Table of Contents

Introduction ........................................................................................................................................... 4
Load Balancing Concepts ......................................................................................................................... 5
SSL Pass-Through ................................................................................................................................ 5
Session Persistence ................................................................................................................................. 6
Destination Address (F5 and NetScaler) ............................................................................................... 6
Source (IP) Address (F5, NetScaler, and NSX-V) .................................................................................. 6
Source IP Address Hash (NSX-V) ............................................................................................................ 6
Email Notifications on Load Balancer ..................................................................................................... 6
One-Arm or Multi-Arm Topologies .......................................................................................................... 6
Prerequisites for Configuring Load Balancers for vRealize Automation ................................................. 7
Complete the vRealize Automation / vRealize Orchestrator Initial Installation ................................. 8
Configuring F5 Big-IP LTM .................................................................................................................... 9
Configure Custom Persistence Profile ..................................................................................................... 9
Configure Monitors ................................................................................................................................. 9
Configure Server Pools .......................................................................................................................... 11
Configure Virtual Servers ...................................................................................................................... 12
Configuring NSX-V ................................................................................................................................ 15
Configure Global Settings ..................................................................................................................... 15
Add Application Profiles ......................................................................................................................... 17
Add Service Monitoring .......................................................................................................................... 18
Add Pools ................................................................................................................................................ 19
Add Virtual Servers ............................................................................................................................... 21
Configuring NSX-T ................................................................................................................................ 22
Add Application Profiles ......................................................................................................................... 22
Add Persistence Profile .......................................................................................................................... 23
Add Active Health Monitor .................................................................................................................... 24
Configure Server Pools .......................................................................................................................... 27
Configure Virtual Servers ....................................................................................................................... 29
Configure Load Balancer ........................................................................................................................ 30
Add Virtual Servers to Load Balancer ..................................................................................................... 31
Configuring Citrix ADC (NetScaler ADC) ............................................................................................ 32
Configure Monitors ......................................................................................................................32
Configure Service Groups ........................................................................................................34
Configure Virtual Servers ..........................................................................................................35
Configure Persistency Group .....................................................................................................36
Troubleshooting ..........................................................................................................................37

Provisioning failures when using OneConnect with F5 BIG-IP for a virtual server with SSL pass-through .................................................................................................................................37

F5 BIG-IP license limits network bandwidth ................................................................................37
Revision History

<table>
<thead>
<tr>
<th>DATE</th>
<th>VERSION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 2019</td>
<td>1.0</td>
<td>Initial version for vRA 8.0 and vRO 8.0</td>
</tr>
</tbody>
</table>

Introduction

This document describes the configuration of the load balancing modules of F5 Networks BIG-IP software (F5), Citrix NetScaler, and NSX load balancers for vRealize Automation and vRealize Orchestrator 8.x in a distributed and highly available deployment. This document is not an installation guide, but a load-balancing configuration guide that supplements the vRealize Automation and vRealize Orchestrator installation and configuration documentation available at VMware vRealize Automation product documentation.

This information is for the following products and versions.

<table>
<thead>
<tr>
<th>PRODUCT</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>F5 BIG-IP LTM</td>
<td>11.x, 12.x, 13.x, 14.x, 15.x</td>
</tr>
<tr>
<td>NSX-V</td>
<td>6.2.x, 6.3.x, 6.4.x (please refer to the VMware Product Interoperability Matrices for more details)</td>
</tr>
<tr>
<td>NSX-T</td>
<td>2.4</td>
</tr>
<tr>
<td>Citrix NetScaler ADC</td>
<td>10.5, 11.x, 12.x, 13.x</td>
</tr>
<tr>
<td>vRealize Automation</td>
<td>8.0</td>
</tr>
<tr>
<td>vRealize Orchestrator</td>
<td>8.0</td>
</tr>
</tbody>
</table>
Load Balancing Concepts

Load balancers distribute work among servers in high-availability 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 Automation and vRealize Orchestrator backup planning.

