Table of Contents

Introduction..............................................................................................................................5
Load Balancing Concepts........................................................................................................5
Environment Prerequisites....................................................................................................5
Overview ................................................................................................................................6
Install and Configure vRealize Orchestrator Cluster ..............................................................6
  Configure vRealize Automation Authentication Provider ....................................................6
  Configure Additional vRealize Orchestrator Plugins ..........................................................8
  Configure the Cluster Mode ..................................................................................................8
  Join the Second vRealize Orchestrator Node to the Cluster ...............................................9
  Verify Cluster Mode on the vRealize Orchestrator Nodes ..................................................9
Configuring F5 Load balancer ..............................................................................................10
  Configure Monitors .............................................................................................................10
  Configure Server and Control Center Pools .......................................................................12
  Configure Virtual Servers ..................................................................................................14
  Validate the vRealize Orchestrator HA Environment .......................................................16
Configuring NSX Load Balancer ...........................................................................................17
  Create and Configure the NSX-Edge ..................................................................................17
  Add Application Profiles ....................................................................................................18
  Add Service Monitoring .....................................................................................................19
  Configure Pools ..................................................................................................................20
  Configure Virtual Servers ..................................................................................................23
Configuring NetScaler Load balancer ..................................................................................25
  Configure Monitors .............................................................................................................25
  Configure Servers ..............................................................................................................27
  Configure Services for Orchestrator Server and Control Center ........................................27
  Configure Virtual Servers ..................................................................................................29
Troubleshooting and Additional Information ......................................................................30
  Configuring SSL Certificates on a vRealize Orchestrator Appliance ................................30
  Configuring Email Notifications on your Load Balancer ...................................................31
  Database Issues ..................................................................................................................31
  Database Network Connectivity ..........................................................................................31
  Using a Different Health Monitor .......................................................................................32
  Using an F5 Version Older than 11 ....................................................................................32
  Accessing Orchestrator Client in HA mode ........................................................................32
## Revision History

<table>
<thead>
<tr>
<th>DATE</th>
<th>VERSION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 2017</td>
<td>1.4</td>
<td>Added NetScaler configuration.</td>
</tr>
<tr>
<td>June 2017</td>
<td>1.3</td>
<td>• Added support for vRealize Orchestrator 7.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added monitor and pool configuration for Control Center service.</td>
</tr>
<tr>
<td>May 2017</td>
<td>1.2</td>
<td>Added support for vRealize Orchestrator 7.2</td>
</tr>
<tr>
<td>August 2016</td>
<td>1.1</td>
<td>Added support for vRealize Orchestrator 7.1</td>
</tr>
<tr>
<td>April 2016</td>
<td>1.0</td>
<td>Initial version.</td>
</tr>
</tbody>
</table>
Introduction

This document describes the setup and configuration of a two-node, highly available vRealize Orchestrator cluster that uses F5 Networks BIG-IP software (F5), NetScaler, or NSX as a load balancer. This document is not an installation guide, but a load-balancing configuration guide that supplements the vRealize Orchestrator installation and configuration documentation available in the vRealize Orchestrator Documentation.

This information is for the following products and versions.

<table>
<thead>
<tr>
<th>PRODUCT</th>
<th>VERSION</th>
<th>DOCUMENTATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>vRealize Orchestrator</td>
<td>6.0.3, 7.0, 7.1, 7.2, 7.3</td>
<td>VMware vRealize Orchestrator Documentation</td>
</tr>
<tr>
<td>F5 BIG IP</td>
<td>11.6.0</td>
<td>AskF5 Knowledge Base</td>
</tr>
<tr>
<td>VMWare NSX</td>
<td>6.2</td>
<td>VMware NSX for vSphere Documentation</td>
</tr>
<tr>
<td>vCenter Single Sign On</td>
<td></td>
<td>Refer to the Support Matrix</td>
</tr>
</tbody>
</table>

Load Balancing Concepts

Load balancers distribute work among servers in high availability (HA) deployments. The system administrator backs up the load balancers on a regular basis at the same time as other components.

Follow your site policy for backing up load balancers, keeping in mind the preservation of network topology and vRealize Orchestrator backup planning.

Following are the advantages of using a load balancer in front of the vRealize Orchestrator cluster:

- Ensures that the deployed cluster is properly balanced for performance of UI traffic.
- Allows all nodes in the cluster to equally participate in the handling of UI sessions and traffic.
- Provides simpler access for the users. Instead of accessing each node individually the user only needs one URL to access the entire cluster and not be concerned with which node is available.
- Provides load balancing, high availability, and ease of configuration.

