



vRealize Automation Load Balancing

Configuration Guide
Version 6.2

TECHNICAL WHITE PAPER
FEBRUARY 2017
VERSION 1.4

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 Multiarm Topologies.....	5
Prerequisites for configuring F5 with vRealize Automation.....	8
Completing the vRealize Automation Initial Installation.....	8
Configuring F5 Big IP with vSphere 5.5 SSO or 6.0 PSC.....	9
Configure Custom Persistence Profile.....	9
Configure Monitors.....	9
Configure Server Pools.....	15
Configure Virtual Servers.....	16
Deploying NSX 6.1 with vSphere 5.5 SSO.....	20
Configure Global Settings.....	20
Add Application Rules.....	22
Add Application Profiles.....	22
Add Service Monitoring.....	23
Add Pools.....	25
Add Virtual Servers.....	27
Troubleshooting.....	29
Configure SSO as active/active.....	29
Provisioning failures when using OneConnect with F5 BIG-IP for a virtual server with SSL pass-through.....	29
F5 BIG-IP license limits network bandwidth.....	30
Proxy Agent ping failure.....	30



Revision History

DATE	VERSION	DESCRIPTION
August 2015	1.0	Initial version
December 2015	1.1	Minor updates
June 2016	1.2	<ul style="list-style-type: none">▪ 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
October 2016	1.3	Updated inaccurate screenshot.
February 2017	1.4	<ul style="list-style-type: none">▪ Added troubleshooting information for F5 configurations▪ Added information about OneConnect configuration to server configuration with F5 load balancers



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

Copyright © 2015 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Introduction

This document describes the configuration of the load balancing modules of F5 Networks BIG-IP software (F5) and NSX load balancers for vRealize Automation 6.2.x in a distributed and high availability deployment. This document is not an installation guide, but a load-balancing configuration guide that supplements the vRealize Automation installation and configuration documentation available in the [vRealize Automation Installation and Configuration](#) guide in the VMware vRealize Automation 6.2 Documentation Center.

This information is for the following products and versions.

PRODUCT	VERSION
F5 BIG IP	Tested for 11.6
NSX	6.1.3, 6.1.4 (versions below 6.1.3 are not supported)
vRealize Automation	6.2.x
vSphere SSO	5.5u2
vSphere Platform Services Controllers (PSC)	6.0

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.

NOTE: SSL pass-through is not supported by vSphere PSC.

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 recommended in this document is the result of extensive testing and represents the best compromise between stability, performance, and scalability.



Destination Address (F5)

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 & 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 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.

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 vRA/vRO node goes down. Currently, NSX does not support email notification for such a scenario.

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](#)

