

# VMware Aria Automation Load Balancing Guide

VMware Aria Automation 8.12

You can find the most up-to-date technical documentation on the VMware website at:

<https://docs.vmware.com/>

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

Copyright © 2023 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

# Contents

- 1 VMware Aria Automation and VMware Aria Automation Orchestrator 5**
- 2 Load Balancing Concepts 6**
  - SSL Pass-Through 6
  - Load balancer notifications 7
  - One-arm and multi-arm topologies 7
- 3 Prerequisites for configuring load balancers for VMware Aria Automation 8**
  - Complete the VMware Aria Automation and VMware Aria Automation Orchestrator initial installation 9
- 4 Configuring NSX-V 10**
  - Configure global settings 10
  - Configure application profiles 12
  - Configure service monitoring 13
  - Configure server pools 15
  - Configure virtual servers 17
- 5 Configuring NSX-T 19**
  - Configure NSX-T application profiles 19
  - Configure NSX-T active health monitor 20
  - Configure NSX-T server pools 23
  - Configure NSX-T virtual servers 24
  - Configure load balancer 26
  - Add virtual servers to load balancer 27
- 6 Configuring F5 Big-IP LTM 28**
  - Configure monitors 28
  - Configure F5 server pools 30
  - Configure F5 virtual servers 31
- 7 Configuring Citrix ADC (NetScaler ADC) 34**
  - Configure Citrix monitors 34
  - Configure Citrix Service Groups 37
  - Configure Citrix Virtual Servers 38
- 8 Configuring AVI Load Balancer 41**
  - Create a health monitor 41

- Create a pool 44
- Create virtual service VIP 46
- Configure virtual service 48

## 9 Troubleshooting 52

- Errors during VMware Aria Automation installation when using NSX-V as a load-balancer for Workspace ONE 52
- Provisioning failures when using OneConnect with F5 BIG-IP 53
- F5 BIG-IP license limits network bandwidth 53
- FortiGate specifics 53

# VMware Aria Automation and VMware Aria Automation Orchestrator

# 1

This document describes the load balancing configuration of VMware Aria Automation and VMware Aria Automation Orchestrator in a distributed and highly available cluster deployment using VMware NSX, F5 Networks BIG-IP (F5), and Citrix NetScaler technologies.

This document is not an installation guide, but rather a configuration guide that supplements the VMware Aria Automation and VMware Aria Automation Orchestrator installation and configuration documentation available in the [VMware Aria Automation product documentation](#).

This information is for the following products and versions.

**Table 1-1.**

Product	Version
NSX-T	2.4, 2.5, 3.0,3.1, and later
NSX-V	6.2.x, 6.3.x, 6.4.x, and later
F5 BIG-IP LTM	11.x, 12.x, 13.x, 14.x, 15.x
Citrix NetScaler ADC	10.5, 11.x, 12.x, 13.x
VMware Aria Automation	8.12 forward
VMware Aria Automation Orchestrator	8.12 forward

Refer to the [VMware Product Interoperability Matrices](#) for more details.

# Load Balancing Concepts

# 2

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 organization's policy for backing up load balancers, keeping in mind the preservation of network topology and VMware products backup planning.

This chapter includes the following topics:

- [SSL Pass-Through](#)
- [Load balancer notifications](#)
- [One-arm and multi-arm topologies](#)

## SSL Pass-Through

SSL pass-through is used with the load balancing configurations.

SSL pass-through is used for these reasons:

- Ease of deployment
  - Not having to deploy the VMware Aria Automation or VMware Aria Automation 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 to the load balancer.
- Ease of communication
  - The individual host names of the load-balanced components are the subject alternate name field of the certificates, so the client can easily communicate with the load balanced nodes.

## Load balancer notifications

It is a recommended practice to enable notifications any time a VMware Aria Automation or VMware Aria Automation Orchestrator node in a server pool goes down.

VMware NSX Data Center supports enabling notifications when an alert is raised in VMware Aria Operations and VMware Aria Operations for Networks. Refer to the VMware Aria Operations and VMware Aria Operations for Networks documentation.

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 email notification with F5 using these methods:

- [Configuring the BIG-IP system to deliver locally generated email messages](#)
- [Configuring custom SNMP traps](#)

## One-arm and multi-arm topologies

One-arm and multi-arm deployments route load balancer traffic differently.

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 VMware Aria Automation and VMware Aria Automation Orchestrator components are deployed in a one-arm configuration. Multi-arm deployments are also supported, and their configuration are generally similar to the one-arm configuration.

### One-arm configuration:



# Prerequisites for configuring load balancers for VMware Aria Automation

## 3

Before configuring load balancers, perform these prerequisites.

- **NSX** - Before you can start a high-availability implementation of VMware Aria Automation or VMware Aria Automation Orchestrator 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 VMware [Product Interoperability Matrix](#).
- **F5 BIG-IP LTM** - Before you can start a high-availability implementation of VMware Aria Automation or VMware Aria Automation Orchestrator using F5 LTM load balancer, ensure that the load balancer is installed and licensed and that the DNS server configuration is complete.
- **NetScaler** - Before you can start a high-availability implementation of VMware Aria Automation or VMware Aria Automation Orchestrator using the NetScaler load balancer, ensure that NetScaler is installed and has at least a Standard Edition license.
- **Certificates** - Request Certificate Authority (CA) signed certificate containing the load-balancer fully qualified domain name and the hostnames of the cluster nodes in the SubjectAltNames section. This configuration enables the load balancer to serve traffic without SSLerrors.
- **Identity provider** - The identity provider is Workspace ONE Access, which is deployed external to the VMware Aria Automation appliances and cluster.

For more information on installation and configuration, see VMware Aria Automation documentation on [docs.vmware.com](https://docs.vmware.com).

If necessary, an external VMware Aria Automation Orchestrator cluster can be configured to work with the VMware Aria Automation system. This can be done after the VMware Aria Automation system is up and running. However, a VMware Aria Automation Highly Available setup already includes an embedded VMware Aria Automation Orchestrator cluster.

This chapter includes the following topics:

- [Complete the VMware Aria Automation and VMware Aria Automation Orchestrator initial installation](#)



# Complete the VMware Aria Automation and VMware Aria Automation Orchestrator initial installation

You must configure your load balancer before completing the initial installation of VMware Aria Automation, VMware Aria Automation Orchestrator.

During the installation process of VMware Aria Automation or VMware Aria Automation 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 VMware Aria Automation or VMware Aria Automation Orchestrator, you must perform these steps.

## Procedure

- 1 Configure the F5, NSX, or NetScaler load balancer. See [Chapter 6 Configuring F5 Big-IP LTM](#), [Chapter 5 Configuring NSX-T](#), and [Chapter 7 Configuring Citrix ADC \(NetScaler ADC\)](#).
- 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 system components as detailed in VMware Aria Automation / VMware Aria Automation 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 NSX-V

# 4

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 VMware Aria Automation components being load balanced.

---

**Note** Refer to the [VMware Workspace One](#) load-balancing documentation in order to configure highly-available identity provider for VMware Aria Automation.

---

This chapter includes the following topics:

- [Configure global settings](#)
- [Configure application profiles](#)
- [Configure service monitoring](#)
- [Configure server pools](#)
- [Configure virtual servers](#)

## Configure global settings

Configure global settings using these steps.

### Procedure

- 1 Log in to the NSX-V, click **Manager > Settings** and select **Interfaces**.
- 2 Select your Edge device from 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.