Environment Prerequisites

- **F5**: Before you start the HA implementation of vRealize Orchestrator by using an F5 load balancer, ensure that F5 is installed and licensed and that the DNS server configuration is complete.
- **NetScaler**: Before you start the HA implementation of vRealize Orchestrator by using a Citrix NetScaler load balancer, ensure that it’s configured properly and has the Standard Edition license applied as a minimum.
- **NSX**: Before you start the HA implementation of vRealize Orchestrator by using NSX as a load balancer, ensure that your NSX topology is configured and that your version of NSX is supported. This document covers the load balancing aspect of an NSX configuration, and assumes that NSX is configured and validated to work properly on the target environment and networks.
  To verify that your version is supported, see the Support Matrix for the current release.
- **Database**: Verify that supported database servers are available. See vRealize Orchestrator Support Matrix for supported databases.
- **vRealize Automation**: If you are using the vRealize Orchestrator cluster to complement a vRealize Automation
system, it is recommended to have the vRealize Automation system configured and available before starting.

- **Certificates:** Create signed or self-signed certificates to contain the vRealize Orchestrator VIP and the hostnames of the vRealize Orchestrator nodes in the SubjectAltNames section. This configuration allows the load balancer to serve traffic without SSL errors. Configuring certificates is a mandatory requirement for integrating a vRealize Orchestrator HA cluster with a vRealize Automation system.

For more information on configuring certificates, see the Troubleshooting section.

**Overview**

The setting up and configuring load balancer for vRealize Orchestrator consists of the following:

1. Deployment of vRealize Orchestrator appliances (two) and configuration of the basic VA settings
2. Configuration of the first node – authentication, plugins, cluster mode
3. Configuration of the second node
4. Verification of vRealize Orchestrator cluster
5. Configure a load balancer (F5 or NSX)
6. Verify the finished HA cluster setup

**Note:** A cluster with more than 2 nodes can also be configured by using this document as a baseline.

**Install and Configure vRealize Orchestrator Cluster**

A vRealize Orchestrator cluster comprises of two or more Orchestrator nodes. Each node is a separate full install of the Orchestrator product.

1. To install a new vRealize Orchestrator appliance, enter an initial root password that you can use to login to the Orchestrator Control Center Interface.
2. If you have not configured date, time, network, and so on while deploying the vRealize Orchestrator appliance, you must now login to the web configuration interface of the vRealize Orchestrator appliance. Log in to the web interface by using https://VROApplianceIP:5480.
3. Configure DNS, networking, and time sync.
4. Configure host name and generate SSL certificate.
5. Enable SSH if it was not configured during deployment.
   
   **Note:** For security reasons, you should consider disabling SSH access after you have fully completed and validated the HA environment.
6. (Optional) If the vRealize Orchestrator service is not already started, use SSH to log in to the vRealize Orchestrator node, and start the vRealize Orchestrator Control Center service. Run the command:

   ```
   service vco-configurator start
   ```

7. Repeat the above steps for all your Orchestrator nodes.

**Configure vRealize Automation Authentication Provider**

If the vRealize Orchestrator cluster is set up to be used with a vRealize Automation system, it is recommended to use it
in a vRealize Automation authentication mode. This enables the use of Single Sign-On (SSO) authentication through vRealize Automation. SSO authentication is used for vRealize Orchestrator version 6.0.3 and earlier and Horizon is used for vRealize Orchestrator version 7.0.x and later.

The vRealize Automation system should be setup and configured before you proceed with configuring authentication provider. Use vRealize Orchestrator Control Center interface to configure the authentication provider on the first node.

1. Access Control Center to start the configuration wizard.
   b. Log in as root with the password you entered during OVA deployment.

2. Select the Standalone Orchestrator deployment type.
   By selecting this type, you configure a single Orchestrator node or the first Orchestrator node of a cluster.

3. Click CHANGE to configure the host name on which Control Center will be accessible.
   If you are about to configure an Orchestrator cluster, enter the host name of the load balancer virtual server.

4. Configure the authentication provider.
   a. On the Configure Authentication Provider page, select vRealize Automation from the Authentication mode drop-down menu.
   b. In the Host address text box, enter your vRealize Automation host address and click CONNECT.
   c. Click Accept Certificate.
   d. In the User name and Password text boxes, enter the credentials of the user account that is configured for SSO connection in vRealize Automation.
      By default, the SSO account is administrator and the name of the default tenant is vsphere.local.
   e. In the Admin group text box, enter the name of an administrators group and click SEARCH.
      For example, vsphere.local\administrators
   f. In the list of groups, double click on the name of the group to select it.
   g. Click SAVE CHANGES.
      A message indicates that you saved successfully and you are redirected to the Control Center main view.

5. (Optional) Configure the Orchestrator node to use an external shared database.

6. Click the settings icon at the upper right corner of the Control Center home page and click Sign out.
   You log out the root account from Control Center. The root account can no longer access Control Center.