SSL Pass-Through

SSL pass-through is used with the load balancing configurations for the following reasons:

- **Ease of deployment.** Not having to deploy the vRealize Automation or vRealize Orchestrator certificates to the load balancer simplifies deployment and reduces complexity
- **No operational overhead.** At the time of certificate renewal, no configuration changes are required on the load balancer
- **Ease of communication.** The individual host names of the load-balanced components are in the subject alternate name field of the certificates, so the client has no problem communicating with the load balanced nodes
Session Persistence

The persistence option overrides any load balancing algorithm option, for example setting dest_addr overrides, setting round robin, and so on. Different components in the vRealize Automation and vRealize Orchestrator architecture benefit from different persistence methods. The configuration described 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, and NSX-V)

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 1500 seconds (25 minutes). 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 1500 seconds to match the vRealize Automation and vRealize Orchestrator GUI timeout.

Source IP Address Hash (NSX-V)

The source IP address is hashed and divided by the total weight of the running servers to designate which server receives the request. This process ensures that the same client IP address always reaches the same server if no server fails or starts. For more information on IP Hash load balancing, see VMware knowledge base article KB 2006129.

Email Notifications on Load Balancer

It is a good practice to set up an email notification on the load balancer that sends emails to the system administrator every time a vRealize Automation or vRealize Orchestrator node goes down. Currently, NSX-V does not support email notification for such a scenario.

For NetScaler, configure specific SNMP traps and an SNMP manager to send alerts. Consult the NetScaler documentation for information on SNMP configuration.

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

- Configuring the BIG-IP system to deliver locally generated email messages
- Configuring custom SNMP traps
- Configuring alerts to send email notifications

One-Arm or Multi-Arm Topologies

In one-arm deployment, the load balancer is not physically in line of the traffic, which means that the load balancer’s ingress and egress traffic goes through the same network interface. Traffic from the client through the load balancer is network address translated (NAT) with the load balancer as its source address. The nodes send their return traffic to the load balancer before being passed back to the client. Without this reverse packet flow, return traffic would try to reach the client directly, causing connections to fail.

In a multi-arm configuration, the traffic is routed through the load balancer. The end devices typically have the load balancer as their default gateway.
The most common deployment is a one-arm configuration. The same principles apply to multi-arm deployments, and they both work with F5 and NetScaler. For this document, the vRealize Automation or vRealize Orchestrator components are deployed as a one-arm configuration as shown in Figure 1. However multi-arm deployments are also supported and their configuration should be similar to the one-arm configuration described in this document.

**Figure 1. One-arm Configuration**

**Prerequisites for Configuring Load Balancers for vRealize Automation**

- **F5 BIG-IP LTM** – Before you start an HA implementation of vRealize Automation or vRealize Orchestrator using an F5 LTM load balancer, ensure that the load-balancer is installed and licensed and that the DNS server configuration is complete.

- **NetScaler** – Before you start an HA implementation of vRealize Automation or vRealize Orchestrator using the NetScaler load balancer, ensure that NetScaler is installed and has configured at least a Standard Edition license.

- **NSX-V/T** – Before you start an HA implementation of vRealize Automation or vRealize Orchestrator using NSX-V/T as a load balancer, ensure that your NSX-V/T topology is configured and that your version of NSX-V/T is supported. This document covers the load balancing aspect of an NSX-V/T configuration and assumes that NSX-V/T is configured and validated to work properly on the target environment and networks. To verify that your version is supported, see the vRealize Automation Support Matrix for the current release.

- **Certificates** – Request Certificate Authority (CA) signed certificate containing the vRealize Automation or vRealize Orchestrator virtual IP and the host names of the vRealize Automation nodes in the SubjectAltNames section. This configuration enables the load balancer to serve traffic without SSL errors.

- **Identity provider** – Starting with vRealize Automation 8.0, the preferred Identity Provider is VMware Identity Manager, which is external to the vRealize Automation Appliance. Please refer to the VMware Identity Manager documentation in regard to load-balancing more than one external appliance.