**Edit Interface | nic0**

Basic Advanced

vNIC# 0

Name \* nic0

Type  Internal  Uplink  Trunk

Connected To \* Prod-01

Connectivity Status  Connected

Configure Subnets

+ ADD DELETE Search

<input type="checkbox"/>	Primary IP Address	Secondary IP Addresses	Subnet Prefix Length
<input type="checkbox"/>	192.168.208.102		24

1 items

CANCEL SAVE

- 5 Add the IP addresses assigned to the virtual IPs and click **Save**.
- 6 Click **Ok** to exit the interface configuration page.
- 7 Navigate to the **Load Balancer** tab and click the **Edit** icon.
- 8 Select **Enable Load Balancer** and **Logging**, if necessary, and click **Save**.

**Edit Load Balancer Global Configuration**

Load Balancer  Enable

Acceleration  Disable

Logging  Enable

Log Level \_\_\_\_\_

CANCEL SAVE

## Configure application profiles

It is required to add application profiles for VMware Aria Automation and for an external VMware Aria Automation Orchestrator (optional).

### Procedure

- 1 Click **Application Profiles** in the left pane.
- 2 Click **Add** to create the application profiles required for the specific product as outlined in this table. Use the default value if nothing is specified.

**Table 4-1. Application Profiles**

Name	Type	Persistence	Expires In
VMware Aria Automation	SSL Passthrough	None	None
VMware Aria Automation Orchestrator	SSL Passthrough	None	None
<p><b>Note</b> Use only for external VMware Aria Automation Orchestrator instances.</p>			

## Results

The completed configuration should look similar to this

screen:

**New Application Profile**
✕

**Application Profile Type** SSL Passthrough ▾ ⓘ

**General** Client SSL Server SSL

---

**Name \*** vRealize Automation / vRealize Orchestrator VA Web

**HTTP Redirect URL** \_\_\_\_\_

**Persistence** None ▾

**Cookie Name** \_\_\_\_\_

**Mode** \_\_\_\_\_ ▾

**Expires in** \_\_\_\_\_ (Seconds)

**Insert X-Forwarded-For HTTP header**  Disable

CANCEL
ADD

## Configure service monitoring

It is required to add service monitors for VMware Aria Automation and for an external VMware Aria Automation Orchestrator (optional).

### Procedure

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

- 2 Click **Add** to create the service monitors required for the specific product as outlined in this table. Use the default value if nothing is specified.

**Table 4-2. Service Monitoring**

Name	Interval	Timeout	Retries	Type	Method	URL	Receive	Expected
VMware Aria Automati on	3	10	3	HTTP	GET	/health	200	200
VMware Aria Automati on Orchestra tor  <b>Note</b> Use only for external VMware Aria Automati on Orchestra tor instances.	3	10	3	HTTP	GET	/health	200	200

**Results**

The completed configuration should look similar to this screen:

### New Service Monitor ×

**Name:**

**Interval:**  (Seconds)

**Timeout:**  (Seconds)

**Max Retries:**

**Type:**

**Expected:**

**Method:**

**URL:**

**Send:**

**Receive:**

**Extension:**

## Configure server pools

It is required to create server pools for VMware Aria Automation, and for an external VMware Aria Automation Orchestrator (optional).

### Procedure

- 1 Click **Pools** in the left pane.

2 Click the **Add** icon to create the pools required for the specific product as outlined in this table.

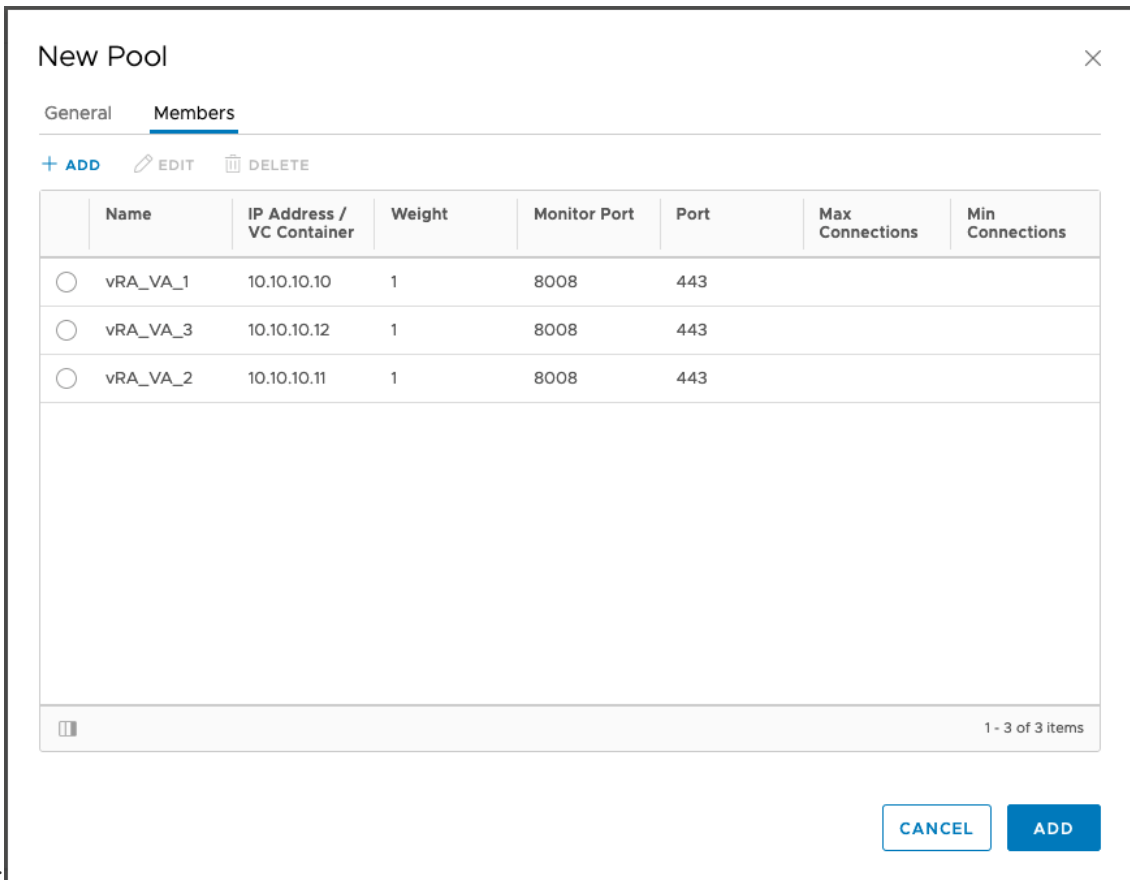
**Table 4-3. Server Pools**

Pool Name	Algorithm	Monitors	Member Name	IP Address/ vCenter Container	Port	Monitor Port
VMware Aria Automation	Least connections	VMware Aria Automation	VA1 VA2 VA	IP Address	443	8008
VMware Aria Automation Orchestrator	Least connections	VMware Aria Automation Orchestrator	VA1 VA2 VA3	IP Address	443	8008

**Note** Use only for external VMware Aria Automation Orchestrator instances.

**Results**

The completed configuration should look similar to this



screen:



## Configure virtual servers

It is required to configure virtual servers for VMware Aria Automation, and for an external VMware Aria Automation Orchestrator (optional).

### Procedure

- 1 Click **Virtual Servers** in the left pane.
- 2 Click the **Add** icon to create the virtual servers required for the different product as outlined in this table. Use default values if nothing is specified.

Name	Acceleration	IP Address	Protocol	Port	Default Pool	Application Profile
vRealize Automation	Not enabled	IP Address	HTTPS	443	vRealize Automation	vRealize Automation
VMware Aria Automation Orchestrator	Not enabled	IP Address	HTTPS	443	vRealize Orchestrator	vRealize Orchestrator
<b>Note</b> Use only for external vRealize Orchestrator instances.						

- 3 (Optional) When using VMware Aria Automation Orchestrator you may need to expose the health check port as a virtual server. In order to do that click the **Add** icon to create a new virtual server for the health check port. Use default values if nothing is specified.

