USER GUIDE

Brocade Services Director Getting Started Guide, 17.2

Supporting Brocade Services Director 17.2

53-1005003-01
8 May 2017

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. assume no liability or responsibility to any person or entity with respect to the accuracy of this document or any loss, cost, liability, or damages arising from the information contained herein or the computer programs that accompany it.

The product described by this document may contain open source software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit http://www.brocade.com/support/oscd.

Contents

Preface

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Brocade technical documentation.

Notes, cautions, and warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE
A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

⚠ CAUTION
A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

⚠ DANGER
A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used to highlight specific words or phrases.

Format	Description
bold text	Identifies command names. Identifies keywords and operands. Identifies the names of GUI elements. Identifies text to enter in the GUI.
italic text	Identifies emphasis. Identifies variables. Identifies document titles.
`Courier font`	Identifies CLI output.

Format	Description
	Identifies command syntax examples.

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
value	In Fibre Channel products, a fixed value provided as input to a command option is printed in plain text, for example, **--show** WWN.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options. In Fibre Channel products, square brackets may be used instead for this purpose.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Brocade resources

Visit the Brocade website to locate related documentation for your product and additional Brocade resources.

White papers, data sheets, and the most recent versions of Brocade software and hardware manuals are available at www.brocade.com. Product documentation for all supported releases is available to registered users at MyBrocade.

Click the **Support** tab and select **Document Library** to access product documentation on MyBrocade or www.brocade.com. You can locate documentation by product or by operating system.

Release notes are bundled with software downloads on MyBrocade. Links to software downloads are available on the MyBrocade landing page and in the Document Library.

Document feedback

Quality is our first concern at Brocade, and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. You can provide feedback in two ways:

- Through the online feedback form in the HTML documents posted on www.brocade.com
- By sending your feedback to documentation@brocade.com

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Contacting Brocade Technical Support

As a Brocade customer, you can contact Brocade Technical Support 24x7 online or by telephone. Brocade OEM customers should contact their OEM/solution provider.

Brocade customers

For product support information and the latest information on contacting the Technical Assistance Center, go to www.brocade.com and select **Support**.

If you have purchased Brocade product support directly from Brocade, use one of the following methods to contact the Brocade Technical Assistance Center 24x7.

Online	Telephone
Preferred method of contact for non-urgent issues: • Case management through the MyBrocade portal. • Quick Access links to Knowledge Base, Community, Document Library, Software Downloads and Licensing tools	Required for Sev 1-Critical and Sev 2-High issues: • Continental US: 1-800-752-8061 • Europe, Middle East, Africa, and Asia Pacific: +800-AT FIBREE (+800 28 34 27 33) • Toll-free numbers are available in many countries. • For areas unable to access a toll-free number: +1-408-333-6061

Brocade OEM customers

If you have purchased Brocade product support from a Brocade OEM/solution provider, contact your OEM/solution provider for all of your product support needs.

- OEM/solution providers are trained and certified by Brocade to support Brocade® products.
- Brocade provides backline support for issues that cannot be resolved by the OEM/solution provider.
- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information, contact Brocade or your OEM.
- For questions regarding service levels and response times, contact your OEM/solution provider.

About This Document

Services Director VA Overview

The Services Director Virtual Appliance (Services Director VA) enables you to configure and manage the Services Director as a virtual appliance. The Services Director VA provides a graphical user interface (GUI) that enables you to:

- Register externally-deployed Traffic Manager instances.
- Deploy Traffic Manager instance hosts.
- Deploy and license Traffic Manager instances using an instance host.
- Deploy and license cloud-based Traffic Manager instances on AWS.
- Transition deployed Traffic Manager instances through a lifecycle.
- Start, stop and restart your Services Director service.
- Protect your instance configurations (on a cluster basis) by taking automated and manual backups.
- Protect your Services Director configuration using a backup system.
- Protect your Traffic Manager passwords using encryption based on a Master Password.
- Perform health and monitoring reporting.
- Perform usage metering.
- Generate system logs and system dumps.

NOTE
Support for individual functions depends on your license type.

NOTE
The GUI is the main interface for the Services Director VA. However, a Command-Line Interface (CLI) is also included. The CLI is described in the *Brocade Services Director Command Reference*.

Using the Getting Started Guide

This manual guides you through the installation, configuration and use of your Services Director VA. It is intended to be both:

- An end-to-end process guide. If you progress through the chapters in order, you will have a fully configured high availability Services Director VA.
- A reference guide for specific functional areas.

The structure of the manual is as follows:

- Installing the Brocade Services Director VA on page 13: Describes the Services Director VA installation process, and the use of the configuration Setup Wizard.
- Adding Traffic Managers to the Services Director on page 67: Describes the process of adding externally-deployed Traffic Manager instances to the Services Director VA. This includes manual registrations, the processing of self-registration requests, and the creation of cloud-based Traffic Manager instances.

NOTE
The installation and configuration of an instance host, and the deployment of Traffic Manager instances is described in the *Brocade Services Director Advanced User Guide*.

- Working with Traffic Managers on page 131: Describes how Traffic Manager instances are represented in the Services Director VA, methods for affecting this representation, and the lifecycle of externally-deployed Traffic Manager instances.

  NOTE
  The operation of traffic management and load balancing on individual Traffic Manager instances is not addressed by the Services Director. This requires use of a Brocade Virtual Traffic Manager for each Traffic Manager instance.

- Working with High Availability on page 199: Describes how to operate a High Availability (HA) pair of Services Director VA nodes. This includes monitoring of status, error conditions, and methods for returning your HA pair to operation.
- Recovering from a Services Director Failure on page 237: Describes how to preserve the configuration of an HA pair, and how to recover a saved configuration for an existing Services Director VA. This also includes how to create a new Services Director VA from a saved configuration.
- Creating and Delivering Services Director Reports on page 257: Describes how to generate and extract output from your Services Director VA. This includes metering logs and system logs.

Installing the Brocade Services Director VA

Installation Overview

The Services Director VA is installed as a virtual machine (VM) using a VMware or KVM-QEMU hypervisor. After the Services Director VA is installed, you use a setup wizard to configure the Services Director VA for use.

Prerequisites

Before you install the Services Director VA and run the Setup Wizard, you must make sure that you have the correct software, files and configuration information.

Required Software for Installation

You need the software listed in the following table to install the Services Director VA using a VMware hypervisor.

Software	Description
VMware vSphere ESXi 5.0+	Brocade assumes that you are familiar with creating and managing VMs using vSphere. For detailed information about creating virtual machines using vSphere, refer to http://www.vmware.com/products/.
Services Director VMware image in OVA format	This image is used to install the Services Director VA. You can obtain the Services Director OVA package from Brocade Support at http://www.brocade.com/en/support.html.

You need the software listed in the following table to install the Services Director VA using a KVM-QEMU hypervisor.

Software	Description
A virtualization toolset, such as libvirt or Virtual Machine Manager (VMM)	Brocade assumes that you are familiar with creating and managing VMs using your chosen toolset. For detailed information about creating virtual machines on KVM-QEMU, refer to http://wiki.qemu.org/KVM.
Services Director KVM image in QCOW2 format	This image is used to install the Services Director VA on a KVM-QEMU hypervisor. You can obtain the Services Director KVM image in QCOW2 format from Brocade Support at http://www.brocade.com/en/support.html.

Required Resources for Virtual Machines

The following table lists the resources required by the Services Director VA .

VA Type	CPU	Memory	Disk
Services Director VA	4 vCPU	8 GB	46 GB

The following table lists the resources required by instance host VAs.

VA Type	CPU	Memory	Disk
Instance Host VA (Small Flavor)	2 vCPU	4 GB	70 GB
Instance Host VA (Large Flavor)	8 vCPU	16 GB	70 GB

Your hardware must support the required configuration.

Required Files and Information

The following table lists the files and information required by the Services Director VA.

NOTE
All required files must be in accessible locations in your infrastructure during the installation process. For example, locate the files on an accessible server, or your local machine.

Information	Description
Hostnames	The hostname for the Services Director. When you are creating a High Availability pair, you will need a hostname for both the Primary and the Secondary Services Director nodes.
DNS Server	(Optional) The IP address for the primary name server. This is not required if you choose to configure your system using IP addresses rather than DNS hostnames. You can also specify a secondary name server if required.
Primary Address	The IP address for the Primary Services Director in a High Availability pair.
Secondary Address	The IP address for the Secondary Services Director in a High Availability pair.
Service Endpoint Address	The Management IP address for your High Availability Services Director installation. This IP address binds to the currently active Services Director.
SSL certification and private key	A self-signed Secure Socket Layer (SSL) certificate and private key file, which are used to protect and authenticate the REST API port. This is a local file or URL using HTTP, FTP, or SCP. For example: `scp://username:password@host/path/filename` Brocade recommends that you do not use a CA-signed certificate.
Services Director License	The Services Director License, either for Cloud Service Providers or Enterprise customers. Refer to Obtaining Services Director Licenses on page 17. NOTE If you have not received your Services Director License, contact Brocade for assistance.

Information	Description
Bandwidth Pack Licenses and Add-On Licenses	For Enterprise Services Director Licenses only. Refer to Obtaining Services Director Licenses on page 17. NOTE If you have not received your Bandwidth Pack or Add-On Licenses, contact Brocade for assistance.
Legacy FLA License	(Optional) The Flexible Licensing Architecture (FLA) Legacy License is for: • Any Traffic Manager instances at version 10.0 or earlier. • Any Traffic Manager instances that do not have an enabled REST API. Refer to Obtaining Services Director Licenses on page 17. Traffic Managers that are at version 10.1 (or later) with their REST API enabled will use a pre-installed Universal License.
Administrator user and password	The administrator password for the Services Director. This password is used to access the Services Director GUI and CLI. The default administrator user is **admin** and the password is **password**.
SMTP server and port	(Optional) The hostname (or IP address if DNS is not configured) of the SMTP server and port. External DNS and external access for SMTP traffic is required for email notification of events and failures to function.
Email notification address	(Optional) A valid email address to which notification of events and failures are to be sent.

Critical Ports That Must Be Open

The following table lists ports must be open on the Services Director VA.

