# Table of Contents

Introduction.......................................................................................................................... 4

Load Balancing Concepts..................................................................................................... 4

SSL Pass-Through................................................................................................................. 4

Session Persistence.............................................................................................................. 4

Source IP Address Hash (NSX) ........................................................................................... 5

Email Notifications on Load Balancer ................................................................................... 5

One-Arm or Multi-Arm Topologies.......................................................................................... 5

Prerequisites for Configuring Load Balancers with vRealize Automation............................. 6

Complete the vRealize Automation Initial Installation .......................................................... 7

Configure vRealize Automation Identity Connectors for Kerberos (Optional) ......................... 9

Configuring F5 Big-IP LTM.................................................................................................. 10

Configure Custom Persistence Profile.................................................................................. 10

Configure Monitors .............................................................................................................. 10

Configure Server Pools......................................................................................................... 12

Configure Virtual Servers ...................................................................................................... 14

Configuring NSX ..................................................................................................................... 17

Configure Global Settings..................................................................................................... 17

Add Application Profiles ...................................................................................................... 19

Add Service Monitoring ........................................................................................................ 20

Add Pools ............................................................................................................................... 21

Add Virtual Servers .............................................................................................................. 22

Configuring Citrix ADC (NetScaler ADC) ........................................................................... 24

Configure Monitors .............................................................................................................. 24

Configure Service Groups ..................................................................................................... 26

Configure Virtual Servers ..................................................................................................... 28

Configure Persistency Group................................................................................................. 30

Troubleshooting .................................................................................................................... 31

Provisioning failures when using OneConnect with F5 BIG-IP for a virtual server with SSL pass-through ......................................................................................................................... 31

F5 BIG-IP license limits network bandwidth .......................................................................... 31

Proxy Agent ping failure ....................................................................................................... 31

Connection reset errors in the catalina.out log file ................................................................. 32

Proxy Agents cannot connect to load balanced Manager Service endpoint .......................... 32
## Revision History

<table>
<thead>
<tr>
<th>DATE</th>
<th>VERSION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 2015</td>
<td>1.0</td>
<td>Initial version</td>
</tr>
<tr>
<td>December 2015</td>
<td>1.1</td>
<td>Minor updates</td>
</tr>
<tr>
<td>December 2015</td>
<td>2.0</td>
<td>Updates for vRealize Automation 7.0</td>
</tr>
<tr>
<td>January 2016</td>
<td>2.1</td>
<td>Minor updates</td>
</tr>
<tr>
<td>May 2016</td>
<td>2.2</td>
<td>Updates for vRealize Automation 7.0.x</td>
</tr>
</tbody>
</table>
| June 2016       | 2.3     | - Updated timeout to 10 seconds for Configure Monitors and Add Service Monitoring in F5 and NSX sections respectively  
- Added source IP persistence and timeout of 1800 seconds for Add Application Profiles section  
- Updated all the screenshots to match the content  
- Updated NSX load balancing method to be round robin |
| August 2016     | 2.4     | - Added configuration for Citrix NetScaler  
- Updated for NSX 6.2 |
| November 2016   | 2.5     | - Updated interval to 5 seconds for Configure Monitors in Citrix NetScaler section  
- Updated timeout to 4 seconds for Configure Monitors in Citrix NetScaler section |
| May 2017        | 2.6     | Minor updates |
| May 2017        | 2.7     | - Added monitor and pool configurations for vRealize Orchestrator Control Center.  
- Added troubleshooting section. |
| May 2018        | 2.8     | - Updated version to 7.4  
- Added information about expected result for load balancer installation  
- Added troubleshooting topic for increasing connection time  
- Revised SSL pass-through information.  
- Revised Configure Persistence Group section |
| November 2018   | 2.9     | - Updated version to 7.5  
- Updated load balancer software versions from the latest testing  
- Added support for three virtual appliances  
- Added support for Manager Service automatic failover  
- Added pools, virtual IPs for port 80  
- General refresh of the document (grammar, style, and formatting |
| December 2018   | 2.9.1   | - Corrected the health monitor receive string to include a backslash. |
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 7.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 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</td>
<td>11.x, 12.x, 13.x</td>
</tr>
<tr>
<td>NSX</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>Citrix NetScaler</td>
<td>10.5, 11.x, 12.x</td>
</tr>
<tr>
<td>vRealize Automation</td>
<td>7.x</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 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 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 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. SSL pass-through is a required implementation for vRealize Automation load balancing.

