller is deployed and you have access to the controller and Avi console.

**Procedure**

1 **Create an IP Group**
   Create an IP group which has a list of Unified Access Gateway servers that need to be used for load balancing.

2 **Create a Custom Health Monitor Profile**
   Create a health monitor profile to monitor the health of Horizon.

3 **Create L7 Pools**
   Pools contain the list of servers assigned to them and perform health monitoring, load balancing, persistence, and functions that involve Avi-Vantage-to-server interaction. The pools establish a communication between Avi Vantage and server.
4 **Install the SSL Certificate Required for VIP**
   The SSL connection is terminated at Avi virtual service. Therefore, the SSL certificate must be assigned to the virtual service. For this assignment to happen, it is necessary to install the SSL certificate at Avi Vantage.

5 **Create L7 Virtual Service**
   Create a virtual service with the Unified Access Gateway server's VIP. The client devices connect to this VIP.

6 **Create a Static Route**
   Specify the default gateway and next hop IP address for a static routing from the Service Engine.

**Create an IP Group**
Create an IP group which has a list of Unified Access Gateway servers that need to be used for load balancing.

IP groups are comma-separated lists of IP addresses you can reference by profiles, policies, and logs. Since the same Unified Access Gateway servers are used as pool members in two different pools, you can attach IP groups to the pool rather than directly attaching servers to the pool. Any configuration changes to the pool members such as addition or removal of servers, you must do the changes at the IP Group level.

**Procedure**
1. From the Avi console, navigate to **Templates > Groups**.
2. Click **Create IP Group**.
3. Enter the **IP Group Name**.
In the **IP Information** section, enter the IP Address of Unified Access Gateway servers.

<table>
<thead>
<tr>
<th>IP Information</th>
<th>IP Group Name</th>
<th>UAG Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select by IP Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>1.1.1.1, 2.2.2.2, 3.3.3.3, 4.4.4.4, 5.5.5.5, 6.6.6.6</td>
<td></td>
</tr>
</tbody>
</table>

Click **Add**.

Click **Save**.

**What to do next**

**Create a Custom Health Monitor Profile**

**Create a Custom Health Monitor Profile**

Create a health monitor profile to monitor the health of Horizon.

**Procedure**

1. From the Avi console, navigate to **Templates > Profiles > Health Monitors**.
2. Click **Create**.
3. On the **New Health Monitor** page, enter the profile information for Horizon.
   a. **Name**: Enter a name for the health monitor. For example, enter the name as **Horizon-HTTPS**.
   b. **Type**: Select **HTTPS**.
   c. **Health Monitor Port**: Enter **443**.
   d. **Client Request Data**: Enter **GET /favicon.ico HTTP/1.0**.
   e. **Response Code**: Select **2XX**.
SSL Attributes: Select the check box.

SSL Profile: Select System-Standard.

4 Click Save.

What to do next

Create L7 Pools.

Create L7 Pools

Pools contain the list of servers assigned to them and perform health monitoring, load balancing, persistence, and functions that involve Avi-Vantage-to-server interaction. The pools establish a communication between Avi Vantage and server.

Pools are added to VS (Virtual Service). One VS points to one pool.

Procedure

1 From the Avi Vantage UI, navigate to Applications > Pools.

2 In the New Pool window, enter the required information in addition to the following:

a Load Balance: Select Consistent Hash with Source IP Addresses as the hash key.

b In the Health Monitors section, click Add Active Monitor.

c Select the health monitor that you created previously.

For example, select Horizon-HTTPS. See Create a Custom Health Monitor Profile.

d Enable SSL: Select the check box.

e SSL Profile: Select System-Standard.

3 Click Next.
4  In the Servers tab, add the previously created IP Group of Unified Access Gateway servers.

5  Navigate to Advanced > Review and review the details.

6  Click Save.

What to do next

Install the SSL Certificate Required for VIP

Install the SSL Certificate Required for VIP

The SSL connection is terminated at Avi virtual service. Therefore, the SSL certificate must be assigned to the virtual service. For this assignment to happen, it is necessary to install the SSL certificate at Avi Vantage.

Note  It is recommended to install a certificate signed by a valid certificate authority instead of using self-signed certificates.

For more information about installing the SSL certificate, see Avi documentation.

What to do next

Create L7 Virtual Service.

Create L7 Virtual Service

Create a virtual service with the Unified Access Gateway server’s VIP. The client devices connect to this VIP.
### Procedure

1. From the Avi Vantage UI, navigate to **Applications > Virtual Services**.
2. Click **Create Virtual Service > Advanced Setup**.
3. In the **New Virtual Service** window, configure the virtual service.

   - **Name**: Enter the virtual service name.
   - **FQDN or IPv4 Address**: Enter the load balancer virtual IP address.
   - **Services**: Enter the port number as 443.
   - **SSL**: Select the check box for the port number 443 to enable SSL.
   - **Application Profile**: Select **System-Secure-HTTP-VDI**.
   - **Pool**: Select the pool that you previously created.
   - **SSL Profile**: Select **System-Standard**.
   - **SSL Certificate**: Select the SSL certificate that you previously installed.

4. Click **Next**.
5. Navigate to the **Advanced** tab.
6. Click **Save**.

**Note**: If you encounter an issue launching the HTML desktops using Avi load balancer, navigate to `install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`, and add `VIP URL/IP address balancedHost=192.168.3.35` to the `locked.properties` file and restart the connection server.
Create a Static Route

Specify the default gateway and next hop IP address for a static routing from the Service Engine.

