vRealize Orchestrator Load Balancing

Configuration Guide
Version 7.4 and 7.5

TECHNICAL WHITE PAPER

FEBRUARY 2019

VERSION 1.1

Table of Contents

Revision History

DATE	VERSION	DESCRIPTION
June 2017	1.4	Added NetScaler configuration.
June 2017	1.3	• Added support for vRealize Orchestrator 7.3 • Added monitor and pool configuration for Control Center service.
May 2017	1.2	Added support for vRealize Orchestrator 7.2
August 2016	1.1	Added support for vRealize Orchestrator 7.1
April 2016	1.0	Initial version.

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.

PRODUCT	VERSION	DOCUMENTATION
vRealize Orchestrator	6.0.3, 7.0, 7.1, 7.2, 7.3	VMware vRealize Orchestrator Documentation
F5 BIG IP	11.6.0	AskF5 Knowledge Base
VMWare NSX	6.2	VMware NSX for vSphere Documentation
vCenter Single Sign On		Refer to the Support Matrix

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.

Session Persistence

The persistence option overrides any load balancing algorithm option, for example setting dest_addr overrides, setting round robin, and so on. The configuration recommended in this document is the result of extensive testing and represents the best balance between stability, performance, and scalability.

- Destination Address (F5 and NetScaler).
  Destination address affinity persistence, also known as sticky persistence, supports TCP and UDP protocols, and directs session requests to the same server based on the destination IP address of a packet.

- Source (IP) Address (F5, NetScaler, & NSX)
  The default source IP address persistence option persists traffic based on the source IP address of the client for the life of that session and until the persistence entry timeout expires. The default for this persistence is 180 seconds. The next time a persistent session from that same client is initiated, it might be persisted to a different member of the pool. This decision is made by the load balancing algorithm and is non-deterministic.
  NOTE: Set the persistence entry timeout to 1800 seconds (30 minutes) to match the vRealize Orchestrator

Control Center GUI timeout.

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

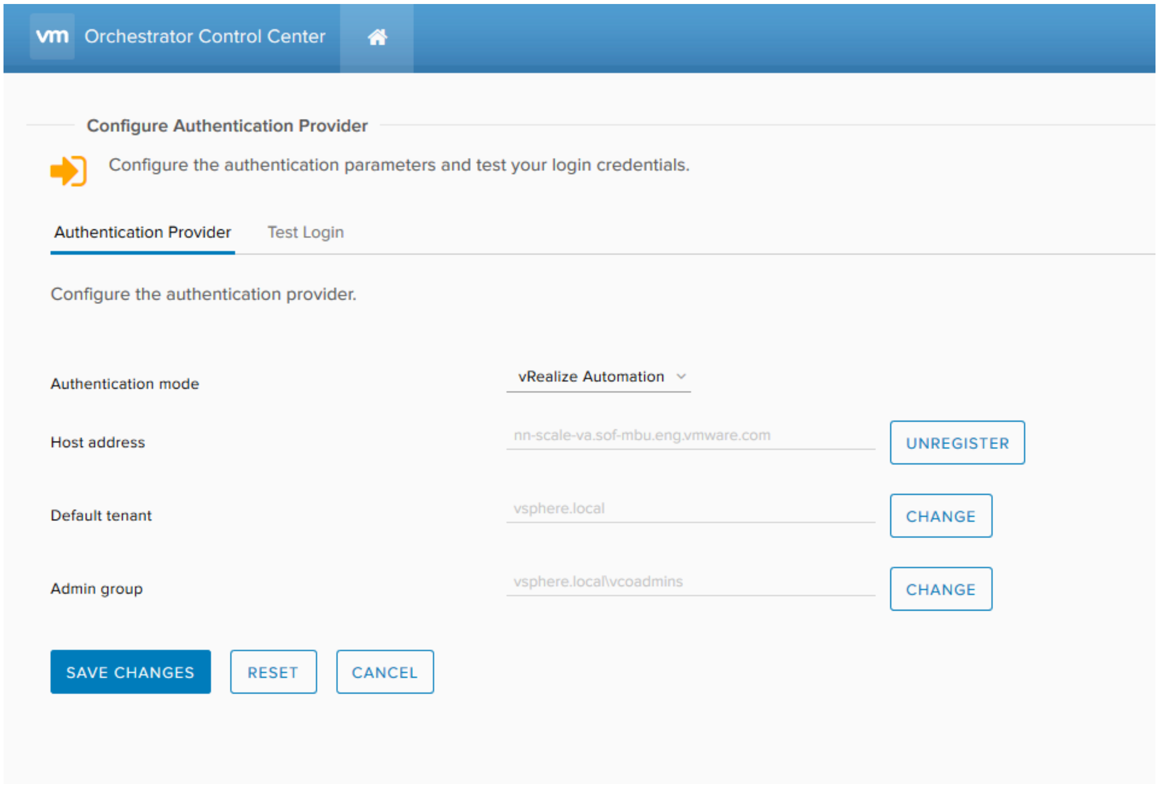
If the vRealize Orchestrator cluster is set up to be used with a vRealize Automation system, it is recommended to use it in a vRealize Automation authentication mode. This enables the use of Single Sign-On (SSO) authentication through vRealize Automation. SSO authentication is used for vRealize Orchestrator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

8. Access Control Center to start the configuration wizard.
   a. Navigate to https://your_orchestrator_server_IP_or_DNS_name:8283/vco-controlcenter.
   b. Log in as `root` with the password you entered during OVA deployment.
9. Select the **Standalone Orchestrator** deployment type.
   By selecting this type, you configure a single Orchestrator node or the first Orchestrator node of a cluster.
10. 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.
11. 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.

12. (Optional) Configure the Orchestrator node to use an external shared database.
13. 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.
14. Click **BACK TO CONTROL CENTER**.
    You are redirected to the VMware Identity Manager (vIDM) login screen.
15. 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:



Configure the authentication parameters and test your login credentials.

Configure the authentication provider.

Authentication mode: vRealize Automation

Host address: nn-scale-va.sof-mbu.eng.vmware.com

Default tenant: vsphere.local

Admin group: vsphere.local\vcoadmins

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:

16. Navigate to **Plug-Ins** > **Manage Plug-ins** tab.
17. Install any new plug-ins by browsing to select the `*.vmoapp` files and click **Install**.
18. 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:

19. Log in to the Control Center interface of the first vRealize Orchestrator node: https://vROApplianceIP_1:8283/vco-controlcenter.

20. 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.

21. 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**.

22. Navigate to **Manage** > **Orchestrator Node Settings**.

23. 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**.

24. 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:

25. Access Control Center of the node you are about to add to the cluster to start the configuration wizard.
    a. Navigate to https://*your_orchestrator_server_IP_or_DNS_name*:8283/vco-controlcenter.
    b. Log in as `root` with the password you entered during OVA deployment.

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

27. 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.

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

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

30. 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.

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

32. 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:

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

34. 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.

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

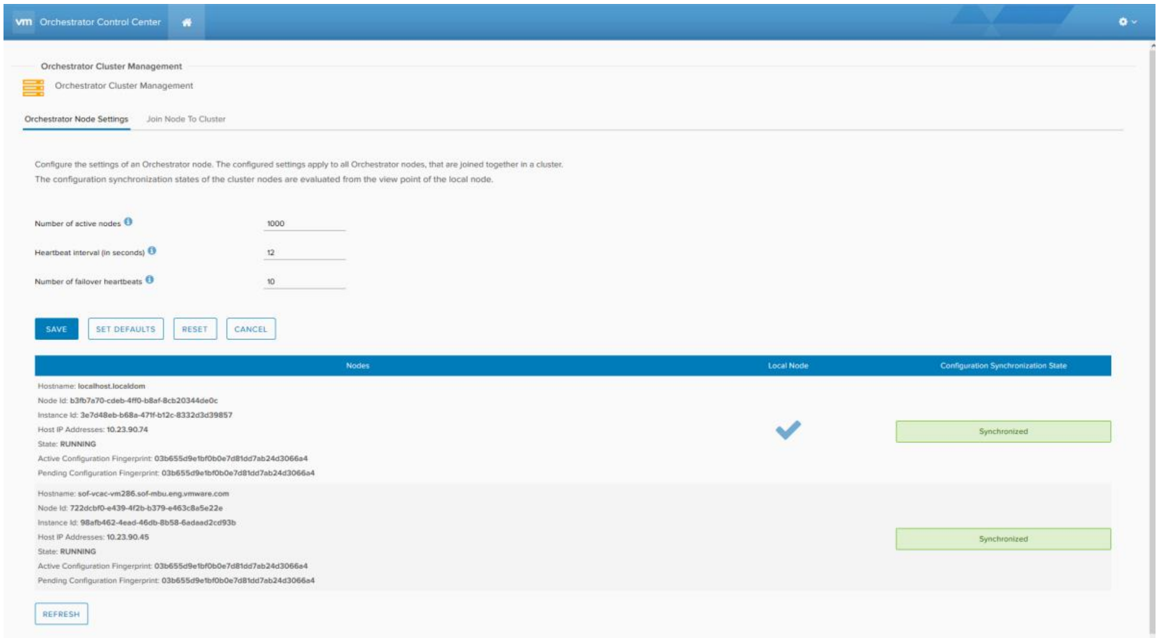
36. Verify all services are properly running by going to Validate Configuration. Each component should have a green tick next to it.