7. Click BACK TO CONTROL CENTER.
   You are redirected to the VMware Identity Manager (vIDM) login screen.

8. Log in to Control Center with the administrator user account in the vsphere.local tenant.
   You see the Role Based Access Management menu option in Control Center.
The completed configuration should look similar to the following screen:

![vRealize Orchestrator Control Center](image)

**Configure Additional vRealize Orchestrator Plugins**

For cluster mode to work properly, each node should have the same set of plugins installed. To configure the same plugins per node, perform the following steps:

1. Navigate to **Plug-Ins > Manage Plug-ins** tab.
2. Install any new plug-ins by browsing to select the *.vmoapp files and click **Install**.
3. Navigate to **Manage > Startup options** and click **Restart** to apply changes. You must wait until the service restarts and the current status is updated to **Running**.

The same set of plugins should be available on all cluster nodes.

**Configure the Cluster Mode**

To configure the cluster mode on the first vRealize Orchestrator node, perform the following steps:

1. Log in to the Control Center interface of the first vRealize Orchestrator node: [https://vROApplianceIP_1:8283/vco-controlcenter](https://vROApplianceIP_1:8283/vco-controlcenter).
2. Navigate to **Database > Configure database** tab. Enter an IP address or DNS name of the external database that you plan to use. Complete the remaining details on the page. See vRealize Orchestrator Support Matrix for supported databases.
3. If you have changed the database, verify that vRealize Orchestrator server is stopped and then reinstall the force plugins. Navigate to **Monitor and control > Troubleshooting > Force plug-ins** and click **Reinstall**.
4. Navigate to **Manage > Orchestrator Node Settings**.
5. Type the number of active nodes you have in the **Number of active nodes**, change **Heartbeat interval** and **Number of failover heartbeats**, if required and click **Save**.

6. Navigate to **Manage > Startup options** and click **Restart** to apply changes. You must wait until the service restarts and the current status is updated to **Running**.

### Join the Second vRealize Orchestrator Node to the Cluster

To join the second node to the cluster, perform the following steps:

1. Access Control Center of the node you are about to add to the cluster to start the configuration wizard.
   b. Log in as **root** with the password you entered during OVA deployment.

2. Select the **Clustered Orchestrator** deployment type.
   By choosing this type, you join the node to an existing Orchestrator cluster.

3. In the **Hostname** text box, enter the host name or IP address of the first Orchestrator server instance.
   This must be the local IP or host name of the Orchestrator instance, to which you are joining the cluster. Do not use the load balancer address.

4. In the **User name** and **Password** text boxes, enter the root credentials of the first Orchestrator server instance.

5. Click **Join**.
   The Orchestrator instance clones the configuration of the node, to which it joins.

6. Click the settings icon at the upper right corner of the Control Center home page and click **Sign out**.
   You log out the **root** account from Control Center. You are redirected to the VMware Identity Manager (vIDM) logout screen. The **root** account can no longer access Control Center.

7. Click **Go back to login page**.
   You are redirected to the VMware Identity Manager (vIDM) login screen.

8. Log in to Control Center with the **administrator** user account in the vsphere.local tenant.

### Verify Cluster Mode on the vRealize Orchestrator Nodes

To verify the cluster mode on both the vRealize Orchestrator node, perform the following steps:

1. Navigate to the Control Center interface page of the first vRealize Orchestrator node:
   https://vROAppliance_IP1:8283/vco-controlcenter

2. Verify the configuration of any existing third-party plugins. It is possible that some of the plugins are not configured correctly after the change of the database. Navigate to **Monitor and Control > Troubleshooting > Force plug-ins reinstall** to stop the server, if required.

3. Verify that the database, network, authentication, and configuration are exactly the same on all clustered nodes.

4. Verify all services are properly running by going to Validate Configuration. Each component should have a green tick next to it.

5. Navigate to **Manage > Orchestrator Cluster Management** and verify that all clustered nodes are in a **RUNNING** state.

   **Note:** If Active/Passive mode is used instead of Active/Active, the passive nodes should be in **STANDBY** state.
6. Repeat the steps for verifying cluster mode on the second vRealize Orchestrator node.

The completed node settings configuration should look similar to the following screen:

![Completed node settings configuration](image)

---

**Configuring F5 Load balancer**

To increase the availability of the VMware vRealize Orchestrator services, you can put the Orchestrator behind a load balancer. To configure F5 load balancer with your vRealize Orchestrator cluster, use the following information.

**Prerequisites**

Configure at least two Orchestrator nodes.

**Configure Monitors**

A monitor is a check which the load balancer software uses to determine whether a node is healthy, and redirect traffic accordingly. If the node is active and operational, monitor will receive an “HTTP 200 OK” response to its query. If the node is inactive (standby), monitor will receive a “HTTP 503 unavailable” response. Any other response or lack of such within the selected time interval is treated as ‘node is down’.

1. Log in to the F5 and from the main menu select *Local Traffic > Monitors*.
2. Click *Create* and provide the required information as given in Table 1. Leave the default when nothing is specified.
3. Click *Finished*.