Port	Open to Connections From	Description	Protocol
22	Any machine that may legitimately need to access the Services Director CLI.	The SSH port used by the CLI.	TCP
443	Any machine that may legitimately need to access the Services Director GUI.	The graphical user interface (GUI).	TCP
8100	Any machine that may legitimately need to access the Services Director REST API, including HA pair peer and vTMs using Legacy FLA.	The Services Director REST API. Also used for licensing Traffic Managers that use Legacy FLA Licensing.	TCP
8101	vTMs using Universal FLA.	The Services Director licensing server port. Used for licensing Traffic Managers that use Universal FLA Licensing.	TCP
9090	Services Director HA pair peer.	Used for High Availability operations.	TCP
9080	Services Director HA pair peer.	Used for High Availability operations.	TCP
3306	Services Director HA pair peer.	Used for High Availability operations.	TCP

Port	Open to Connections From	Description	Protocol
9070	Services Director HA pair peer.	Used for High Availability operations.	TCP
24007	Services Director HA pair peer.	Used for High Availability operations.	TCP
24009-24012	Services Director HA pair peer.	Used for High Availability operations.	TCP

The following table lists ports must be open on all Traffic Manager instances.

Port	Description	Protocol
9070	The REST API port.	TCP
9080	The control port used for cluster operations.	TCP
9090	The graphical user interface (GUI).	TCP

Installing and Configuring the Services Director VA on VMware

Perform the following procedure to install and configure the Services Director VA on VMware.

NOTE
All required files must be in accessible locations in your infrastructure during the installation process. For example, locate the files on an accessible server, or your local machine.

NOTE
This procedure assumes that you have DHCP or DNS enabled as required by your network.

1. Obtain the Services Director OVA package from Brocade Support. Refer to Obtaining the Services Director VA OVA Package on page 16.
2. Obtain the Services Director license from your Brocade account team. For details about obtaining your license keys, refer to Obtaining Services Director Licenses on page 17.
3. Install the Services Director OVA package on vSphere to create the Services Director VA. Refer to Creating a VM in vSphere on page 17.
4. Power on the Services Director VA in vSphere and access the Services Director VA with any browser, using its HTTP URL. Log in using the default username (**admin**) and password (**password**).
5. The Setup Wizard runs automatically. Use the wizard to configure your Primary Services Director. Refer to Installing and Configuring the Services Director VA Using the Setup Wizard on page 28.
6. Repeat this process for the Secondary Services Director to form an HA pair.

Obtaining the Services Director VA OVA Package

The Services Director VA is provided by Brocade Support as an OVA package that contains the VMX and VMDK files necessary to create virtual resources. The Services Director OVA package enables you to create a Services Director VA on ESXi.

You obtain the Services Director OVA package from Brocade support at http://www.brocade.com/en/support.html.

Obtaining Services Director Licenses

License tokens are automatically emailed to you when you order your product. If you have not received your license tokens, contact your Brocade sales representative.

> NOTE
> If you need assistance locating your local Brocade sales representative, visit https://www.brocade.com/en/how-to-buy.html.

You must redeem your license tokens at the Brocade License Redemption Portal at https://my.brocade.com. To redeem a license token you must have a support site login and password, and a self-signed SSL certificate.

> NOTE
> You cannot use a CA-signed certificate.

All licenses are emailed to you as attachments.

> NOTE
> You will receive a Legacy FLA License as part of the redemption process. However, if you intend to use only Traffic Manager instances that are at version 10.1 (or later), each with its REST API enabled, you do not need to install this Legacy FLA license. You will instead use a Universal License that comes pre-installed with the Services Director.

Creating a VM in vSphere

To create a virtual machine (VM) in vSphere, you must install the Services Director OVA package on a VMware ESXi host using the vSphere client.

> NOTE
> You must be familiar with installing, configuring, and managing VMs using VMware vSphere. The following instructions may vary. For detailed information about creating a VM in vSphere, refer to http://www.vmware.com/products/vsphere-hypervisor/.

1. Log in to vSphere.
2. Click **File** > **Deploy OVF template**. The deployment wizard starts.
3. On the **Source** page, click **Browse** , select the OVA package, click **Open** and then click **Next**.
4. On the **OVF Template Details** page, verify that the OVA package is the one you want to deploy and click **Next**.
5. On the **Name and Location** page, enter a **Name** for the VM and click **Next**.
6. On the **Host/Cluster** page, select a host datastore. This will store the VM and its virtual disk files. Then, click **Next**.

   > NOTE
   > Ensure that the host datastore you select has enough capacity to install the OVA package. See Required Resources for Virtual Machines on page 14.

7. On the **Storage** page, select the required destination storage and a datastore, and click **Next**.
8. On the **Disk Format** page, select the **Thick provisioned** format and click **Next** to pre-allocate all storage.
9. On the **Network Mapping** page, map your VMNetworkLAN source network to a destination network using the pull-down list. Then, click **Next**.

   > NOTE
   > There is no need to connect the auxiliary interface. The auxiliary interface can be safely disconnected in the Virtual Machine settings after initial deployment, because this interface is not used by the Brocade Services Director.

10. On the **Ready to Complete** page, verify the deployment settings, select the **Power on after deployment** check box if required, and click **Finish**.
11. When the deployment finishes, click **Close**. The new VM appears under the VM inventory.

    You can now configure the Services Director VA using the Setup Wizard, refer to Installing and Configuring the Services Director VA Using the Setup Wizard on page 28.

Accessing the Services Director VA on VMware

To access the Services Director VA, you need the IP address of its management interface.

If DHCP is available, you need to find out the allocated IP address. To do this:

1. Log in to the Services Director VA using the vSphere console.
2. Do not use the jumpstart setup wizard.
3. Obtain the allocated DHCP IP address of the VA using the following commands:

```
<host> > enable
<host> # show interfaces
```

If DHCP is not available:

1. Log in to the Services Director VA using the vSphere console.
2. Use the jumpstart setup wizard.
3. Set a static IP address, netmask and the default gateway IP address.

You can now access the Services Director VA with a browser, using the Services Director VA's IP address. Configure the Services Director VA using the Setup Wizard, refer to Installing and Configuring the Services Director VA Using the Setup Wizard on page 28.

Installing and Configuring the Services Director VA on KVM-QEMU

The Brocade Services Director Virtual Appliance is supported for production use on the KVM-QEMU hypervisor running on either an Ubuntu 14.04 or a RHEL/CentOS 6.x/7.x server.

The Services Director VA is available on KVM-QEMU as a 64-bit version only.

Perform the following steps to install and configure the Services Director VA on KVM-QEMU.

NOTE
All required files must be in accessible locations in your infrastructure during the installation process. For example, locate the files on an accessible server, or your local machine.

NOTE
This procedure assumes that you have DHCP or DNS enabled as required by your network.

1. Obtain the Services Director Kernel Virtual Machine (KVM) image in QCOW2 format from Brocade Support. Refer to Obtaining the Services Director VA KVM Image on page 19.
2. Obtain the Services Director license from your Brocade account team. For details about obtaining your license keys, refer to Obtaining Services Director Licenses on page 17.

3. Prepare a server that supports KVM. Supported servers are Ubuntu 14.04 and RHEL/CentOS 6.x/7.x.
4. Install the Services Director QCOW2 virtual machine on your server. This process creates the Services Director VA. Refer to Creating the Services Director VA on a KVM Server on page 19.
5. Access the Services Director VA. Refer to Accessing the Services Director VA on KVM on page 27.
   The setup wizard runs automatically.
6. Use the setup wizard to configure your Primary Services Director. Refer to Installing and Configuring the Services Director VA Using the Setup Wizard on page 28.
7. Repeat steps 3 - 6 for the Secondary Services Director to form a High Availability (HA).

Obtaining the Services Director VA KVM Image

The Services Director VA is provided by Brocade Support as a KVM image in QCOW2 format. This image contains the files necessary to create a Services Director VA on a KVM-QEMU hypervisor on all supported server platforms.

You obtain the Services Director KVM image in QCOW2 format from Brocade Support at http://www.brocade.com/en/support.html.

Obtaining Services Director Licenses

License tokens are automatically emailed to you when you order your product. If you have not received your license tokens, contact your Brocade sales representative.

> NOTE
> If you need assistance locating your local Brocade sales representative, visit https://www.brocade.com/en/how-to-buy.html.

You must redeem your license tokens at the Brocade License Redemption Portal at https://my.brocade.com. To redeem a license token you must have a support site login and password, and a self-signed SSL certificate.

> NOTE
> You cannot use a CA-signed certificate.

All licenses are emailed to you as attachments.

> NOTE
> You will receive a Legacy FLA License as part of the redemption process. However, if you intend to use only Traffic Manager instances that are at version 10.1 (or later), each with its REST API enabled, you do not need to install this Legacy FLA license. You will instead use a Universal License that comes pre-installed with the Services Director.

Creating the Services Director VA on a KVM Server

To create the Services Director VA on a KVM server, you must install the Services Director KVM image on a KVM server. There are many virtualization systems in common use; the following two examples describe the installation of your Services Director VA:

- Using the command line interface (CLI) of the libvirt toolset. Refer to Creating a VM Using the libvirt Command Line Interface on page 20.

  For detailed information about libvirt, refer to https://libvirt.org/.
- Using the graphical user interface (GUI) of the Virtual Machine Manager graphical toolset. Refer to Creating a VM Using the VMM Graphical User Interface on page 21.

  For detailed information about VMM, refer to https://virt-manager.org/.

However your image is installed, the following settings must be used for the virtual machine:

- X86_64 architecture.
- Four virtual CPUs.
- 8192 MB (8 GB) of memory.
- Write-through caching mode.
- Two Ethernet adapters with an e1000 model, connected using a bridge.
- A hard drive with IDE or VIRTIO bus type for the KVM image in QCOW2 format.

NOTE
The installation and configuration of your chosen toolset is outside the scope of this document. Refer to your tool's documentation for details.

Creating a VM Using the libvirt Command Line Interface

NOTE
To perform this procedure, you must have the required tools installed on a KVM-QEMU hypervisor, and be familiar with installing, configuring, and managing VMs.

1. Copy the KVM image to an appropriate designated directory (storage pool). Your System Administrator determines which storage pool to use. Give the file a unique name. For example, the filename might be of the form “image_xx.qcow2”. Images can only be used once.
   For the purposes of this example, this directory is `/vms/pool/sd0`.
2. Install the required VM by issuing a **virt-install** command using the following syntax:

```
virt-install --import
   --name=<servicedirector_name>
   --disk <image_pool_path>/image.qcow2,format=qcow2,bus=<bus>,cache=writethrough
   --os-type=linux
   --network bridge=<bridge_name>,model=<model for primary interface>
   --network bridge=<bridge_name>,model=<model for auxiliary interface>
   --ram=8192 --arch=x86_64 --vcpus=4
```

   Where **bus** can be set to either 'ide' or 'virtio'.

   For example:

```
virt-install --import
   --name=sd_kvm_07
   --disk /vms/pool/sd0/image.qcow2,format=qcow2,bus=ide,cache=writethrough
   --os-type=linux
   --network bridge=br0,model=e1000
   --network bridge=br0,model=e1000
   --ram=8192 --arch=x86_64 --vcpus=4
```

   NOTE
   After the installation completes, a number of background initialization tasks take place. As a result, the CLI will offer reduced functionality for a short period. Brocade recommends waiting at least two minutes before attempting to access the Services Director.