37. 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.

38. 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:


vm Orchestrator Control Center
Orchestrator Cluster Management
Orchestrator Cluster Management
Orchestrator Node Settings
Join Node To Cluster
SAVE
SET DEFAULTS
RESET
CANCEL
REFRESH

Configure the settings of an Orchestrator node. The configured settings apply to all Orchestrator nodes, that are joined together in a cluster.
The configuration synchronization states of the cluster nodes are evaluated from the view point of the local node.

Number of active nodes: 1000

Heartbeat interval (in seconds): 12

Number of failover heartbeats: 10

Nodes	Local Node	Configuration Synchronization State
Hostname: localhost.localdom Node Id: b3fb7a70-cdeb-4ff0-b8af-8cb20344de0c Instance Id: 3e7d48eb-b68a-471f-b12c-8332d3d39857 Host IP Addresses: 10.23.90.74 State: RUNNING Active Configuration Fingerprint: 03b655d9e1bf0b0e7d81dd7ab24d3066a4 Pending Configuration Fingerprint: 03b655d9e1bf0b0e7d81dd7ab24d3066a4	✓	Synchronized
Hostname: sof-vcac-vm286.sof-mbu.eng.vmware.com Node Id: 722dcbf0-e439-4f2b-b379-e463c8a5e22e Instance Id: 98afb462-4ead-46db-8b58-6adaad2cd93b Host IP Addresses: 10.23.90.45 State: RUNNING Active Configuration Fingerprint: 03b655d9e1bf0b0e7d81dd7ab24d3066a4 Pending Configuration Fingerprint: 03b655d9e1bf0b0e7d81dd7ab24d3066a4		Synchronized

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 Custom Persistence Profile

39. You can configure persistence profile for your F5 load balancer.Log in to the F5 load balancer and select **Local Traffic** > **Profiles** > **Persistence**.

40. Click **Create**.

41. Enter the name *source_addr_vro* and select Source Address Affinity from the drop-down menu.

42. Enable Custom mode.

43. Set the Timeout to 1800 seconds (30 minutes).

44. Click **Finished**.

Configure Monitors

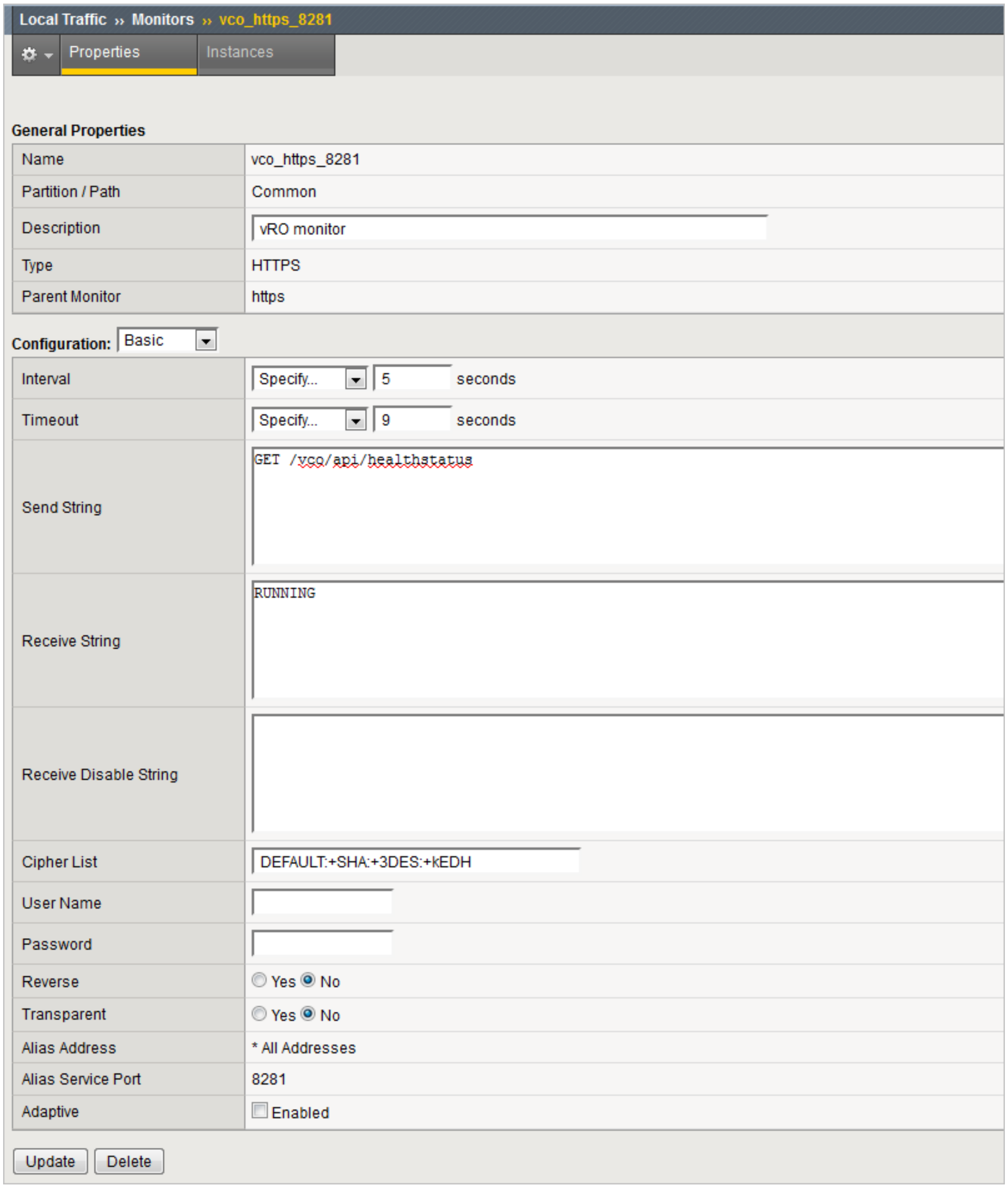
A monitor is a check which the load balancer software uses to determine whether a node is healthy, and redirect traffic accordingly. If the node is active and operational, monitor will receive an “HTTP 200 OK” response to its query. If the node is inactive (standby), monitor will receive a “HTTP 503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

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

TABLE 1 - CONFIGURE MONITORS

MONITOR	INTERVAL	TIMEOUT	RETRIES	TYPE	SEND STRING	RECEIVE STRING	ALIAS SERVICE PORT
vro-https-8281	5	9	3	HTTPS (443)	GET /vco/api/healthstatus	RUNNING	8281
vro-https-8283	5	9	3	HTTPS (443)	GET /vco-controlcenter/docs/	HTTP/1\.(0 |1) (200)	8283

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



General Properties

Name	vco_https_8281
Partition / Path	Common
Description	vRO monitor
Type	HTTPS
Parent Monitor	https

Configuration: Basic

Interval	Specify... 5 seconds
Timeout	Specify... 9 seconds
Send String	GET /vco/api/healthstatus
Receive String	RUNNING
Receive Disable String	
Cipher List	DEFAULT:+SHA:+3DES:+kEDH
User Name	
Password	
Reverse	○ Yes ● No
Transparent	○ Yes ● No
Alias Address	* All Addresses
Alias Service Port	8281
Adaptive	☐ Enabled

Configure Server and Control Center Pools

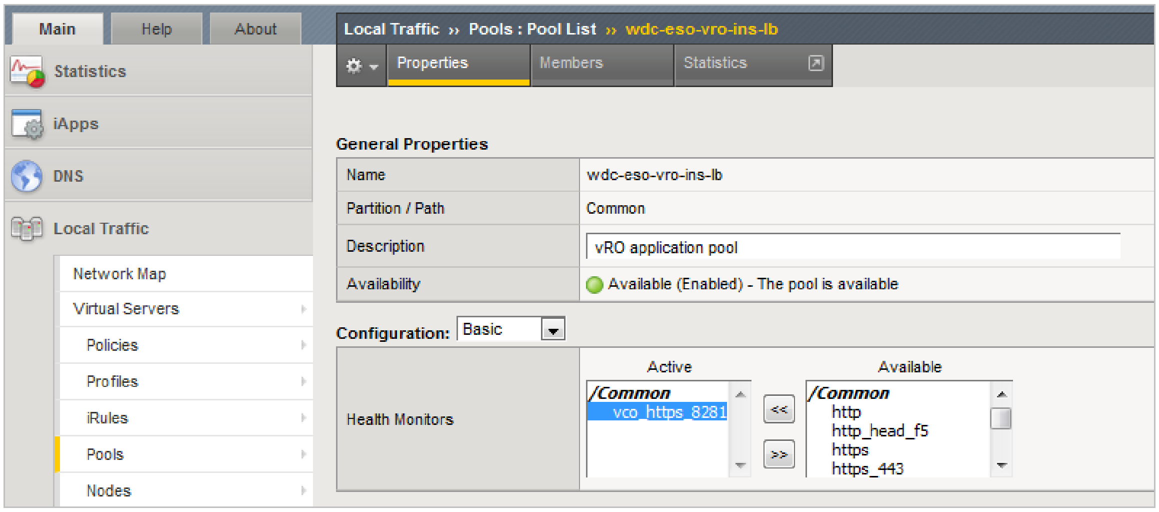
You can configure server and Control Center pools for your F5 load balancer by using the following steps.