For more information on installation and configuration, see vRealize Automation product documentation.

If required, external vRealize Orchestrator cluster can be configured to work with the vRealize Automation system. This can be done after the vRealize Automation system is up and running. However, a vRealize Automation Highly-Available setup already includes an embedded vRealize Orchestrator cluster.
Complete the vRealize Automation / vRealize Orchestrator Initial Installation

During the installation process of vRealize Automation or vRealize Orchestrator, a load balancer typically will route half of the traffic to the secondary nodes, which will not yet be configured, causing the installation to fail. To avoid these failures and to complete the initial installation of vRealize Automation or vRealize Orchestrator, you must perform the following tasks.

1. Configure the F5, NSX, or NetScaler load balancer. See Configuring F5 BIG-IP, Configuring NSX, and Configuring Citrix NetScaler
2. Turn off the health monitors or change them temporarily to default ICMP, and ensure traffic is still forwarding to your primary nodes
3. Disable all secondary nodes from the load balancer pools
4. Install and configure all the system components as detailed in vRealize Automation / vRealize Orchestrator Installation and Configuration documentation
5. When all components are installed, enable all non-primary nodes on the load balancer
6. Configure the load balancer with all monitors (health checks) enabled.
   After you complete this procedure, update the monitor that you created in Configure Monitors
7. Ensure that all nodes are in the expected state with the health monitor enabled in the load balancer after installation. The pool, service groups, and virtual server of the virtual appliance nodes should be available and running. All virtual appliance nodes should be available, running, and enabled
Configuring F5 Big-IP LTM

This document assumes that the F5 device is already deployed in the environment and can access vRealize Automation / vRealize Orchestrator components over a network.

- The F5 device can be either physical or virtual
- The F5 LTM load balancer can be deployed in either one-arm or multi-arm topologies
- The Local Traffic module (LTM) must be configured and licensed as either Nominal, Minimum, or Dedicated. You can configure the LTM on the System > Resource Provisioning page

If you are using an F5 LTM version prior to 11.x, you might need to change your health monitor settings related to the Send string. For more information about how to set up your health monitor send string for the different versions of F5 LTM, see HTTP health checks may fail even though the node is responding correctly.

Configure Custom Persistence Profile

You can configure the persistence profile for your F5 load balancer.

1. Log in to the F5 and select Local Traffic > Profiles > Persistence
2. Click Create
3. Enter the name source_addr_vra and select Source Address Affinity from the drop-down menu
4. Enable Custom mode
5. Set the Timeout to 1500 seconds (25 minutes)
6. Click Finished

Configure Monitors

You need to add the following monitors for vRealize Automation / vRealize Orchestrator.

1. Log in to the F5 load balancer and select Local Traffic > Monitors.
2. Click Create and provide the required information.
   Leave the default value when nothing is specified.

<table>
<thead>
<tr>
<th>NAME</th>
<th>TYPE</th>
<th>INTERVAL</th>
<th>TIME OUT</th>
<th>SEND STRING</th>
<th>RECEIVE STRING</th>
<th>ALIAS SERVICE PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>vra_http_va_web</td>
<td>HTTP</td>
<td>3</td>
<td>10</td>
<td>GET /health HTTP/1.0/</td>
<td>\n\n\n\n</td>
<td>HTTP/1.0(1) (200)</td>
</tr>
</tbody>
</table>
Example

The configuration for a VA monitor should look similar to the following screen:
Configure Server Pools

You must configure the following server pools for vRealize Automation / vRealize Orchestrator.