**TABLE 1 - CONFIGURE MONITORS**

<table>
<thead>
<tr>
<th>MONITOR</th>
<th>INTERVAL</th>
<th>TIMEOUT</th>
<th>RETRIES</th>
<th>TYPE</th>
<th>SEND STRING</th>
<th>RECEIVE STRING</th>
<th>ALIAS SERVICE PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>vro-https-8281</td>
<td>5</td>
<td>9</td>
<td>3</td>
<td>HTTPS</td>
<td>GET /vco/api/healthstatus</td>
<td>RUNNING</td>
<td>8281</td>
</tr>
</tbody>
</table>
The completed configuration of the monitors should look similar to the following screen:

<table>
<thead>
<tr>
<th>vro-https-8283</th>
<th>5</th>
<th>9</th>
<th>3</th>
<th>HTTPS (443)</th>
<th>GET /vco-controlcenter/docs/</th>
<th>HTTP/1.0</th>
<th>(200)</th>
<th>8283</th>
</tr>
</thead>
</table>

GET /vco/aui/healthstatus

Receive String

RUNNING

Receive Disable String

Closer List

User Name

Password

Reverse

Transparent

Alias Address

Alias Service Port

Adaptive

Enabled

Update  Delete
Configure Server and Control Center Pools

You can configure server and Control Center pools for your F5 load balancer by using the following steps.

1. Log in to the F5 load balancer and select **Local Traffic > Pools**.
2. Click **Create** and provide the required information. Leave the default when nothing is specified.
3. Repeat steps 1 and 2 for each entry in Table 2.
4. Click **Finished**.

**TABLE 2 – CONFIGURE SERVER AND CONTROL CENTER POOLS**

<table>
<thead>
<tr>
<th>POOL NAME</th>
<th>LB METHOD</th>
<th>HEALTH MONITORS</th>
<th>NODE NAME</th>
<th>ADDRESS</th>
<th>SERVICE PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>vro-pool-8281</td>
<td>Round Robin</td>
<td>vro-https-8281</td>
<td>&lt;vro-node1- hostname.domain.com&gt;</td>
<td>&lt;vro-node1-IP&gt;</td>
<td>8281</td>
</tr>
<tr>
<td>vro-pool-8281</td>
<td>Round Robin</td>
<td>vro-https-8281</td>
<td>&lt;vro-node2- hostname.domain.com&gt;</td>
<td>&lt;vro-node2-IP&gt;</td>
<td>8281</td>
</tr>
<tr>
<td>vro-pool-8283</td>
<td>Ratio</td>
<td>vro-https-8283</td>
<td>&lt;vro-node1- hostname.domain.com&gt;</td>
<td>&lt;vro-node1-IP&gt;</td>
<td>8283</td>
</tr>
<tr>
<td>vro-pool-8283</td>
<td>Ratio</td>
<td>vro-https-8283</td>
<td>&lt;vro-node2- hostname.domain.com&gt;</td>
<td>&lt;vro-node2-IP&gt;</td>
<td>8283</td>
</tr>
</tbody>
</table>

The completed configuration of the pool should look similar to the following screen:

The green status indicates that the node is active. Both vRealize Orchestrator nodes should be shown as active.
The completed configuration of all the pools should look similar to the following screen:

Configure Virtual Servers
You can configure virtual servers for your F5 load balancer by using the following steps.
1. Log in to the F5 load balancer and select **Local Traffic > Virtual Servers**.
2. Click **Create** and provide the required information as given in Table 3. Leave the default when nothing is specified.
3. Click **Finished**.

**TABLE 3 — CONFIGURE VIRTUAL SERVERS**

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
<th>TYPE</th>
<th>DESTINATION ADDRESS</th>
<th>SERVICE PORT</th>
<th>SOURCE ADDRESS TRANSLATION</th>
<th>DEFAULT POOL</th>
</tr>
</thead>
<tbody>
<tr>
<td>vro-lb-8281</td>
<td>vRealize Orchestrator virtual server</td>
<td>Performance (Layer 4)</td>
<td>&lt;vro-lb-IP&gt;</td>
<td>8281</td>
<td>Automap</td>
<td>vro-pool-8281</td>
</tr>
<tr>
<td>vro-lb-8283</td>
<td>vRealize Orchestrator control center</td>
<td>Performance (Layer 4)</td>
<td>&lt;vro-lb-IP&gt;</td>
<td>8283</td>
<td>Automap</td>
<td>vro-pool-8283</td>
</tr>
</tbody>
</table>

**Note:** You cannot connect to the vRealize Orchestrator Smart Client via load balancer IP as it is not supported. However, you can connect directly to each node.