3. List the VMs on this hypervisor:

   ```
   virsh list
   ```

   The response includes your VM (along with other VMs, if any):

   ```
    Id   Name                 State
   --------------------------------
    356  pchaudh-07           running
    542  sramakrishnan-0b     running
    593  sd_kvm_07            running
   ```

4. Access the console of the VM you have just deployed:

   ```
   virsh console <vm_name>
   ```

   For example:

   ```
   virsh console sd_kvm1
   ```

   NOTE
   To exit the console, use ctrl+].

Creating a VM Using the VMM Graphical User Interface

NOTE
To perform this procedure, you must have the required tools installed on a KVM-QEMU hypervisor, and be familiar with installing, configuring, and managing VMs.

1. Copy the KVM image to an appropriate designated directory (storage pool). Your System Administrator determines which storage pool to use. The image filename must be “image.qcow2”.

   For the purposes of this example, this directory is `/var/lib/libvirt/images`.
2. Start the VMM GUI:

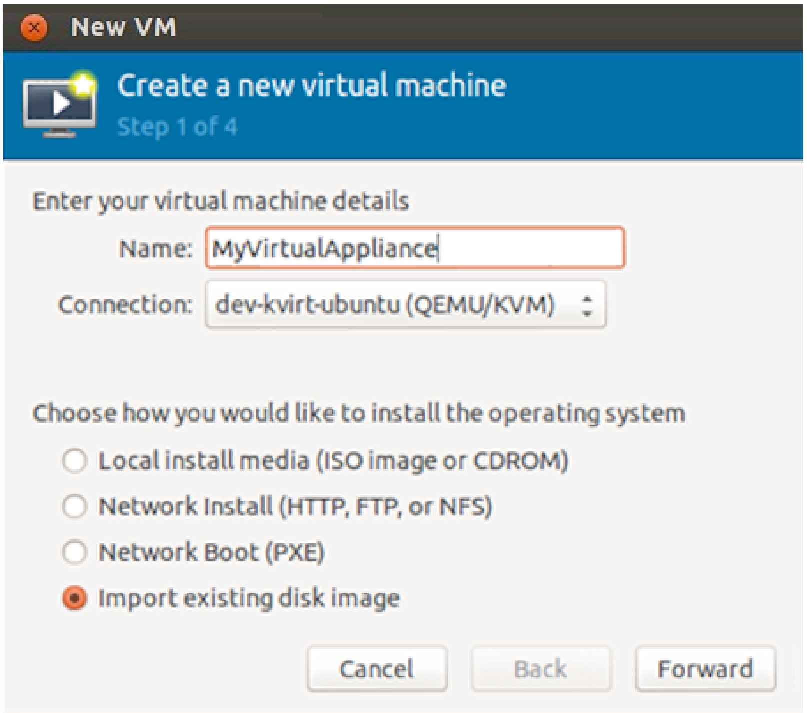
   ```
   virt-manager --connect=qemu+ssh://my-kvm-host.com/system
   ```

   In this command, “my-kvm-host.com” is the host machine name. An SSH tunnel is used to connect to the KVM-QEMU host. You must have an SSH account and corresponding public key stored on this machine for authentication.

   Refer to the VMM documentation for information on alternative connection methods.

3. Click **New** to start the process of creating a new virtual machine.

FIGURE 1 Creating a New Virtual Machine Wizard: 1 of 4



New VM

Create a new virtual machine

Step 1 of 4

Enter your virtual machine details

Name: MyVirtualAppliance

Connection: dev-kvirt-ubuntu (QEMU/KVM)

Choose how you would like to install the operating system

○ Local install media (ISO image or CDROM)

○ Network Install (HTTP, FTP, or NFS)

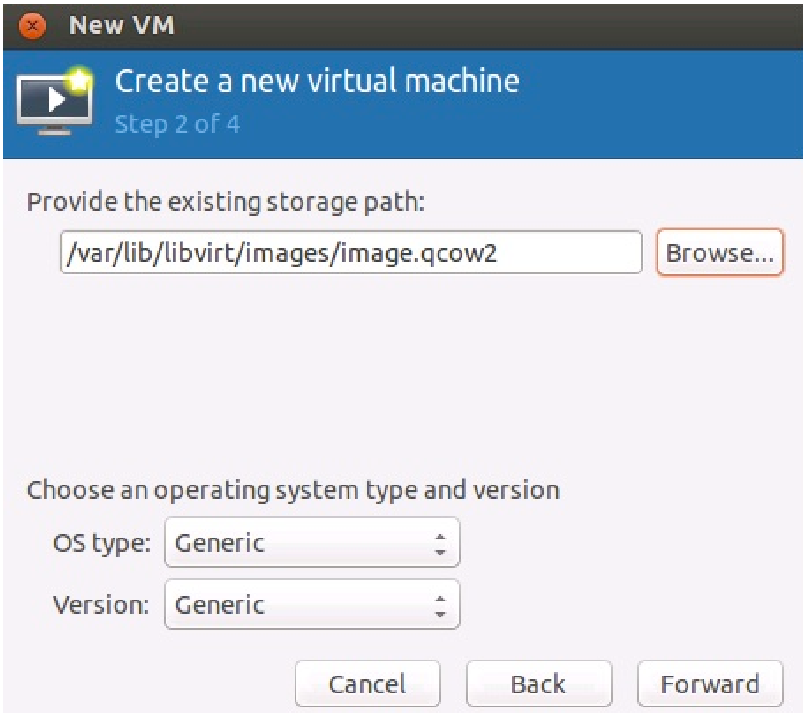
○ Network Boot (PXE)

● Import existing disk image

4. Enter a **Name** for your virtual appliance that corresponds with the name used for the disk image file.
5. Select **Import existing disk image** from the list of options.

6. Click **Forward** to proceed. The next page of the wizard appears:

FIGURE 2 Creating a New Virtual Machine Wizard: 2 of 4



New VM

Create a new virtual machine

Step 2 of 4

Provide the existing storage path:

/var/lib/libvirt/images/image.qcow2

Choose an operating system type and version

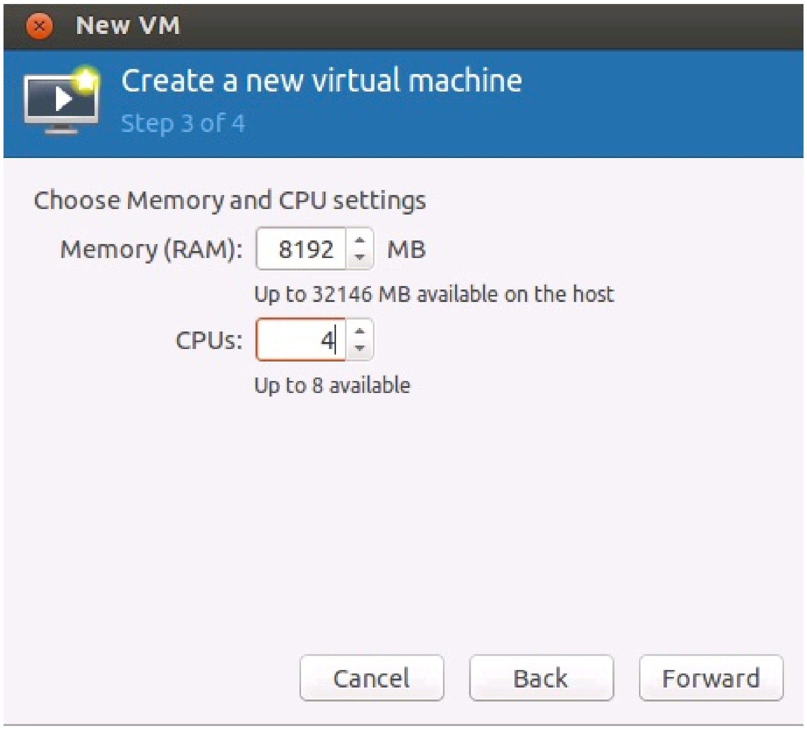
OS type: Generic

Version: Generic

7. Click **Browse** to select the storage pool location and disk image file for this virtual machine.
8. Ensure that the **OS type** is Generic.
9. Ensure that the **Version** is Generic.

10. Click **Forward** to proceed. The next page of the wizard appears:

FIGURE 3 Creating a New Virtual Machine Wizard: 3 of 4



Choose Memory and CPU settings

Memory (RAM): 8192 MB

Up to 32146 MB available on the host

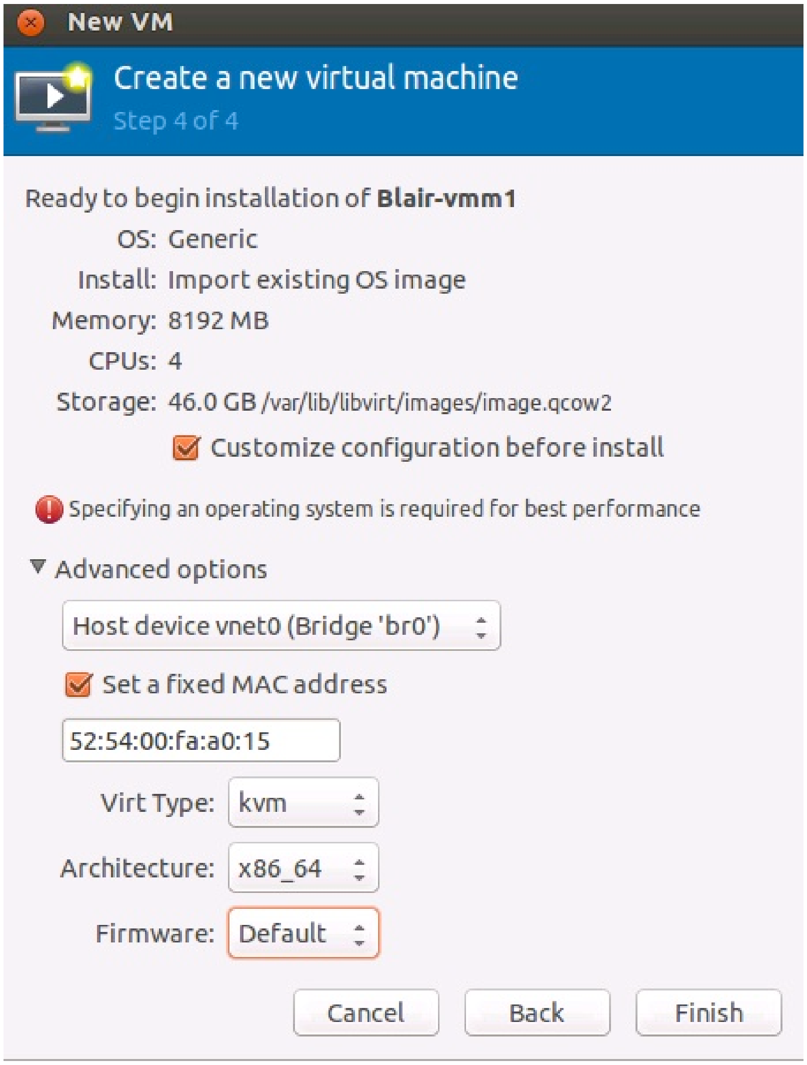
CPUs: 4

Up to 8 available

11. Set the **Memory (RAM)** to 8192 MB
12. Set the **CPUs** to 4.

13. Click **Forward** to proceed. The next page of the wizard appears:

FIGURE 4 Creating a New Virtual Machine Wizard: 4 of 4



Ready to begin installation of **Blair-vmm1**

OS: Generic

Install: Import existing OS image

Memory: 8192 MB

CPUs: 4

Storage: 46.0 GB /var/lib/libvirt/images/image.qcow2

☑ Customize configuration before install

Specifying an operating system is required for best performance

Advanced options

Host device vnet0 (Bridge 'br0')