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)

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 (30 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 1800 seconds to match the vRealize Automation GUI timeout.

Source IP Address Hash (NSX)

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](https://kb.vmware.com/s/article/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 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 components are deployed as a one-arm configuration as shown in **Figure 1**.
Prerequisites for Configuring Load Balancers with vRealize Automation

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

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

- **NSX** – Before you start an HA implementation of vRealize Automation 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 vRealize Automation Support Matrix for the current release.

- **Certificates** – Request Certificate Authority (CA) signed or create self-signed certificates containing the vRealize Automation 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. If you need to replace the self-signed certificates with CA signed certificates, see the VMware knowledge base article KB 2107816. For more information about certificate troubleshooting and supportability, see the VMware knowledge base article KB 2106583.

- **Identity provider** – Starting with vRealize Automation 7.0, the preferred Identity Provider is VMware Identity Manager, which is embedded in the vRealize Automation Appliance.

- **Database** – Verify that supported database servers are available for vRealize Infrastructure-as-a-Service (IaaS) nodes. IaaS components require a Microsoft SQL Server instance.
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 Initial Installation**

During the installation process of vRealize Automation, a load balancer 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, 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 TCP, and ensure traffic is still forwarding to your primary nodes.
3. Disable all secondary nodes (VA and IaaS) from the load balancer pools.
4. Install and configure all the system components as detailed in vRealize Automation 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.

After you have configured a directory for at least one tenant, ensure that the **IdP Hostname** is set to the load balancer virtual IP for the vRealize Automation virtual appliances and all available **connectors** are enabled and configured for authentication for each virtual appliance node.
7. Ensure that all nodes are in the expected state with the health monitor enabled in the load balancer after installation.
   
a. 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.

b. The pool, service groups, and virtual server of the Web nodes should be available and running.

   All Web nodes should be available, running, and enabled.

c. The pool, service groups, and virtual server of the Manager Service nodes should be available and running.
   
   • The active Manager Service node should appear as online, and enabled in the load balancer
   • Each passive Manager Service node should appear as offline, but enabled in the load balancer

   **Note:** Starting with vRealize Automation 7.3.x, the Manager Service uses active-passive configuration and supports automatic failover. It is normal to have the passive nodes detected as offline, however; they should be enabled so the load balancer can start forwarding traffic to them automatically once a passive node is promoted to active one. For more information, see About Automatic Manager Service Failover in Installing vRealize Automation.
Configure vRealize Automation Identity Connectors for Kerberos (Optional)

If you require your vRealize Automation users to be authenticated by using Kerberos and they log in to the administration console by using Windows Single Sign-on, then you must configure the identity connectors.

1. Connect vRealize Automation to an Active Directory by using the IWA method.
2. Configure policies and methods for Kerberos authentication.
3. Open the administration console and navigate to Administration > Directories Management > Connectors. See Using Directories Management to Create an Active Directory in Configuring vRealize Automation.
4. In the Worker column, select a worker to view the connector details and navigate to the Auth Adapters page.
5. Click KerberosIdpAdapter. You will be redirected to the vIDM Console.
7. Select Enable Redirect.
8. In Redirect Host Name, enter the FQDN of the appliance you are configuring.
9. Configure the KerberosIdpAdapter on all the connectors in your cluster. Ensure the configuration of the adapter is identical on all the connectors, except for the Redirect Host Name value, which should be specific to each connector.