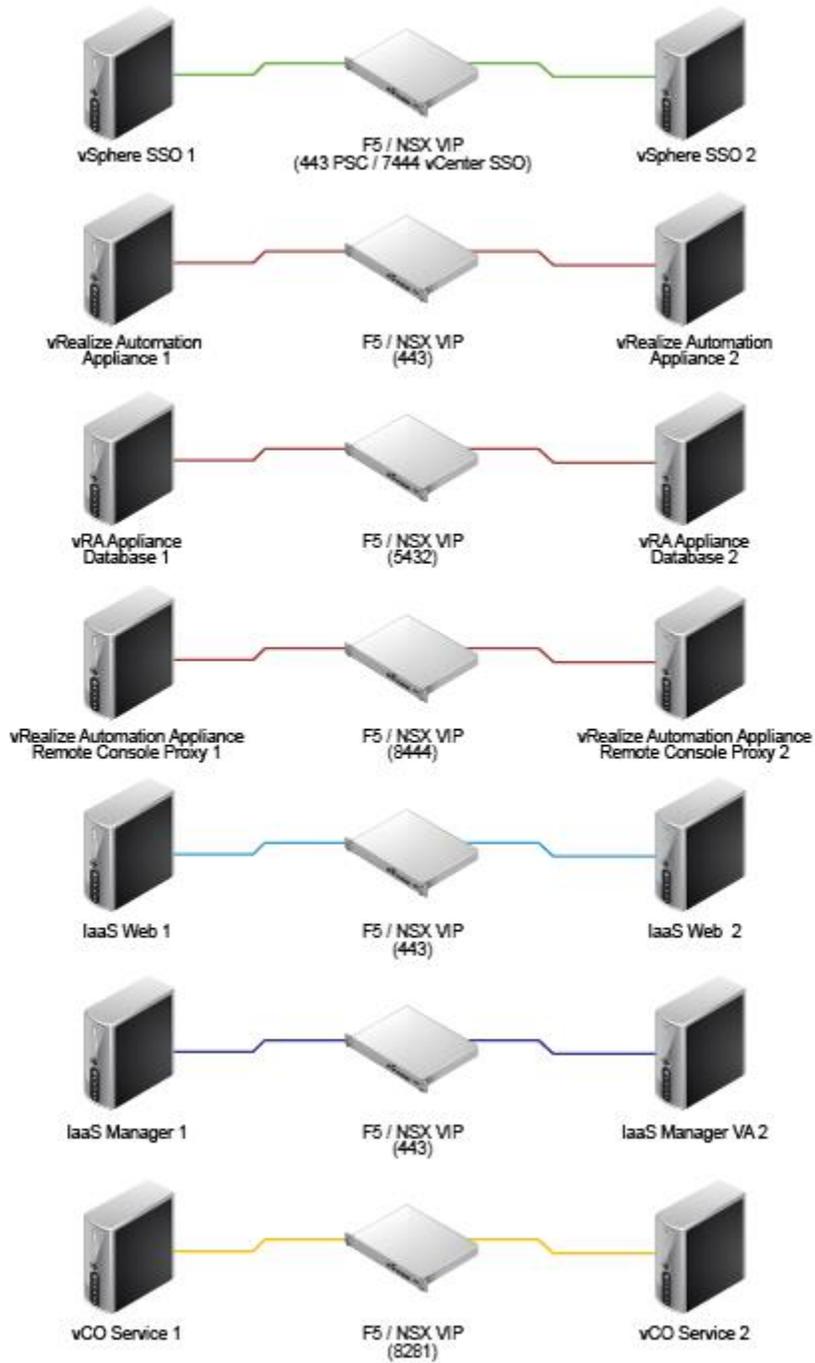
One-arm or Multiarm Topologies

In one-arm deployment, the components to be load balanced and the virtual IP (VIP) of the load balancer are on the same network. 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 traffic, return traffic goes directly back to the client and connections fail.

In a multiarm 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 configurations in the figure assumes a one-arm configuration, as this is most commonly deployed. The same principles apply to multiarm deployments, and they both work with F5. For the purpose of this document, the vRealize Automation components are deployed as a one-arm configuration as shown in [Figure 1](#).





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

Copyright © 2015 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

FIGURE 1. ONE-ARM CONFIGURATION



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

Copyright © 2015 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Prerequisites for configuring F5 with vRealize Automation

- **F5** - Before you start the 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.
- **NSX** - Before you start the 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](#).
- **Certificates** - Create signed or self-signed certificates to contain the vRealize Automation VIP and the hostnames of the vRealize Automation nodes in the SubjectAltNames section. This configuration allows the load balancer to serve traffic without SSL errors. If you need to replace the self-signed certificates with your own CA signed certificates, see VMware Knowledge base article [KB 2107816](#). For more information about certificate troubleshooting and supportability, see the VMware knowledge base article [KB 2106583](#).
- **Identity provider** - Deploy and configure vSphere SSO 5.5 u2 or vSphere 6 PSC instances.
For information on how to fully configure vSphere 6 PSC HA, see the [vCenter Server deployment guide](#).
- **Database** – Verify that supported database servers are available for vRealize Appliance and Infrastructure as a Service (IaaS) nodes. IaaS components require an MS SQL server instance. For more information about configuring vRealize Appliance database server in replication mode, see VMware knowledge base article [KB 2108923](#).

For more information on installation and configuration see [vRealize Automation installation and configuration](#).

If required, external 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.

For more information see the following VMware knowledge base articles:

- Configure a Cluster in vRealize Orchestrator: [KB 2118344](#)
- Configure the F5 Load Balancer to work with an Orchestrator Cluster: [KB 2118472](#)
- Configure the NSX Load Balancer to work with an Orchestrator Cluster: [KB 2118527](#)

Completing the vRealize Automation Initial Installation

During the initial setup process, the load balancer with all nodes enabled routes half of the traffic to the secondary nodes, which are not yet installed, and the installation fails. Infrastructure components setup and the join cluster command of the VA nodes also fail. To avoid these failures and to finish the initial installation of vRealize Automation, you must perform the following tasks.

1. Configure the load balancer as described in [Configuring F5 Big IP with vSphere 5.5 SSO or 6.0 PSC](#).
2. Turn off the health monitors or change them temporarily to default TCP and verify that the traffic is still forwarding to your primary node.
3. Disable all secondary nodes from the load balancer pools.
4. Install and configure all of the system components as detailed in [vRealize Automation Installation and Configuration](#).
5. When all of the components are installed, enable all nodes on the load balancer and restore health checks.
6. Configure either the F5 or NSX load balancer with all of the monitors enabled



After you complete this procedure, update the monitor that you created in [Configure Monitors](#).

For more information about how to download the IaaS installer, see [Download the IaaS Installer](#).

Configuring F5 Big IP with vSphere 5.5 SSO or 6.0 PSC

This document assumes that the F5 device is already deployed in the environment and is configured with network connectivity to the vRealize Automation components.

- The F5 can be either physical or virtual and can be deployed in one-arm or multiarm 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

NOTE: Although configuration steps are the same, some properties are different when you configure F5 with vSphere 6 PSC and vSphere 5.5u2 SSO. The differences are listed in the tables in this section. The main difference is in the ports being used – 7444 (SSO) vs 443 (PSC).

If you are using an F5 version older than 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](#).

For more information about the vSphere 6 PSC HA setup, see [VMware vCenter Server 6.0 Deployment Guide](#).

Configure Custom Persistence Profile

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

Configure monitors by using vSphere 6 PSC or by using vSphere 5.5 u2 SSO. For more information on how to configure monitoring of the vRealize Automation appliance databases, see the VMware knowledge base article [KB 2127052](#).

1. Log in to the F5 load balancer and select **Local Traffic > Monitors**.
2. Click **Create** and provide the required information. Leave the default 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**.