☑ Set a fixed MAC address

52:54:00:fa:a0:15

Virt Type: kvm

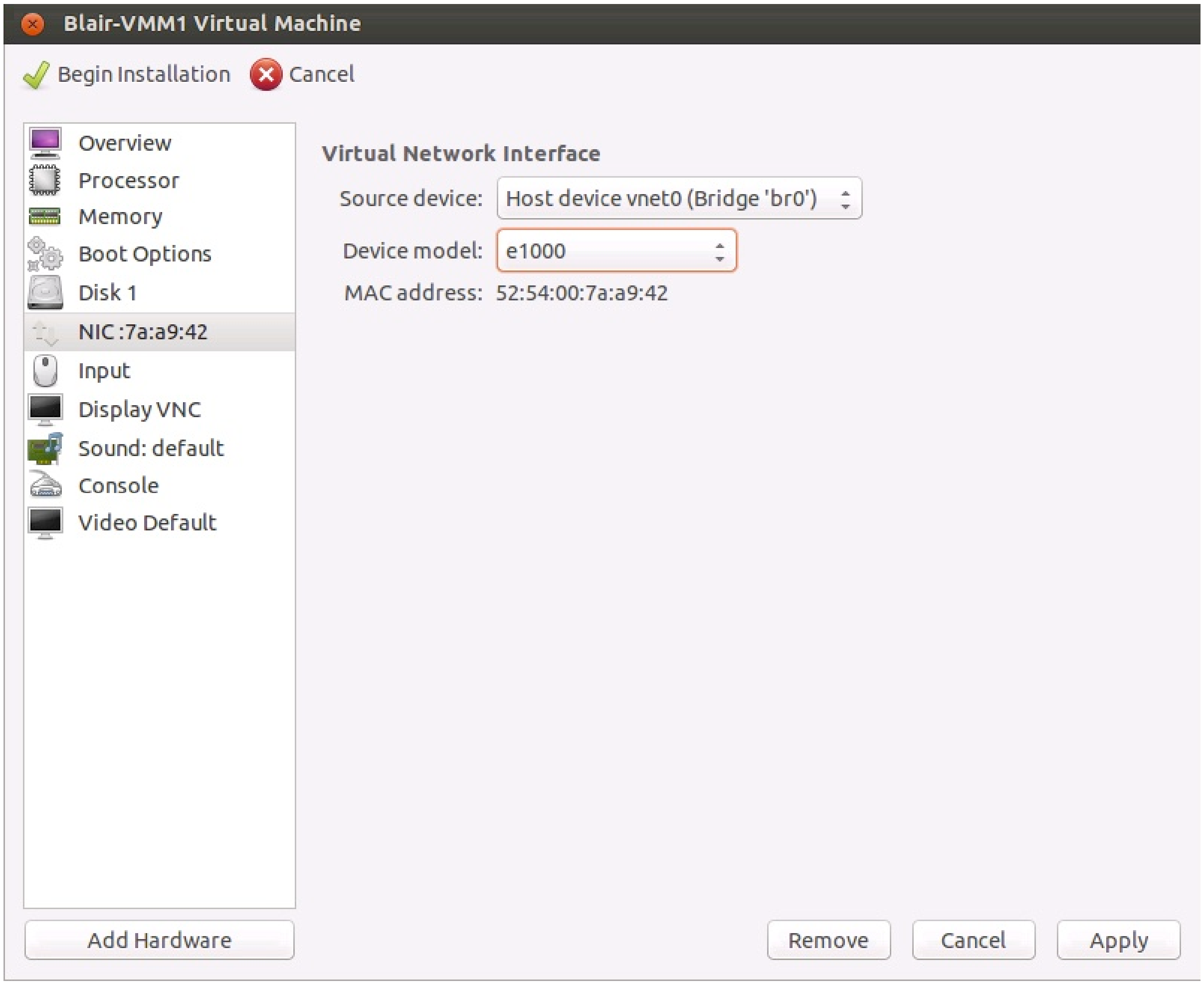
Architecture: x86_64

Firmware: Default

14. Check that the summary information is correct.
15. Ensure that the **Customize configuration before install** check box is selected.
16. Expand **Advanced options**.
17. Set **Architecture** to x86_64.
18. Click **Finish**. A configuration dialog box appears.
19. Select **Disk 1** to update disk settings:
    - Under **Advanced Options**, ensure that **Storage format** is set to qcow2.
    - Under **Advanced Options**, ensure that **Disk bus** is set to either IDE or Virtio.
    - Under **Performance Options**, ensure that **Cache mode** is set to writethrough.
    - Click **Apply**.

20. Select **Virtual Network Interface** to view Virtual Network Interface settings.

FIGURE 5 Configuring the KVM Virtual Machine: Virtual Network Interface



Virtual Network Interface

Source device: Host device vnet0 (Bridge 'br0')

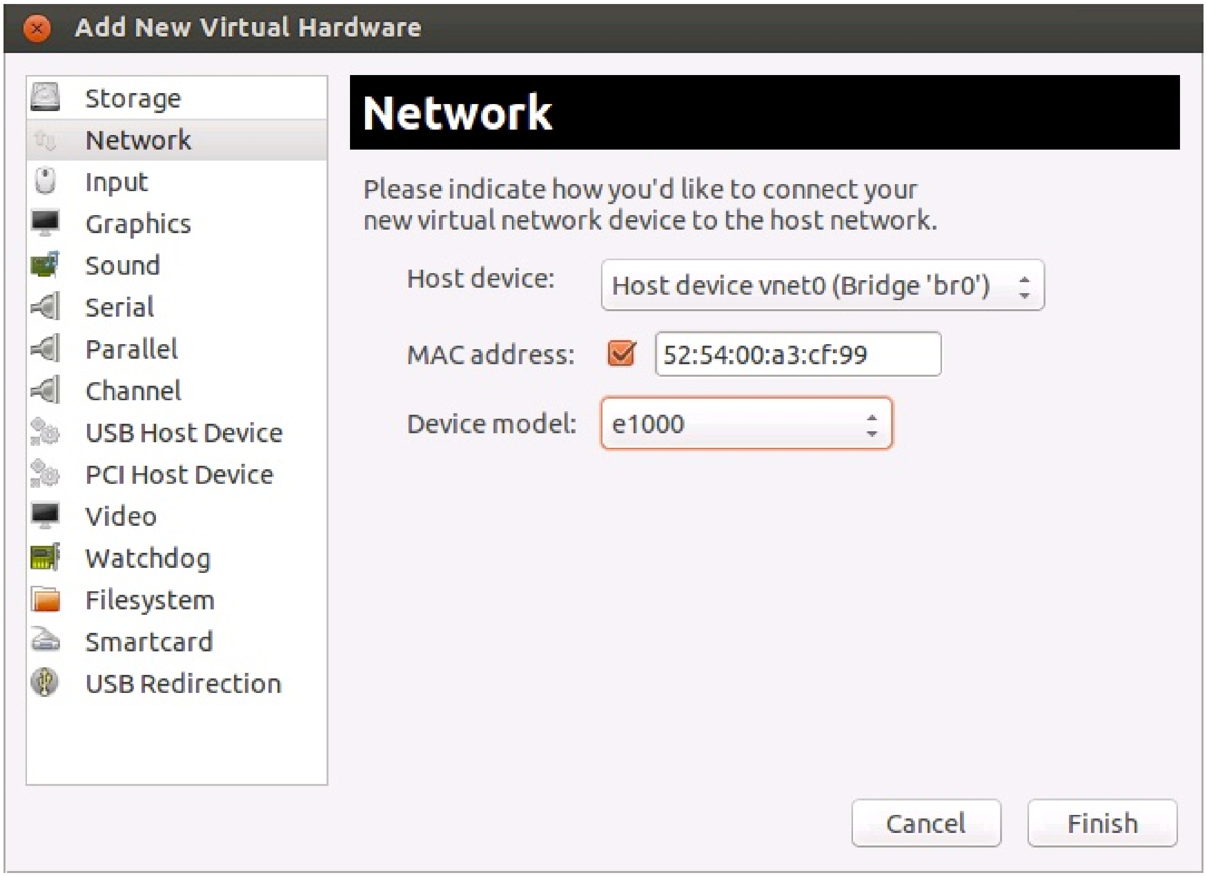
Device model: e1000

MAC address: 52:54:00:7a:a9:42

21. Ensure that the **Source device** is the br0 bridge.
22. Set the **Device model** to e1000.
23. Click **Apply**.
24. Click **Add Hardware**.

25. Click **Network**. The dialog box updates.

FIGURE 6 Configuring the KVM Virtual Machine: Network



Network

Please indicate how you'd like to connect your new virtual network device to the host network.

Host device: Host device vnet0 (Bridge 'br0')

MAC address: ☑ 52:54:00:a3:cf:99

Device model: e1000

26. Ensure that the **Host device** is the br0 bridge.
27. Set the **Device model** to e1000.
28. Click **Finish**.
29. Select **Begin installation** to complete the installation process.

> NOTE
> After the installation completes, a number of background initialization tasks take place. As a result, the CLI will offer reduced functionality for a short period. Brocade recommends waiting at least two minutes before attempting to access the Services Director VA.

Accessing the Services Director VA on KVM

To access the Services Director VA, you need the IP address of its management interface.

If DHCP is available, you need to find out the allocated IP address.