1. Log in to the F5 load balancer and select Local Traffic > Pools
2. Click Create and provide the required information. Leave the default value when nothing is specified
3. Enter each pool member as a New Node and add it to the New Members

Table 2 – Configure Server Pools

<table>
<thead>
<tr>
<th>NAME</th>
<th>HEALTH MONITORS</th>
<th>LOAD BALANCING METHOD</th>
<th>NODE NAME</th>
<th>ADDRESS</th>
<th>SERVICE PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>pl_vra-va-00_443</td>
<td>vra_https_va_web</td>
<td>Least connections (member)</td>
<td>ra-vra-va-01</td>
<td>IP Address</td>
<td>443</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ra-vra-va-02</td>
<td>IP Address</td>
<td>443</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ra-vra-va-03</td>
<td>IP Address</td>
<td>443</td>
</tr>
</tbody>
</table>
Example

Your pool configuration should look similar to the following screen.

Configure Virtual Servers

You must configure the following virtual servers for vRealize Automation / vRealize Orchestrator.

1. Log in to the F5 load balancer and select Local Traffic > Virtual Servers
2. Click Create and provide the required information. Leave the default value when nothing is specified
3. Repeat steps 1 and 2 for each entry in Table 3
4. For an overall view and status of the virtual servers, select LTM > Network Map

TABLE 3 – CONFIGURE VIRTUAL SERVERS

<table>
<thead>
<tr>
<th>NAME</th>
<th>TYPE</th>
<th>DESTINATION ADDRESS</th>
<th>SERVICE PORT</th>
<th>SOURCE ADDRESS TRANSLATION</th>
<th>DEFAULT POOL</th>
<th>DEFAULT PERSISTENCE PROFILE</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs_vra-va-00_443</td>
<td>Performance (Layer 4)</td>
<td>IP Address</td>
<td>443</td>
<td>Auto Map</td>
<td>pl_vra-va-00_443</td>
<td>source_addr_vra</td>
</tr>
</tbody>
</table>
## Example

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

<table>
<thead>
<tr>
<th>General Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Type</strong></td>
</tr>
<tr>
<td><strong>Source Address</strong></td>
</tr>
<tr>
<td><strong>Destination Address/Mask</strong></td>
</tr>
<tr>
<td><strong>Service Port</strong></td>
</tr>
<tr>
<td><strong>Notify Status to Virtual Address</strong></td>
</tr>
<tr>
<td><strong>State</strong></td>
</tr>
</tbody>
</table>

### Configuration: Basic

<table>
<thead>
<tr>
<th>Protocol</th>
<th>TCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Profile (Client)</td>
<td>fastL4</td>
</tr>
<tr>
<td>HTTP Profile (Client)</td>
<td>None</td>
</tr>
<tr>
<td>HTTP Profile (Server)</td>
<td>Use Client Profile</td>
</tr>
<tr>
<td>HTTP Proxy Connect Profile</td>
<td>None</td>
</tr>
<tr>
<td>VLAN and Tunnel Traffic</td>
<td>All VLANs and Tunnels</td>
</tr>
<tr>
<td>Source Address Translation</td>
<td>Auto Map</td>
</tr>
</tbody>
</table>

### Acceleration: Basic

| iSession Profile | None |
| Rate Class | None |

### Resources

<table>
<thead>
<tr>
<th>Resources</th>
<th>Enabled</th>
<th>Available</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>iRules</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Default Pool</strong></td>
<td>pi_vma-va-00_443</td>
<td></td>
</tr>
<tr>
<td><strong>Default Persistence Profile</strong></td>
<td>source_addr_25min</td>
<td></td>
</tr>
<tr>
<td><strong>Failback Persistence Profile</strong></td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

[See image for more details]
The completed configuration should look similar to the following screen:

<table>
<thead>
<tr>
<th>Virtual Server</th>
<th>Pools</th>
<th>Pool Members</th>
<th>Nodes</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs_vra-va-00_443</td>
<td>pl_vra-va-00_443</td>
<td>dz-vra8-node1.sof-mbu.eng.vmware.com 192.168.10.30</td>
<td>dz-vra8-node1.sof-mbu.eng.vmware.com 192.168.10.30</td>
</tr>
<tr>
<td></td>
<td></td>
<td>dz-vra8-node2.sof-mbu.eng.vmware.com 192.168.10.31</td>
<td>dz-vra8-node2.sof-mbu.eng.vmware.com 192.168.10.31</td>
</tr>
<tr>
<td></td>
<td></td>
<td>dz-vra8-node3.sof-mbu.eng.vmware.com 192.168.10.32</td>
<td>dz-vra8-node3.sof-mbu.eng.vmware.com 192.168.10.32</td>
</tr>
</tbody>
</table>
Configuring NSX-V