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

Copyright © 2015 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

TABLE 1 - CONFIGURE MONITORS

NAME	TYPE	INTERVAL	TIMEOUT	SEND STRING	RECEIVE STRING	ALIAS SERVICE PORT
vra_https_psc_443 Use this information to configure monitors by using vSphere 6 PSC.	HTTPS	3	10	GET /websso/SAML2/Metadata/vsphere.local\r\n	entityId	
vra_https_sso_7444 Use this information to configure monitors by using vSphere 5.5 u 2 SSO	HTTPS	3	10	GET /websso/SAML2/Metadata/vsphere.local\r\n	entityId	7444
vra_https_va_web	HTTPS	3	10	GET /vcac/services/api/status\r\n	REGISTERED	443
vra_https_iaas_web	HTTPS	3	10	GET / \r\n		
vra_https_iaas_mgr	HTTPS	3	10	GET /VMPS2\r\n	BasicHttpBinding_VMPSPProxyAgent_policy	
vro_https_8281 The vRealize Orchestrator profile appears only if Orchestrator HA is already configured with that load balancer.	HTTPS	3	10	GET /vco/api/docs/index.html HTTP/1.1\r\nHost:\r\n\r\nConnection: close\r\n\r\n	200 OK	
vra_appDB For information about how to configure Appliance Database (appDB), see the VMware knowledge base article KB 2108923 .	-	-	-	-	-	



Example

The completed configuration should look similar to the following screen.



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

Copyright © 2015 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Local Traffic » Monitors » **New Monitor...**

General Properties

Name	vra_https_va_web
Description	Services on the vRealize Automation Virtual Appliance
Type	HTTPS ▼
Parent Monitor	https ▼

Configuration: Basic ▼

Interval	3 seconds
Timeout	10 seconds
Send String	GET /vcac/services/api/health\r\n
Receive String	HTTP/1\.(0 1) (200 204)
Receive Disable String	
Cipher List	DEFAULT:+SHA:+3DES:+kEDH
User Name	
Password	
Reverse	<input type="radio"/> Yes <input checked="" type="radio"/> No
Transparent	<input type="radio"/> Yes <input checked="" type="radio"/> No
Alias Address	* All Addresses
Alias Service Port	443 HTTPS ▼

Cancel Repeat Finished





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

Copyright © 2015 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Configure Server Pools

Configure server pools by using vSphere 6 PSC or by using vSphere 5.5 u2 SSO.

1. Log in to the F5 load balancer and select **Local Traffic > Pools**.
2. Click **Create** and provide the required information. Leave the default when nothing is specified.
3. 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 of information in Table 2.
5. To check the network map for an overall view of the server pools, select **LTM > Network Map**.

TABLE 2 – CONFIGURE SERVER POOLS

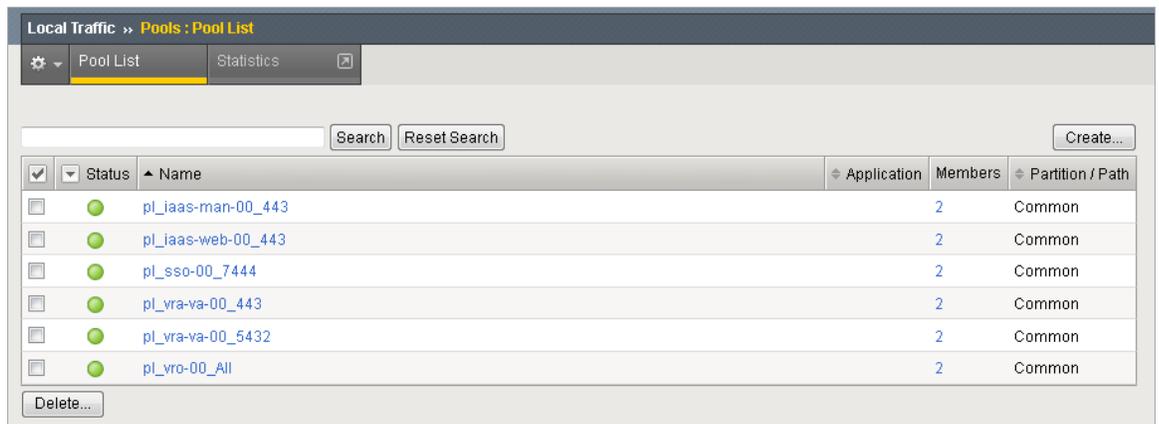
NAME	HEALTH MONITORS	LOAD BALANCING METHOD	NODE NAME	ADDRESS	SERVICE PORT
pl_psc-00_443 Use this information to configure server pools by using vSphere 6 PSC.	vra_https_psc_443	Round Robin	ra-sso-01	10.26.38.51	443
			ra-sso-02	10.26.38.52	443
pl_sso-00_7444 Use this information to configure server pools by using vSphere 5.5 u2 SSO.	vra_https_sso_7444	Round Robin	ra-sso-01	10.26.38.51	7444
			ra-sso-02	10.26.38.52	7444
pl_vra-va-00_443	vra_https_va_web	Round Robin	ra-vra-va-01	10.26.38.44	443
			ra-vra-va-02	10.26.38.45	443
pl_iaas-web-00_443	vra_https_iaas_web	Round Robin	ra-web-01	10.26.38.49	443
			ra-web-02	10.26.38.50	443
pl_iaas-man-00_443	vra_https_iaas_mgr	Round Robin	ra-man-01	10.26.38.46	443
			ra-man-02	10.26.38.59	443
pl_vra-va-00_8444 Works only with vRealize Automation 6.2.1 or higher (6.2.x)	vra_https_va_web	Round Robin	ra-vra-va-01	10.26.38.44	8444
			ra-vra-va-02	10.26.38.45	8444
pl_vra-va-00_5432 For information about how to configure Appliance Database (appDB), see the VMware knowledge base article KB 2108923 .	vra_appDB	Round Robin	ra-vra-va-01	10.26.38.44	5432



			ra-vra-va-02	10.26.38.45	5432
pl_vro-00_All The vRealize Orchestrator profile appears only if Orchestrator HA is already configured with that load balancer.	vro_https_8281	Round Robin	ra-vro-01	10.26.38.47	*
			ra-vro-02	10.26.38.48	*

Example

The completed configuration should look similar to the following screen.