The configuration of the virtual server should look similar to the following screen:
The completed configuration of the virtual servers should look similar to the following screen:

![Virtual Server Configuration Screen](image1)

This concludes the cluster configuration with F5 as a load balancer. You should now validate that your new setup is functional.
Validate the vRealize Orchestrator HA Environment

You can validate the vRealize Orchestrator HA environment by using the F5 interface. All the entries should be listed in green at this point.

1. In the F5 interface, select **Local Traffic > Network Map**.
2. Execute a set of test workflows for your newly configured cluster in order to ensure it is fully functional.
Configuring NSX Load Balancer

The NSX virtual networking solution includes the capability of deploying an edge services gateway as a load balancer.

Prerequisites

The following are the prerequisites for a functional NSX load balancer used with vRealize Orchestrator cluster:

- This document assumes that NSX deployment is already deployed in the environment and is fully functional.
- The NSX deployment is of version 6.2 or higher.
- NSX Edge is deployed and has access to the network on which vRealize Orchestrator is deployed.

Create and Configure the NSX-Edge

1. Log in to the vCenter Server where NSX has been set up.
3. Select the Configure Firewall default policy check box and Accept the Default Traffic Policy as shown in the following screen.
4. Double-click to select your Edge device from the list.
5. Select the Manage tab, click Load Balancer tab and click the Edit icon.
6. Select Enable Load Balancer and Enable Acceleration, if required, and click OK.
7. Select the Manage tab, click Settings, and select Interfaces menu.
8. Select the first vNIC and click the **Edit** icon to edit the first vNIC, this is your Load Balancer virtual appliance.

9. Assign a primary IP address to the NSX Edge and assign the secondary IP addresses that can be used as the virtual server addresses.

10. Click the **Add** icon to assign a static IP address to this virtual interface. The configuration should look similar to the following screen:

![vRealize Orchestrator Load Balancing configuration screen](image)

Add Application Profiles

1. Log in to the vCenter Server where NSX has been set up.

2. Navigate to **Home > Networking & Security > NSX Edges** and select your previously created NSX edge.

3. Select the **Load Balancer** tab and click on the **Application Profiles** menu.

4. Click the **Add** icon to create the application profiles required for vRealize Orchestrator by using information in Table 4. Leave the default when nothing is specified.

5. Click **OK**.

**TABLE 4 – APPLICATION PROFILES**

<table>
<thead>
<tr>
<th>NAME</th>
<th>TYPE</th>
<th>ENABLED SSL PASS-THROUGH</th>
<th>PERSISTENCE</th>
<th>CLIENT AUTHENTICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>vROProfile</td>
<td>HTTPS</td>
<td>Yes</td>
<td>None</td>
<td>Ignore</td>
</tr>
</tbody>
</table>
The completed configuration should look similar to the following screen.

Add Service Monitoring

1. Log in to the vCenter Server where NSX has been set up.
2. Navigate to **Home > Networking & Security > NSX Edges** and select your previously created NSX edge.
3. Select the **Load Balancer** tab and click on the **Service Monitoring** menu.
4. Click the **Add** icon to create a new monitor required for vRealize Orchestrator by using information in Table 5. Leave the default when nothing is specified.

**TABLE 5 – ADD SERVICE MONITORING**

<table>
<thead>
<tr>
<th>MONITOR NAME</th>
<th>INTERVAL TIME</th>
<th>MAX RETRIES</th>
<th>TYPE</th>
<th>METHOD</th>
<th>URL</th>
<th>EXPECTED</th>
<th>RECEIVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>vro-https-8281</td>
<td>3</td>
<td>9</td>
<td>3</td>
<td>HTTPS</td>
<td>GET /vco/api/healthstatus</td>
<td></td>
<td>RUNNING</td>
</tr>
<tr>
<td>vro-https-8283</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/vco-controlcenter/docs/</td>
<td>vco-controlcenter/docs/</td>
<td></td>
</tr>
</tbody>
</table>
The completed configuration should look similar to the following screen.

![Edit Service Monitor](image)

**Configure Pools**

1. Log in to the vCenter Server where NSX has been set up.
2. Navigate to **Home > Networking & Security > NSX Edges** and select your previously created NSX edge.
3. Select the **Load Balancer** tab and click **Pools**.
4. Click the **Add** icon to create a new pool required for vRealize Orchestrator by using information in Table 6.

   Leave the default when nothing is specified.

**TABLE 6 – POOL CHARACTERISTICS**

<table>
<thead>
<tr>
<th>POOL NAME</th>
<th>ALGORITHM</th>
<th>MONITORS</th>
</tr>
</thead>
<tbody>
<tr>
<td>vROPool</td>
<td>Round Robin</td>
<td>vro-https-8281</td>
</tr>
<tr>
<td>vROControlCenter</td>
<td>IP-HASH</td>
<td>vro-https-8283</td>
</tr>
</tbody>
</table>
Click the *Add* icon to add new members to the pool by using information in Table 7.