Name	Acceleration	IP Address	Protocol	Port	Default Pool	Application Profile
VMware Aria Automation	Not enabled	IP Address	HTTP	8008	vRealize Automation	vRealize Automation
VMware Aria Automation Orchestrator	Not enabled	IP Address	HTTP	8008	vRealize Orchestrator	vRealize Orchestrator
<b>Note</b> Use only for external instances.						

4

### Results

The completed configuration should look similar to this screen.

### New Virtual Server ✕

**Virtual Server \***  Enable

**Acceleration \***  Disable

**Application Profile:** vRealize Automation VA Web ▼

**Name: \*** vs\_vra-va-web\_443

**Description:**

**IP Address: \*** 10.10.10.8 [Select IP Address](#)

**Protocol:** HTTPS ▼

**Port / Port Range: \*** 443  
e.g.: 9000,9010-9020

**Default Pool:** pool\_vra-va-web\_443 ▼

# Configuring NSX-T

# 5

Before configuring, the NSX-T must be deployed in the environment and the Tier-1 gateway with the load balancer must have access to the VMware Aria Suite components over a network.

---

**Note** Refer to the [VMware Workspace One](#) load-balancing documentation to configure highly-available identity provider for VMware Aria Automation.

---

This chapter includes the following topics:

- [Configure NSX-T application profiles](#)
- [Configure NSX-T active health monitor](#)
- [Configure NSX-T server pools](#)
- [Configure NSX-T virtual servers](#)
- [Configure load balancer](#)
- [Add virtual servers to load balancer](#)

## Configure NSX-T application profiles

You can add an application profile in NSX-T for HTTPS requests.

### Procedure

- 1 Navigate to **Networking > Load Balancing > Profiles**.
- 2 Select **Application** as the profile type.
- 3 Click **Add Application Profile** and select **Fast TCP Profile**.
- 4 Enter a name for the profile.

## Results

The completed application profile for the HTTPS request should look similar to this screen:

The screenshot displays the 'PROFILES' section of the VMware Aria Automation interface. The navigation menu includes 'LOAD BALANCERS', 'VIRTUAL SERVERS', 'SERVER POOLS', 'PROFILES', 'MONITORS', and 'About'. The 'Select Profile Type' dropdown is set to 'APPLICATION'. An 'ADD APPLICATION PROFILE' button is visible. Below this is a table with columns for Name, Type, Idle Timeout (sec), and HA Flow Mirroring. The table contains one entry: 'vRA\_HTTPS' with Type 'Fast TCP' and Idle Timeout '1800'. The HA Flow Mirroring toggle is 'Disabled'. Below the table is a form for editing the profile, with fields for Description, Tags, and Connection Close Timeout (set to 8). The form includes 'SAVE' and 'CANCEL' buttons.

Name	Type	Idle Timeout (sec)	HA Flow Mirroring
vRA_HTTPS	Fast TCP	1800	Disabled

Form fields:

- Description: Enter Description
- Tags: Tag (Required), Scope (Optional) (checked)
- Connection Close Timeout: 8

Buttons: SAVE, CANCEL

## Configure NSX-T active health monitor

To configure an active health monitor for NSX-T follow these steps.

### Procedure

- 1 Navigate to **Networking > Load Balancing > Monitors**.
- 2 Click **Add Active Monitor** and select **HTTP**.
- 3 Enter a name for the health monitor.

4 Configure the health monitor as outlined in this table:

**Table 5-1. Configure Health Monitor**

Name	Monitoring Port	Interval	Timeout	Fall Count	Type	Method	URL	Response Code	Response Body
VMware Aria Automation	8008	3	10	3	HTTP	GET	/health	200	None
VMware Aria Automation Orchestrator	8008	3	10	3	HTTP	GET	/health	200	None
<p><b>Note</b> Use only for external VMware Aria Automation Orchestrator instances.</p>									

## Results

The completed configuration should look similar to these screens.

LOAD BALANCERS VIRTUAL SERVERS SERVER POOLS PROFILES **MONITORS** About

Select Monitor Type ACTIVE

ADD ACTIVE MONITOR COLLAPSE ALL vRealize

Name	Protocol	Monitoring Port	Monitoring Interval	Timeout Period (sec)	Server Pools
vRealize Automation VA *	HTTP	8008	3	10	

Description: Enter Description

Fall Count: 3

Tags: Tag (Req) Scope (O) ✓  
Maximum 30 tags are allowed.

Rise Count: 3

Additional Properties

HTTP Request [Configure](#) HTTP Response [Configure](#)

SAVE CANCEL

### HTTP Request and Response Configuration

Active Health Monitor -

HTTP Request Configuration HTTP Response Configuration

HTTP Response Code

200 X

1 or more response codes

HTTP Response Body

## Configure NSX-T server pools

You must configure server pools for VMware Aria Automation, and an external VMware Aria Automation Orchestrator (optional).

### Procedure

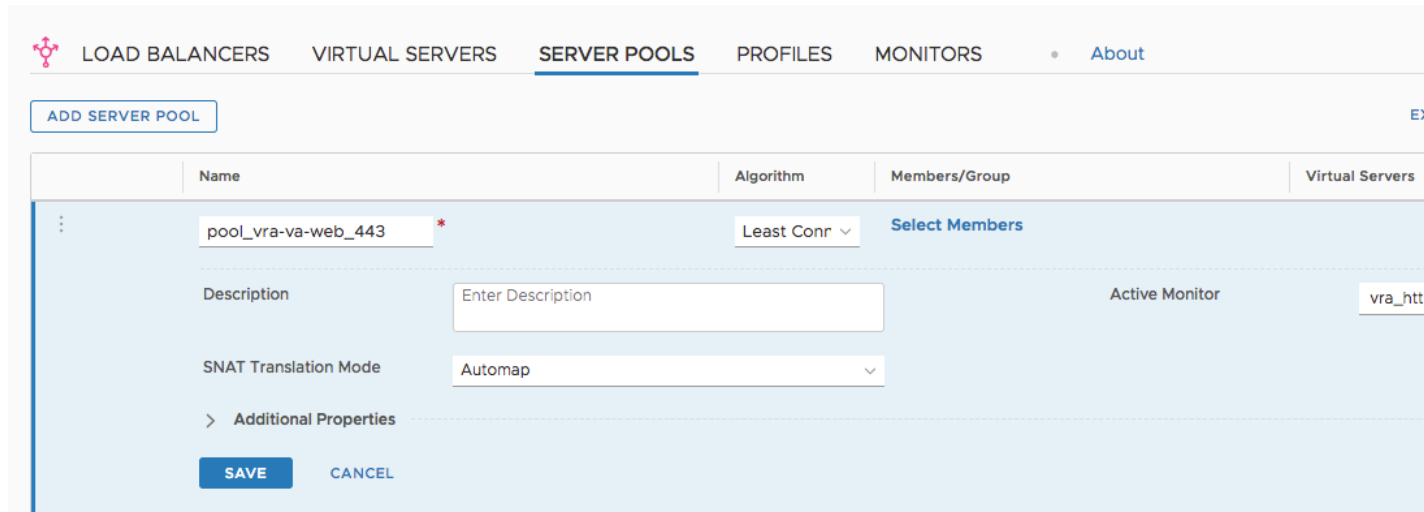
- 1 Navigate to **Networking > Load Balancing > Server Pools**.
- 2 Click **Add Server Pool**.
- 3 Enter a name for the pool.
- 4 Configure the pool as outlined in this table:

**Table 5-2. Configure Server Pools**

Pool Name	Algorithm	Active Monitor	Name	IP	Port
VMware Aria Automation	Least Connections	VMware Aria Automation	VA1 VA2 VA3	IP	443
VMware Aria Automation Orchestrator	Least Connections	VMware Aria Automation Orchestrator	VA1 VA2 VA3	IP	443
<p><b>Note</b> Use only for external VMware Aria Automation Orchestrator instances.</p>					

## Results

The completed configuration should look similar to these screens.