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

TABLE 2 – CONFIGURE SERVER AND CONTROL CENTER POOLS

POOL NAME	LB METHOD	HEALTH MONITORS	NODE NAME	ADDRESS	SERVICE PORT
vro-pool-8281	Round Robin	vro-https-8281	<vro-node1-hostname.domain.com>	<vro-node1-IP>	8281
vro-pool-8281	Round Robin	vro-https-8281	<vro-node2-hostname.domain.com>	<vro-node2-IP>	8281
vro-pool-8283	Ratio	vro-https-8283	<vro-node1-hostname.domain.com>	<vro-node1-IP>	8283
vro-pool-8283	Ratio	vro-https-8283	<vro-node2-hostname.domain.com>	<vro-node2-IP>	8283

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



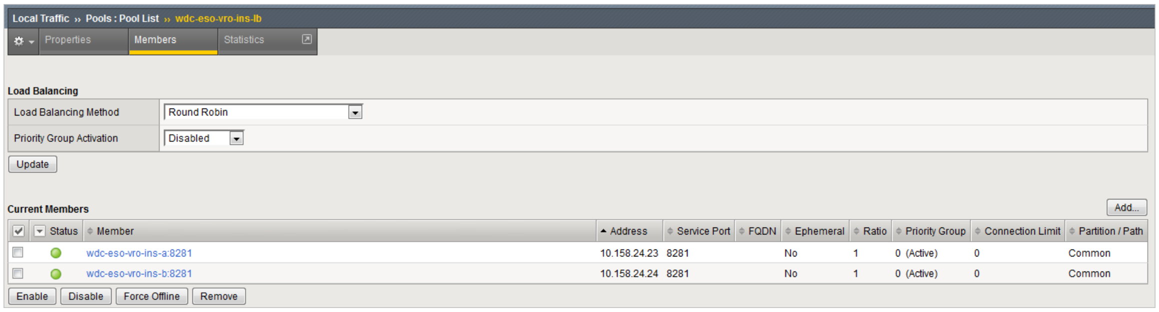
General Properties

Name	wdc-eso-vro-ins-lb
Partition / Path	Common
Description	vRO application pool
Availability	● Available (Enabled) - The pool is available

Configuration: Basic

	Active	Available
Health Monitors	/Common vco_https_8281	/Common http http_head_f5 https https_443

The green status indicates that the node is active. Both vRealize Orchestrator nodes should be shown as active.



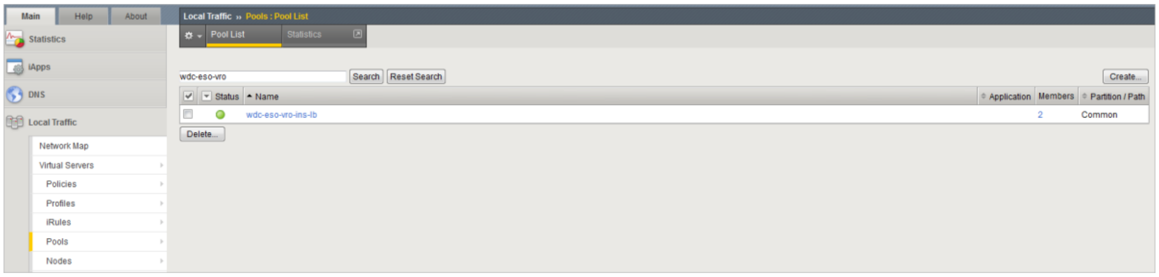
Load Balancing

Load Balancing Method	Round Robin
Priority Group Activation	Disabled

Current Members

☑	Status	Member	Address	Service Port	FQDN	Ephemeral	Ratio	Priority Group	Connection Limit	Partition / Path
□	●	wdc-eso-vro-ins-a:8281	10.158.24.23	8281		No	1	0 (Active)	0	Common
□	●	wdc-eso-vro-ins-b:8281	10.158.24.24	8281		No	1	0 (Active)	0	Common

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



wdc-eso-vro

Status	Name	Application	Members	Partition / Path
●	wdc-eso-vro-ins-lb		2	Common

Configure Virtual Servers

You can configure virtual servers for your F5 load balancer by using the following steps.

52. Log in to the F5 load balancer and select **Local Traffic** > **Virtual Servers**.

53. Click **Create** and provide the required information as given in Table 3. Leave the default when nothing is specified.

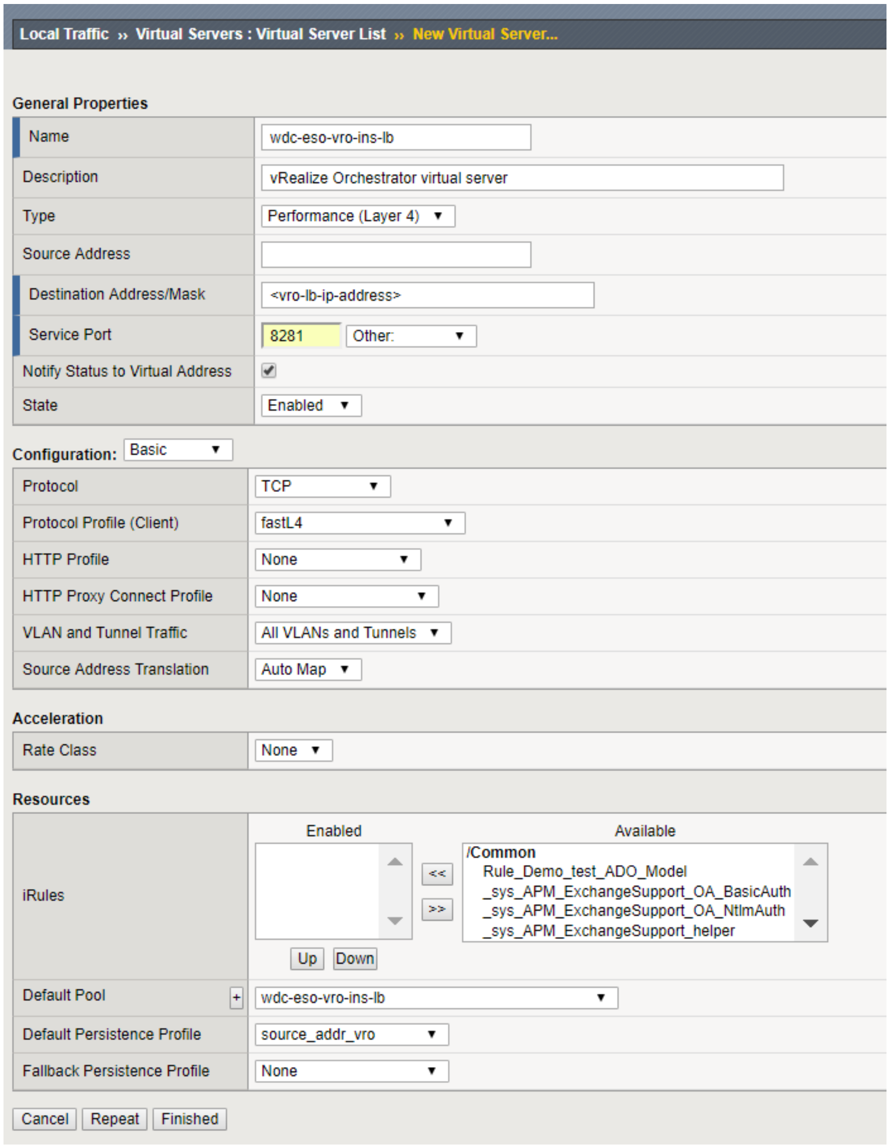
54. Click **Finished**.

TABLE 3 – CONFIGURE VIRTUAL SERVERS

NAME	DESCRIPTION	TYPE	DESTINATION ADDRESS	SERVICE PORT	SOURCE ADDRESS TRANSLATION	DEFAULT POOL	DEFAULT PERSISTENCE PROFILE
vro-lb-8281	vRealize Orchestrator virtual server	Performance (Layer 4)	<vro-lb-IP>	8281	Automap	vro-pool-8281	source_addr_vro
vro-lb-8283	vRealize Orchestrator control center	Performance (Layer 4)	<vro-lb-IP>	8283	Automap	vro-pool-8283	source_addr_vro

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:



Local Traffic » Virtual Servers : Virtual Server List » New Virtual Server...