Procedure

1. Log in to the Avi Controller console as an administrator.
2. Click **Infrastructure > Routing > Static Route**.
3. Click **Create** and enter the **Gateway Subnet** and **Next Hop**.
   
   For example, enter the gateway subnet as 0.0.0.0/0 and next hop as 192.168.3.1.
4. Click **Save**.
Preparing a Virtual Machine for Cloning

You can create a pool of desktop machines by cloning a vCenter Server virtual machine (VM). Before you create the desktop pool, you need to prepare and configure this VM, which will be the parent, or master image of the clones.

This chapter includes the following topics:

- Create Instant-Clone Desktop Pools
- Install Horizon Agent

Create Instant-Clone Desktop Pools

An instant-clone desktop pool is an automated desktop pool. vCenter Server creates the desktop VMs based on the settings that you specify when you create the pool.

Procedure

1. Log in to your Horizon Connection Server host.
2. Click Inventory > Desktops.
3. Click Add.
4. Select Automated Desktop Pool and click Next.
5. Select Instant Clones, select the vCenter Server instance, and click Next.
6. Select one of the following and click Next:
   - Floating: In a floating user assignment, users are assigned random desktops from the pool. Floating instant-clones are compatible with App Volumes. For a floating instant-clone desktop pool, the MAC address is preserved on a resync or refresh.
   - Dedicated: In a dedicated user assignment, each user is assigned a particular remote desktop and returns to the same desktop at each login. Between each login and logout, the computer name and MAC address is retained for the same desktop. Any other changes that the user makes to the desktop are not preserved. Dedicated instant-clones with Refresh OS Disk After Logoff to Always are compatible with App Volumes.
7. Select Use VMware vSAN, and click Next.
8  Enter an ID and unique name for the pool and click **Next**.

If you have multiple Horizon Connection Server configurations, ensure that another Connection Server configuration does not use the same pool ID. A Connection Server configuration can consist of a single Connection Server or multiple Connection Servers.

9  Specify the pool provisioning settings and click **Next**.

![Add Pool - Windows-10-1909-Default-Pool](image)

- **Type**
- **vCenter Server**
- **User Assignment**
- **Storage Optimization**
- **Desktop Pool ID**
- **Provisioning Settings**
- **vCenter Settings**
- **Desktop Pool Settings**
- **Remote Display Settings**
- **Guest Customization**

**Default Image**
- **Parent VM in vCenter**
  - `/SDC-Datacenter/vm/Gold_img`
- **Snapshot**
  - `/Snapshot-1`

**Virtual Machine Location**
- **VM Folder Location**
  - `/SDC-Datacenter/vm/Workloads`

**Resource Settings**
- **Cluster**
  - `/SDC-Datacenter/host/Cluster-1`
- **Resource Pool**
  - `/SDC-Datacenter/host/Cluster-1/Resources/Compute-ResourcePool/Horizon`
- **Datastores**
  - 1 selected
- **Network**
  - 1 selected

10  In the **vCenter Settings** wizard, verify the details in and click **Next**.

- **Select the parent VM.**
- **Select the snapshot of the master image to use for the desktop pool.**
  - The instant-clone desktop pool that is created is based on the snapshot and inherits those memory settings.
- **Select the folder in vCenter Server for the desktop VMs.**
- **Select the vCenter Server cluster for the desktop VMs.**
  - For example, select Horizon-User-ResourcePool.
- **Select the datastores for the desktop VMs.**
  - For example, select WorkloadDatastores.
- **Select the networks to use for the instant-clone desktop pool.**
11 In the Desktop Pool Settings wizard, edit the settings, if necessary and click **Next**.

12 Specify the following and click **Next**:

- **Default Display Protocol**: The remote display protocol to use as the default for the remote desktop.
- **Allow Users to Choose Protocol**: Indicates whether to allow the users to override the default or not.

13 Specify the following and click **Next**:

- **AD Container**: Specify the Active Directory container’s relative distinguished name. For example: CN=Computers.
- **Allow reuse of preexisting computer account**: Select this option to use existing computer accounts in Active Directory when the virtual machine names of new instant clones match the existing computer account names.

14 In the Ready to Complete wizard, select **Entitle users after adding Pool**, and click **Submit**.

**Install Horizon Agent**

You must install Horizon Agent on virtual machines that are managed by vCenter Server so that Connection Server can communicate with them. Install Horizon Agent on all virtual machines that you use as templates for full-clone desktop pools, parents for linked-clone desktop pools, master images for instant-clone desktop pools, and machines in manual desktop pools.

**Procedure**

1. Download and save the installer to your Windows VM.
2. To start the installation process, right-click the installer file and select **Run as Administrator**.
   
   The installer filename is `VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe`, where `y.y.y` is the version number and `xxxxxx` is the build number.
3. Accept the VMware license terms.
4. Select whether to enable or disable FIPS mode.
   
   This option is available only if FIPS mode is enabled in Windows.
5. Select your custom setup options.
6. Accept or change the destination folder.
7. Follow the prompts in the Horizon Agent installation program and finish the installation.

**Note** If you did not enable Remote Desktop support during guest operating system preparation, the Horizon Agent installation program prompts you to enable it. If you do not enable Remote Desktop support during Horizon Agent installation, you must enable it manually after the installation is finished.
If you selected the USB redirection option, restart the virtual machine to enable USB support. In addition, the **Found New Hardware** wizard might start. Follow the prompts in the wizard to configure the hardware before you restart the virtual machine.

What to do next

Capture the snapshot and deploy the desktop pools. After you deploy the desktop pools, open the **Horizon Client > New Server** and enter the URL of the load balancer VIP to access Horizon desktop pools.