### Configure Server Pool Members

Server Pool - pool\_iaas-manager\_443

Enter individual members

Select a group

ADD MEMBER

Search

Name	IP	Port	Weight	State	Backup Member	Max Concurrent Connections
:		443	1	Enabled	<input type="radio"/> Disabled	
:		443	1	Enabled	<input type="radio"/> Disabled	

CANCEL

APPLY

## Configure NSX-T virtual servers

It is required to configure virtual servers for VMware Aria Automation, and for an external VMware Aria Automation Orchestrator (optional).

### Procedure

- 1 Navigate to **Networking > Load Balancing > Virtual Servers**.
- 2 Click **Add virtual server** and select **Layer**.



3 Configure the virtual servers as outlined in this table:

**Table 5-3. Configure Virtual Servers**

Name	Type	Application Profile	IP Address	Port	Server Pool	Persistence Profile
VMware Aria Automation	L4 TCP	VMware Aria Automation	IP	443	VMware Aria Automation	None
VMware Aria Automation Orchestrator	L4 TCP	VMware Aria Automation Orchestrator	IP	443	VMware Aria Automation Orchestrator	None
<p><b>Note</b> Use only for external VMware Aria Automation Orchestrator instances.</p>						

4 (Optional) In cases where VMware Aria Operations is used you may need to expose the health check port as a virtual server. In order to achieve that create a new virtual server according to the following table:

Name	Type	Application Profile	IP Address	Port	Server Pool	Persistence Profile
VMware Aria Automation	L4 TCP	VMware Aria Automation	IP	8008	VMware Aria Automation	None
VMware Aria Automation Orchestrator	L4 TCP	VMware Aria Automation Orchestrator	IP	8008	VMware Aria Automation Orchestrator	None
<p><b>Note</b> Use only for external VMware Aria Automation Orchestrator instances.</p>						

**Results**

The completed configuration should look similar to this screen.

The screenshot shows the VMware Aria Automation interface for configuring a load balancer. The 'VIRTUAL SERVERS' tab is selected. A table lists the virtual server configuration:

Name	IP Address	Ports	Type	Load Balancer	Server
vs_vra-va-web_443	10.10.10.10 <small>e.g. 10.10.10.10</small>	443	L4 TCP	r34r3r4	pool

Below the table, the configuration form is displayed with the following fields:

- Description:** Enter Description
- Persistence:** Disabled
- Additional Properties:**
  - Max Concurrent Connections:** Unlimited
  - Sorry Server Pool:** Select Server Pool
  - Max New Connection Rate:** Unlimited
  - Default Pool Member Ports:** 443
  - Admin State:** Enabled
  - Access Log:** Disabled
  - Tags:** Tag (Required), Scope (Optional)

Buttons for **SAVE** and **CANCEL** are located at the bottom of the form.

## Configure load balancer

Specify a load balancer for each VMware Aria Automation, and for an external VMware Aria Automation Orchestrator (optional) instance.

### Procedure

- 1 Navigate to **Networking > Load Balancing > Load Balancers**.
- 2 Click **Add Load Balancer**.
- 3 Enter a name and select the appropriate **Load Balancer Size** (depends on VMware Aria Automation cluster size).
- 4 Select the **Tier 1 Logical Router**.

**Note** In NSX-T version 2.4, the monitor health checks are performed using the IP address of Tiers-1 uplink (or first service port for Tiers-1 standalone SR) for all load balancer server pools. Ensure that server pools are accessible from this IP address.

## Results

The configuration should look similar to this screen:

The screenshot shows the VMware Aria Automation interface for configuring a load balancer. The navigation menu includes 'LOAD BALANCERS', 'VIRTUAL SERVERS', 'SERVER POOLS', 'PROFILES', 'MONITORS', and 'About'. A button 'ADD LOAD BALANCER' is visible. The configuration form includes the following fields:

- Name:** vra75\_lb
- Size:** Small
- Tier-1 Gateway:** vRA-LB-Tier-1-Router
- Description:** Enter Description
- Tags:** Tag (Required) and Scope (Optional) with a checkmark icon. A note states 'Maximum 30 tags are allowed.'
- Error Log Level:** (Dropdown menu)
- Admin State:** Turned on (Green toggle)

At the bottom, there are 'SAVE' and 'CANCEL' buttons.

## Add virtual servers to load balancer

Once you've configured the load balancer, you can add virtual servers.

### Procedure

- 1 Navigate to **Networking > Load Balancing > Virtual Servers**.
- 2 Edit the configured virtual servers.
- 3 Assign the previously configured load balancer as the **Load Balancer**.

## Results

The configuration should look similar to this screen:

The screenshot shows the VMware Aria Automation interface for configuring a virtual server. The navigation menu includes 'LOAD BALANCERS', 'VIRTUAL SERVERS', 'SERVER POOLS', 'PROFILES', 'MONITORS', and 'About'. A button 'ADD VIRTUAL SERVER' is visible. The configuration form includes the following fields:

- Name:** vs\_vra-va-web\_443
- IP Address:** 192.168.205.10
- Ports:** 443
- Type:** L4 TCP
- Load Balancer:** vRA\_LB
- Application Profile:** vRA\_HTTPS
- Description:** Enter Description
- Persistence:** Disabled

At the bottom, there are 'SAVE' and 'CANCEL' buttons.

# Configuring F5 Big-IP LTM

# 6

Before configuring your F5 device, it must be deployed in the environment with access to VMware Aria Suite components over a network.

---

**Note** Refer to the [Workspace One](#) load-balancing documentation to configure highly-available identity provider for VMware Aria Automation.

---

For configuration, the F5 device must meet these requirements:

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

If you are using an F5 LTM 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 LTM, see [HTTP health checks may fail even though the node is responding correctly](#).

This chapter includes the following topics:

- [Configure monitors](#)
- [Configure F5 server pools](#)
- [Configure F5 virtual servers](#)

## Configure monitors

It is required to add monitors for VMware Aria Automation, and for an external VMware Aria Automation Orchestrator (optional).

### Procedure

- 1 Log in to the F5 load balancer and navigate to **Local Traffic > Monitor**.

- 2 Click **Create** and configure the monitor as outlined in this table. Use the default value if nothing is specified.

**Table 6-1. Configure Monitors**

Name	Type	Interval	Timeout	Send String.	Receive String.	Alias Service Port
VMware Aria Automation	HTTP	3	10	GET /health HTTP/ 1.0\r\n\r\n	HTTP/1\.(0 1) (200)	8008
VMware Aria Automation Orchestrator	HTTP	3	10	GET /health HTTP/ 1.0\r\n\r\n	HTTP/1\.(0 1) (200)	8008
<p><b>Note</b> Use only for external VMware Aria Automation Orchestrator instances.</p>						

## Results

The configuration should look similar to this

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

**General Properties**

Name	vra_http_va_web
Description	
Type	HTTP
Parent Monitor	http

**Configuration:** Basic

Interval	3 seconds
Timeout	10 seconds
Send String	GET /health HTTP/1.0\r\n\r\n
Receive String	HTTP/1.\.(0 1) (200)
Receive Disable String	
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	8008 Other: <input type="text"/>
Adaptive	<input type="checkbox"/> Enabled

Cancel Repeat Finished

screen.

## Configure F5 server pools

It is required to configure service pools for VMware Aria Automation, and for an external VMware Aria Automation Orchestrator (optional).

### Procedure

- 1 Log in to the F5 load balancer and navigate to **Local Traffic > Pools**.

- Click **Create** and configure the pool as outlined in this table. Use the default value if nothing is specified.