General Properties

Name	wdc-eso-vro-ins-lb
Description	vRealize Orchestrator virtual server
Type	Performance (Layer 4)
Source Address	
Destination Address/Mask	<vro-lb-ip-address>
Service Port	8281 Other:
Notify Status to Virtual Address	☑
State	Enabled

Configuration: Basic

Protocol	TCP
Protocol Profile (Client)	fastL4
HTTP Profile	None
HTTP Proxy Connect Profile	None
VLAN and Tunnel Traffic	All VLANs and Tunnels
Source Address Translation	Auto Map

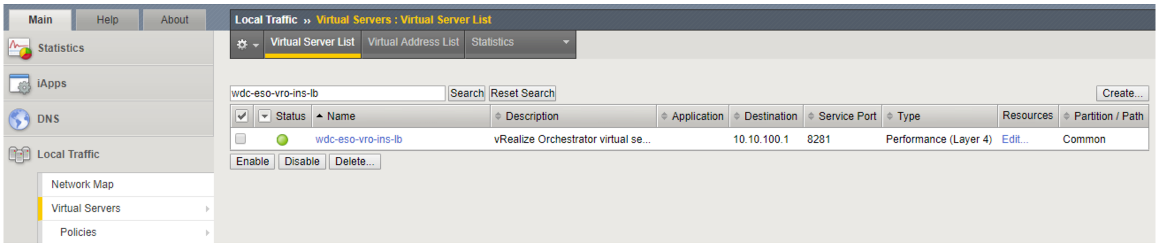
Acceleration

Rate Class	None

Resources

iRules	Enabled: (none) Available: /Common Rule_Demo_test_ADO_Model _sys_APM_ExchangeSupport_OA_BasicAuth _sys_APM_ExchangeSupport_OA_NtlmAuth _sys_APM_ExchangeSupport_helper
Default Pool	wdc-eso-vro-ins-lb
Default Persistence Profile	source_addr_vro
Fallback Persistence Profile	None

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



Local Traffic » Virtual Servers : Virtual Server List

Search: wdc-eso-vro-ins-lb

☑	Status	Name	Description	Application	Destination	Service Port	Type	Resources	Partition / Path
□	●	wdc-eso-vro-ins-lb	vRealize Orchestrator virtual se...		10.10.100.1	8281	Performance (Layer 4)	Edit...	Common

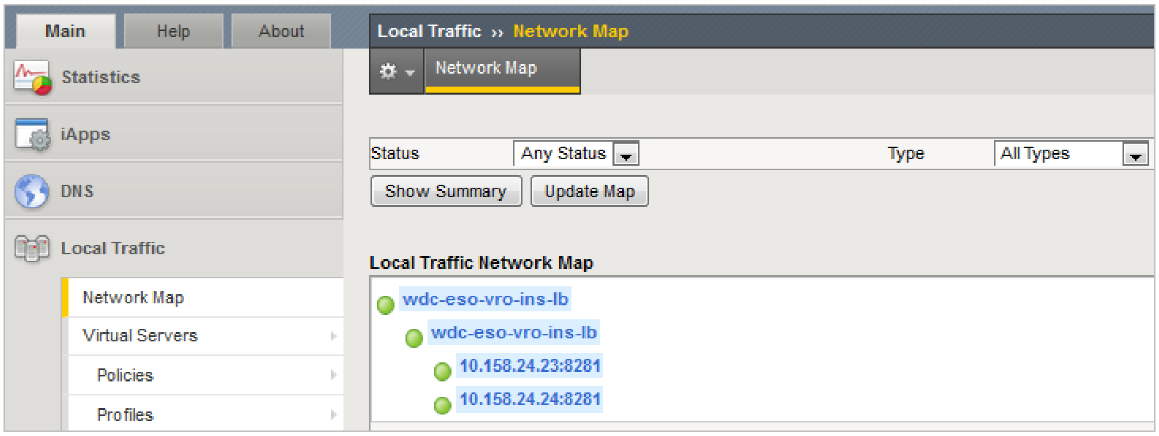
This concludes the cluster configuration with F5 as a load balancer. You should now validate that your new setup is functional.

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.

55. In the F5 interface, select **Local Traffic > Network Map**.

56. 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:

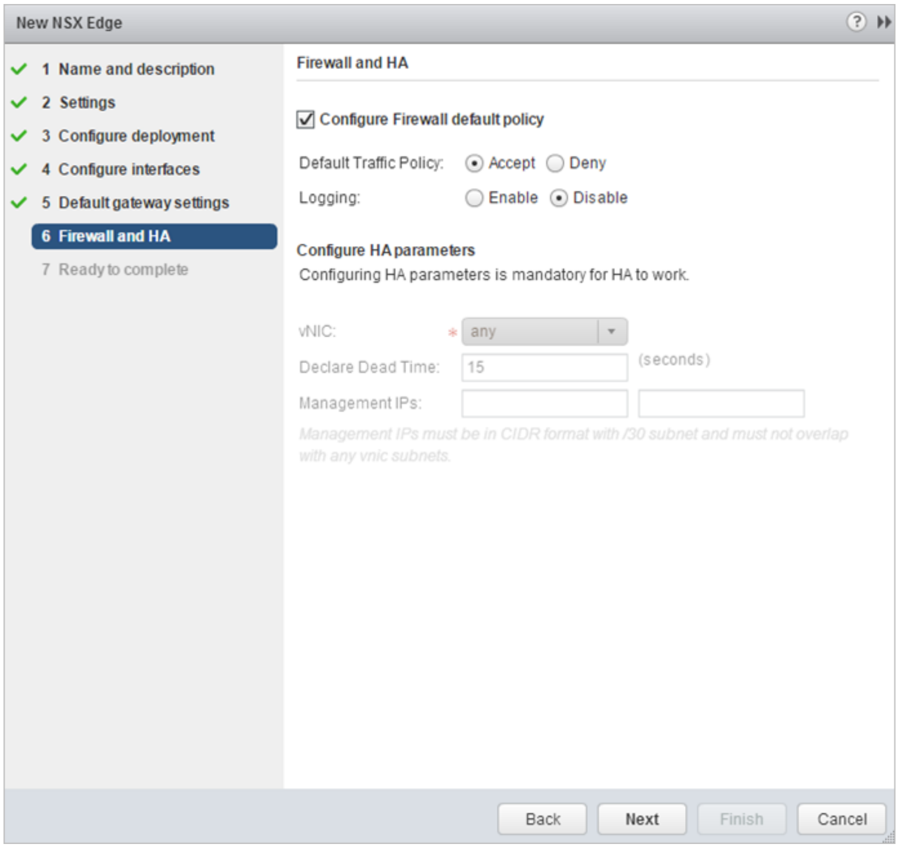
- This document assumes that NSX deployment is already deployed in the environment and is fully functional.
- The NSX deployment is of version 6.2 or higher.
- NSX Edge is deployed and has access to the network on which vRealize Orchestrator is deployed.

Create and Configure the NSX-Edge

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

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

59. Select the **Configure Firewall default policy** check box and **Accept** the **Default Traffic Policy** as shown in the following screen.



Firewall and HA

☑ Configure Firewall default policy

Default Traffic Policy: ● Accept ○ Deny

Logging: ○ Enable ● Disable

Configure HA parameters

Configuring HA parameters is mandatory for HA to work.

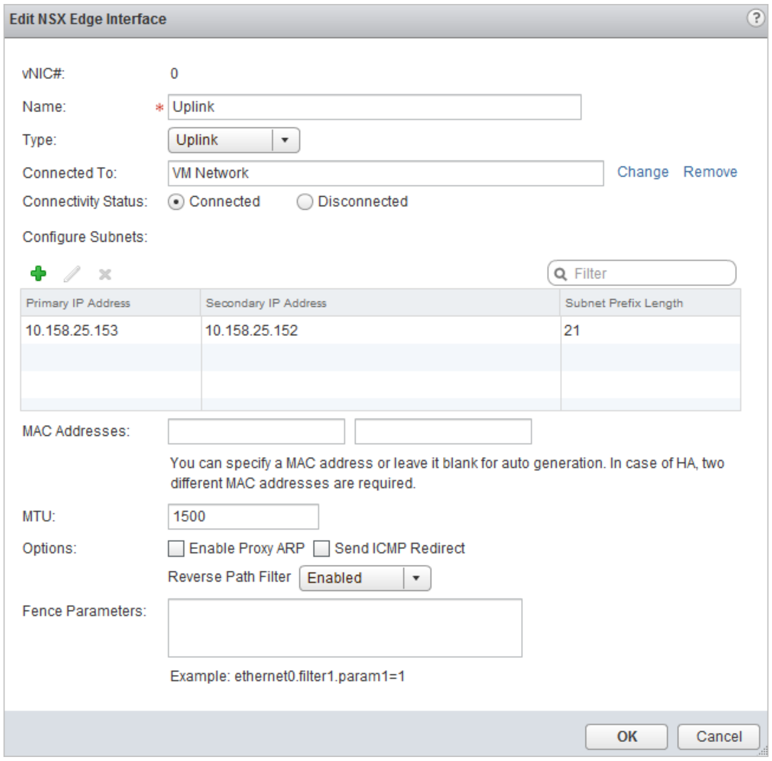
vNIC: * any

Declare Dead Time: 15 (seconds)

Management IPs:

Management IPs must be in CIDR format with /30 subnet and must not overlap with any vnic subnets.

