Configure Avi
Vantage for VMware
Horizon

Avi Technical Reference (v18.2)
Configure Avi Vantage for VMware Horizon

Overview

This article shows how Avi Vantage can be configured for load balancing in VMware Horizon deployments. Avi Vantage can be deployed in front of Unified Access Gateways (UAG) and/or in front of the connection servers as required.

Prerequisites

To configure Avi Vantage for VMware Horizon deployments, ensure the following prerequisites are met:

* The Horizon environment is up and running
* The Avi Controller is deployed. Refer to Installing Avi Vantage for VMware vCenter for more information
* The vCenter cloud on the Avi Controller is created

Avi Vantage for UAG Load Balancing

There are three ways to deploy Avi Vantage for UAG load balancing:

- Single Virtual IP (VIP) with two virtual services
- Single L4 virtual service
- (n+1) VIP
Avi Vantage for Connection Server Load Balancing

Avi Vantage can be used to load balance traffic to the connection servers as well. A single virtual service (L4 or L7) can service both internal clients directly and external clients via UAG.

Refer to the [Connection Server Load Balancing](#) section to know more.

Configuring UAG Load Balancing

The following steps are one-time configurations for UAG load balancing: 1. Create custom health monitor for UAG 2. Create SSL profile and install SSL certificate (required for L7 VIP)

Configuring Single VIP with Two Virtual Services

Single VIP with two virtual services can be configured as shown below:

1. [Create IP group with UAG as members](#)
2. [Create custom Health Monitor for UAG](#)
3. [Create pools](#)
4. [Create SSL profile and install SSL certificate](#)
5. [Create an L7 virtual service](#)
6. [Create an L4 virtual service](#) using the L7 virtual service as shared VIP and specify all the ports required for secondary protocols

Creating IP Group

IP groups are comma-separated lists of IP addresses that may be referenced by profiles, policies, and logs. Since same UAG servers are used as pool members in two different pools, IP groups can be attached to the pool instead of directly attaching servers to the pool. Any configuration change to the pool members like addition or removal of servers needs to be done at the IP Group level.

To create an IP group, 1. From the Avi UI, navigate to Templates > Groups > IP Groups. 2. Click on Create IP Group. 3. Under IP Information, enter the IP Address to be added, and click on Add Server.
4. Click on Save.

Creating Custom Health Monitor for Horizon

To create a custom health monitor, 1. From the Avi UI, navigate to Templates > Profiles > Health Monitors. 2. Click on Create. 3. Select the vCenter cloud that was created for Horizon. 4. Enter the following details in the New Health Monitor screen.

```
<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Interval</td>
<td>30</td>
</tr>
<tr>
<td>Receive Timeout</td>
<td>10</td>
</tr>
<tr>
<td>Client Requested Data</td>
<td>GET /favicon.ico HTTP/1.0</td>
</tr>
<tr>
<td>Response Code</td>
<td>2xx</td>
</tr>
</tbody>
</table>
```

The New Health Monitor screen is as shown below:
5. Click on Save.

**Creating Pools**

Pools maintain the list of servers assigned to them and perform health monitoring, load balancing, persistence, and functions that involve Avi Vantage-to-server interaction. A typical virtual service will point to one pool.
A pool includes the IP address of the UAG servers i.e. UAG server01 and UAG server02.

Create two pools: * For L7 (HTTPS) i.e. Horizon-L7-pool * For secondary protocols named as Horizon-L4-pool

These two pools are required to attach to the two virtual services which will be created.

Consistent hash with source IP address as the key should be configured as the hash algorithm to maintain source IP affinity.

**Creating the Horizon L7 Pool**

To create the pool, 1. In Avi Vantage, navigate to Applications > Pools. 2. Select the vCenter cloud from the Select Cloud sub-screen. 3. Click on Next. 4. Click on Create Pool. 5. In the New Pool: screen, update the details as shown below:

- **Load Balance**: Consistent Hash with Source IP Address as the hash key.
- **Health Monitors**: Passive Health Monitor
- **Enable SSL**: Check the box
- **SSL Profile**: System Standard

**Note**: The load balancing algorithm is configured as Consistent Hash with Source IP Address as the hash key.

6. To bind the monitor, click on Add Active Monitor and select the HTTPS monitor that was created. 7. Click on Next. 8. Click on Enable SSL and select the appropriate SSL profile as shown below:
9. Click on Next.
10. In the Step 2: Servers tab, add the IP Group of the UAG servers created earlier.