**Table 6-2. Configure Server Pools**

Name	Health Monitors	Load Balancing Method	Node Name	Address	Service Port
VMware Aria Automation	VMware Aria Automation	Least Connections (member)	VA1 VA2 VA3	IP Address	443
VMware Aria Automation Orchestrator	VMware Aria Automation Orchestrator	Least Connections (member)	VA1 VA2 VA3	IP Address	443

**Note** Use only for external VMware Aria Automation Orchestrator instances.

- Enter each pool member as a **New Node** and add it to the **New Members** group.

**Results**

The configuration should look similar to this screen.

**Local Traffic » Pools : Pool List » pl\_vra-va-00\_443**

Properties | **Members** | Statistics

**Load Balancing**

Load Balancing Method: Least Connections (member)

Priority Group Activation: Disabled

Update

**Current Members**

<input checked="" type="checkbox"/>	Status	Member	Address	Service Port	FQDN	Ephemeral	Ratio	Priority Group
<input type="checkbox"/>	<span style="color: green;">●</span>	dz-vra8-node1.sof-mbu.eng.vmware.com:443	192.168.10.30	443		No	1	0 (Active)
<input type="checkbox"/>	<span style="color: green;">●</span>	dz-vra8-node2.sof-mbu.eng.vmware.com:443	192.168.10.31	443		No	1	0 (Active)
<input type="checkbox"/>	<span style="color: green;">●</span>	dz-vra8-node3.sof-mbu.eng.vmware.com:443	192.168.10.32	443		No	1	0 (Active)

Enable | Disable | Force Offline | Remove

## Configure F5 virtual servers

It is required to configure virtual servers for VMware Aria Automation, and for an external VMware Aria Automation Orchestrator (optional).

**Procedure**

- 1 Log in to the F5 load balancer and navigate to **Local Traffic > Virtual Servers**.
- 2 Click **Create** and configure the virtual server as outlined in this table. Use the default value if nothing is specified.

**Table 6-3. Configure Virtual Servers**

Name	Type	Destination Address	Service Port	Source Address Translation	Default Pool	Default Persistence Profile
VMware Aria Automation	Performance (Layer 4)	IP Address	443	Auto Map	VMware Aria Automation	None
VMware Aria Automation Orchestrator	Performance (Layer 4)	IP Address	443	Auto Map	VMware Aria Automation Orchestrator	None
<p><b>Note</b> Use only for external VMware Aria Automation Orchestrator instances.</p>						

- 3 (Optional) In cases where VMware Aria Operations is used you may need to expose the health check port as a virtual server. In order to achieve that click **Create** and configure a new virtual server as outlined in this table. Use the default value if nothing is specified:

Name	Type	Destination Address	Service Port	Source Address Translation	Default Pool	Default Persistence Profile
VMware Aria Automation	Performance (Layer 4)	IP Address	8008	Auto Map	VMware Aria Automation	None
VMware Aria Automation Orchestrator	Performance (Layer 4)	IP Address	8008	Auto Map	VMware Aria Automation Orchestrator	None
<p><b>Note</b> Use only for external VMware Aria Automation Orchestrator instances.</p>						

- 4 For an overall view and the status of the virtual servers, select **Local Traffic > Virtual Servers**.

**Results**

The configuration should look similar to these screens.



**General Properties**

Name	vs_vra-va-00_443
Description	
Type	Performance (Layer 4)
Source Address	<input checked="" type="radio"/> Host <input type="radio"/> Address List
Destination Address/Mask	<input checked="" type="radio"/> Host <input type="radio"/> Address List 192.168.10.33
Service Port	<input checked="" type="radio"/> Port <input type="radio"/> Port List 443 HTTPS
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
State	Enabled

**Configuration:** Basic

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

**Acceleration:** Basic

iSession Profile	None
Rate Class	None

**Resources**

iRules	Enabled	Available
	<input type="text"/>	<pre> /Common _sys_APM_ExchangeSupport_OA_BasicAuth _sys_APM_ExchangeSupport_OA_NtimAuth _sys_APM_ExchangeSupport_helper _sys_APM_ExchangeSupport_main                     </pre>
Default Pool	+ pl_vra-va-00_443	
Default Persistence Profile	None	
Fallback Persistence Profile	None	

Cancel Repeat Finished

● vs\_vra-va-00\_443

STATS DIAGRAM

List other virtual servers that share these pools  List other pools that use these nodes

Virtual Server

Pools

Pool Members

● vs\_vra-va-00\_443  
192.168.10.33:443

● pl\_vra-va-00\_443

● dz-vra8-node1.sof-mbu.er  
192.168.10.30

● dz-vra8-node2.sof-mbu.er  
192.168.10.31

● dz-vra8-node3.sof-mbu.er  
192.168.10.32

# Configuring Citrix ADC (NetScaler ADC)

# 7

Before you configure Citrix ADC, ensure the NetScaler device is deployed in the environment with access to the vRealize Components.

For configuration, the Citrix ADC must meet these requirements:

- You can use either a virtual or physical NetScaler.
- The Citrix load balancer can be deployed in either a one-arm or multi-arm topologies.
- Enable the load balancer and SSL modules by navigating to **NetScaler > System > Settings > Configure > Basic Features**.

This chapter includes the following topics:

- [Configure Citrix monitors](#)
- [Configure Citrix Service Groups](#)
- [Configure Citrix Virtual Servers](#)

## Configure Citrix monitors

You can configure a Citrix monitor by performing these steps.

### Procedure

- 1 Log in to the NetScaler load balancer and navigate to **NetScaler > Traffic Management > Load Balancing > Monitors**.

- Click **Add** and configure the monitor as outlined in this table. Use the default value if nothing is specified.

**Table 7-1. Configure Citrix Monitors**

Name	Type	Interval	Timeout	Retries	Success Retries	HTTP Request/Send String	Response Codes	Receive String	Dest. Port	Secure
VMware Aria Automation	HTTP	5	4	3	1	GET / health	200	None	8008	No
VMware Aria Automation Orchestrator	HTTP	5	4	3	1	GET / health	200	None	8008	No
<p><b>Note</b> Use only for external VMware Aria Automation Orchestrator instances.</p>										

## Results

The configuration should look similar to this

### ← Create Monitor

Name\*  
 ⓘ

Type\*  
 > ⓘ

**Basic Parameters**

Interval  
  ▾

Response Time-out  
  ▾ ⓘ

Response Codes  
 +  
 ×

Custom Header

HTTP Request  
 ⓘ

Secure

**Advanced Parameters**

Destination IP

Destination Port  
 ⓘ

Down Time  
  ▾

TROFS Code

TROFS String

Dynamic Time-out  
 ⓘ

Deviation  
  ▾

Dynamic Interval

Retries  
 ⓘ

screen.

## Configure Citrix Service Groups

You can configure service groups by performing these steps.

### Procedure

- 1 Log in to the NetScaler load balancer and navigate to **NetScaler > Traffic Management > Load Balancing > Service Groups**.
- 2 Click **Add** and configure the service groups as outlined in this table.

**Table 7-2. Configure Service Groups**

Name	Health Monitors	Protocol	SG Members	Address	Port
VMware Aria Automation	VMware Aria Automation	SSL Bridge	VA1 VA2 VA3	IP Address	443
VMware Aria Automation Orchestrator	VMware Aria Automation Orchestrator	SSL Bridge	VA1 VA2 VA3	IP Address	443
<p><b>Note</b> Use only for external VMware Aria Automation Orchestrator instances.</p>					

## Results

The configuration should look similar to this

← **Load Balancing Service Group**

Basic Settings			
Name	pl_vra-va-00_443	Cache Type	SERVER
Protocol	SSL_BRIDGE	Cacheable	NO
State	ENABLED	Health Monitoring	YES
Effective State	● UP	AppFlow Logging	ENABLED
Traffic Domain	0	Monitoring Connection Close Bit	NONE
Comment		Number of Active Connections	0
		AutoScale Mode	DISABLED

3 Service Group Members >

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

1 Service Group to Monitor Binding >

Done

screen:

## Configure Citrix Virtual Servers

You can configure virtual servers by performing these steps.