60. Double-click to select your Edge device from the list.
61. Select the **Manage** tab, click **Load Balancer** tab and click the **Edit** icon.
62. Select **Enable Load Balancer** and **Enable Acceleration,** if required, and click **OK**.
63. Select the **Manage** tab, click **Settings**, and select **Interfaces** menu.
64. Select the first vNIC and click the **Edit** icon to edit the first vNIC, this is your Load Balancer virtual appliance.
65. Assign a primary IP address to the NSX Edge and assign the secondary IP addresses that can be used as the virtual server addresses.
66. Click the **Add** icon to assign a static IP address to this virtual interface. The configuration should look similar to the following screen:



Edit NSX Edge Interface

vNIC#: 0

Name: * Uplink

Type: Uplink

Connected To: VM Network

Connectivity Status: ● Connected ○ Disconnected

Configure Subnets:

Primary IP Address	Secondary IP Address	Subnet Prefix Length
10.158.25.153	10.158.25.152	21

MAC Addresses:

You can specify a MAC address or leave it blank for auto generation. In case of HA, two different MAC addresses are required.

MTU: 1500

Options: □ Enable Proxy ARP □ Send ICMP Redirect

Reverse Path Filter: Enabled

Fence Parameters:

Example: ethernet0.filter1.param1=1

Add Application Profiles

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

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

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

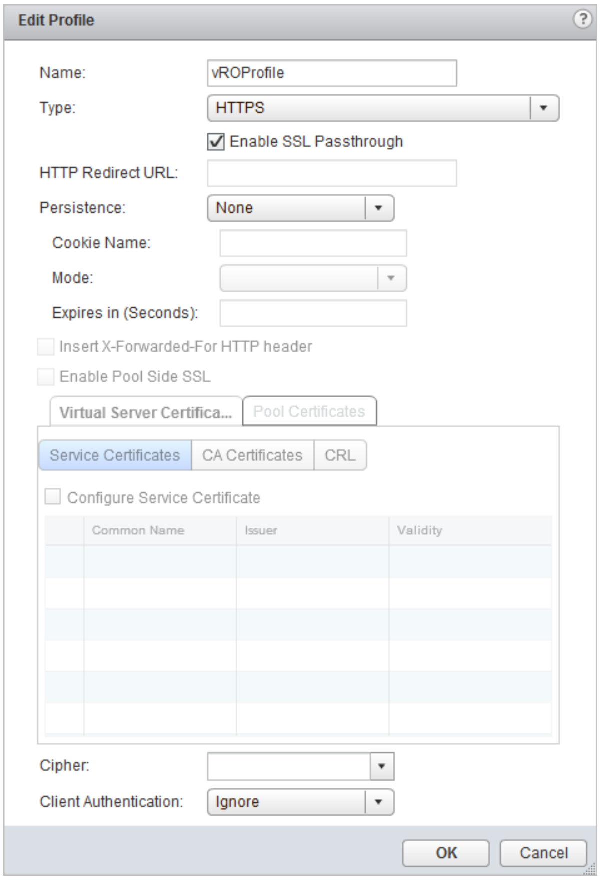
70. Click the **Add** icon to create the application profiles required for vRealize Orchestrator by using information in Table 4. Leave the default when nothing is specified.

71. Click **OK**.

TABLE 4 – APPLICATION PROFILES

NAME	TYPE	ENABLED SSL PASS-THROUGH	PERSISTENCE	CLIENT AUTHENTICATION
vROProfile	HTTPS	Yes	None	Ignore

The completed configuration should look similar to the following screen.



Edit Profile

Name: vROProfile

Type: HTTPS

☑ Enable SSL Passthrough

HTTP Redirect URL:

Persistence: None

Cookie Name:

Mode:

Expires in (Seconds):

□ Insert X-Forwarded-For HTTP header

□ Enable Pool Side SSL

□ Configure Service Certificate

Cipher:

Client Authentication: Ignore

Add Service Monitoring

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

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

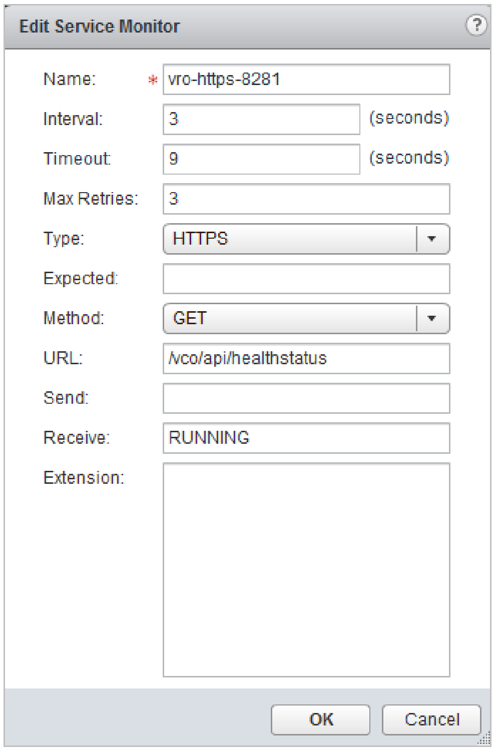
74. Select the **Load Balancer** tab and click on the **Service Monitoring** menu.

75. 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

MONITOR NAME	INTERVAL	TIMEOUT	MAX RETRIES	TYPE	METHOD	URL	EXPECTED	RECEIVE
vro-https-8281	3	9	3	HTTPS	GET	/vco/api/healthstatus		RUNNING
vro-https-8283	3	10	3	HTTPS	GET	/vco-controlcenter/docs/	200	

The completed configuration should look similar to the following screen.



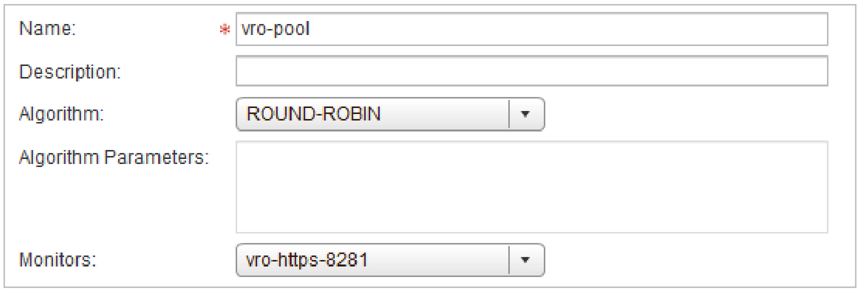
Name: * vro-https-8281
Interval: 3 (seconds)
Timeout: 9 (seconds)
Max Retries: 3
Type: HTTPS
Expected:
Method: GET
URL: /vco/api/healthstatus
Send:
Receive: RUNNING
Extension:

Configure Pools

76. Log in to the vCenter Server where NSX has been set up.
77. Navigate to **Home >Networking & Security >NSX Edges** and select your previously created NSX edge.
78. Select the **Load Balancer** tab and click **Pools**.
79. Click the **Add** icon to create a new pool required for vRealize Orchestrator by using information in Table 6Table 5. Leave the default when nothing is specified.

TABLE 6 – POOL CHARACTERISTICS

POOL NAME	ALGORITHM	MONITORS
vROPool	Round Robin	vro-https-8281
vROControlCenter	IP-HASH	vro-https-8283

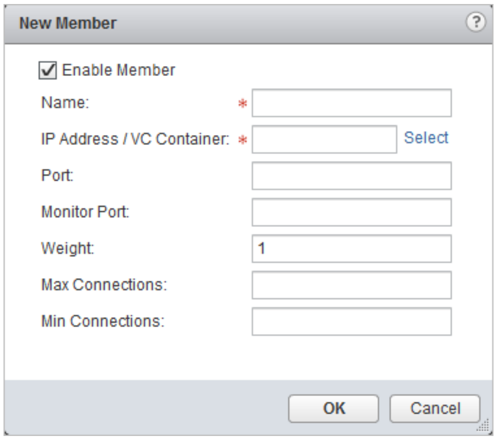


Name: *	vro-pool
Description:	
Algorithm:	ROUND-ROBIN
Algorithm Parameters:	
Monitors:	vro-https-8281

80. Click the **Add** icon to add new members to the pool by using information in Table 7.

TABLE 7: POOL NODES CHARACTERISTICS

ENABLED MEMBER	NAME	IP ADDRESS / VC CONTAINER	MONITOR PORT	PORT
yes	HA-cluster-vro1	<vro-Node1 IP>	8281	8281
yes	HA-cluster-vro2	<vro-Node2 IP>	8281	8281
yes	HA-cluster-vro1	<vro-Node1 IP>	8283	8283
yes	HA-cluster-vro2	<vro-Node2 IP>	8283	8283