Configure Virtual Servers

Configure virtual server by using vSphere 6 PSC or by using vSphere 5.5 u2 SSO.

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 when nothing is specified.
NOTE: PSC requires SSL termination. For additional steps for importing the SSL certificates and configuring the virtual servers, see the Appendix in the [VMware vCenter Server 6.0 Deployment Guide](#).
3. Repeat steps 1 and 2 for each entry in Table 3.
NOTE: For virtual servers that use SSL pass-through, verify that **OneConnect Profile** is set to **None**.
4. To check the network map for an overall view of the virtual servers, select **LTM > Network Map**.

TABLE 3 – CONFIGURE VIRTUAL SERVERS

NAME	TYPE	DESTINATION ADDRESS	SERVICE PORT	SOURCE ADDRESS TRANSLATION	DEFAULT POOL	DEFAULT PERSISTENCE PROFILE
------	------	---------------------	--------------	----------------------------	--------------	-----------------------------



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

Copyright © 2015 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

vs_psc-00_443 Use this information to configure virtual servers by using vSphere 6 PSC.	Performance (Layer 4)	10.26.38.39	443	Auto Map	pl_psc-00_443	None
vs_sso-00_7444 Use this information to configure virtual servers by using vSphere 5.5 u2 SSO.	Performance (Layer 4)	10.26.38.39	7444	Auto Map	pl_sso-00_7444	None
vs_vra-va-00_443	Performance (Layer 4)	10.26.38.40	443	Auto Map	pl_vra-va-00_443	source_addr_vra
vs_web-00_443	Performance (Layer 4)	10.26.38.41	443	Auto Map	pl_iaas-web-00_443	source_addr_vra
vs_man-00_443	Performance (Layer 4)	10.26.38.42	443	Auto Map	pl_iaas-man-00_443	None
vs_vra-va-00_8444 Works only with vRealize Automation 6.2.1 or higher (6.2.x)	Performance (Layer 4)	10.26.38.40	8444	Auto Map	pl_vra-va-00_8444	source_addr_vra
vs_vro-00_8281 The vRealize Orchestrator profile appears only if Orchestrator HA is already configured with that load balancer.	Performance (Layer 4)	10.26.38.43	8281	Auto Map	pl_vro-00_All	source_addr_vra
vs_vra-va-00_5432 For information about how to configure Appliance Database (appDB), see the VMware knowledge base article KB 2108923 .	Performance (Layer 4)	10.26.38.40	5432	Auto Map	pl_vra-va-00_5432	None



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

Copyright © 2015 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Example

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

General Properties

Name	vs_vra_va_00_443
Description	
Type	Performance (Layer 4) ▼
Source	
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 10.23.38.40
Service Port	443 HTTPS ▼
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
State	Enabled ▼

Configuration: Basic ▼

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

Acceleration

Rate Class	None ▼
SPDY Profile	None ▼

Resources

iRules	<table><thead><tr><th>Enabled</th><th>Available</th></tr></thead><tbody><tr><td></td><td><ul style="list-style-type: none">./Common._sys_APM_ExchangeSupport_OA_BasicAuth._sys_APM_ExchangeSupport_OA_NtlmAuth._sys_APM_ExchangeSupport_helper._sys_APM_ExchangeSupport_main</td></tr></tbody></table>	Enabled	Available		<ul style="list-style-type: none">./Common._sys_APM_ExchangeSupport_OA_BasicAuth._sys_APM_ExchangeSupport_OA_NtlmAuth._sys_APM_ExchangeSupport_helper._sys_APM_ExchangeSupport_main
Enabled	Available				
	<ul style="list-style-type: none">./Common._sys_APM_ExchangeSupport_OA_BasicAuth._sys_APM_ExchangeSupport_OA_NtlmAuth._sys_APM_ExchangeSupport_helper._sys_APM_ExchangeSupport_main				
Default Pool	+ pl_vra-va-00_443 ▼				
Default Persistence Profile	source_addr_vra ▼				
Fallback Persistence Profile	None ▼				