![Edit Pool: Horizon-L7-pool](image)

11. Click on Next. 12. Navigate to Step 3: Advanced tab > Step 4: Review. 13. Click on Next and then click on Save.

**Creating the Horizon L4 Pool**

Create a pool with the name *Horizon-L4-pool*. Ensure that the pool configuration (port, UAG server IP, load balancing algorithm, health monitor etc.) is the same as the Horizon L7 Pool.

**Note:** Configure the default server port to 443 and the load balancing algorithm as *Consistent Hash with Source IP Address*. 

![New Pool: Horizon-L4-Pool](image)
Under the Step 2: Servers tab, add the IP Group of the UAG servers created earlier.

Install the SSL certificate Required for L7 VIP

The SSL connection is being terminated at Avi virtual service. Therefore, the SSL certificate must be assigned to the virtual service. It is advised to install a certificate which is signed by a valid certificate authority instead of using self-signed certificates.

Install the certificate in Avi Vantage, and ensure the CA certificate is imported and linked. For instructions, refer to Import Certificates.

Note: For this set up, a certificate named Horizon_Certificate has been installed.

Creating L7 Virtual Service

To create the new L7 virtual service,

1. From the Avi UI, navigate to Applications > Virtual Services.
2. Click on Create Virtual Service > Advanced Setup.
3. Use the System-Secure-HTTP-VDI as the Application Profile
4. Configure the virtual service as shown below:
4. Click on Next.
5. Click on Next.
6. Click on Next > Save.

**Creating L4 Virtual Service**

Create another virtual service which will share the same IP address as that of the L7 VIP. This will make sure that we need only one virtual IP address for both the primary and secondary protocols. L7 virtual service will handle the primary protocol and the tunnel whereas L4 virtual service will handle other secondary protocols.

To create an L4 virtual service, 1. Click on Create Virtual Service > Advanced Setup. 2. In the New Virtual Service screen, click on Switch to Advanced under VIP Address as shown below:

3. Select the L7 virtual service that was created as the Virtual Service for VIP Sharing as shown below:
4. Under Service Port > Services, click on Switch to Advanced. 5. Add the port numbers for the secondary protocols as shown below: * 443 UDP to override TCP/UDP and use System-UDP-Fast-Path-VDI as the profile * Add 8443 for Blast * Add 8443 UDP to override TCP/UDP and use System-TCP-Proxy as the profile * Add 4172 for PCoIP * Add 4172 UDP to override TCP/UDP and use System-UDP-Fast-Path-VDI as the profile
The virtual service is configured as shown below:

6. Under the section Pool, select the option Pool and choose the Horizon Pool as shown below:

7. Click on Next. Click on Next > Save.

With this, the configuration is complete and ready to use the Avi load balancer for Horizon.

Note: Ensure the following: * L4 and L7 pools have the same configuration. * The option Disable Port Translation is enabled under Advanced Settings for an L4 pool.

**Best Practice**

It is recommended to create a new SSL profile and bind the same to the virtual service instead of using the default SSL profile for higher security ratings. To create a new SSL profile, 1. In the Avi UI, navigate to Templates > Security > SSL/TLS Profile > Create > Application Profile. 2. In the New SSL/TLS Profile screen, select the Ciphers and the TLS version. 3. Enable TLS 1.1 and TLS 1.2 for backward compatibility with older Horizon clients.
4. Click on Save.

This profile will ensure that there are no issues with backward compatibility with old clients and also avoid security related issues.

**Configuring Single L4 Virtual Service on Avi Vantage**

In this design, a single Virtual Service with an L4 profile services all protocols.

**Configuring L4 Virtual Service on Avi Vantage**

L4 virtual service configuration on Avi Vantage is done in the following steps:

1. Create custom health monitor for UAG.
2. Create a Pool
3. Create an L4 Virtual Service

**Creating a Pool**

1. From the Avi UI, navigate to Applications > Pools.
2. Click on Pool.
3. Configure the pool as shown below:
4. Click on +Add Health Monitor and select the *Horizon HTTPS Monitor* that was created.

```
Horizon HTTPS
```


6. Select Disable Port Translation as shown below:

```
Connection Pool Settings

Connection Idle Timeout  60000  ms
Connection Life Timeout  600000  ms
Connection Max Used Times  0
Max Cache Connections Per Server  0

Other Settings

Disable Port Translation  
Default Server Timeout  0  ms
```

![Image of the interface showing the settings for disabling port translation]
6. Click on Next > Save.