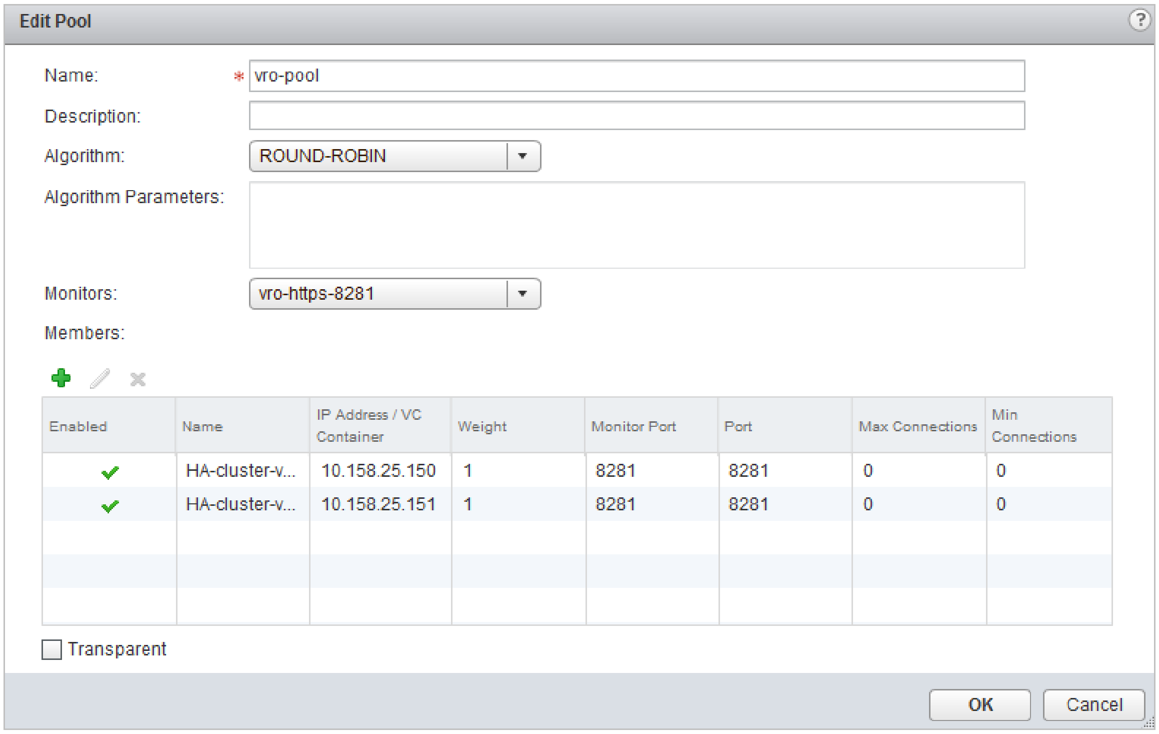


New Member

☑ Enable Member

Name: *	
IP Address / VC Container: *	
Port:	
Monitor Port:	
Weight:	1
Max Connections:	
Min Connections:	

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.



Name: * vro-pool

Description:

Algorithm: ROUND-ROBIN

Algorithm Parameters:

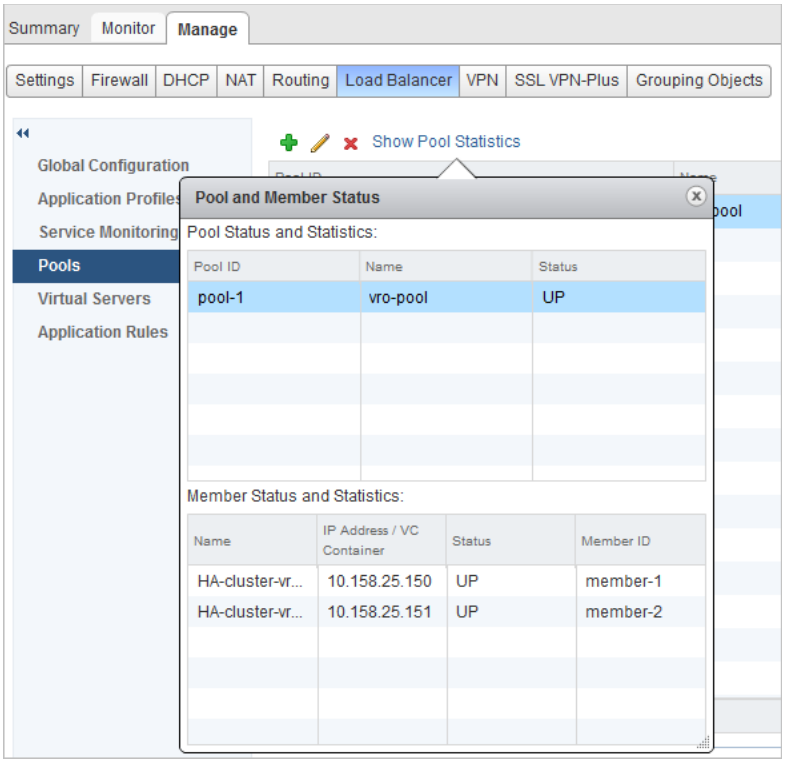
Monitors: vro-https-8281

Members:

Enabled	Name	IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	Min Connections
✓	HA-cluster-v...	10.158.25.150	1	8281	8281	0	0
✓	HA-cluster-v...	10.158.25.151	1	8281	8281	0	0

□ Transparent

Verify that the pool is in a UP state by clicking on the **Show Pool Statistics** link.



Pool Status and Statistics:

Pool ID	Name	Status
pool-1	vro-pool	UP

Member Status and Statistics:

Name	IP Address / VC Container	Status	Member ID
HA-cluster-vr...	10.158.25.150	UP	member-1
HA-cluster-vr...	10.158.25.151	UP	member-2

Configure Virtual Servers

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

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

83. 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.

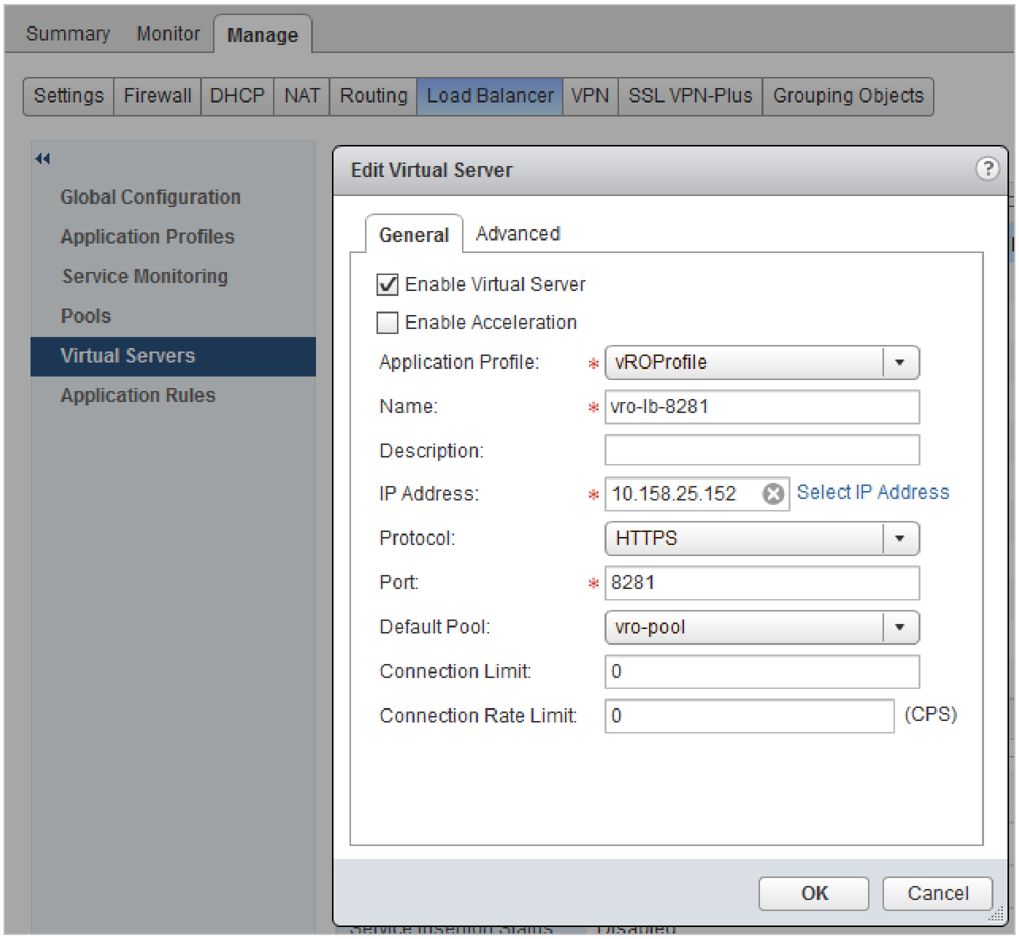
84. Table 8Table 5. Leave the default when nothing is specified.

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

TABLE 8 – VIRTUAL SERVER CHARACTERISTICS

ENABLE VIRTUAL SERVER	APPLICATION PROFILE	NAME	IP ADDRESS	PROTOCOL	PORT	DEFAULT POOL
Yes	vROProfile	vro-lb-8281	<vro-lb-ip>	HTTPS	8281	vROPool
Yes	vROProfile	vro-lb-8283	<vro-lb-ip>	HTTPS	8283	vROControlCenter

The completed configuration should look similar to the following screen.