### Procedure

- 1 Log in to the NetScaler load balancer and navigate to **NetScaler > Traffic Management > Load Balancing > Virtual Servers**.

- Click **Add** and configure the virtual server as outlined in this table. Use the default value if nothing is specified.

**Table 7-3. Configure Virtual Servers**

	Name	Protocol	Destination Address	Port	Load Balancing Method	Service Group Binding
	VMware Aria Automation	SSL Bridge	IP Address	443	Least Connections	VMware Aria Automation
	VMware Aria Automation Orchestrator	SSL Bridge	IP Address	443	Least Connections	VMware Aria Automation Orchestrator
	<p><b>Note</b> Use only for external VMware Aria Automation Orchestrator instances.</p>					

- (Optional) In cases where vRealize Operations is used you may need to expose the health check port as a virtual server. Use the default value if nothing is specified. Click **Add** and configure new virtual server as outlined in this table.

	Name	Protocol	Destination Address	Port	Load Balancing Method	Service Group Binding
	VMware Aria Automation	HTTP	IP Address	8008	Least Connections	VMware Aria Automation
	VMware Aria Automation Orchestrator	HTTP	IP Address	8008	Least Connections	VMware Aria Automation Orchestrator
	<p><b>Note</b> Use only for external VMware Aria Automation Orchestrator instances.</p>					

**Results**

The configuration should look similar to this screen:

## ← Load Balancing Virtual Server

Load Balancing Virtual Server | [Export as a Template](#)

**Basic Settings** ✎

Name	vs_vra-va-00_443	Listen Priority	-
Protocol	SSL_BRIDGE	Listen Policy Expression	NONE
State	● UP	Redirection Mode	IP
IP Address	10.71.226.23	Range	1
Port	443	IPset	-
Traffic Domain	0	RHI State	PASSIVE
		AppFlow Logging	ENABLED
		Retain Connections on Cluster	NO

**Services and Service Groups**

**No** Load Balancing Virtual Server Service Binding >

**1** Load Balancing Virtual Server ServiceGroup Binding >

**Traffic Settings** ✎ ✕

Health Threshold	0	Priority Queuing	
Client Idle Time-out	180	Sure Connect	
Minimum Autoscale Members	0	Down State Flush	ENABLED
Maximum Autoscale Members	0	Layer 2 Parameters	OFF
ICMP Virtual Server Response	PASSIVE	Trofs Persistence	ENABLED

Done



# Configuring AVI Load Balancer



You can configure an AVI load balancer by performing these steps.

Ensure that you have deployed a Service Engine in the vCenter where the vRealize Automation instance is located and that the Service Engine interface is configured in the same network as the vRealize Automation.

This chapter includes the following topics:

- [Create a health monitor](#)
- [Create a pool](#)
- [Create virtual service VIP](#)
- [Configure virtual service](#)

## Create a health monitor

You can create an active monitor by following these steps.

### Procedure

- 1 Go to **Templates** tab, under the Profiles click the **Health Monitors** entry.

2 Click **Create** and enter the following details.

Appliance Name	Type	Interval	Timeout	Successful checks	Failed checks	Health Monitor Port	Client request header	Response code
VMware Aria Automation	HTTP	5	4	3	3	8008	GET / health HTTP/1.0	2XX
VMware Aria Automation Orchestrator	HTTP	5	4	3	3	8008	GET / health HTTP/1.0	2XX
<p><b>Note</b> Use for external VMware Aria Automation Orchestrator instances only.</p>								

vmw NSX-ALB

HEALTH MONITOR vra

### CREATE HEALTH MONITOR

vra

General HTTP Server Maintenance Mode RBAC

#### General

Name\* vra

Description  
Enter Description

Type HTTP

Is Federated

Send Interval 5 Seconds Receive Timeout 4 Seconds

Successful Checks 3 Failed Checks 3

CANCEL SAVE

vmw NSX-ALB

HEALTH MONITOR vra

### CREATE HEALTH MONITOR

vra

General HTTP Server Maintenance Mode RBAC

#### HTTP

Health Monitor Port 8008

#### Authentication

Authentication Type New Technology LAN Manager (NTLM)