Creating L4 Virtual Service

1. From the Avi UI, navigate to Applications > Virtual Services.
2. Click on Create Virtual Services > Advanced Setup.
3. In the New Virtual Service: screen, enter the virtual service name and other details.
4. Under Service Port, click on Switch to Advanced.
5. Add the following port numbers for both the primary and secondary protocols:
   - 443 for primary HTTPS protocol
   - 443 UDP to override TCP/UDP and use System-UDP-Fast-Path-VDI as the profile
   - 8443 for Blast
   - 8443 UDP to override TCP/UDP and use System-UDP-Fast-Path-VDI as the profile
   - 4172 for PCoIP
   - 4172 UDP to override TCP/UDP and use System-UDP-Fast-Path-VDI as the profile

Note: The application profile and the pool (Horizon-L4-pool) are bound to the virtual service.
6. Click on Next > Next > Save.

With this, the configuration is complete and ready to use the Avi Vantage load balancer for Horizon.

**Configuration Automation**

If required, use Ansible playbooks or Terraform to automate the configuration for shared VIP and L4 VIP.

**Configuring (n+1)VIP in Avi Vantage**

In this design, only the primary HTTPS protocol will be load balanced by Avi. UAGs have to be configured with public IPs and the Blast External URL and PCoIP External URL on each UAG will be configured to the same UAG.

Follow the steps below to configure (n+1)VIP in Avi Vantage: 1. Create a custom health monitor for UAG 2. Create a Pool 3. Create an L7 Virtual Service

**Create a Pool**

1. From the Avi UI, navigate to Applications > Pools. 2. Click on Create Pool. 3. In the New Pool: screen enter details as shown below:
4. To bind the monitor, click on Add Active Monitor and select the **HTTPS monitor** that was created. Note: It is recommended to create a HTTPS type monitor with the required timers. Set the timeout interval to be more than six seconds to account for any delay caused by connection servers response to the health monitor probes, if connection servers are configured with full logging level (used for debugging). 5. Click on Next. 6. Click on Add Server. 7. Add the IP address of UAG server01. 8. Click on Add Server. 9. Add the IP address of UAG server02.

The New Pool: screen appears as shown below:
10. Click on Next > Save.

Note: Ensure that connection multiplexing is disabled for the System-Secure-HTTP-VDI profile. To know how to disable connection multiplexing, click here.

Creating L7 Virtual Service

To create the L7 virtual service,

1. From the Avi UI, navigate to Applications > Virtual Services.
2. Click on Create Virtual Service > Advanced Setup.
3. Configure the virtual service as shown below:

4. Click on Next.

Load Balancing Traffic to Connection Servers

Both L4 and L7 virtual services are supported to load balance traffic to connection servers. You can choose to use either one, as required.

Using an L4 Virtual Service

Creating Custom Health Monitor for Connection Servers

1. From the Avi UI, navigate to Templates > Profiles > Health Monitors.
2. Click on Create.
3. In the New Health Monitor screen, select the Type as HTTPS.
4. Set the Send Interval to 30 seconds and Receive Timeout to 10 seconds. The New Health Monitor screen is as shown below:

5. Select the Response Code as 2xx.
6. Select an appropriate SSL Profile.

7. Click on Save.
Creating a Pool

Pool members are connection servers. Use the appropriate load balancing algorithm, as required. Least Connections or Round Robin can be used as the preferred method.

To create a pool, from the Avi UI, 1. Navigate to Applications > Pools. 2. Click on Create Pool. 3. Enter the details as shown below:

4. Click on Next. 5. Enter the Server IP Address and click on Add Server.

6. Click Next and enter the details as required under the Advanced tab. 7. Click Next and click Save.
Creating an L4 Virtual Service

To create the L4 virtual service, 1. Navigate to Applications > Virtual Services. 2. Click on Create Virtual Service > Advanced Setup. 3. Enable SSL and choose the required SSL Profile. 4. Select the System-L4-Application as the Application Profile.