The Enable Redirect option directs HTTPS access for all client computers to a vRealize Automation node on port 443. The user’s browser is redirected away from the load balancing vRealize Automation endpoint to the appliance’s FQDN to perform authentication. After authentication, the user’s browser is redirected to the load balancing vRealize Automation FQDN.

Configuring the same HOST SPN (the load balancing FQDN) for each computer object in AD is not supported because Kerberos authentication relies on SPNs configured in Active Directory, which should be unique for every host. The only way to enable single sign-on for all members of a vRealize Automation cluster is to tell vIDM to redirect from the load balancing FQDN to the individual node, verify the ticket, and then redirect to the FQDN.

If you do not want to expose individual vRealize Automation appliances directly to the user and you still require Kerberos authentication, then your best option is to federate the vRealize Automation solution with a third-party SAML identity provider such as Active Directory Federation Services.
Configuring F5 Big-IP LTM

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

- The F5 device can be either physical or virtual
- The F5 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 version before 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, 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 1800 seconds (30 minutes).
6. Click Finished.

Configure Monitors

You need to add the following monitors for vRealize Automation.

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.
3. Repeat steps 1 and 2 for each row of information in Table 1.
4. To check the network map for an overall view of the monitors, select LTM > Network Map.

**Table 1 - Configure Monitors**

<table>
<thead>
<tr>
<th>NAME</th>
<th>TYPE</th>
<th>INTERVAL</th>
<th>TIMEOUT</th>
<th>SEND STRING</th>
<th>RECEIVE STRING</th>
<th>ALIAS SERVICE PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>vra_https_va_web</td>
<td>HTTPS</td>
<td>3</td>
<td>10</td>
<td>GET /vcac/services/api/health\n</td>
<td>HTTP/1.(0</td>
<td>1) (200</td>
</tr>
<tr>
<td>vra_https_iaas_web</td>
<td>HTTPS</td>
<td>3</td>
<td>10</td>
<td>GET /wapi/api/status/web\n</td>
<td>REGISTERED</td>
<td></td>
</tr>
<tr>
<td>vra_https_iaas_mngr</td>
<td>HTTPS</td>
<td>3</td>
<td>10</td>
<td>GET /VMPSProvision\n</td>
<td>ProvisionService</td>
<td></td>
</tr>
<tr>
<td>vro_https_8283</td>
<td>HTTPS</td>
<td>3</td>
<td>10</td>
<td>GET /vco-controlcenter/docs/</td>
<td>HTTP/1.(0</td>
<td>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.

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.
4. Repeat steps 1, 2, and 3 for each row in
5. Table 2.
6. **Note**: The environment depicted in
Table 2 is an example. Your environment might contain two or three vRealize Automation virtual appliance nodes and two or more nodes per IaaS role.

7. Select `pl_iaas-man-00_443` on Local Traffic -> Pools. Click *Advanced* in the configuration section and Select *Drop for Action on Service Down*. Click *OK* and click *Finished*.