#### Client Request Header

User Input GET /health HTTP/1.0

Converted Value Preview GET /health HTTP/1.0

Client Request Body

CANCEL SAVE

vmw NSX-ALB

HEALTH MONITOR vra

### CREATE HEALTH MONITOR

vra

General HTTP Server Maintenance Mode RBAC

## Create a pool

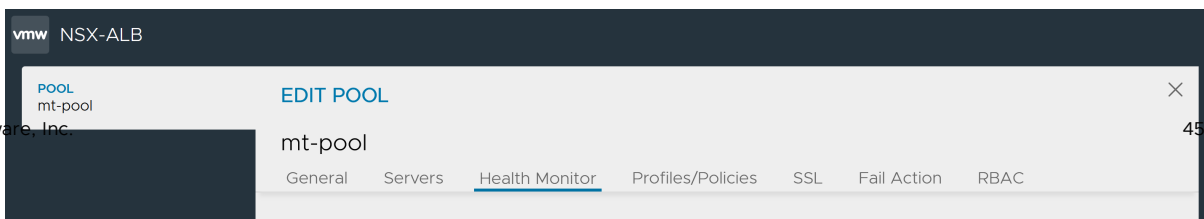
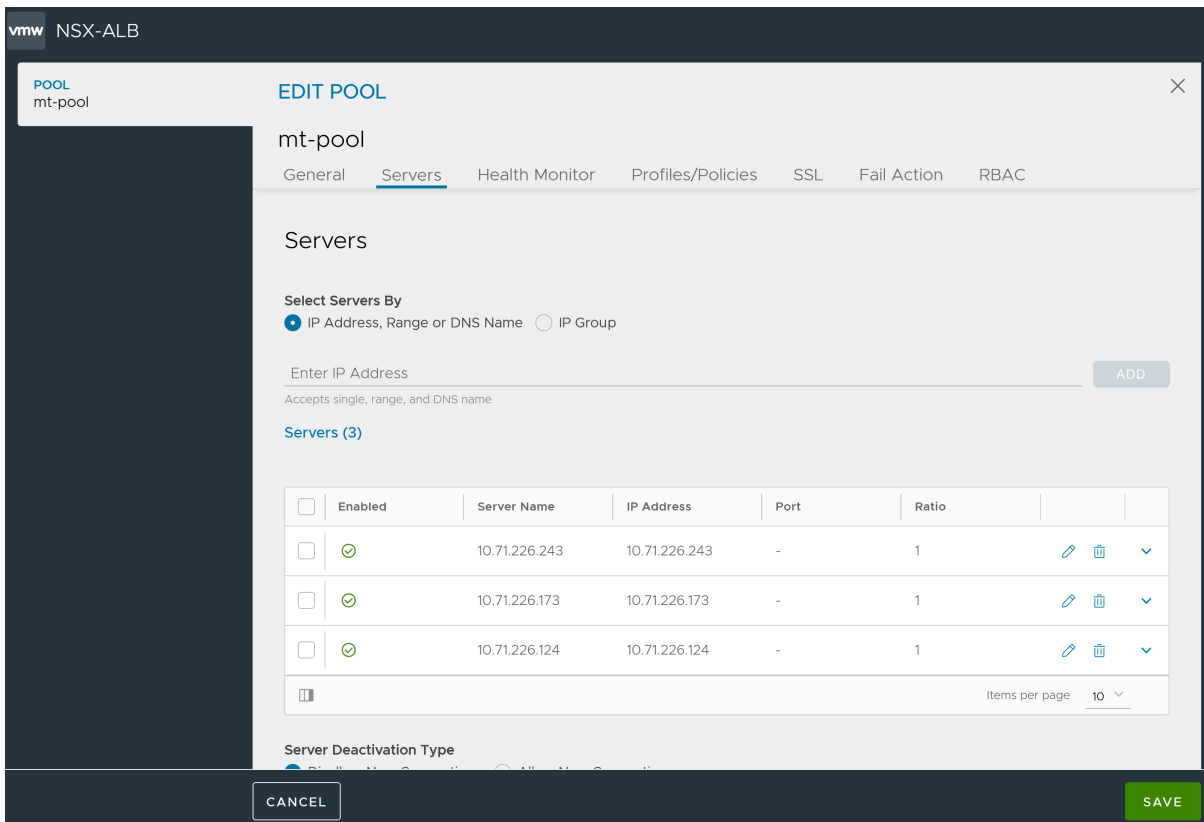
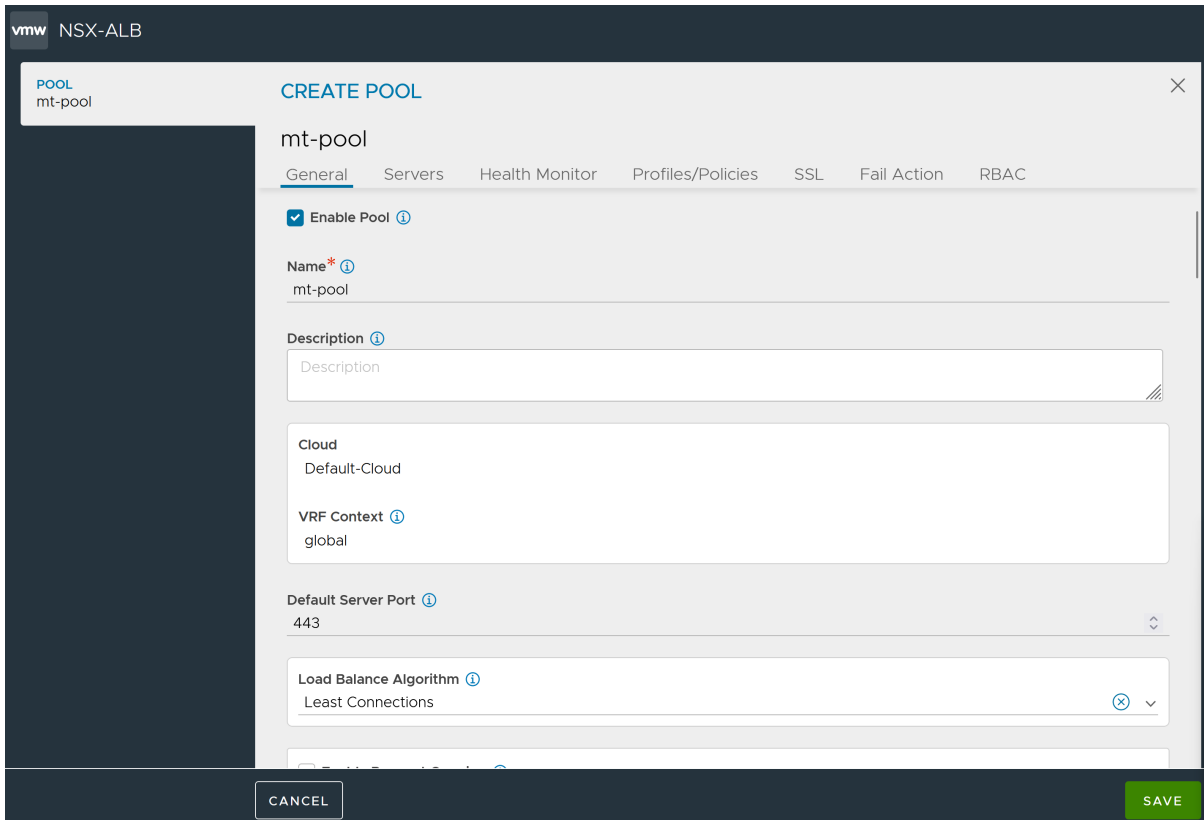
You can create pools for an AVI load balancer by performing the following steps.

### Procedure

- 1 Navigate to the **Menu** and click **Applications**.
- 2 Click the **Pool** tab and enter the following details.

Appliance Name	Default Server Port	Lookup Server by Name	Real time metrics
VMware Aria Automation	443	Enabled	Enabled
VMware Aria Automation Orchestrator	443	Enabled	Enabled
<b>Note</b> Use only for external VMware Aria Automation Orchestrator instances.			

3 Click **Next** and add servers to the pool.



## Create virtual service VIP

Before creating a virtual service, you must create a virtual service VIP.

### Procedure

- 1 Select **Applications**.
- 2 Select **VS VIPs**
- 3 Select **Create**.
- 4 Respond to prompts in the creation wizard with the following information:

Appliance Name	Name	IPv4 Address	Placement Network
VMware Aria Automation	Name of the VIP	Enter the IPv4 Address	Click <i>Add</i> and Select <i>Placement Network</i> from the list
VMware Aria Automation Orchestrator	Name of the VIP	Enter the IPv4 Address	Click <i>Add</i> and Select <i>Placement Network</i> from the list
<p><b>Note</b> Use only for external VMware Aria Automation Orchestrator instances.</p>			

### Example

Use the following screens as reference only.

vmw NSX-ALB

VS VIP  
vra-test-vs-VsVip

**CREATE VS VIP** |

vra-test-vs-VsVip

General RBAC

General

Name\*   
vra-test-vs-VsVip

Cloud  
Default-Cloud

VRF Context   
global

VIPs (0)\*

ADD

<input type="checkbox"/>	Enabled	VIP ID	IP Address	IPv6 Address
We couldn't find any objects!				

Items per page 10

BGP Peer Labels

CANCEL SAVE

vmw NSX-ALB

VS VIP  
vra-test-vs-VsVip

VIP  
1

**EDIT VIP** |

1

General

Enable VIP

Private IP

IPv4 Address\*   
10.71.226.220

IPv6 Address   
Enter IPv6 Address

Placement Network (1)

ADD

<input type="checkbox"/>	Network	IPv4 Subnet	IPv6 Subnet
<input type="checkbox"/>	10.71.226 (vlan1226) (DHCP+Static)	10.71.226.0/24	-

Items per page 10

CANCEL SAVE

vmw NSX-ALB

VS VIP  
vra-test-vs-VsVip

CREATE VS VIP | [icon] [icon]

vra-test-vs-VsVip

General RBAC

General

Name\* ⓘ  
vra-test-vs-VsVip

Cloud  
Default-Cloud

VRF Context ⓘ  
global

VIPs (1)\* ⓘ

ADD

<input type="checkbox"/>	Enabled	VIP ID	IP Address	IPv6 Address	
<input checked="" type="checkbox"/>	✓	1	10.71.226.220	-	[edit] [delete]

Items per page 10

BGP Peer Labels ⓘ

CANCEL SAVE

## Configure virtual service

You can configure virtual service for an AVI load balancer by following these steps.

To configure virtual service:

### Procedure

- 1 From the menu, click **Applications**.
- 2 Click the **Virtual Services** tab, and then click **Create Virtual Service**.



3 Enter these configuration details.

Appliance Name	VS VIP	TCP/UDP Profile	Application Profile	Services	Pool
VMware Aria Automation	VIP Address or FQDN	System-TCP-Proxy	System-L4-Application	443	vRealize Automation
VMware Aria Automation Orchestrator	VIP Address or FQDN	System-TCP-Proxy	System-L4-Application	443	vRealize Orchestrator

**Note** Use for external VMware Aria Automation Orchestrator instances only.

Figure 8-1.

