vRealize Orchestrator
Load Balancing

Configuration Guide
Version 7.0.x, 7.1, and 7.2

TECHNICAL WHITE PAPER
MAY 2017
VERSION 1.2
# Table of Contents

Introduction .................................................................................................................. 4  
Load Balancing Concepts .............................................................................................. 4  
Environment Prerequisites........................................................................................... 4  
Overview ...................................................................................................................... 5  
Install and Configure vRealize Orchestrator Cluster ..................................................... 5  
  Configure vRealize Automation Authentication Provider .............................................. 5  
  Configure Additional vRealize Orchestrator Plugins .................................................. 7  
  Configure the Cluster Mode ........................................................................................ 7  
  Join the Second vRealize Orchestrator Node to the Cluster ........................................ 8  
  Verify Cluster Mode on the vRealize Orchestrator Nodes .......................................... 8  
Configuring F5 Load balancer ....................................................................................... 9  
  Configure Monitors ................................................................................................... 9  
  Configure Server Pools ............................................................................................. 11  
  Configure Virtual Servers .......................................................................................... 12  
  Validate the vRealize Orchestrator HA Environment ................................................ 14  
Configuring NSX Load Balancer .................................................................................. 15  
  Create and Configure the NSX-Edge ........................................................................ 15  
  Add Application Profiles ......................................................................................... 16  
  Add Service Monitoring ............................................................................................ 17  
  Configure Pools ........................................................................................................ 18  
  Configure Virtual Servers ........................................................................................ 20  
Troubleshooting and Additional Information ................................................................ 22  
  Configuring SSL Certificates on a vRealize Orchestrator Appliance ......................... 22  
  Configuring Email Notifications on your Load Balancer ............................................ 22  
  Database Issues ........................................................................................................ 22  
  Database Network Connectivity ................................................................................ 23  
  Using a Different Health Monitor .............................................................................. 23  
  Using an F5 Version Older than 11 ......................................................................... 23  
  Accessing Orchestrator Client in HA mode ............................................................... 23
# Revision History

<table>
<thead>
<tr>
<th>DATE</th>
<th>VERSION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<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) 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</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.
- **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.
- **Certicates**: 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 will enable usage of Single Sign-On (SSO) authentication through vRealize Automation. SSO authentication is used for vRealize Orchestrator 6.0.3 and earlier versions and Horizon is used for vRealize Orchestrator 7.0.x and higher versions.

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. Navigate to the first vRealize Orchestrator node home page: https://vROApplianceIP_1:8281/vco and click the
Orchestrator Control Center link.

2. Orchestrator Control Center interface appears on https://vROApplianceIP_1:8283/vco-controlcenter.

3. On the log in pop-up screen, enter root for User name and root password for Password, and click OK.

4. Import vRealize Automation certificate:
   a. Navigate to Manage > Certificates > Trusted Certificates and click the Import button.
   b. Enter vRealize Automation host address in the Import from URL field.
   c. Click the Import button and the certificate is imported.

5. Navigate to Manage > Configure Authentication Provider and perform the following steps:
   a. For Authentication mode, select vRealize Automation from the dropdown menu.
   b. Enter vRealize Automation Host address: VRAApplianceHost and click the Connect button. VRAApplianceHost is your vRealize Automation VA IP or vRealize Automation VA Load Balancer IP.
   c. Wait for the host to connect. Configure the authentication parameters is displayed.
   d. Enter Identity service User name: <Your vRealize Automation administrator user name.> For example: administrator.
   e. Enter Identity service Password: <Your vRealize Automation administrator password>
   f. Leave the default value for Configure licenses.
   g. Enter the Default tenant or leave the default value: vsphere.local.
   h. Click the Register button.
   i. Type the Orchestrator administrator group in the Admin group field, which is the SSO group where the administrator is located, for example: vcoadmins, and click Search.
   j. Select the group that you find, for example: vsphere.local/vcoadmins, and click Save Changes. The message confirming that the configuration is saved appears.

The completed configuration should look similar to the following screen:
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.

**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. Navigate to the Control Center interface of the first vRealize Orchestrator node: https://vROApplianceIP_1:8283/vco-controlcenter.
2. On the log in pop-up screen, enter root for User name and root password for Password, and click OK.
3. 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.
4. 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.

6. 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.

7. 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. Navigate to the Control Center interface of the second vRealize Orchestrator node:

2. On the log in pop-up screen, enter vRealize Orchestrator User name and Password, and click OK.

3. Navigate to Manage > Join Node To Cluster

4. Type remote Orchestrator server, first vRealize Orchestrator node - vROApplianceIP_1, hostname or IP address in the Hostname text box.

5. Type remote Control Center, first vRealize Orchestrator node - vROApplianceIP_1 credentials in the Username and Password text boxes.

6. Click the Join button and the second node successfully joins the cluster.

**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. Navigate to Manage > Orchestrator Node Settings 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.

5. 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:
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:
Configure Server Pools

You can configure server 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 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>
</tbody>
</table>

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

![F5 Load Balancer Interface](image)

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:

![Completed Configuration 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>
</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:

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.
2. Navigate to **Home > Networking & Security > NSX Edges** and create your own NSX edge.
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:

![](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.

![Edit Profile](image)

**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</th>
<th>TIMEOUT</th>
<th>MAX RETRIES</th>
<th>TYPE</th>
<th>METHOD</th>
<th>URL</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</td>
<td>/vco/api/healthstatus</td>
<td>RUNNING</td>
</tr>
</tbody>
</table>
The completed configuration should look similar to the following screen.

**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>vROPoll</td>
<td>Round Robin</td>
<td>vro-https-8281</td>
</tr>
</tbody>
</table>

**NSX Monitor Configuration**

This online monitor requires a custom extension for vRealize Orchestrator, which has been configured in Table 5.
5. 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>
</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.

![Pool Statistics](image)

### Configure Virtual Servers

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 **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 8 & Table 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>vROProfile</td>
<td>vro-lb-8281</td>
<td>vro-lb-ip</td>
<td>HTTPS</td>
<td>8281</td>
<td>vROPool</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.
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 and 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.