8. To check the network map for an overall view of the server pools, select *LTM > Network Map*. 
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_80</td>
<td>http</td>
<td>Least connections (member)</td>
<td>ra-vra-va-01</td>
<td>IP Address</td>
<td>80</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ra-vra-va-02</td>
<td>IP Address</td>
<td>80</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ra-vra-va-03</td>
<td>IP Address</td>
<td>80</td>
</tr>
<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>
<tr>
<td>*pl_vra-va-00_8444</td>
<td>vra_https.va_web</td>
<td>Least connections (member)</td>
<td>ra-vra-va-01</td>
<td>IP Address</td>
<td>8444</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ra-vra-va-02</td>
<td>IP Address</td>
<td>8444</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ra-vra-va-03</td>
<td>IP Address</td>
<td>8444</td>
</tr>
<tr>
<td>pl_vro-cc-00_8283</td>
<td>vro_https_8283</td>
<td>Least connections (member)</td>
<td>ra-vra-va-01</td>
<td>IP Address</td>
<td>8283</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ra-vra-va-02</td>
<td>IP Address</td>
<td>8283</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ra-vra-va-03</td>
<td>IP Address</td>
<td>8283</td>
</tr>
<tr>
<td>pl_iaas-web-00_443</td>
<td>vra_https.iaas_web</td>
<td>Least connections (member)</td>
<td>ra-web-01</td>
<td>IP Address</td>
<td>443</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ra-web-02</td>
<td>IP Address</td>
<td>443</td>
</tr>
<tr>
<td>pl_iaas-man-00_443</td>
<td>vra_https.iaas_mgr</td>
<td>**Least connections (member)</td>
<td>ra-man-01</td>
<td>IP Address</td>
<td>443</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ra-man-02</td>
<td>IP Address</td>
<td>443</td>
</tr>
</tbody>
</table>

* Port 8444 is optional – it is required only if you want to use remote console from vRealize Automation.

** The Manager Service uses **active-passive type of configuration** hence the load balancer will always send the traffic to the current active node regardless of the load-balancing method.
**Example**

Your pool configuration should look similar to the following screen.

![Pool Configuration Screen](image)

**Configure Virtual Servers**

You must configure the following virtual servers for vRealize Automation.

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>
<thead>
<tr>
<th>TABLE 3 – CONFIGURE VIRTUAL SERVERS</th>
</tr>
</thead>
</table>

<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_80</td>
<td>Performance (HTTP)</td>
<td>IP Address</td>
<td>80</td>
<td>Auto Map</td>
<td>pl_vra-va-00_80</td>
<td>None</td>
</tr>
<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>
<tr>
<td>vs_vra-va-00_8444</td>
<td>Performance (Layer 4)</td>
<td>IP Address</td>
<td>8444</td>
<td>Auto Map</td>
<td>pl_vra-va-00_8444</td>
<td>source_addr_vra</td>
</tr>
<tr>
<td>vs_vro-00_8283</td>
<td>Performance (Layer 4)</td>
<td>IP Address</td>
<td>8283</td>
<td>Auto Map</td>
<td>pl_vro-cc-00_8283</td>
<td>source_addr_vra</td>
</tr>
<tr>
<td>vs_web-00_443</td>
<td>Performance (Layer 4)</td>
<td>IP Address</td>
<td>443</td>
<td>Auto Map</td>
<td>pl_iaas-web-00_443</td>
<td>source_addr_vra</td>
</tr>
<tr>
<td>vs_man-00_443</td>
<td>Performance (Layer 4)</td>
<td>IP Address</td>
<td>443</td>
<td>Auto Map</td>
<td>pl_iaas-man-00_443</td>
<td>None</td>
</tr>
</tbody>
</table>
Example
The completed configuration should look similar to the following screen:
Configuring NSX

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

Configure Global Settings

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

1. Log in to the NSX, 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 Edge and click the Edit icon.

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

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

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>
<thead>
<tr>
<th>TABLE 4 – ADD APPLICATION PROFILES</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
</tr>
<tr>
<td>---------------------------</td>
</tr>
<tr>
<td>IaaS Manager</td>
</tr>
<tr>
<td>IaaS Web</td>
</tr>
<tr>
<td>vRealize Automation VA Web</td>
</tr>
<tr>
<td>vRealize Orchestrator Control Center</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.