Cancel Repeat Finished



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

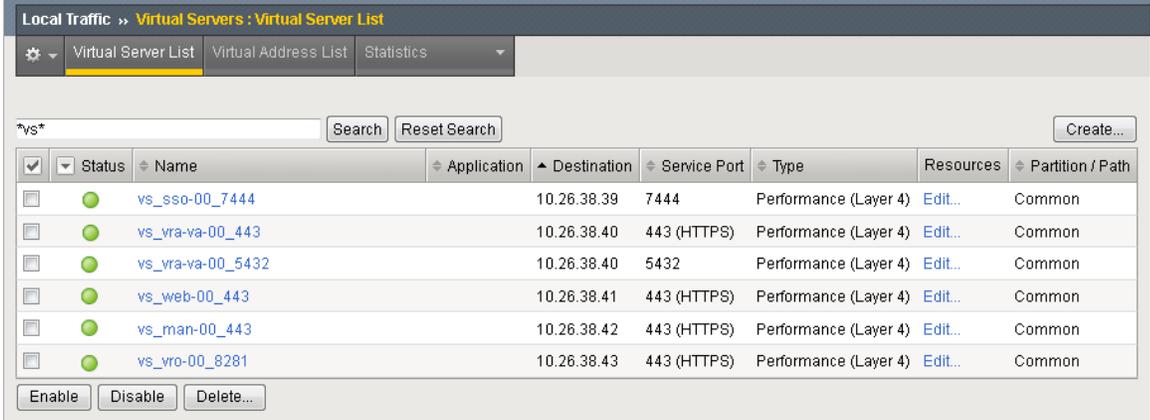
Copyright © 2015 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.



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

Copyright © 2015 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

The completed configuration should look similar to the following screen.



<input type="checkbox"/>	Status	Name	Application	Destination	Service Port	Type	Resources	Partition / Path
<input type="checkbox"/>	●	vs_sso-00_7444		10.26.38.39	7444	Performance (Layer 4)	Edit...	Common
<input type="checkbox"/>	●	vs_vra-va-00_443		10.26.38.40	443 (HTTPS)	Performance (Layer 4)	Edit...	Common
<input type="checkbox"/>	●	vs_vra-va-00_5432		10.26.38.40	5432	Performance (Layer 4)	Edit...	Common
<input type="checkbox"/>	●	vs_web-00_443		10.26.38.41	443 (HTTPS)	Performance (Layer 4)	Edit...	Common
<input type="checkbox"/>	●	vs_man-00_443		10.26.38.42	443 (HTTPS)	Performance (Layer 4)	Edit...	Common
<input type="checkbox"/>	●	vs_vro-00_8281		10.26.38.43	443 (HTTPS)	Performance (Layer 4)	Edit...	Common

Deploying NSX 6.1 with vSphere 5.5 SSO

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

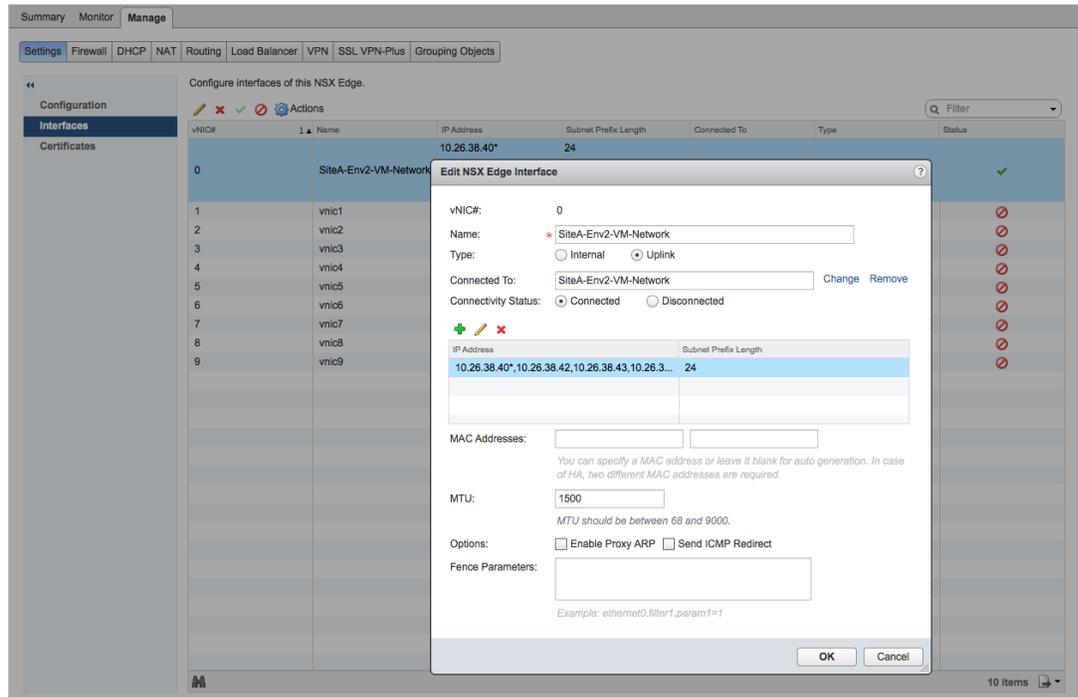
Configure Global Settings

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

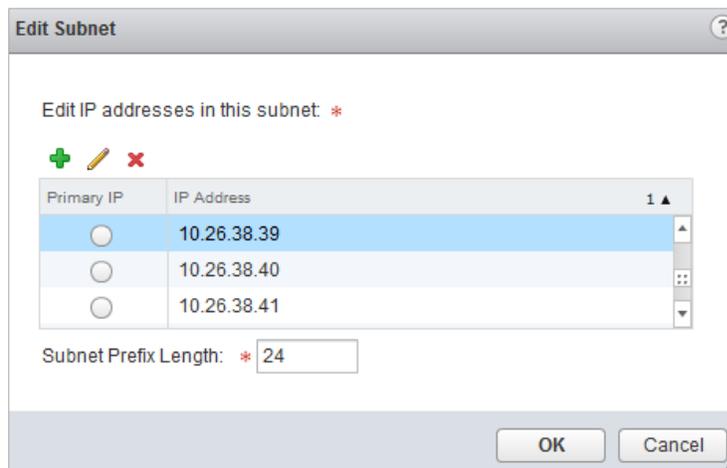


VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Copyright © 2015 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.