You can deploy a new NSX-V Edge Services Gateway or reuse an existing one. However, it must have network connectivity to and from the vRealize Automation / vRealize Orchestrator components being load balanced.

Configure Global Settings

You can configure the global settings by using the following steps.

1. Log in to the NSX-V, click the Manage tab, click Settings, and select Interfaces.
2. Double-click on your Edge device in the list.
3. Click vNIC# for the external interface that hosts the virtual IP addresses and click the Edit icon.
4. Select the appropriate network range for the NSX-V Edge and click the Edit icon.

* This interface might look slightly different in NSX-V 6.1.x and earlier.

5. Add the IP addresses assigned to the virtual IPs and click OK.
6. Click OK to exit the interface configuration page.
7. Go to the Load Balancer tab and click the Edit icon.
8. Select Enable Load Balancer, Enable Acceleration, and Logging, if required, and click OK.

* This interface might look slightly different in NSX-V 6.1.x and earlier.
Add Application Profiles

You must add application profiles for the different components of vRealize Automation / vRealize Orchestrator.

1. Click **Application Profiles** in the pane on the left.

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

**TABLE 4 – ADD APPLICATION PROFILES**

<table>
<thead>
<tr>
<th>NAME</th>
<th>TYPE</th>
<th>TIMEOUT</th>
<th>PERSISTENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>vRealize Automation / vRealize Orchestrator VA Web</td>
<td>SSL Passthrough</td>
<td>1500 seconds</td>
<td>Source IP</td>
</tr>
</tbody>
</table>

**Example**

The completed configuration should look similar to the following screen:
Add Service Monitoring

You must add service monitors for the different components of vRealize Automation / vRealize Orchestrator.

1. Click Service Monitoring in the left pane.
2. Click the Add icon to create the service monitors required for vRealize Automation / vRealize Orchestrator using information in Table 5. Leave the default value when nothing is specified.

**TABLE 5 – ADD SERVICE MONITORING**

<table>
<thead>
<tr>
<th>NAME</th>
<th>INTERVAL</th>
<th>TIMEOUT</th>
<th>RETRIES</th>
<th>TYPE</th>
<th>METHOD</th>
<th>URL</th>
<th>RECEIVE</th>
<th>EXPECTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>vRealize Automation / vRealize Orchestrator VA Web</td>
<td>3</td>
<td>10</td>
<td>3</td>
<td>HTTP</td>
<td>GET</td>
<td>/health</td>
<td></td>
<td>200</td>
</tr>
</tbody>
</table>

The completed configuration should look similar to the following screen:

![New Service Monitor](image)
Add Pools

You must create the following pools for vRealize Automation / vRealize Orchestrator.

1. Click **Pools** in the left pane.
2. Click the **Add** icon to create the pools required for vRealize Automation / vRealize Orchestrator using the information in Table 6.