1. Click **Service Monitoring** in the left pane.

2. Click the **Add** icon to create the service monitors required for vRealize Automation 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 VA Web</td>
<td>3</td>
<td>10</td>
<td>3</td>
<td>HTTPS</td>
<td>GET</td>
<td>/vcac/services/api/health</td>
<td></td>
<td>200, 204 (for 7.0)</td>
</tr>
<tr>
<td>IaaS Web</td>
<td>3</td>
<td>10</td>
<td>3</td>
<td>HTTPS</td>
<td>GET</td>
<td>/wapi/api/status/web</td>
<td>REGISTERED</td>
<td></td>
</tr>
<tr>
<td>IaaS Manager</td>
<td>3</td>
<td>10</td>
<td>3</td>
<td>HTTPS</td>
<td>GET</td>
<td>/VMPSProvision</td>
<td>ProvisionService</td>
<td></td>
</tr>
<tr>
<td>vRealize Orchestrator Control Center</td>
<td>3</td>
<td>10</td>
<td>3</td>
<td>HTTPS</td>
<td>GET</td>
<td>/vco-controlcenter/docs/</td>
<td></td>
<td>200</td>
</tr>
</tbody>
</table>

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

You must create the following pools for vRealize Automation.

1. Click Pools in the left pane.

2. Click the Add icon to create the pools required for vRealize Automation using the information in Table 6.
   - The environment depicted in Table 6 is an example. Your environment might contain two or three vRealize Automation virtual appliance nodes and two or more nodes per IaaS role.
   - You can either use the IP address of the pool members or select them as a Virtual Center Container.

<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_80</td>
<td>Least connections</td>
<td>default_http_monitor</td>
<td>vRA VA1</td>
<td>IP Address 80</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vRA VA2</td>
<td>IP Address 80</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vRA VA3</td>
<td>IP Address 80</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pool_vra-va-web_443</td>
<td>Least connections</td>
<td>vRA VA Web</td>
<td>vRA VA1</td>
<td>IP Address 443</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vRA VA2</td>
<td>IP Address 443</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vRA VA3</td>
<td>IP Address 443</td>
<td></td>
<td></td>
</tr>
<tr>
<td>*pool_vra-rconsole_8444</td>
<td>Least connections</td>
<td>vRA VA Web</td>
<td>vRA VA1</td>
<td>IP Address 8444 444</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vRA VA2</td>
<td>IP Address 8444 443</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vRA VA3</td>
<td>IP Address 8444 443</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pool_vro-cc_8283</td>
<td>Least connections</td>
<td>vRealize Orchestrator Control Center</td>
<td>vRA VA1</td>
<td>IP Address 8283</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vRA VA2</td>
<td>IP Address 8283</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vRA VA3</td>
<td>IP Address 8283</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pool_iaas-web_443</td>
<td>Least connections</td>
<td>IaaS Web</td>
<td>IaaS Web1</td>
<td>IP Address 443</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>IaaS Web2</td>
<td>IP Address 443</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pool_iaas-manager_443</td>
<td>**Least connections</td>
<td>IaaS Manager</td>
<td>IaaS Man1</td>
<td>IP Address 443</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>IaaS Man2</td>
<td>IP Address 443</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Port 8444 is optional – it is required only if you want to use remote console from vRealize Automation.
** The Manager Service uses active-passive type of configuration hence the load balancer will always send the traffic to the current active node regardless of the load balancing method.
Add Virtual Servers

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

1. Click **Virtual Servers** on the left pane.
2. Click the **Add** icon to create the virtual servers required for vRealize Automation 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_80</td>
<td>IP Address</td>
<td>HTTP</td>
<td>80</td>
<td>pool_vra-va-web_80</td>
<td>vRA VA</td>
<td></td>
</tr>
<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>
<tr>
<td>vs_iaas-web_443</td>
<td>IP Address</td>
<td>HTTPS</td>
<td>443</td>
<td>pool_iaas-web_443</td>
<td>IaaS Web</td>
<td></td>
</tr>
<tr>
<td>vs_iaas-manager_443</td>
<td>IP Address</td>
<td>HTTPS</td>
<td>443</td>
<td>pool_iaas-manager_443</td>
<td>IaaS Manager</td>
<td></td>
</tr>
<tr>
<td>*vs_vra-va-rconsole_8444</td>
<td>IP Address</td>
<td>HTTPS</td>
<td>8444</td>
<td>pool_vra-rconsole_8444</td>
<td>vRA VA</td>
<td></td>
</tr>
<tr>
<td>vs_vro-cc_8283</td>
<td>IP Address</td>
<td>HTTPS</td>
<td>8283</td>
<td>pool_vro-cc_8283</td>
<td>vRealize Orchestrator Control Center</td>
<td></td>
</tr>
</tbody>
</table>

* Port 8444 is optional – it is required only if you want to use remote console from vRealize Automation.
The completed configuration 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 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 8. Leave the default value when nothing is specified.