☑ Enable Virtual Server

□ Enable Acceleration

Application Profile: * vROProfile

Name: * vro-lb-8281

Description:

IP Address: * 10.158.25.152 Select IP Address

Protocol: HTTPS

Port: * 8281

Default Pool: vro-pool

Connection Limit: 0

Connection Rate Limit: 0 (CPS)

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

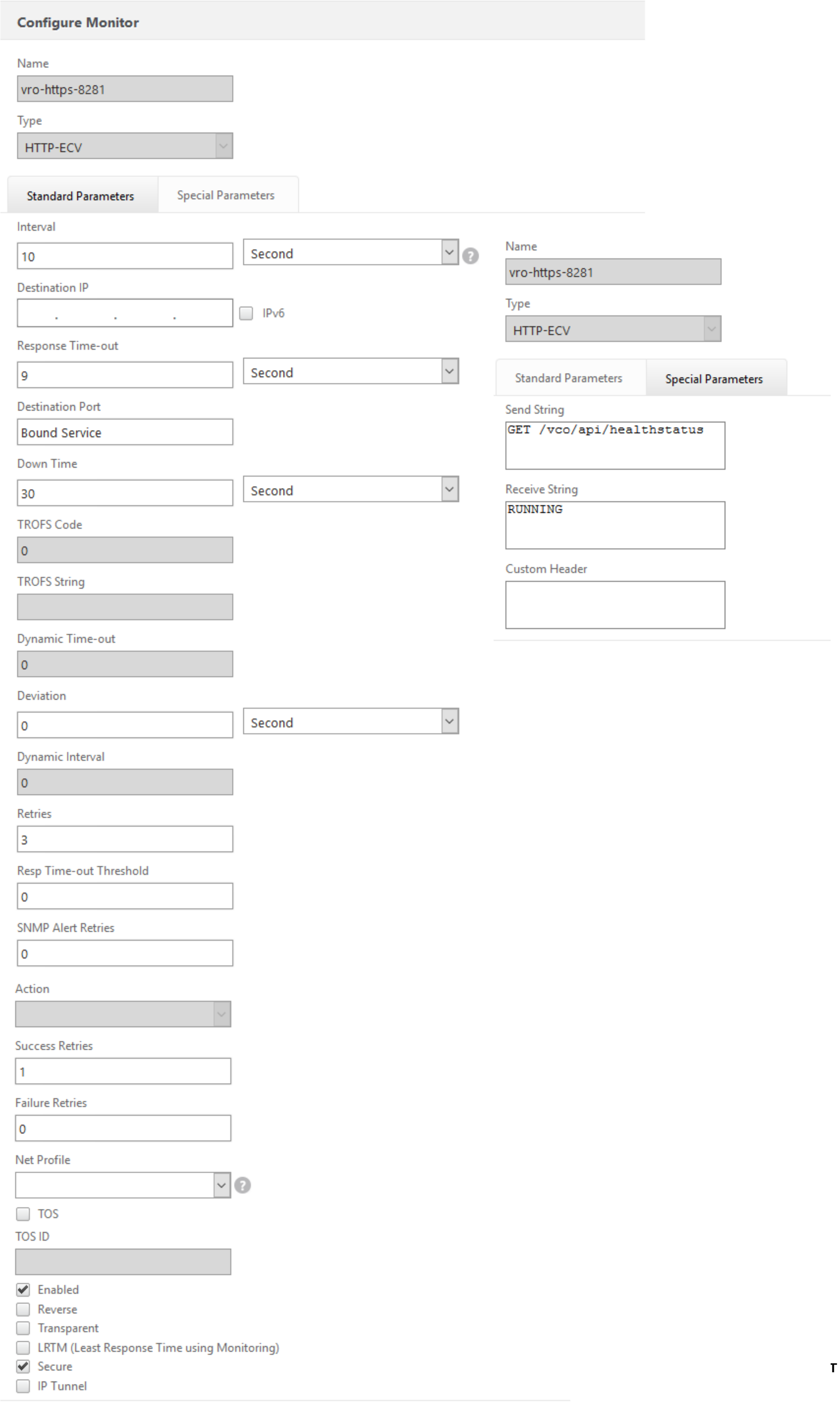
A monitor in NetScaler is a check that the load balancer software uses to determine whether a node is healthy and redirect traffic accordingly. If the node is active and operational, monitor receives an “HTTP 200 OK” response to its query. If the node is inactive (standby), monitor receives an “HTTP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

85. Log in to the NetScaler web console and select **Traffic Management > Load Balancing > Monitors**.
86. Click **Add** and provide the required information as given in Table 9 - Configure MonitorsTable 9. Leave all unspecified options with their default values.
87. Click **Create**.

TABLE 9 - CONFIGURE MONITORS

MONITOR	INTERVAL	TIMEOUT	RETRIES	TYPE	SEND STRING/HTTP REQUEST	RECEIVE STRING	SECURE OPTION
vro-https-8281	10	9	3	HTTP-ECV	GET /vco/api/healthstatus	RUNNING	Enabled
vro-https-8283	10	9	3	HTTP	GET /vco-controlcenter/docs/	<title>Swagger UI</title>	Enabled

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



Configure Monitor

Name: vro-https-8281

Type: HTTP-ECV

Standard Parameters | Special Parameters

Interval: 10 Second

Destination IP: . . . □ IPv6

Response Time-out: 9 Second

Destination Port: Bound Service

Down Time: 30 Second

TROFS Code: 0

TROFS String:

Dynamic Time-out: 0

Deviation: 0 Second

Dynamic Interval: 0

Retries: 3

Resp Time-out Threshold: 0

SNMP Alert Retries: 0

Action:

Success Retries: 1

Failure Retries: 0

Net Profile:

□ TOS

TOS ID:

☑ Enabled

□ Reverse

□ Transparent

□ LRTM (Least Response Time using Monitoring)

☑ Secure

□ IP Tunnel

Name: vro-https-8281

Type: HTTP-ECV

Standard Parameters | Special Parameters

Send String:

```
GET /vco/api/healthstatus
```

Receive String:

```
RUNNING
```

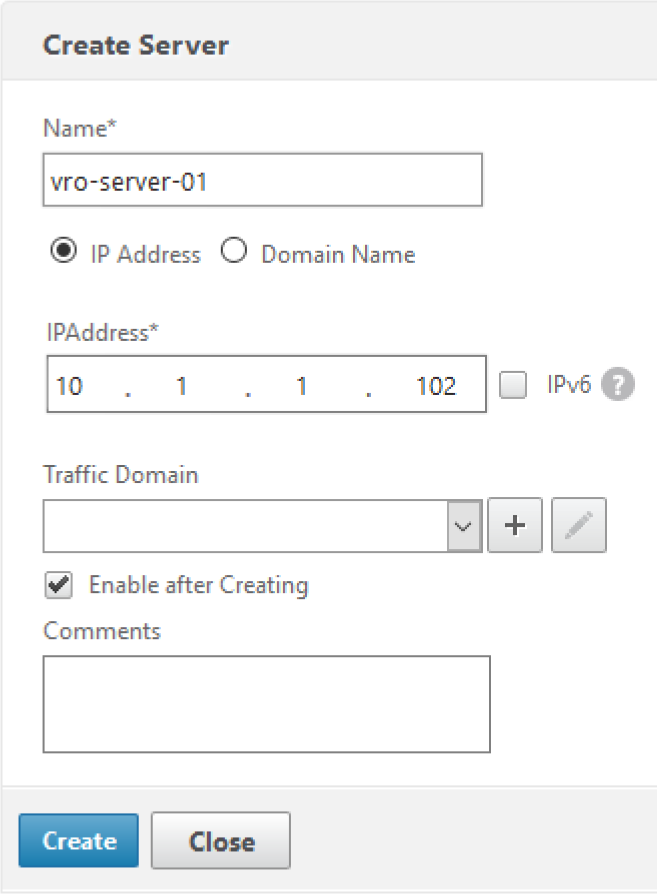
Custom Header:

Configure Servers

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

88. Log in to the NetScaler web console and select **Traffic Management > Load Balancing > Servers**.
89. 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.
90. Click **Enable after Creating**.
91. Choose a traffic domain if it applies to your configuration.
92. Click **Create**.

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



Create Server

Name*: vro-server-01

● IP Address ○ Domain Name

IPAddress*: 10 . 1 . 1 . 102 □ IPv6

Traffic Domain:

☑ Enable after Creating

Comments:

Configure Services for Orchestrator Server and Control Center

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

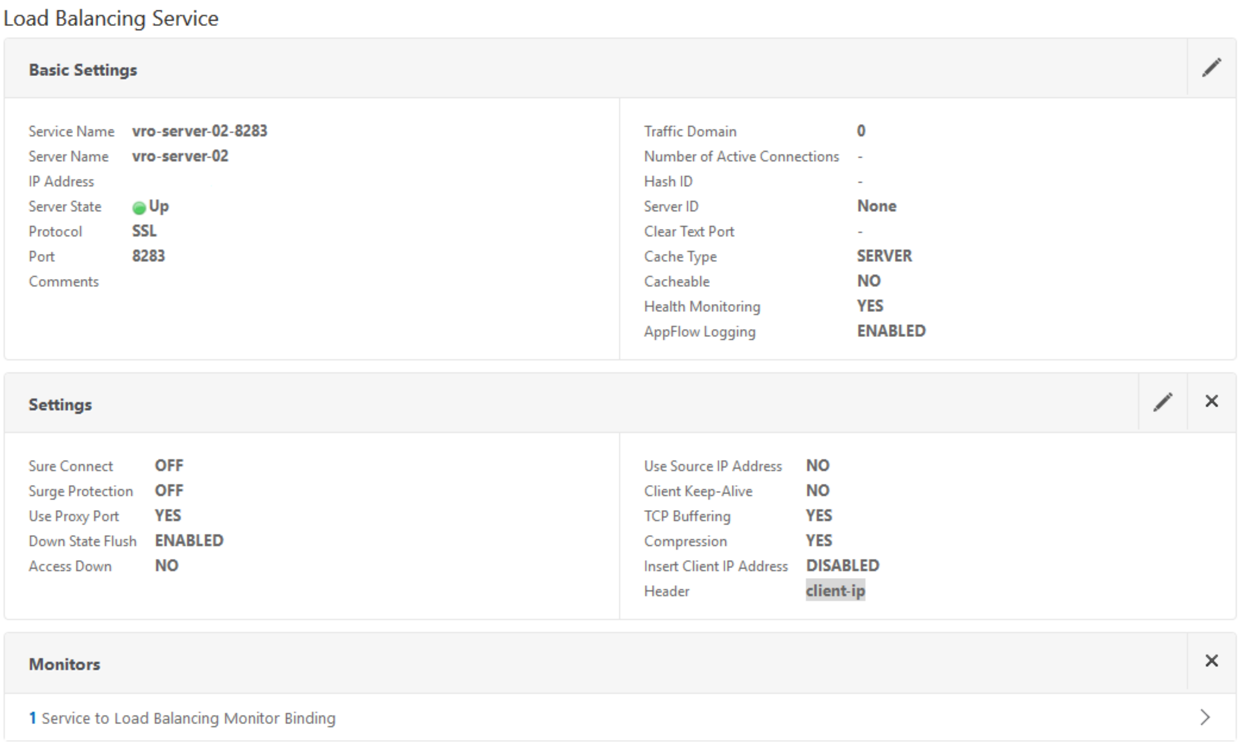
93. Log in to the NetScaler web console and select **Traffic Management > Load Balancing > Services**.
94. Click **Add** and provide the required information. Leave all unspecified options with their default values. For service names, use the convention accepted in your organization.

95. Choose a traffic domain if it applies to your configuration.
96. Click **OK**.
97. Under the **Monitors** section click on the existing binding.
98. Click **Add Binding**.
99. Under **Select Monitor** click to select a monitor.
100. Choose a monitor by clicking on the monitor for the current service as specified in TABLE 10.
101. Click **Select**.
102. Click **Bind**.
103. Click **Close**.
104. Click **Done**.
105. Repeat these steps for each entry in TABLE 10.

TABLE 10 – CONFIGURE SERVER AND CONTROL CENTER SERVICES

SERVICE NAME	EXISTING SERVER	PROTOCOL	HEALTH MONITORS	SERVICE PORT
vro-server-01-8281	vro-server-01	SSL_BRIDGE	vro-https-8281	8281
vro-server-02-8281	vro-server-02	SSL_BRIDGE	vro-https-8281	8281
vro-server-01-8283	vro-server-02	SSL_BRIDGE	vro-https-8283	8283
vro-server-02-8283	vro-server-02	SSL_BRIDGE	vro-https-8283	8283

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



Load Balancing Service

Basic Settings

Service Name	vro-server-02-8283	Traffic Domain	0
Server Name	vro-server-02	Number of Active Connections	-
IP Address		Hash ID	-
Server State	● Up	Server ID	None
Protocol	SSL	Clear Text Port	-
Port	8283	Cache Type	SERVER
Comments		Cacheable	NO
		Health Monitoring	YES
		AppFlow Logging	ENABLED

Settings

Sure Connect	OFF	Use Source IP Address	NO
Surge Protection	OFF	Client Keep-Alive	NO
Use Proxy Port	YES	TCP Buffering	YES
Down State Flush	ENABLED	Compression	YES
Access Down	NO	Insert Client IP Address	DISABLED
		Header	client-ip

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.

106. Log in to the F5 load balancer and select **Traffic Management** > **Load Balancing** > **Virtual Servers**.

107. 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.

108. Choose a traffic domain if it applies to your configuration.

109. Click **OK**.

110. Under **Services and Service Groups** click **No load Balancing Virtual Service Binding**.

111. Under **Select Service** click to select the two services.

112. Choose a service by clicking on the respective service as specified in Table 11.

113. Click **Select**.

114. Click **Bind**.

115. Click **Continue**.

116. Choose a persistence from the options as specified in Table 11.

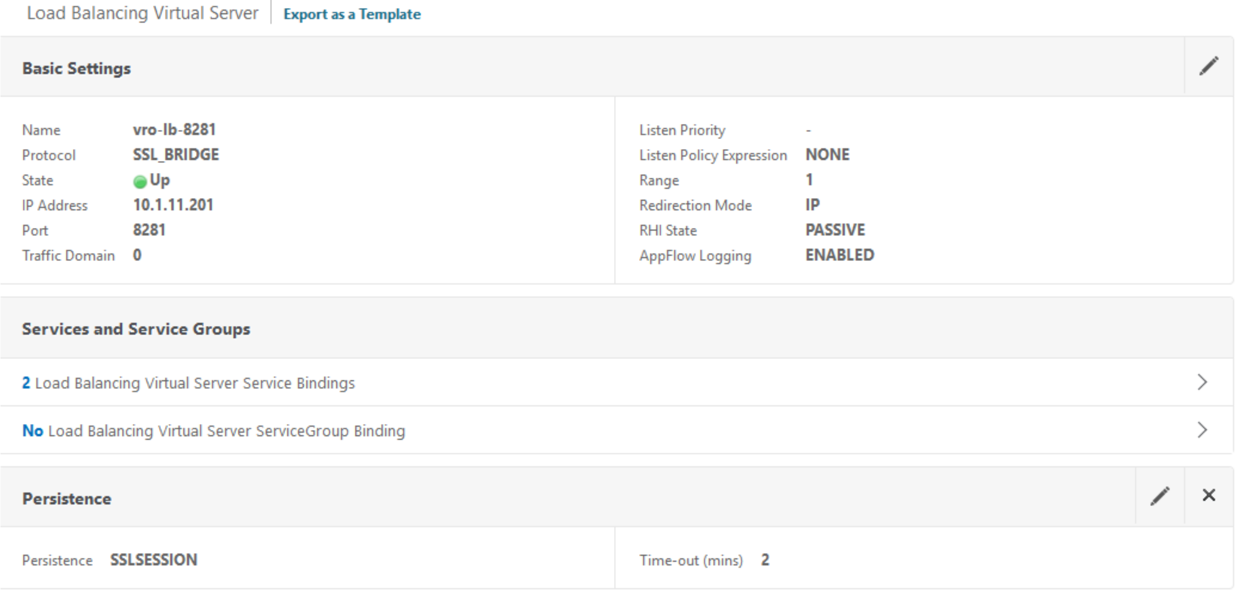
117. Repeat these steps for the vRealize Orchestrator Control Center virtual server.

TABLE 11 – CONFIGURE VIRTUAL SERVERS

NAME	COMMENTS	PROTOCOL	DESTINATION ADDRESS	SERVICE PORT	PERSISTENCE	SERVICES
vro-lb-8281	vRealize Orchestrator virtual server	SSL_BRIDGE	<vro-lb-IP>	8281	SSLSESSION or SOURCEIP or NONE	vro-server-01-8281 & vro-server-02-8281
vro-lb-8283	vRealize Orchestrator control center	SSL_BRIDGE	<vro-lb-IP>	8283	SSLSESSION or SOURCEIP	vro-server-01-8283 & vro-server-02-8283

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:



Name vro-lb-8281
Protocol SSL_BRIDGE
State Up
IP Address 10.1.11.201
Port 8281
Traffic Domain 0

Listen Priority -
Listen Policy Expression NONE
Range 1
Redirection Mode IP
RHI State PASSIVE
AppFlow Logging ENABLED

2 Load Balancing Virtual Server Service Bindings

No Load Balancing Virtual Server ServiceGroup Binding

Persistence SSLSESSION
Time-out (mins) 2

Configure Persistence Groups

118. Log in to the NetScaler web console and select **NetScaler** > **Traffic Management > Load Balancing > Persistency Groups**.

119. Click **Add**.

120. Enter the name source_addr_vro and select **Persistence** > **SOURCEIP** from the drop-down menu.

121. Set the Timeout to 30 minutes.

122. Add all related Virtual Servers.

123. Click **OK**.

124. Repeat these steps to create a second persistence group.

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:

https://support.f5.com/kb/en-us/solutions/public/3000/600/sol3664.html

https://support.f5.com/kb/en-us/solutions/public/3000/700/sol3727.html

https://support.f5.com/kb/en-us/solutions/public/3000/600/sol3667.html

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:

125. Log in as an administrator to the machine on which SQL Server is installed.
126. 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.
127. Expand the list on the left.
128. Click **Protocols** for <MSSQL-version>.
129. Right-click **TCP/IP** and select **Enable**.
130. Right-click **TCP/IP** and select **Properties**.
131. Click the **IP Addresses** tab.
132. Under **IP1**, **IP2**, and **IPAll**, set the TCP Port value to **1433**.
133. Click **OK**.

134. 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:

https://support.f5.com/kb/en-us/solutions/public/3000/200/sol3224.html

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.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com