**TABLE 6 - ADD POOLS**

<table>
<thead>
<tr>
<th>POOL NAME</th>
<th>ALGORITHM</th>
<th>MONITORS</th>
<th>MEMBER NAME</th>
<th>EXAMPLE IP ADDRESS / VCENTER CONTAINER</th>
<th>PORT</th>
<th>MONITOR PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>pool_vra-va-web_443</td>
<td>Least connections</td>
<td>vRA VA Web</td>
<td>vRA VA1</td>
<td>IP Address</td>
<td>443</td>
<td>8008</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vRA VA2</td>
<td>IP Address</td>
<td>443</td>
<td>8008</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vRA VA3</td>
<td>IP Address</td>
<td>443</td>
<td>8008</td>
</tr>
</tbody>
</table>
The completed configuration should look similar to the following screen:

```
New Pool

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address / VC Container</th>
<th>Weight</th>
<th>Monitor Port</th>
<th>Port</th>
<th>Max Connections</th>
<th>Min Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>vRA_VA_1</td>
<td>10.10.10.10</td>
<td>1</td>
<td>8008</td>
<td>443</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vRA_VA_3</td>
<td>10.10.10.12</td>
<td>1</td>
<td>8008</td>
<td>443</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vRA_VA_2</td>
<td>10.10.10.11</td>
<td>1</td>
<td>8008</td>
<td>443</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

1 - 3 of 3 Items
Add Virtual Servers

You must to add the following Virtual Servers for vRealize Automation / vRealize Orchestrator.

1. Click Virtual Servers on the left pane.

2. Click the Add icon to create the virtual servers required for vRealize Automation / vRealize Orchestrator using the information in Table 7. Leave the default value when nothing is specified.

**TABLE 7 - ADD VIRTUAL SERVERS**

<table>
<thead>
<tr>
<th>NAME</th>
<th>IP ADDRESS</th>
<th>PROTOCOL</th>
<th>PORT</th>
<th>DEFAULT POOL</th>
<th>APPLICATION PROFILE</th>
<th>APPLICATION RULE</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs_vra-va-web_443</td>
<td>IP Address</td>
<td>HTTPS</td>
<td>443</td>
<td>pool_vra-va-web_443</td>
<td>vRA VA</td>
<td></td>
</tr>
</tbody>
</table>

The completed configuration should look similar to the following screen.
Configuring NSX-T

This document assumes that the NSX-T is already deployed in the environment and the Tier-1 gateway with the load balancer can access the vRealize Automation / vRealize Orchestrator components over a network.

Note: NSX-T 2.3 has a known issue, HTTPS monitor is not supported for FAST TCP virtual server’s pool, which is fixed in 2.4.

Add Application Profiles

Add the Application Profile for HTTPS requests

1. Go to Networking → Load Balancing → PROFILES
2. Select Profile Type APPLICATION
3. Click the ADD APPLICATION PROFILE and select Fast TCP Profile
4. Choose a Name for the profile

Example

The completed configuration for an application profile for HTTPS request should look similar to the following screen:
Add Persistence Profile

1. Go to Networking → Load Balancing → PROFILES
2. Select Profile Type PERSISTENCE
3. Click the ADD PERSISTENCE PROFILE and select Source IP
4. Choose a Name for the profile
5. Set Persistence Entry Timeout to 1500s (25 minutes)

Example

The completed configuration for a persistence profile should look similar to the following screen:
Add Active Health Monitor

1. Go to Networking → Load Balancing → MONITORS
2. Click the Add ACTIVE MONITOR, select HTTP
3. Choose a Name for the Health Monitor. Set Monitoring Port, Monitoring Interval, Timeout Period, Fall Count and Rise Count (please refer to the table and example below)
4. Click HTTP Request Configure (please refer to the table and example below)
5. Click HTTP Response Configure (please refer to the table and example below)

**TABLE 8 – CONFIGURE HEALTH MONITORS**

<table>
<thead>
<tr>
<th>NAME</th>
<th>MONITORING PORT</th>
<th>INTERVAL</th>
<th>TIMEOUT</th>
<th>FALL COUNT</th>
<th>TYPE</th>
<th>METHOD</th>
<th>URL</th>
<th>RESPONSE CODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>vra_https_va_web</td>