**TABLE 8 – CONFIGURE MONITORS**

<table>
<thead>
<tr>
<th>NAME</th>
<th>TYPE</th>
<th>INTERVAL</th>
<th>TIMEOUT</th>
<th>SEND STRING</th>
<th>RECEIVE STRING</th>
<th>DEST. PORT</th>
<th>SECURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>vra_https_va_web</td>
<td>HTTP</td>
<td>5</td>
<td>4</td>
<td>GET /vcac/services/api/health</td>
<td>HTTP\1.(0</td>
<td>1) (200)204)</td>
<td>443</td>
</tr>
<tr>
<td>vra_https_iaas_web</td>
<td>HTTP-ECV</td>
<td>5</td>
<td>4</td>
<td>GET /wapi/api/status/web</td>
<td>REGISTERED</td>
<td>443</td>
<td>yes</td>
</tr>
<tr>
<td>vra_https_iaas_mgr</td>
<td>HTTP-ECV</td>
<td>5</td>
<td>4</td>
<td>GET /VMPSProvision</td>
<td>ProvisionService</td>
<td>443</td>
<td>yes</td>
</tr>
<tr>
<td>vro_https_8283</td>
<td>HTTP</td>
<td>5</td>
<td>4</td>
<td>GET /vco-controlcenter/docs</td>
<td>HTTP\1.(0</td>
<td>1) (200)</td>
<td>8283</td>
</tr>
</tbody>
</table>
Example

The completed configuration for a virtual appliance monitor should look similar to the following screen:
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 9.

   Note: The environment depicted in Table 9 is an example. Your environment might contain two or three vRealize Automation virtual appliance nodes and two or more nodes per IaaS role.

**Table 9 – 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_80</td>
<td>http-ecv</td>
<td>HTTP</td>
<td>ra-vra-va-01</td>
<td>IP Address</td>
<td>80</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ra-vra-va-02</td>
<td>IP Address</td>
<td>80</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ra-vra-va-03</td>
<td>IP Address</td>
<td>80</td>
</tr>
<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>
<tr>
<td>*pl_vra-va-00_8444</td>
<td>vra_https_va_web</td>
<td>SSL Bridge</td>
<td>ra-vra-va-01</td>
<td>IP Address</td>
<td>8444</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ra-vra-va-02</td>
<td>IP Address</td>
<td>8444</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ra-vra-va-03</td>
<td>IP Address</td>
<td>8444</td>
</tr>
<tr>
<td>pl_vro-cc-00_8283</td>
<td>vro_https_8283</td>
<td>SSL Bridge</td>
<td>ra-vra-va-01</td>
<td>IP Address</td>
<td>8283</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ra-vra-va-02</td>
<td>IP Address</td>
<td>8283</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ra-vra-va-03</td>
<td>IP Address</td>
<td>8283</td>
</tr>
<tr>
<td>pl_iaas-web-00_443</td>
<td>vra_https_ihas_web</td>
<td>SSL Bridge</td>
<td>ra-web-01</td>
<td>IP Address</td>
<td>443</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ra-web-02</td>
<td>IP Address</td>
<td>443</td>
</tr>
<tr>
<td>pl_iaas-man-00_443</td>
<td>vra_https_ihas_mgr</td>
<td>SSL Bridge</td>
<td>ra-man-01</td>
<td>IP Address</td>
<td>443</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ra-man-02</td>
<td>IP Address</td>
<td>443</td>
</tr>
</tbody>
</table>