1. Log in to the Services Director VA using the KVM console.

NOTE
Do not use the jumpstart setup wizard.

2. Obtain the allocated DHCP IP address of the VA using the following commands:

```
<host> > enable
<host> # show interfaces
```

If DHCP is not available, complete the following steps.

1. Log in to the Services Director VA using the KVM console.
2. Use the jumpstart setup wizard to set a static IP address, netmask, and the default gateway IP address.

You can now access the Services Director VA with a browser, using the IP address of the Services Director VA. To configure the Services Director VA using the setup wizard, refer to Installing and Configuring the Services Director VA Using the Setup Wizard on page 28.

Installing and Configuring the Services Director VA Using the Setup Wizard

After you have created the VM for your Services Director, you install and configure the Services Director VA using the Setup Wizard. The Setup Wizard enables you to:

- Select the role for this Services Director. That is, *Primary* or *Secondary*. A Primary Services Director can run as a standalone node, and assumes an active role in managing services. A Secondary Services Director is joined to the Primary Services Director and can be promoted to the active role in the event of a failure. When a Secondary Services Director is joined to the Primary Services Director in the setup wizard, a High Availability (HA) pair is formed.
- Specify a Service Endpoint Address for the Services Director. If the Service Endpoint Address is in a private network behind a NAT device, you must specify both the internal and external IP addresses for the Service Endpoint Address.
- Select whether to manage your Services Director (and vTM instances) using DNS hostnames or IP addresses. The option you choose depends on your deployment environment.
- Import your licenses. Licenses are required to complete the setup of the Services Director.
- Define a master password. This password is used to encrypt the administration passwords of all Traffic Managers.

The Setup Wizard automatically starts the first time you log in to the Services Director VA with a browser.

NOTE
The Setup Wizard is also used during recovery after a Services Director failure. For details, refer to *Brocade Services Director Advanced User Guide*.

Installing and Configuring a Primary Services Director

To install and configure a Primary Services Director, perform the following prodedure:

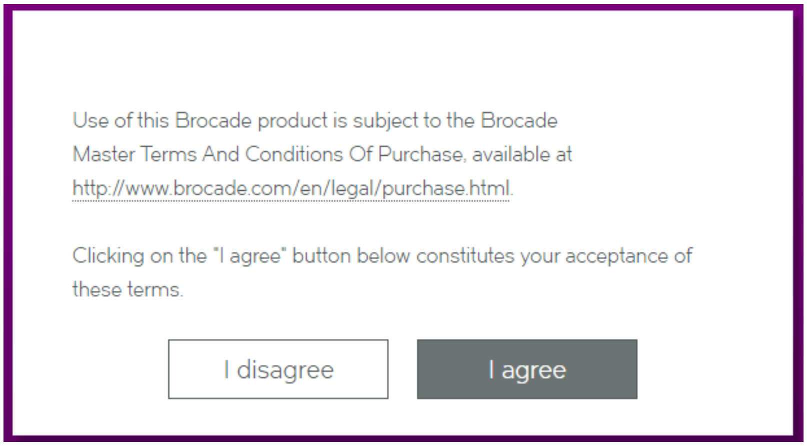
1. Start the installation process, refer to Starting a Services Director Installation on page 29.
2. Define a Service Endpoint Address (SEA), refer to Defining a Service Endpoint Address on page 36.
3. Redeem a license token, refer to Redeeming a License Token on page 39.
4. Generate a self-signed SSL certificate, refer to Generating a Self-Signed SSL Certificate on page 40.
5. Add certificates and licenses, refer to Adding Certificates and Licenses on page 43.

6. Complete the installation, refer to Completing the Services Director Installation on page 51.

Starting a Services Director Installation

1. Right-click the VM you created in vSphere and select **Power** and then **Power On**.
2. In the vSphere Client UI, click the Services Director VA that you created.
3. On the right side, click the **Summary** tab and make a note of the IPv4 address for the VM. This is the IP address you will use to access your Services Director VA. You may need to wait for a moment to allow the VM to fully start after the VM is powered on.
4. To connect to Services Director VA for the first time, access your Services Director VA in a browser window using its IP address. A statement about the End User License Agreement appears.

FIGURE 7 Setup Wizard: EULA Page



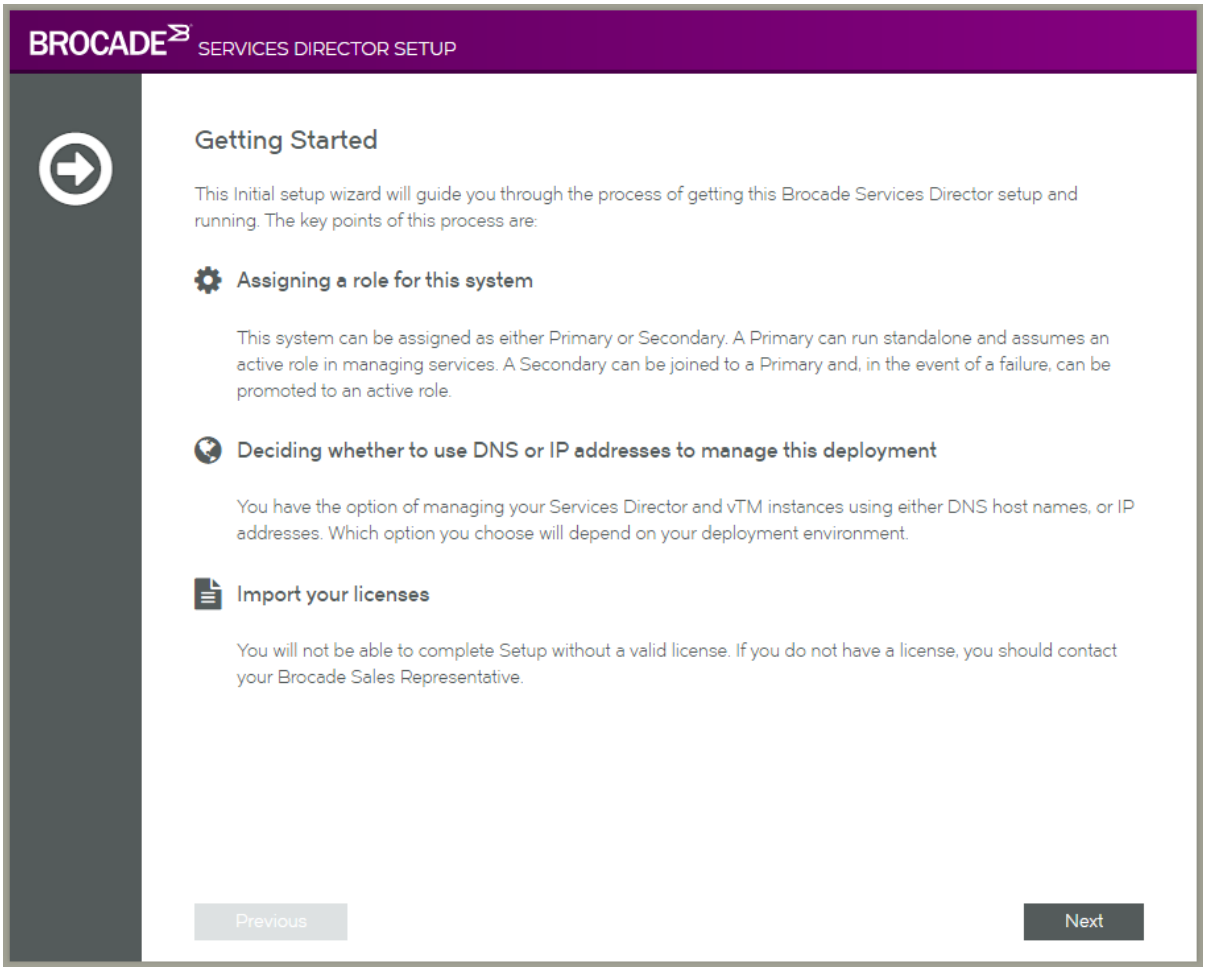
Use of this Brocade product is subject to the Brocade Master Terms And Conditions Of Purchase, available at http://www.brocade.com/en/legal/purchase.html.

Clicking on the "I agree" button below constitutes your acceptance of these terms.

5. Click **I agree** to continue.

6. Log in using the default value for the administrator user (**admin**) and the default password (**password**), and click **Sign In**. The Setup Wizard starts automatically.

FIGURE 8 Setup Wizard: Getting Started Page



Getting Started

This Initial setup wizard will guide you through the process of getting this Brocade Services Director setup and running. The key points of this process are:

Assigning a role for this system

This system can be assigned as either Primary or Secondary. A Primary can run standalone and assumes an active role in managing services. A Secondary can be joined to a Primary and, in the event of a failure, can be promoted to an active role.