<td>8008</td>
<td>3</td>
<td>10</td>
<td>3</td>
<td>HTTP</td>
<td>GET</td>
<td>/health</td>
<td>200</td>
</tr>
</tbody>
</table>

**Example**

The completed configuration for a health monitor should look similar to the following screens:
<table>
<thead>
<tr>
<th>Header Name</th>
<th>Header Value</th>
</tr>
</thead>
</table>

Request Header not found

HTTP Request Body
<table>
<thead>
<tr>
<th>HTTP Request Configuration</th>
<th>HTTP Response Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Request Configuration</td>
<td>HTTP Response Configuration</td>
</tr>
<tr>
<td>HTTP Response Code</td>
<td>200</td>
</tr>
<tr>
<td></td>
<td>1 or more response codes</td>
</tr>
<tr>
<td>HTTP Response Body</td>
<td></td>
</tr>
</tbody>
</table>
Configure Server Pools

You need to configure the following server pools for vRealize Automation / vRealize Orchestrator

1. Go to Networking → Load Balancing → SERVER POOLS
2. Click the ADD SERVER POOL
3. Choose a Name for the pool
4. Set Algorithm as LEAST_CONNECTION
5. Configure SNAT Translation as Auto Map
6. Click Select Members and ADD MEMBER (please refer to the table and example below)

**Table 9 – Configure Server Pools**

<table>
<thead>
<tr>
<th>POOL NAME</th>
<th>ALGORITHM</th>
<th>ACTIVE MONITOR</th>
<th>NAME</th>
<th>IP</th>
<th>PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>pool_vra-va-web_443</td>
<td>Least connections</td>
<td>vra_https_va_web</td>
<td>vra_va1</td>
<td>IP</td>
<td>443</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vra_va2</td>
<td>IP</td>
<td>443</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vra_va3</td>
<td>IP</td>
<td>443</td>
</tr>
</tbody>
</table>
Example

The completed configuration for a server pool should look similar to the following screen:
Configure Virtual Servers

You need to add the following Virtual Servers for vRealize Automation.

1. Go to Networking → Load Balancing → VIRTUAL SERVERS
2. Click the ADD VIRTUAL SERVER, select Layer (please refer to the table below)
3. Choose a Name for Virtual Server
4. Assign IP Address (Virtual IP) and Port (please refer to the table below)
5. Choose the Server Pool previously configured
6. Choose the Application Profile previously configured
7. Set Persistence (please refer to the table below)
8. Set the Default Pool Member Ports (please refer to the table below)

<table>
<thead>
<tr>
<th>NAME</th>
<th>TYPE</th>
<th>APPLICATION PROFILE</th>
<th>IP ADDR</th>
<th>PORT</th>
<th>SERVER POOL</th>
<th>PERSISTENCE PROFILE</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs_vra-va-web_443</td>
<td>L4 TCP</td>
<td>vRA_HTTPS</td>
<td>IP</td>
<td>443</td>
<td>pool_vra-va-web_443</td>
<td>source_addr_vra</td>
</tr>
</tbody>
</table>

**Example**

The completed configuration for a virtual server should look similar to the following screen:
Configure Load Balancer

You need to specify a load-balancer configuration parameter for vRealize Automation.

1. Go to Networking → Load Balancing → LOAD BALANCERS
2. Click the ADD LOAD BALANCER
3. Choose a Name, select appropriate Load Balancer Size (depends on vRA cluster size)
4. Choose the pre-created Tier 1 Logical Router

Note: In NSX-T v2.4, the monitor health checks are done using the IP address of Tiers-1 uplink (or first service port for Tiers-1 standalone SR) for all server pools of the load-balancer. Please ensure that server pools are reachable from this IP address.

Example

The completed configuration for a load balancer should look similar to the following screen:
Add Virtual Servers to Load Balancer

1. Go to Networking → Load Balancing → VIRTUAL SERVERS
2. Edit configured Virtual Servers
3. Assign Load Balancer as the previously configured Load Balancer

Example

The completed configuration for a virtual server should look similar to the following screen:
Configuring Citrix ADC (NetScaler ADC)

Before starting this configuration, ensure that the NetScaler device is deployed in the environment and has access to the vRealize Automation / vRealize Orchestrator components.