* Port 8444 is optional – it is required only if you want to use remote console from vRealize Automation.
Example

Load Balancing Service Group

Basic Settings

- Name: pl_vra-vra-00_443
- Protocol: SSL_BRIDGE
- State: ENABLED
- Effective State: UP
- Traffic Domain: 0
- Comment:

- Cache Type: SERVER
- Cacheable: YES
- Health Monitoring: ENABLED
- AppFlow Logging: NONE
- Monitoring Connection Close Bit: 0
- Number of Active Connections: 0
- AutoScale Mode: DISABLED

Service Group Members

3 Service Group Members

Settings

- SureConnect: OFF
- Surge Protection: OFF
- Use Proxy Port: YES
- Down State Flush: ENABLED
- Use Client IP: NO
- Client Keep-alive: NO
- TCP Buffering: YES
- Client IP Header: DISABLED
- AutoScale Mode: DISABLED

Monitors

1 Service Group to Monitor Binding

Done
**Configure Virtual Servers**


2. Click Add and provide the required information for each entry in Table 10. Leave the default value when nothing is specified.

**Table 10 – 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_80</td>
<td>HTTP</td>
<td>IP Address</td>
<td>80</td>
<td>Least connections</td>
<td>pl_vra-va-00_80</td>
</tr>
<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>
<tr>
<td>vs_web-00_443</td>
<td>SSL Bridge</td>
<td>IP Address</td>
<td>443</td>
<td>Least connections</td>
<td>pl_iaas-web-00_443</td>
</tr>
<tr>
<td>vs_man-00_443</td>
<td>SSL Bridge</td>
<td>IP Address</td>
<td>443</td>
<td><strong>Least connections</strong></td>
<td>pl_iaas-man-00_443</td>
</tr>
<tr>
<td>*vs_vra-va-00_8444</td>
<td>SSL Bridge</td>
<td>IP Address</td>
<td>8444</td>
<td>Least connections</td>
<td>pl_vra-va-00_8444</td>
</tr>
<tr>
<td>vs_vro-cc-00_8283</td>
<td>SSL Bridge</td>
<td>IP Address</td>
<td>8283</td>
<td>Least connections</td>
<td>pl_vro-cc-00_8283</td>
</tr>
</tbody>
</table>

* Port 8444 is optional – it is required only if you want to use remote console from vRealize Automation.

** The Manager Service uses an active-passive type of configuration hence the load balancer will always send the traffic to the current active node regardless of the load-balancing method.
Example

### Load Balancing Virtual Server

**Basic Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>SSL_BRIDGE</td>
</tr>
<tr>
<td>Protocol</td>
<td>SSL_BRIDGE</td>
</tr>
<tr>
<td>State</td>
<td>UP</td>
</tr>
<tr>
<td>IP Address</td>
<td>10.23.90.21</td>
</tr>
<tr>
<td>Port</td>
<td>443</td>
</tr>
<tr>
<td>Traffic Domain</td>
<td>0</td>
</tr>
<tr>
<td>Listen Priority</td>
<td>NONE</td>
</tr>
<tr>
<td>Listen Policy</td>
<td>NONE</td>
</tr>
<tr>
<td>Range</td>
<td>1</td>
</tr>
<tr>
<td>IP Address</td>
<td>10.23.90.21</td>
</tr>
<tr>
<td>Port</td>
<td>443</td>
</tr>
<tr>
<td>Traffic Domain</td>
<td>0</td>
</tr>
<tr>
<td>Retain Connections</td>
<td>NO</td>
</tr>
</tbody>
</table>