Deciding whether to use DNS or IP addresses to manage this deployment

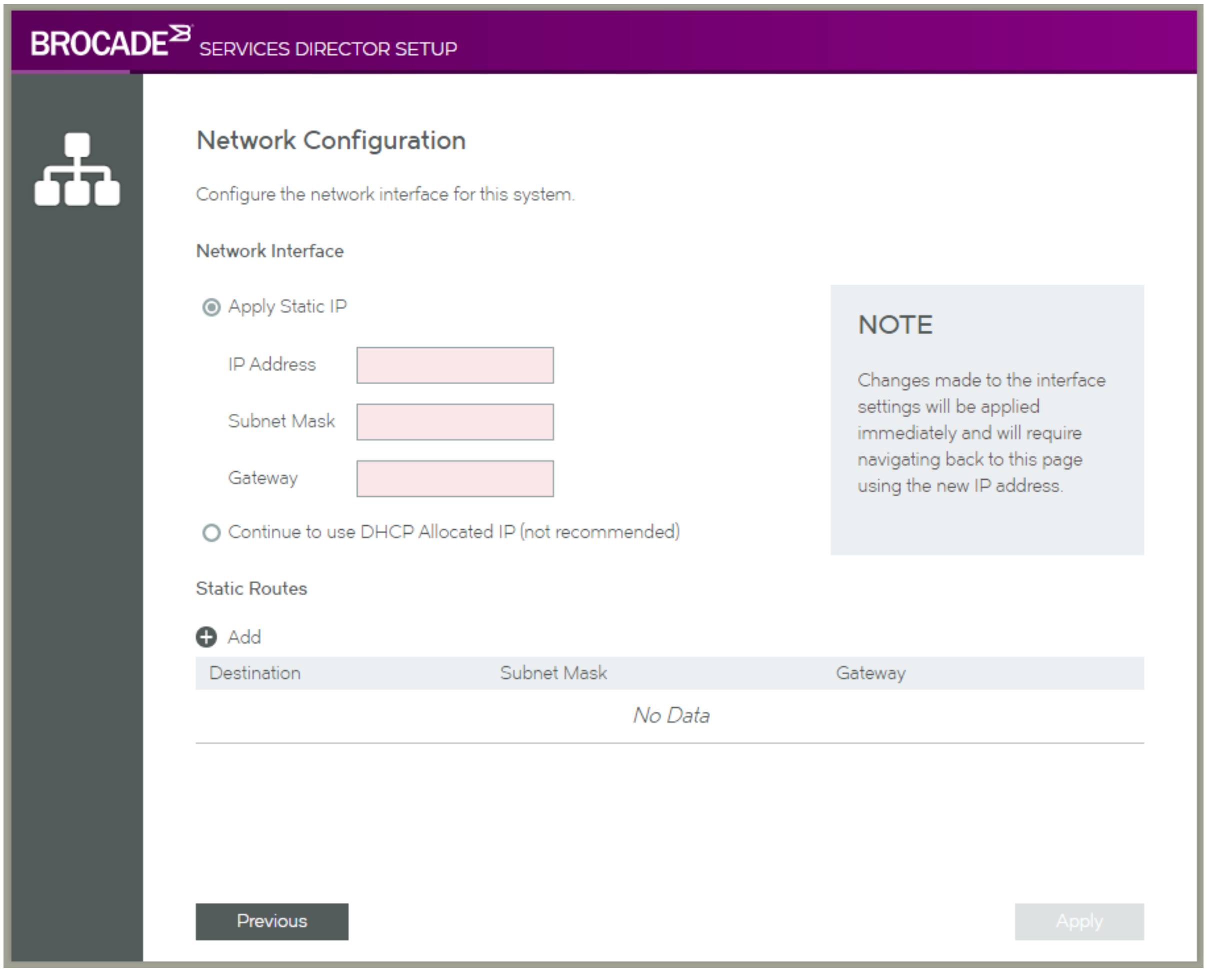
You have the option of managing your Services Director and vTM instances using either DNS host names, or IP addresses. Which option you choose will depend on your deployment environment.

Import your licenses

You will not be able to complete Setup without a valid license. If you do not have a license, you should contact your Brocade Sales Representative.

7. Click **Next**. The **Network Configuration** page appears.

FIGURE 9 Setup Wizard: Network Configuration Page



Network Configuration

Configure the network interface for this system.

Network Interface

● Apply Static IP

IP Address

Subnet Mask

Gateway

○ Continue to use DHCP Allocated IP (not recommended)

NOTE

Changes made to the interface settings will be applied immediately and will require navigating back to this page using the new IP address.

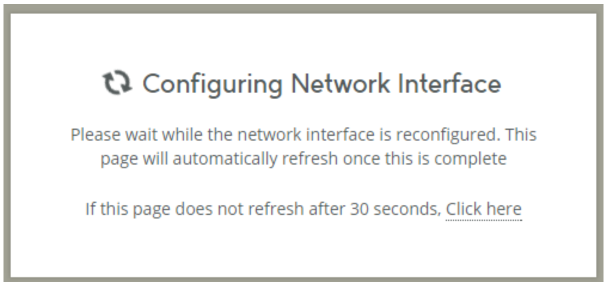
Static Routes

Destination	Subnet Mask	Gateway
	No Data	

8. Select one of the following options:
   - **Static IP**. Then, complete an **IP Address**, **Subnet Mask** and **Gateway**. The system confirms that the gateway can be pinged.
   - **DHCP Allocated IP**. Brocade does not recommend the use of this option. A DHCP server must be available so that the system can request the IP address from it.

9. Click **Next**. A progress screen appears while the network interface is configured.

FIGURE 10 Setup Wizard: Configuring Network Interface Page



Configuring Network Interface

Please wait while the network interface is reconfigured. This page will automatically refresh once this is complete

If this page does not refresh after 30 seconds, Click here

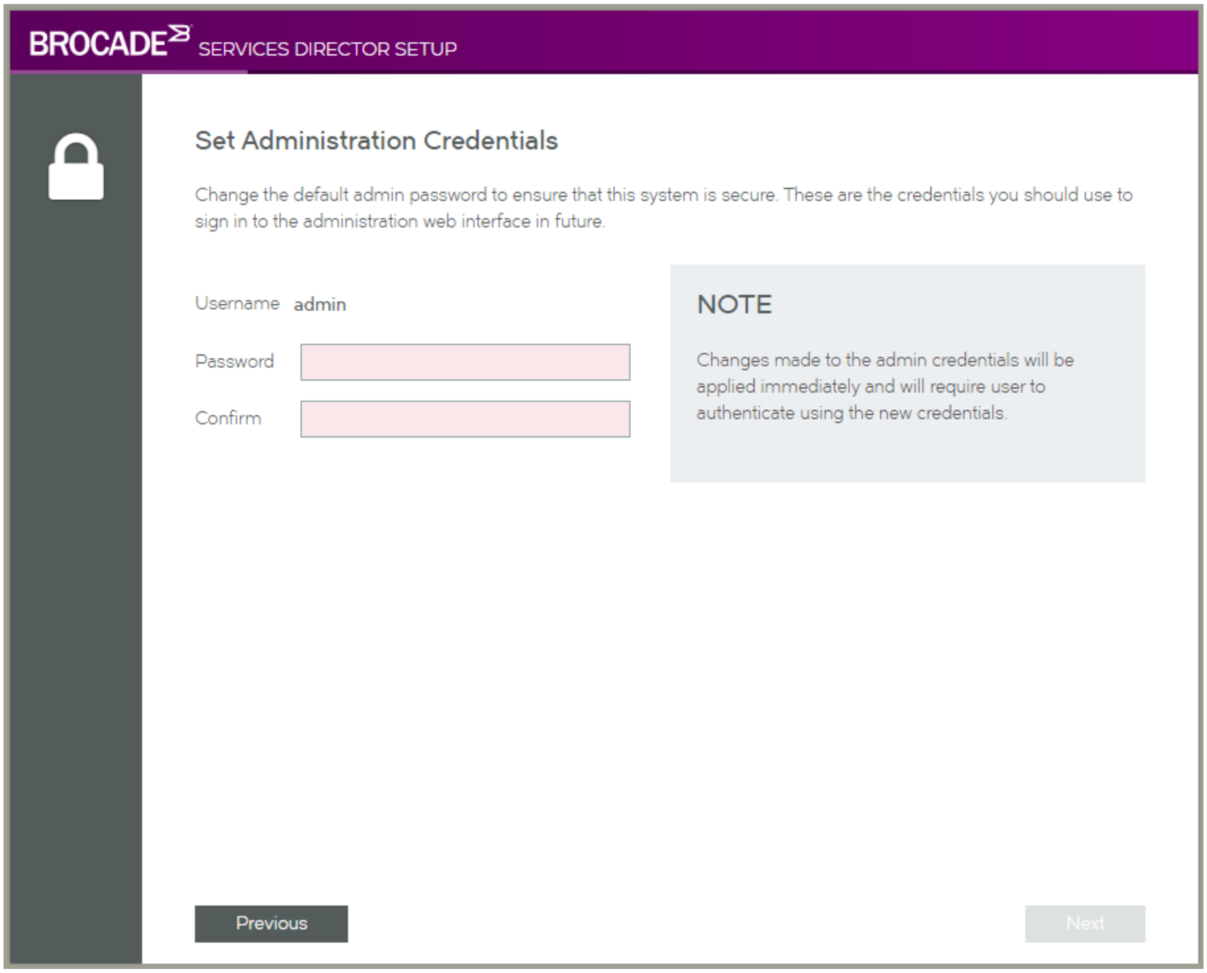
The outcome of this process depends on whether you selected **Static IP** or **DHCP Allocated IP**.

- **Static IP**. The browser will automatically access the wizard using the specified IP address. Log in, and continue the Setup Wizard.
- **DHCP Allocated IP**. Manually direct your browser to the allocated IP to continue this wizard. Log in, and continue the Setup Wizard.

10. Click **Next**.

    The **Set Administration Credentials** page appears. This page requires you to set the default password for the **admin** login.

    FIGURE 11 Setup Wizard: Set Administration Credentials Page



Set Administration Credentials

Change the default admin password to ensure that this system is secure. These are the credentials you should use to sign in to the administration web interface in future.

Username admin

Password

Confirm

NOTE

Changes made to the admin credentials will be applied immediately and will require user to authenticate using the new credentials.

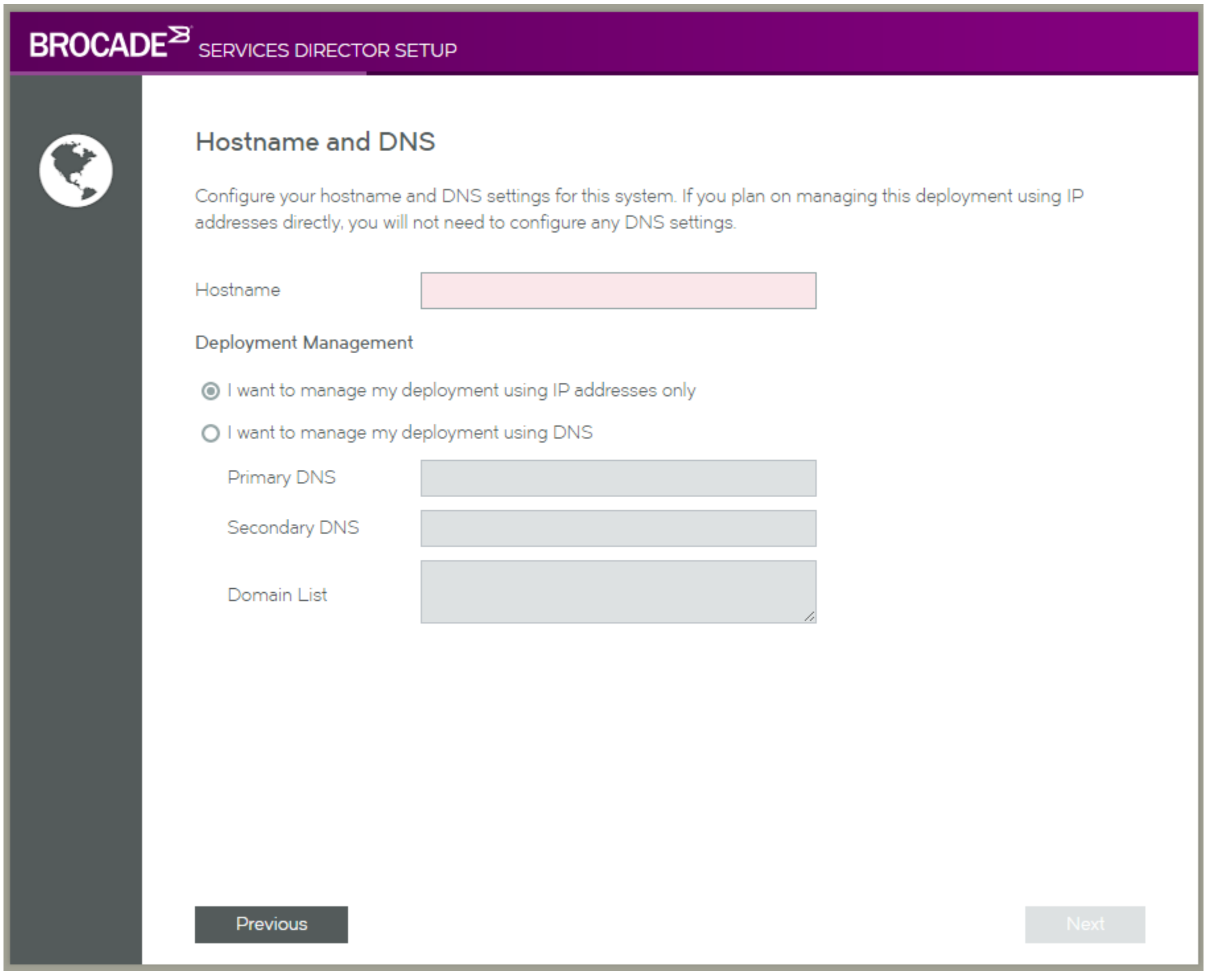
11. Enter (and confirm) a password and click **Next**.