**TABLE 7: POOL NODES CHARACTERISTICS**

<table>
<thead>
<tr>
<th>ENABLED MEMBER</th>
<th>NAME</th>
<th>IP ADDRESS / VC CONTAINER</th>
<th>MONITOR PORT</th>
<th>PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>yes</td>
<td>HA-cluster-vro1</td>
<td>&lt;vro-Node1 IP&gt;</td>
<td>8281</td>
<td>8281</td>
</tr>
<tr>
<td>yes</td>
<td>HA-cluster-vro2</td>
<td>&lt;vro-Node2 IP&gt;</td>
<td>8281</td>
<td>8281</td>
</tr>
<tr>
<td>yes</td>
<td>HA-cluster-vro1</td>
<td>&lt;vro-Node1 IP&gt;</td>
<td>8283</td>
<td>8283</td>
</tr>
<tr>
<td>yes</td>
<td>HA-cluster-vro2</td>
<td>&lt;vro-Node2 IP&gt;</td>
<td>8283</td>
<td>8283</td>
</tr>
</tbody>
</table>

The completed configuration should look similar to the following screen. The green check marks in the *Enabled* column indicates that both the nodes are active.
Verify that the pool is in a UP state by clicking on the **Show Pool Statistics** link.
Configure Virtual Servers

1. Log in to the vCenter Server where NSX has been set up.
3. Select the Load Balancer tab and click Virtual Servers.

*Click the Add icon to create a new virtual server required for vRealize Orchestrator by using information in Note.* The port number of the virtual server should correspond to the port number of the pool.
4. Table 8Table 5. Leave the default when nothing is specified.

**Note:** The port number of the virtual server should correspond to the port number of the pool.

### TABLE 8 – VIRTUAL SERVER CHARACTERISTICS

<table>
<thead>
<tr>
<th>ENABLE VIRTUAL SERVER</th>
<th>APPLICATION PROFILE</th>
<th>NAME</th>
<th>IP ADDRESS</th>
<th>PROTOCOL</th>
<th>PORT</th>
<th>DEFAULT POOL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>vROPProfile</td>
<td>vro-lb-8281</td>
<td>&lt;vro-lb-ip&gt;</td>
<td>HTTPS</td>
<td>8281</td>
<td>vROPool</td>
</tr>
<tr>
<td>Yes</td>
<td>vROPProfile</td>
<td>vro-lb-8283</td>
<td>&lt;vro-lb-ip&gt;</td>
<td>HTTPS</td>
<td>8283</td>
<td>vROControlCenter</td>
</tr>
</tbody>
</table>
The completed configuration should look similar to the following screen.

This concludes the vRealize Orchestrator cluster configuration with NSX as a load balancer.
You should now validate that your new setup is functional by execution a set of test-workflows against it.
Configuring NetScaler Load balancer

To increase the availability of the VMware vRealize Orchestrator services, you can put the Orchestrator behind a load balancer. To configure NetScaler load balancer with your vRealize Orchestrator cluster, use the following information.

**Prerequisites**

Configure at least two Orchestrator nodes.

Verify that the NetScaler appliance has at least a Standard Edition license applied.

**Configure Monitors**

A monitor in NetScaler is a check that the load balancer software uses to determine whether a node is healthy and redirect traffic accordingly. If the node is active and operational, monitor receives an “HTTP 200 OK” response to its query. If the node is inactive (standby), monitor receives an “HTTP 503 unavailable” response. Any other response or lack of response within the selected time interval is treated as ‘node is down’.

5. Log in to the NetScaler web console and select Traffic Management > Load Balancing > Monitors.

6. Click Add and provide the required information as given in Table 9 - Configure Monitors Table 9. Leave all unspecified options with their default values.

7. Click Create.

**Table 9 - Configure Monitors**

<table>
<thead>
<tr>
<th>MONITOR</th>
<th>INTERVAL</th>
<th>TIMEOUT</th>
<th>RETRIES</th>
<th>TYPE</th>
<th>SEND STRING/HTTP REQUEST</th>
<th>RECEIVE STRING</th>
<th>SECURE OPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>vro-https-8281</td>
<td>10</td>
<td>9</td>
<td>3</td>
<td>HTTP-ECV</td>
<td>GET /vco/api/healthstatus</td>
<td>RUNNING</td>
<td>Enabled</td>
</tr>
<tr>
<td>vro-https-8283</td>
<td>10</td>
<td>9</td>
<td>3</td>
<td>HTTP</td>
<td>GET /vco-controlcenter/docs/</td>
<td>&lt;title&gt;Swagger UI&lt;/title&gt;</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

The completed configuration of the monitors should look similar to the following screen:
### Configure Monitor