- You can use either virtual or physical NetScaler
- The Citrix load balancer can be deployed in either one-arm or multi-arm topologies
- Enable the Load Balancer and SSL modules. You can do so from NetScaler > System > Settings > Configure Basic Features page.

Configure Monitors

1. Log in to the NetScaler load balancer and select NetScaler > Traffic Management > Load Balancing > Monitors.
2. Click Add and provide the required information for each row in Table 11. Leave the default value when nothing is specified.

<table>
<thead>
<tr>
<th>TABLE 11 – CONFIGURE MONITORS</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
</tr>
<tr>
<td>vra_https_va_web</td>
</tr>
</tbody>
</table>
Configure Service Groups

1. Log in to the NetScaler load balancer and select **NetScaler > Traffic Management > Load Balancing > Service Groups**.

2. Click **Add** and provide the required information for each row in Table 12.

**TABLE 12 – CONFIGURE SERVICE GROUPS**

<table>
<thead>
<tr>
<th>NAME</th>
<th>HEALTH MONITORS</th>
<th>PROTOCOL</th>
<th>SG MEMBERS</th>
<th>ADDRESS</th>
<th>PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>pl_vra-va-00_443</td>
<td>vra_https_va_web</td>
<td>SSL Bridge</td>
<td>ra-vra-va-01</td>
<td>IP Address</td>
<td>443</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ra-vra-va-02</td>
<td>IP Address</td>
<td>443</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ra-vra-va-03</td>
<td>IP Address</td>
<td>443</td>
</tr>
</tbody>
</table>
Configure Virtual Servers


2. Click Add and provide the required information for each entry in Table. Leave the default value when nothing is specified.

**TABLE 13 – CONFIGURE VIRTUAL SERVERS**

<table>
<thead>
<tr>
<th>NAME</th>
<th>PROTOCOL</th>
<th>DESTINATION ADDRESS</th>
<th>PORT</th>
<th>LOAD BALANCING METHOD</th>
<th>SERVICE GROUP BINDING</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs_vra-va-00_443</td>
<td>SSL Bridge</td>
<td>IP Address</td>
<td>443</td>
<td>Least connections</td>
<td>pl_vra-va-00_443</td>
</tr>
</tbody>
</table>

![Load Balancing Virtual Server](image)
Configure Persistency Group

1. Log in to the NetScaler and select NetScaler > Traffic Management > Load Balancing > Persistency Groups
2. Click Add
3. Enter the name source_addr_vra and select Persistence > SOURCEIP from the drop-down menu
4. Set the Timeout to 25 minutes
5. Add all Virtual Servers related to vRealize Automation / vRealize Orchestrator
   - vs_vra-va-00_443
6. Click OK
Troubleshooting

Provisioning failures when using OneConnect with F5 BIG-IP for a virtual server with SSL pass-through

When you use the OneConnect feature with F5 BIG-IP for a virtual server, provisioning tasks sometimes fail. OneConnect ensures connections from the load balancer to the back-end servers are multiplexed and reused. This lowers the load on the servers and makes them more resilient.

Using OneConnect with a virtual server that has SSL pass-through is not recommended by F5 and might result in failed provisioning attempts. This happens because the load balancer attempts to establish a new SSL session over an existing session while the back-end servers. Expect the client to either close or renegotiate the existing session, which results in a dropped connection.

Disable OneConnect to resolve this issue.

1. Log in to the F5 load balancer and select Local Traffic > Virtual Servers > Virtual Server List.
2. Click the name of the virtual server to modify.
3. Choose None for the OneConnect Profile option in the Acceleration section and click Finish.

F5 BIG-IP license limits network bandwidth

If you experience provisioning failures or issues loading vRealize Automation console pages, especially during periods of a high utilization, network traffic to and from the load balancer might exceed what the F5 BIG-IP license allows.

To check if the BIG-IP platform is currently experiencing this issue, see How the BIG-IP VE system enforces the licensed throughput rate.