    NOTE
    The percent ("%") and UNICODE characters are not supported for this password.

    NOTE
    Administration credentials can be updated at any time after the Services Director VA is operational. See Updating Administration Credentials on page 62.

The **Hostname and DNS** page appears. This page enables you to choose whether to manage your Services Director using either IP addresses or DNS.

FIGURE 12 Setup Wizard: Hostname and DNS Page



BROCADE SERVICES DIRECTOR SETUP

Hostname and DNS

Configure your hostname and DNS settings for this system. If you plan on managing this deployment using IP addresses directly, you will not need to configure any DNS settings.

Hostname

Deployment Management

● I want to manage my deployment using IP addresses only

○ I want to manage my deployment using DNS

Primary DNS

Secondary DNS

Domain List

12. For the **Hostname**, enter the management address for the Services Director.
    - If this management address can be resolved using DNS, enter its hostname.
    - If this management address cannot be resolved using DNS, enter its IP address.

      NOTE
      Where no DNS is configured, the use of hostnames should be avoided in the product.

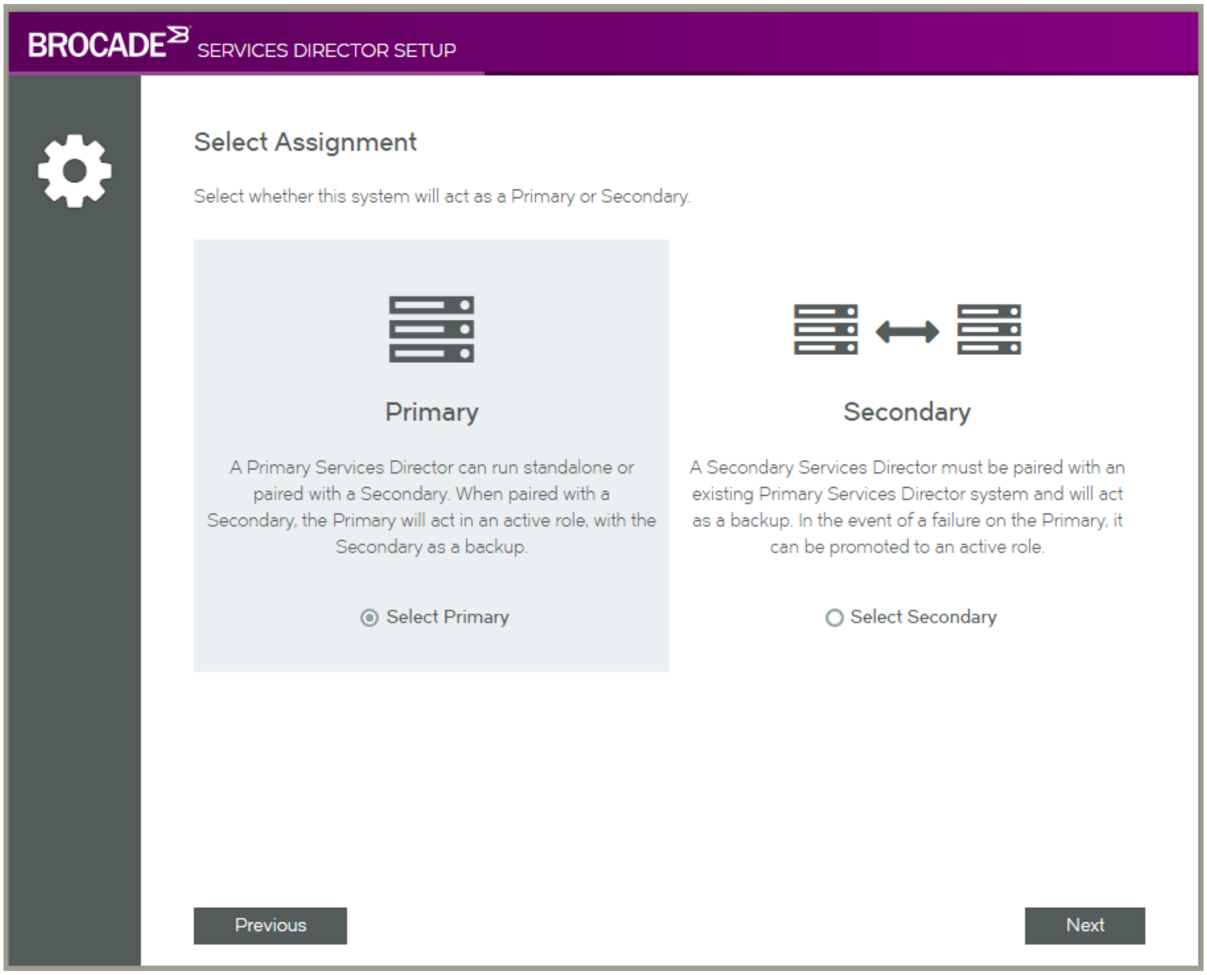
13. Select one of the following options:
    - **I want to manage my deployment using IP addresses only**. Select this where no DNS is configured.

      Ensure that you specify the Services Director's IP address as its **Hostname** (see above).
    - **I want to manage my deployment using DNS**. This requires you to have one or more configured DNS name servers in place.

      Ensure that you specify a resolveable hostname as the Services Director's **Hostname** (see above). Then, specify:
      - **Primary DNS**
      - **Secondary DNS** (Optional)
      - **Domain List** (Optional) An ordered list of domain names. If you specify domains, the system automatically finds the appropriate domain for each of the hosts that you specify in the system.

14. Click **Next**. The **Select Assignment** page appears. This page enables you to select the role of the Services Director.

FIGURE 13 Setup Wizard: Select Assignment Page



Select Assignment

Select whether this system will act as a Primary or Secondary.

Primary

A Primary Services Director can run standalone or paired with a Secondary. When paired with a Secondary, the Primary will act in an active role, with the Secondary as a backup.

● Select Primary

Secondary

A Secondary Services Director must be paired with an existing Primary Services Director system and will act as a backup. In the event of a failure on the Primary, it can be promoted to an active role.

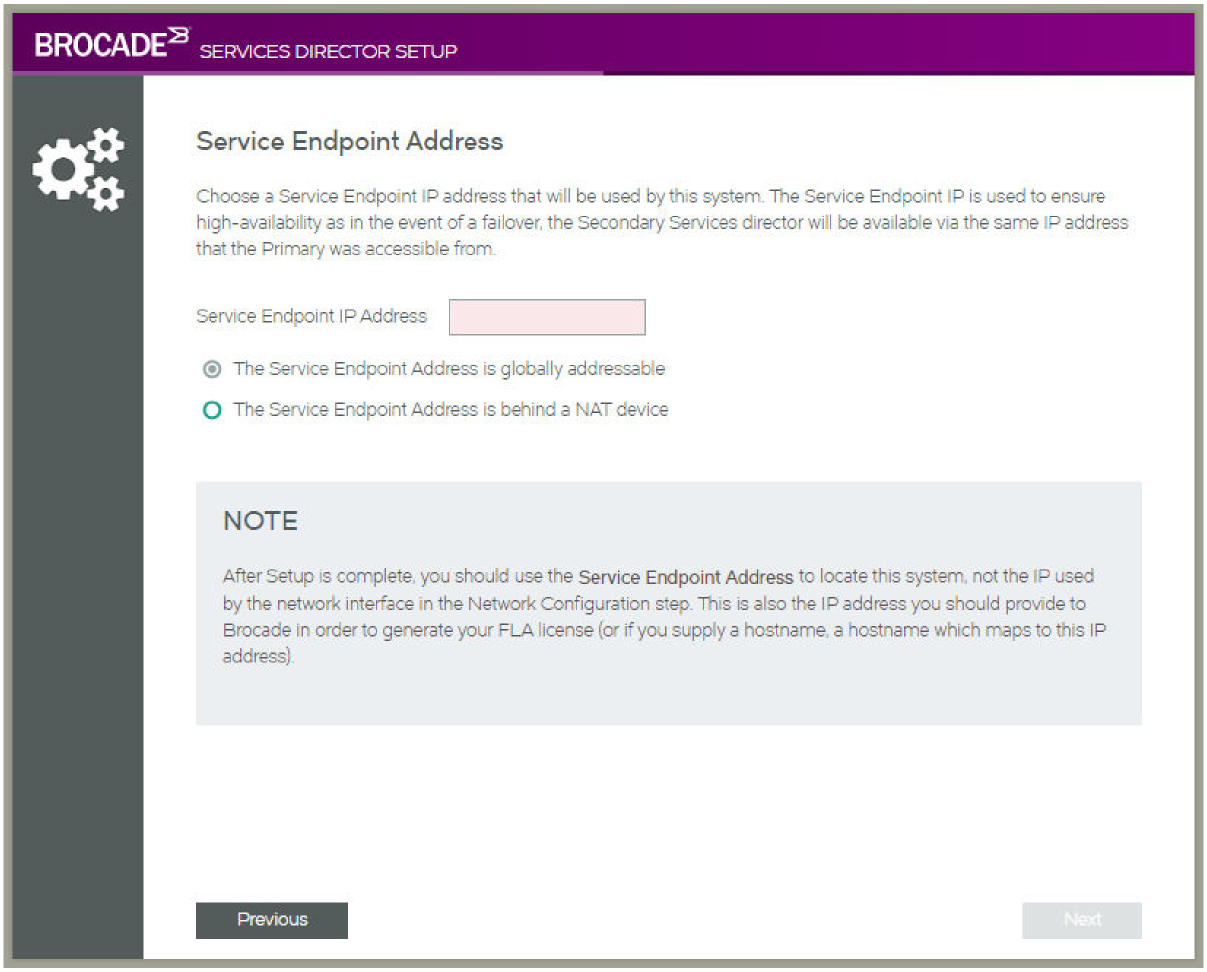
○ Select Secondary

15. Click **Select Primary** to indicate that the Services Director will act as a Primary Services Director, either as a standalone node or in an HA Pair.
16. Click **Next**, and continue this process from Defining a Service Endpoint Address on page 36.