**Name:** vRO-https-0281  
**Type:** HTTP-ECV

#### Standard Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Unit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interval</td>
<td>10</td>
<td>Second</td>
<td></td>
</tr>
<tr>
<td>Destination IP</td>
<td></td>
<td></td>
<td>IPv6</td>
</tr>
<tr>
<td>Response Time-out</td>
<td>9</td>
<td>Second</td>
<td></td>
</tr>
<tr>
<td>Destination Port</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bound Service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Down Time</td>
<td>30</td>
<td>Second</td>
<td></td>
</tr>
<tr>
<td>TROFS Code</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TROFS String</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dynamic Time-out</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deviation</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dynamic Interval</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retries</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resp Time-out Threshold</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMP Alert Retries</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Success Retries</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failure Retries</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Net Profile</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOS ID</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Special Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send String</td>
<td>GET /vco/api/healthstatus</td>
<td></td>
</tr>
<tr>
<td>Receive String</td>
<td>RUNNING</td>
<td></td>
</tr>
<tr>
<td>Custom Header</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Enabled:** Yes  
**Reverse:** No  
**Transparent:** No  
**LTETM (Least Response Time using Monitoring):** Yes  
**Secure:** Yes  
**IP Tunnel:** No
Configure Servers

You can configure servers for the Orchestrator Server and Control Center services in your NetScaler load balancer.

1. Log in to the NetScaler web console and select Traffic Management > Load Balancing > Servers.
2. Click Add and provide the server name and its IP Address information for each Orchestrator appliance. For server names, use the convention accepted in your organization.
3. Click Enable after Creating.
4. Choose a traffic domain if it applies to your configuration.
5. Click Create.

The completed configuration of a server should look similar to the following screen:

Configure Services for Orchestrator Server and Control Center

You can configure Orchestrator Server and Control Center services for your NetScaler load balancer.

1. Log in to the NetScaler web console and select Traffic Management > Load Balancing > Services.
2. Click Add and provide the required information. Leave all unspecified options with their default values. For service names, use the convention accepted in your organization.
3. Choose a traffic domain if it applies to your configuration.
4. Click OK.
5. Under the Monitors section click on the existing binding.
6. Click Add Binding.
7. Under Select Monitor click to select a monitor.
8. Choose a monitor by clicking on the monitor for the current service as specified in Table 10.
9. Click Select.
10. Click Bind.
11. Click Close.
12. Click Done.
13. Repeat these steps for each entry in Table 10.

**Table 10 – Configure Server and Control Center Services**

<table>
<thead>
<tr>
<th>SERVICE NAME</th>
<th>EXISTING SERVER</th>
<th>PROTOCOL</th>
<th>HEALTH MONITORS</th>
<th>SERVICE PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>vro-server-01-8281</td>
<td>vro-server-01</td>
<td>SSL_BRIDGE</td>
<td>vro-https-8281</td>
<td>8281</td>
</tr>
<tr>
<td>vro-server-02-8281</td>
<td>vro-server-02</td>
<td>SSL_BRIDGE</td>
<td>vro-https-8281</td>
<td>8281</td>
</tr>
<tr>
<td>vro-server-01-8283</td>
<td>vro-server-02</td>
<td>SSL_BRIDGE</td>
<td>vro-https-8283</td>
<td>8283</td>
</tr>
<tr>
<td>vro-server-02-8283</td>
<td>vro-server-02</td>
<td>SSL_BRIDGE</td>
<td>vro-https-8283</td>
<td>8283</td>
</tr>
</tbody>
</table>
The completed configuration of the pool should look similar to the following screen:

**Load Balancing Service**

<table>
<thead>
<tr>
<th>Service Name</th>
<th>vro-server-02::8283</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>vro-server-02</td>
</tr>
<tr>
<td>IP Address</td>
<td></td>
</tr>
<tr>
<td>Server State</td>
<td>Up</td>
</tr>
<tr>
<td>Protocol</td>
<td>SSL</td>
</tr>
<tr>
<td>Port</td>
<td>8283</td>
</tr>
</tbody>
</table>

**Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Domain</td>
<td>0</td>
</tr>
<tr>
<td>Number of Active Conn.</td>
<td>-</td>
</tr>
<tr>
<td>Hash ID</td>
<td>None</td>
</tr>
<tr>
<td>Server ID</td>
<td>-</td>
</tr>
<tr>
<td>Clear-Text Port</td>
<td>-</td>
</tr>
<tr>
<td>Cache Type</td>
<td>SERVER</td>
</tr>
<tr>
<td>Cacheable</td>
<td>NO</td>
</tr>
<tr>
<td>Health Monitoring</td>
<td>YES</td>
</tr>
<tr>
<td>AppFlow Logging</td>
<td>ENABLED</td>
</tr>
</tbody>
</table>

**Monitors**

1 Service to Load Balancing Monitor Binding

The green mark next to Server State indicates that the node is active. Both vRealize Orchestrator nodes should have the Server State as UP for all of their services.