**Services and Service Groups**

1. Load Balancing Virtual Server Service Binding

2. Load Balancing Virtual Server Service Group Binding

**Persistence**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Persistence</td>
<td>SOURCEIP</td>
</tr>
<tr>
<td>Time-out (mins)</td>
<td>30</td>
</tr>
<tr>
<td>IPv4 Netmask</td>
<td>255.255.255.255</td>
</tr>
<tr>
<td>IPv6 Mask Length</td>
<td>128</td>
</tr>
</tbody>
</table>

**Traffic Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Threshold</td>
<td>0</td>
</tr>
<tr>
<td>Client Idle Time-out</td>
<td>180</td>
</tr>
<tr>
<td>Minimum Autoscale Members</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Autoscale Members</td>
<td>0</td>
</tr>
<tr>
<td>ICMP Virtual Server Response</td>
<td>PASSIVE</td>
</tr>
<tr>
<td>Priority Queuing</td>
<td></td>
</tr>
<tr>
<td>Sure Connect</td>
<td></td>
</tr>
<tr>
<td>Down State Flush</td>
<td></td>
</tr>
<tr>
<td>Layer 2 Parameters</td>
<td></td>
</tr>
<tr>
<td>Troub Persistence</td>
<td></td>
</tr>
<tr>
<td>Troub Persistence</td>
<td></td>
</tr>
</tbody>
</table>

**Done**
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 30 minutes.
5. Add all Virtual Servers related to vRealize Automation.
   - vra_80
   - vra_443
   - vro_443
   - web_443
   - controlcenter_8283
6. Click OK.

Example

The completed configuration should look like the following screen.
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.

Proxy agent ping failure

After starting the Manager Service on a second manager server, the proxy agent is unable to reconnect. This happens because the F5 appliance is still maintaining an SSL session with the agent by sending keepalives while the agent is trying to establish a new session.

To configure the load balancer to drop all packets and prevent it from sending keepalives to resolve this issue:

1. Log in to the F5 load balancer and select Local Traffic > Pools.
2. Select the Manager Service pool.
3. Click Advanced in the Configuration section.
4. Select Drop for the Action On Service Down option.
5. Click OK and click Finished.
Connection reset errors in the catalina.out log file

When the system is under a heavy load due to many simultaneously requested provisions through the IaaS components, you might see connection reset errors in the catalina.out log file on the vRealize Automation appliances. This can happen when a session between the appliances and the Web servers expires. You can work around this problem by increasing the timeout setting for your load balancer.

F5

Use the AskF5 procedure K7166: “Changing the idle timeout for a protocol profile” at https://support.f5.com/csp/article/K7166 to change the Idle Timeout for a virtual server. Perform this procedure on the Web Service virtual load balancer server and set the timeout initially to 600 seconds. A best practice is to gradually increase the timeout until there are no connection reset errors.

NetScaler

Use the Citrix procedure in “Setting a Time-out Value for Idle Client Connections” at https://docs.citrix.com/en-us/netscaler/11/traffic-management/load-balancing/load-balancing-manage-clienttraffic/client-idle-timeout-value.html to change the Idle Timeout for a virtual server. Perform this procedure on the Web Service virtual load balancer server and set the timeout initially to 600 seconds. A best practice is to gradually increase the timeout until there are no connection reset errors.

NSX

Use the procedure in the knowledge base article 2147156 to change the Idle Timeout for a virtual server. Perform this procedure on the Web Service virtual load balancer server and set the timeout initially to 600 seconds. A best practice is to gradually increase the timeout until there are no connection reset errors.

Proxy Agents cannot connect to load balanced Manager Service endpoint

With NSX as a load balancing solution, after a Manager Service failover the proxy agents cannot connect to the load balanced Manager Service.

This issue occurs when the IIS role is installed on the servers that are running the Manager Service. When a Manager Service is stopped, the monitors configured on NSX are flagged as DOWN. Because IIS is running and accepting connections on port 443, NSX keeps the established sessions, and the Proxy Agent service keeps trying to reuse the session.

To resolve this issue, remove the IIS role from the servers that are running the Manager Service. The Manager Service is a self-hosted service that does not require IIS.