The screenshot shows the configuration page for a Virtual Server (VS) in VMware Aria Automation. The interface includes the following sections:

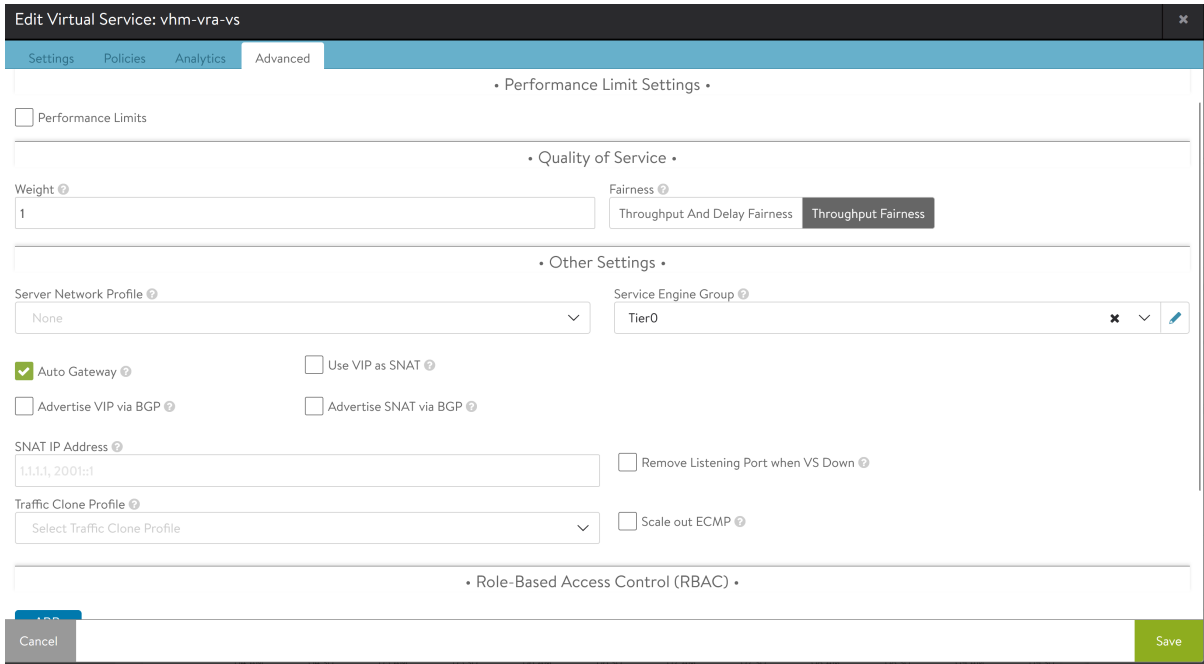
- General:** Name (mt-vs), Enabled (checked), Traffic Enabled (checked).
- VIP Address:** VS VIP (10.71.226.220).
- Profiles:** TCP/UDP Profile (System-TCP-Proxy), Application Profile (System-L4-Application).
- Service Port:** Services (443), with an option to "Switch to Advanced" and a "+ Add Port" button.
- Pool:** Pool (selected), Pool Group (unselected), Pool (mt-vs-pool), and an option to "Ignore network reachability constraints for the server pool" (unchecked).
- Other Settings:** Description field.

Buttons for "Cancel" and "Save" are located at the bottom of the configuration form.

4 Click **Next** to navigate to the **Advanced** tab and enter the following information.

Appliance Name	Service Engine Group	Use VIP as SNAT
VMware Aria Automation	SE Group where the appropriate SE is located	Enabled and Disabled are supported
VMware Aria Automation Orchestrator	SE Group where the appropriate SE is located	Enabled and Disabled are supported

**Note** Use for external VMware Aria Automation Orchestrator instances only.



- (Optional) In cases where VMware Aria Operations is used you may need to expose the health check port as a virtual server. In order to do that create a new virtual server by clicking the **Virtual Services** tab, and then click **Create Virtual Service**. Use the information from the table below to achieve that:

Appliance Name	VS VIP	TCP/UDP Profile	Application Profile	Services	Pool
VMware Aria Automation	VIP Address or FQDN	System-TCP-Proxy	System-L4-Application	8008	vRealize Automation
VMware Aria Automation Orchestrator	VIP Address or FQDN	System-TCP-Proxy	System-L4-Application	8008	vRealize Orchestrator

**Note** Use for external VMware Aria Automation Orchestrator instances only.

Click **Next** to navigate to the **Advanced** tab and enter the following information

Appliance Name	Server Network Profile	SE Group	Use VIP, as SNAT
VMware Aria Automation	System-TCP-Proxy	SE Group where the appropriate SE is located	Enabled and Disabled are supported
VMware Aria Automation Orchestrator <b>Note</b> Use for external VMware Aria Automation Orchestrator instances only.	System-TCP-Proxy	SE Group where the appropriate SE is located	Enabled and Disabled are supported

In this section you can find various of known problematic scenarios and common errors.

This chapter includes the following topics:

- Errors during VMware Aria Automation installation when using NSX-V as a load-balancer for Workspace ONE
- Provisioning failures when using OneConnect with F5 BIG-IP
- F5 BIG-IP license limits network bandwidth
- FortiGate specifics

## Errors during VMware Aria Automation installation when using NSX-V as a load-balancer for Workspace ONE

If you see errors when installing VMware Aria Automation while using Workspace ONE as load-balancer, follow these troubleshooting steps.

When using NSX-V as a load-balancer for VMware Workspace ONE there might be specific network limitations which will result in errors and timeouts during the installation of VMware Aria Automation similar to:

```
2020-06-30 09:10:08.751+0000 INFO 16 --- [or-http-epoll-3]
com.vmware.identity.rest.RestClient : POST https://default-49-29.sqa.local/SAAS/API/1.0/
oauth2/token?grant_type=client_credentials
2020-06-30 09:10:08.755+0000 WARN 16 --- [or-http-epoll-3]
r.netty.http.client.HttpClientConnect : [id: 0x754860c7, L:/10.244.0.206:48686 !
R:default-49-29.sqa.local/10.198.49.29:443] The connection observed an error
reactor.netty.http.client.PrematureCloseException: Connection prematurely closed BEFORE
response
```

You can mitigate those errors by extending the NSX-V idle connection close time to 5 minutes instead of the default of 1 second.

This can be achieved with an application rule containing the following:

```
timeout http-keep-alive 300s
```

## Provisioning failures when using OneConnect with F5 BIG-IP

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 navigate to **Local Traffic > Virtual Servers > Virtual Servers List**.
- 2 Click the name of the virtual server you want to modify.
- 3 In the **Acceleration** section, select **None** for the **OneConnect Profile**.
- 4 Click **Finish**.

## F5 BIG-IP license limits network bandwidth

You might experience provisioning failures or problems loading VMware Aria Automation console pages due to load balancer network traffic exceeding the F5 BIG-IP license limit.

To check if the BIG-IP platform is experiencing this problem, see [How the BIG-IP VE system enforces the licensed throughput rate](#).

## FortiGate specifics

Applicable for cases where there is a Fortigate Firewall between the Load balancer and the vRealize Automation cluster nodes.

FortiGate firewall has service interface listening on 8008 and 8010 ports. In case there is a FortiGate firewall between the load balancer (of all kinds) and the VMware Aria Automation nodes, the monitoring would send requests to the port 8008 of the firewall and thus become invalid.

The obvious solution is to change the configuration of the FortiGate firewall so it wouldn't listen on 8008.

Any other solution (like creating a DNAT on the firewall and changing the above mentioned best practice settings) would be considered unsupported and should be performed at personal risk