**Configure Virtual Servers**

You can configure virtual servers for your NetScaler load balancer.

1. Log in to the F5 load balancer and select Traffic Management > Load Balancing > Virtual Servers.
2. Click Add and provide the required information as given in Table 11. Leave all unspecified options with their default values. For virtual server names, use the convention accepted in your organization.
3. Choose a traffic domain if it applies to your configuration.
4. Click OK.
5. Under Services and Service Groups click No load Balancing Virtual Service Binding.
6. Under Select Service click to select the two services.
7. Choose a service by clicking on the respective service as specified in Table 11.
8. Click Select.
9. Click Bind.
10. Click Continue.
11. Choose a persistence from the options as specified in Table 11.
12. Repeat these steps for the vRealize Orchestrator Control Center virtual server.
### TABLE 11 – CONFIGURE VIRTUAL SERVERS

<table>
<thead>
<tr>
<th>NAME</th>
<th>COMMENTS</th>
<th>PROTOCOL</th>
<th>DESTINATION ADDRESS</th>
<th>SERVICE PORT</th>
<th>PERSISTENCE</th>
<th>SERVICES</th>
</tr>
</thead>
<tbody>
<tr>
<td>vro-lb-8281</td>
<td>vRealize Orchestrator virtual server</td>
<td>SSL_BRIDGE</td>
<td>&lt;vro-lb-IP&gt;</td>
<td>8281</td>
<td>SSLSESSION or SOURCEIP or NONE</td>
<td>vro-server-01-8281 &amp; vro-server-02-8281</td>
</tr>
<tr>
<td>vro-lb-8283</td>
<td>vRealize Orchestrator control center</td>
<td>SSL_BRIDGE</td>
<td>&lt;vro-lb-IP&gt;</td>
<td>8283</td>
<td>SSLSESSION or SOURCEIP</td>
<td>vro-server-01-8283 &amp; vro-server-02-8283</td>
</tr>
</tbody>
</table>

**Note:** You cannot connect to the vRealize Orchestrator Smart Client via load balancer IP, as it is not supported. However, you can connect directly to each node.

The configuration of the virtual server should look similar to the following screen:

---

**Troubleshooting and Additional Information**

**Configuring SSL Certificates on a vRealize Orchestrator Appliance**

If you are required to replace the self-signed certificates with your own CA signed certificates, see the official documentation: [https://www.vmware.com/support/pubs/orchestrator_pubs.html](https://www.vmware.com/support/pubs/orchestrator_pubs.html) and [KB 2007032](https://kb.vmware.com/kb/2007032).
The following KBs are also applicable when integrating vRealize Orchestrator with vRealize Automation: KB 2106583, KB 2107816

**Configuring Email Notifications on your Load Balancer**

You should set up an email notification on the Load Balancer to send emails to the system administrator every time a vRealize Automation or vRealize Orchestrator node goes down.

**F5:**

You can set up an email notification with F5 by using the following methods:


**NSX:**

At the time of writing this document, NSX does not support email notification for such a scenario.

**Database Issues**

When you are using MSSQL with vRealize Orchestrator, you must configure the database to enable TCP/IP. For MSSQL 2008 this can be done by following those steps:

1. Log in as an administrator to the machine on which SQL Server is installed.
2. Click Start > All Programs > Microsoft SQL Server 2008 R2 > Configuration Tools > SQL Server Configuration Manager. The SQL Server Configuration Manager could be different in the various MSSQL versions.
3. Expand the list on the left.
4. Click Protocols for <MSSQL-version>.
5. Right-click TCP/IP and select Enable.
6. Right-click TCP/IP and select Properties.
7. Click the IP Addresses tab.
8. Under IP1, IP2, and IPAll, set the TCP Port value to 1433.
9. Click OK.
10. Restart the SQL Server.

For more information about how to setup database to use with Orchestrator, see VMware documentation: Installing and Configuring vRealize Orchestrator.

**Database Network Connectivity**

Robust network connectivity between database and Orchestrator node is an operational requirement.

Whenever SQL failure is detected, the node that is unable to connect to the database shuts down to prevent incorrect workflows execution. If there are other nodes with a working connection to the database, they continue with the workflow executions. You need to manually restart the failed node.
Using a Different Health Monitor

Using a different health monitor (URL and response check) is possible, but not supported. This might change in a subsequent version of vRealize Orchestrator.

Using an F5 Version Older than 11

If you are using an F5 version older than 11.x, you should change your health monitor settings related to the send string. For more information about how to set up your health monitor send string in the different versions of F5, see the following F5 support information:


Accessing Orchestrator Client in HA mode

Load balancing of the Orchestrator client UI (TCP ports 8286, 8287) is not supported due to technical limitations. You should access the client UI on each node directly. If you use the Orchestrator client via load balancer, you may see incomplete or incorrect data.