5. Add the IP addresses assigned to the VIPs, and click **OK**.
6. Click **OK** to exit the interface configuration subpage.

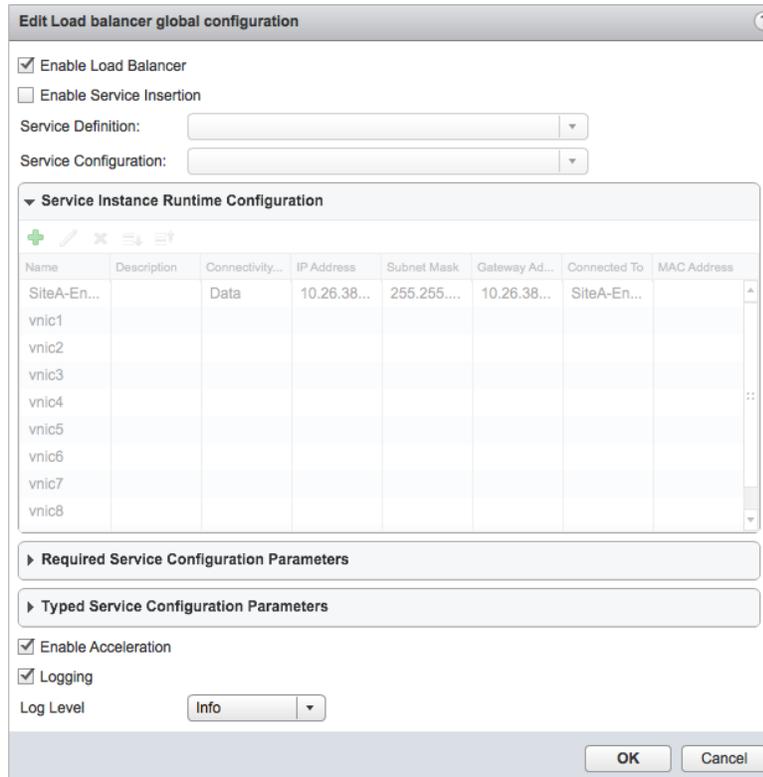


7. Select the **Load Balancer** tab and click the **Edit** icon.
8. Select **Enable Load Balancer**, **Enable Acceleration**, and **Logging**, if required, and click **OK**.



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

Copyright © 2015 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.



Add Application Rules

You can add application rules for vRealize Automation by using vSphere 5.5 u2 SSO.

1. Click **Application Rules** in the left pane.
2. Click **Add** icon to create the Application Rules required for vRealize Automation using information in Table 4.

TABLE 4 – ADD APPLICATION RULES

NAME	SCRIPT
SSO	<pre># detect if pool "pool_sso_primary_7444" is still UP acl sso_primary_down nbsrv(pool_sso_primary_7444) eq 0 # use pool "pool_sso_secondary_7444" if "pool_sso_primary_7444" is dead use_backend pool_sso_secondary_7444 if sso_primary_down</pre>

Add Application Profiles

You can add application profiles for different components of vRealize Automation.



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

Copyright © 2015 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

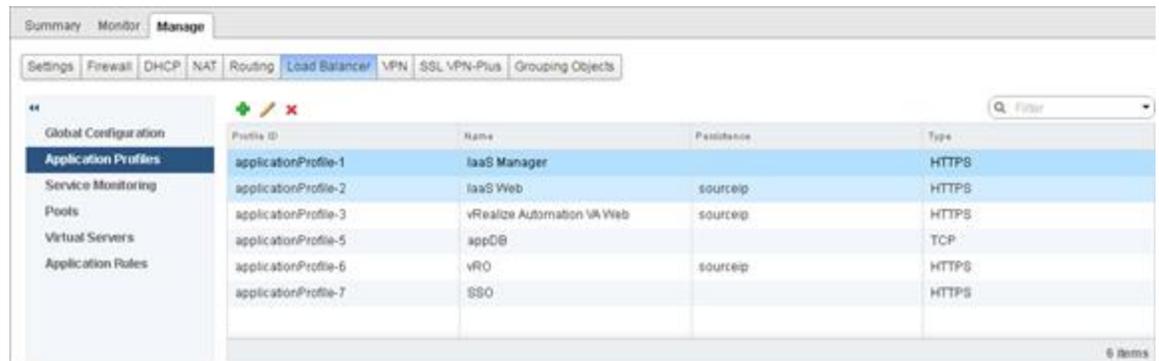
1. Click **Application Profiles** on the window pane on the left.
2. Click the **Add** icon to create the Application Profiles required for vRealize Automation using information in Table 5. Leave the default when nothing is specified.