![New Virtual Service: Connection Server Virtual Service L4](image)

5. Select the Connection Server Pool L4 as the Application Profile.

![New Virtual Service: Connection Server Virtual Service L4](image)

5. Click on Next and navigate to Step 4: Advanced. 6. Click on Save.

Similarly, you can use the L4 SSL with the Application Profile System-SSL-Application instead of System-L4-Application.

Using an L7 Virtual Service

Create Custom Health Monitor for Connection Servers

1. From the Avi UI, navigate to Templates > Profiles > Health Monitors. 2. Click on Create. 3. In the New Health Monitor screen, select the Type as HTTPS. 4. Set the Send Interval to 30 seconds and Receive Timeout to 10 seconds. The New Health Monitor screen is as shown below:
5. Select the Response Code as 2xx. 6. Select an appropriate SSL Profile.

7. Click on Save.

Creating a Pool

If connection servers are configured in the replication mode then persistence on the connection server is not required. In the non-replication mode, use Consistent Hash - Source IP address as the load balancing algorithm.

Enable SSL to backend with appropriate SSL profile(System-Standard used in example). To create a pool, from the Avi UI, 1. Navigate to Applications > Pools. 2. Click on Create Pool. 3. Enter the details as shown below:
3. Click on Next. 4. Enter the Server IP Address and click on Add Server.

5. Click Next and enter the details as required under the Advanced tab. 6. Click Next and click Save.

Creating an L7 Virtual Service

To create the L7 virtual service, 1. Navigate to Applications > Virtual Services. 2. Click on Create Virtual Service > Advanced Setup. 3. Enable SSL and choose the required SSL Profile. 4. Select the Connection Server Pool as shown below:
5. Click on Next and navigate to Step 4: Advanced. 6. Click on Save.

The following are the changes in the UAG server when the load balancer is present between the UAG and connection server:

**Horizon Settings**

- **Enable Horizon**: YES
- **Connection Server URL**: 
- **Connection Server URL Thumbprint**: 
- **Connection Server IP mode**: IPv4
- **Enable PCOIP**: YES
- **Disable PCOIP Legacy Certificate**: NO

- The connection server URL should point to the Avi load balancer.
The connection server URL thumbprint:

- For an L7 virtual service: The connection server URL thumbprint is taken from the certificate that is bound to the Avi load balancer.
- For an L4 virtual service: The connection server URL thumbprint is be taken from the certificate that is present in the connection server itself.
- For an L4 virtual service with SSL (System-SSL-Application) the connection server URL thumbprint is taken from the certificate that is bound to the Avi load balancer.

### Enabling WAF For Horizon

Avi Vantage supports WAF for HTTP/HTTPS traffic for Horizon deployments. WAF rules are supported for L7 virtual service for primary protocol (XML/API) traffic.

Notes: * It is recommend to use the default CRS rules. The other rules for response inspection are not required and these signatures or rules should not be enabled in CRS rules. * It is mandatory to add the WAF policy and whitelist URI containing /ice/tunnel/ and /ice/reconnect to make sure the WAF feature works seamlessly with the horizon application. Similarly, whitelist other /ice/ related URIs, if any. Whitelisting all URIs beginning with /ice is a best practice.

Create a L7 virtual service (or use the existing virtual service) and follow the steps mentioned below:

1. **Creating a WAF profile**
   
   Navigate to Template > WAF > WAF Profile. Click on create to create a new profile. Provide the desired name and leave the remaining fields as default as shown below.

2. **Creating WAF policy**
   
   Navigate to Template > WAF > WAF Policy. Select the WAF profile created in the previous step. The default profile can be used too.
3. Adding a whitelist rule

This whitelist makes sure WAF does not block the request having URI which contains /ice/tunnel. This is a mandatory step. Select the Whitelist tab, click on Add Rule.

Provide the following attributes: * Criteria: Contains * String Value: /ice/tunnel/ * Action: ALLOW
To whitelist all URIs beginning with /ice, create the rule as shown below:

Similarly, you can create another whitelist rule for /ice/reconnect.

3. Associating with the required virtual service

Once the WAF profile is ready, navigate to Application > Virtual Service. Select the required L7 virtual service and associate the WAF policy created in the previous step as shown below.
Suggested Reading

- [Reference Architecture for Horizon](#)
- [GSLB Configuration Guide for Horizon](#)