TABLE 5 – APPLICATION PROFILES

NAME	TYPE	ENABLE SSL PASS-THROUGH	TIMEOUT	PERSISTENCE
IaaS Manager	HTTPS	Checked	-	None
IaaS Web	HTTPS	Checked	1800 seconds	Source IP
SSO	HTTPS	Checked	-	None
vRealize Automation VA Web	HTTPS	Checked	1800 seconds	Source IP
vRO The vRealize Orchestrator profile appears only if Orchestrator HA is already configured with that load balancer.	HTTPS	Checked	1800 seconds	Source IP
appDB For information about how to configure Appliance Database (appDB), see the VMware knowledge base article KB 2108923 .	TCP	N/A	-	none

Example

The completed configuration should look similar to the following screen.



Add Service Monitoring

You can add service monitoring for 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 6. Leave the default when nothing is specified.



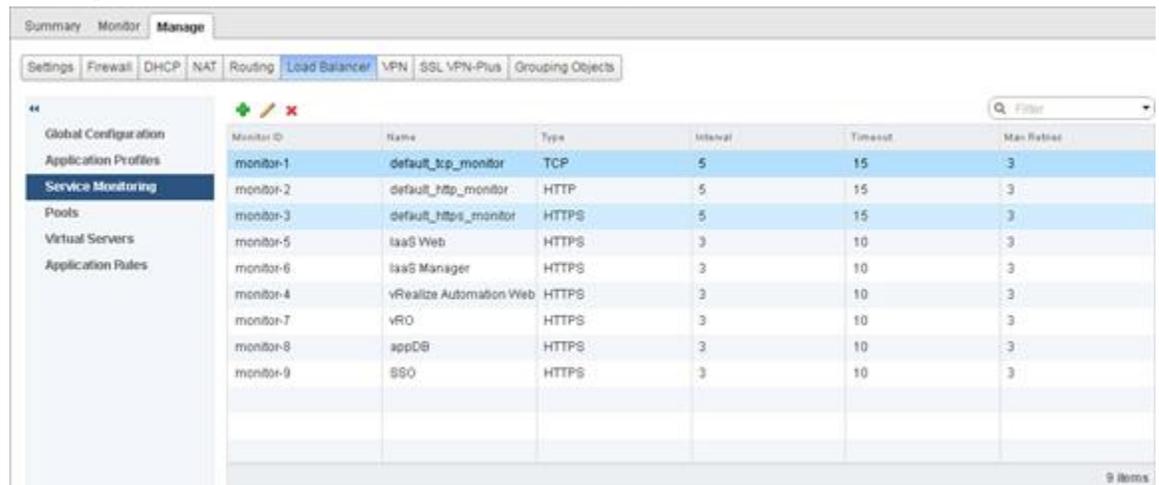
VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Copyright © 2015 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

TABLE 6 – ADD SERVICE MONITORING

NAME	INTERVAL	TIME OUT	RETRIES	TYPE	METHOD	URL	RECEIVE:
SSO	3	10	3	HTTPS	GET	/websso/HealthStatus	GREEN
vRealize Automation VA Web	3	10	3	HTTPS	GET	/vcac/services/api/status	REGISTERED
IaaS Web	3	10	3	HTTPS	GET		
IaaS Manager	3	10	3	HTTPS	GET	/VMPS2	BasicHttpBinding_VMSPProxyAgent_policy
appDB For information about how to configure Appliance Database (appDB), see the VMware knowledge base article KB 2108923 .	-	-	-	-	-	-	-
vRO The vRealize Orchestrator profile appears only if Orchestrator HA is already configured with that load balancer.	3	10	3	HTTPS	GET	vco/api/docs/index.html HTTP/1.1\r\nHost:\r\n\r\nConnection: close\r\n\r\n	200 OK

The completed configuration should look similar to the following screen.



Add Pools



You can add pools for vRealize Automation using vSphere 5.5 u2 SSO.

1. Click **Pools** in the left pane.
2. Click the **Add** icon to create the Pools required for vRealize Automation using information in Table 7. Leave the default when nothing is specified.
3. You can either use the IP address of the pool members, or select them as a Virtual Center Container.

TABLE 7 - ADD POOLS

POOL NAME	ALGORITHM	MONITORS	MEMBER NAME	EXAMPLE IP ADDRESS / VCENTER CONTAINER	PORT	MONITOR PORT
pool_sso_primary_7444 Use this information to add pools by using vSphere 5.5 u2 SSO.	ROUND_R OBIN	SSO	SSO1	10.26.38.51	7444	
pool_sso_secondary_7444 Use this information to add pools by using vSphere 5.5 u2 SSO.	ROUND_R OBIN	SSO	SSO2	10.26.38.52	7444	
pool_vra-va-web_443	ROUND_R OBIN	vRA VA Web	vRA VA1	10.26.38.44	443	
			vRA VA2	10.26.38.45	443	
pool_iaas-web_443	ROUND_R OBIN	IaaS Web	IaaS Web1	10.26.38.49	443	
			IaaS Web2	10.26.38.50	443	
pool_iaas-manager_443	ROUND_R OBIN	IaaS Manager	IaaS Man1	10.26.38.49	443	
			IaaS Man2	10.26.38.50	443	
pool_vra-rconsole_8444	ROUND_R OBIN	vRA VA Web	vRA VA1	10.26.38.44	8444	443
Works only with vRealize Automation 6.2.1 and higher versions.			vRA VA2	10.26.38.45	8444	443
pool_appDB_5432 For information about how to configure Appliance Database (appDB), see the VMware knowledge base article KB 2108923 .	ROUND_R OBIN	appDB	appDBnode 1	10.26.38.44	5432	5480
			appDBnode 2	10.26.38.45	5432	5480
pool_vro_8281 The vRealize Orchestrator profile	ROUND_R OBIN	vRO	vRO1	10.26.38.44	8281	



appears only if Orchestrator HA is already configured with that load balancer.						
			vRO2	10.26.38.45	8281	

Add Virtual Servers

You can add virtual servers required for vRealize Automation by using the following steps.

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 8. Leave the default when nothing is specified.

TABLE 8 - ADD VIRTUAL SERVERS

NAME	IP ADDRESS	PROTOCOL	PORT	DEFAULT POOL	APPLICATION PROFILE	APPLICATION RULE
vs_sso_7444 Use this information to add virtual servers by using vSphere 5.5 u2 SSO.	10.26.38.39	HTTPS	7444	pool_sso_primary_7444	SSO	SSO
vs_vra-va-web_443	10.26.38.40	HTTPS	443	pool_vra-va-web_443	vRA VA	
vs_iaas-web_443	10.26.38.41	HTTPS	443	pool_iaas-web_443	IaaS Web	
vs_iaas-manager_443	10.26.38.42	HTTPS	443	pool_iaas-manager_443	IaaS Manager	
vs_vra-va-rconsole_8444 Works only with vRealize Automation 6.2.1.	10.26.38.40	HTTPS	8444	pool_vra-rconsole_8444	vRA VA	
vs_appDB_5432 For information about how to configure Appliance Database (appDB), see the VMware knowledge base article KB 2108923 .	10.26.38.40	TCP	5432	pool_appDB_5432	appDB	
vs_vro_8281 The vRealize Orchestrator profile appears only if Orchestrator HA is already configured with that load balancer.	10.26.38.43	HTTPS	8281	pool_vro_8281	vRO	

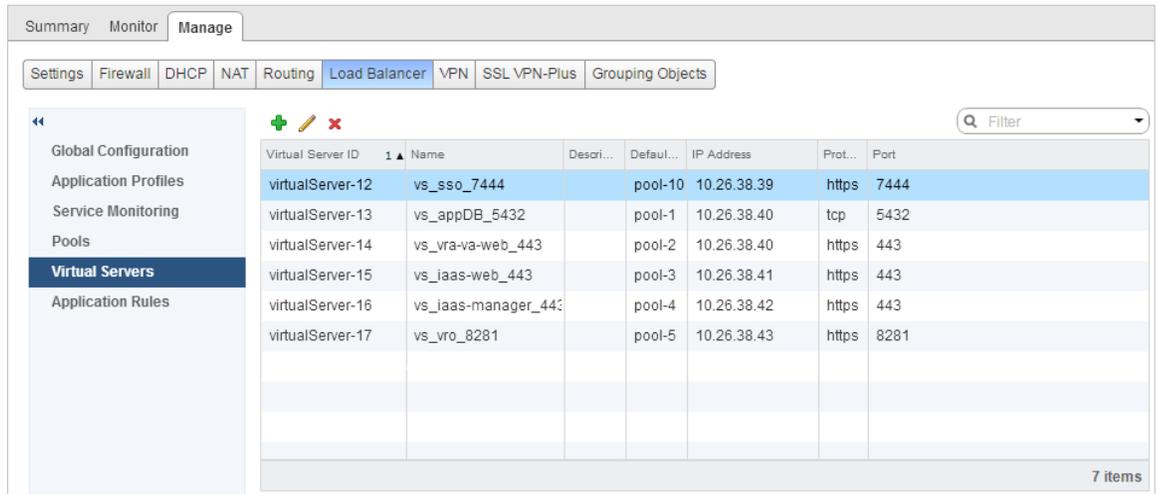




VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Copyright © 2015 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

The completed configuration should look similar to the following screen.



The screenshot shows the F5 BIG-IP configuration interface. The 'Manage' tab is active, and the 'Load Balancer' sub-tab is selected. A table lists several virtual servers, with the first one highlighted in blue. The table has columns for Virtual Server ID, Name, Description, Default Pool, IP Address, Protocol, and Port.

Virtual Server ID	Name	Descri...	Defaul...	IP Address	Prot...	Port
virtualServer-12	vs_sso_7444		pool-10	10.26.38.39	https	7444
virtualServer-13	vs_appDB_5432		pool-1	10.26.38.40	tcp	5432
virtualServer-14	vs_vra-va-web_443		pool-2	10.26.38.40	https	443
virtualServer-15	vs_laas-web_443		pool-3	10.26.38.41	https	443
virtualServer-16	vs_laas-manager_443		pool-4	10.26.38.42	https	443
virtualServer-17	vs_vro_8281		pool-5	10.26.38.43	https	8281

Troubleshooting

Configure SSO as active/active

The way SSO sessions are currently logged out, it is not possible to configure SSO as active/active.

The workaround for the F5 configuration is to set the persistence type to destination address. This ensures that all traffic to the SSO virtual server is sent to a single pool member. When the pool member becomes unavailable, the traffic is sent to another pool member, this behavior is effectively active passive.

The workaround for the NSX configuration is to use an AppRule and 2 pools. "Pool-SSO1" with only SSO-server1 and "Pool-SSO2" with only SSO-server2. The AppRule sends traffic to "Pool-SSO1" as long as the pool is up, else it sends traffic to "SSO-Pool2".

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.

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**.



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

Copyright © 2015 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.