Defining a Service Endpoint Address

After you choose to define a Primary Services Director, the **Service Endpoint Address** page appears.

FIGURE 14 Setup Wizard: Define a Service Endpoint Address Page



Service Endpoint Address

Choose a Service Endpoint IP address that will be used by this system. The Service Endpoint IP is used to ensure high-availability as in the event of a failover, the Secondary Services director will be available via the same IP address that the Primary was accessible from.

Service Endpoint IP Address

● The Service Endpoint Address is globally addressable

○ The Service Endpoint Address is behind a NAT device

NOTE

After Setup is complete, you should use the **Service Endpoint Address** to locate this system, not the IP used by the network interface in the Network Configuration step. This is also the IP address you should provide to Brocade in order to generate your FLA license (or if you supply a hostname, a hostname which maps to this IP address).

1. If the Service Endpoint Address for the Services Director HA pair is globally addressable:
   - Select **The Service Endpoint Address is globally addressable**.
   - Enter the **Service Endpoint IP Address** for the Services Director HA pair.

     NOTE
     A Service Endpoint Address is required for a standalone Primary Services Director. It must be different from the IP address of the Primary Services Director.

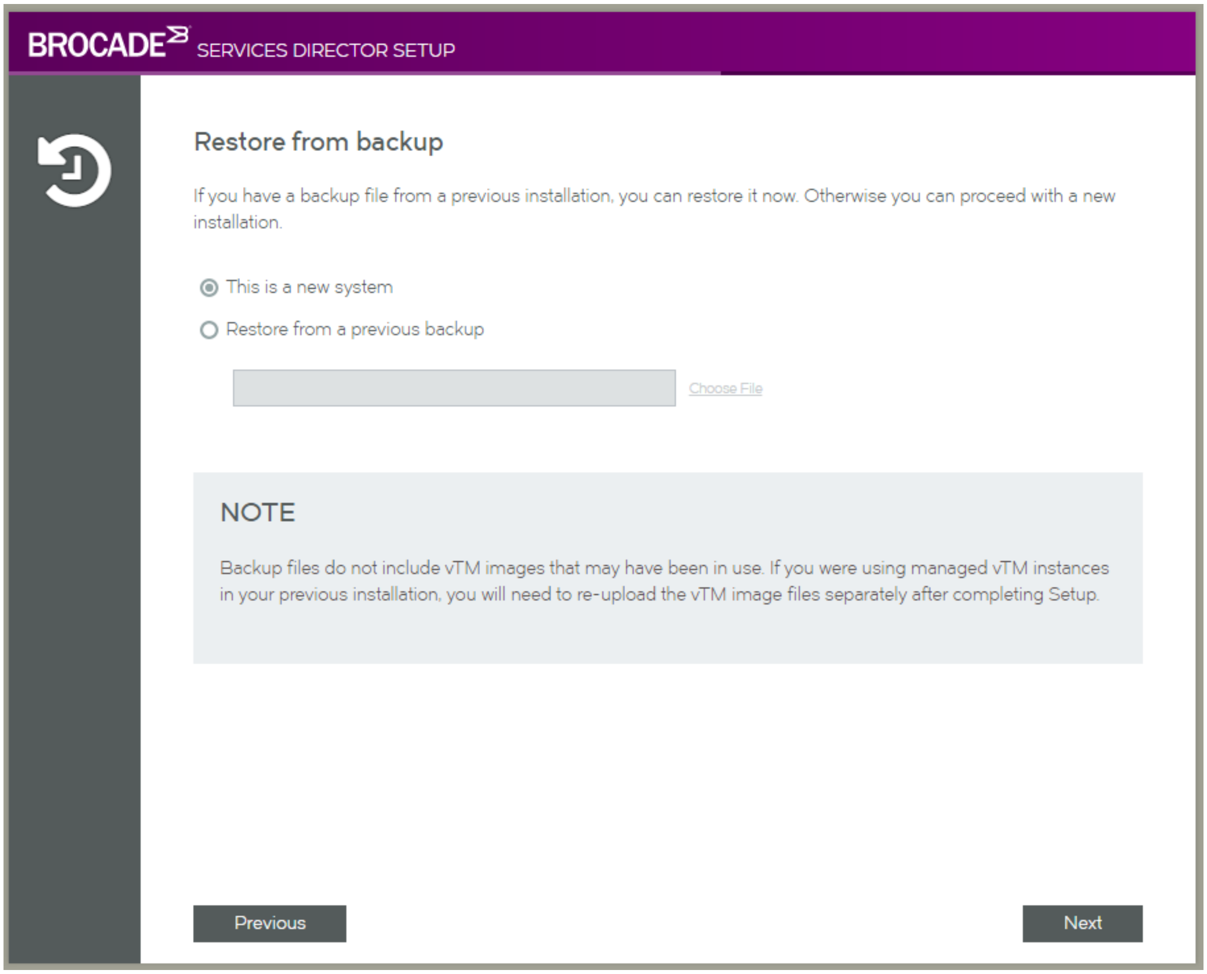
2. If Service Endpoint Address for the Services Director HA pair is in a private network behind a NAT device:
   - Select **The Service Endpoint Address is behind a NAT device**. The available properties update to include an **External IP Address**.
   - Enter the internal NAT Service Endpoint Address for your Services Director HA pair as the **Service Endpoint IP Address**.
   - Enter the external NAT address for your Services Director HA pair as the **External IP Address**.

     NOTE
     A Service Endpoint Address is required for a standalone Primary Services Director. It must be different from the IP address of the Primary Services Director.

3. Click **Next** to display the **Restore from Backup** page.

   This page enables you to restore a backup of your Services Director after a failure. Refer to *Brocade Services Director Advanced User Guide* for details.

FIGURE 15 Setup Wizard: Restore from Backup Page



Restore from backup

If you have a backup file from a previous installation, you can restore it now. Otherwise you can proceed with a new installation.

● This is a new system

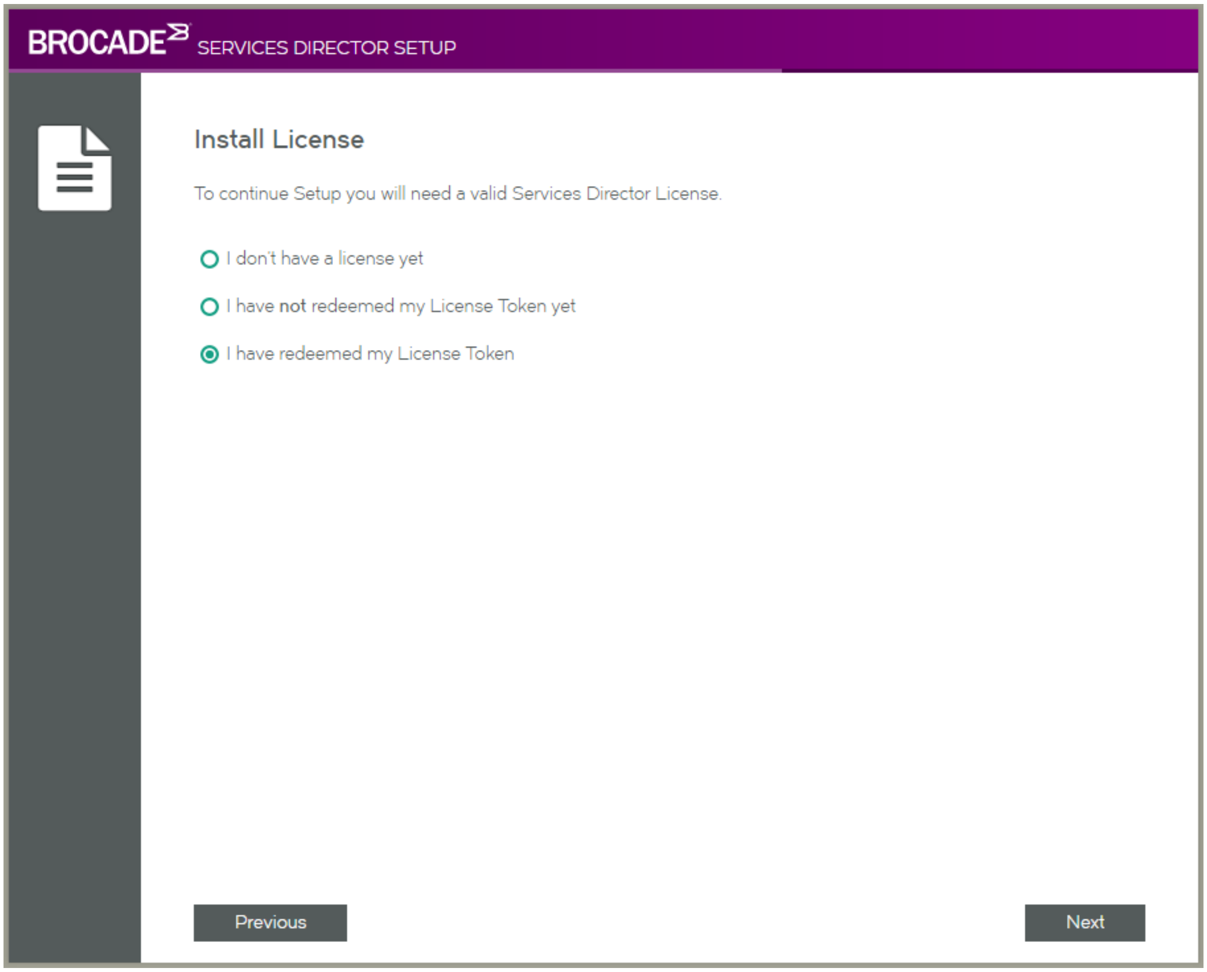
○ Restore from a previous backup

NOTE

Backup files do not include vTM images that may have been in use. If you were using managed vTM instances in your previous installation, you will need to re-upload the vTM image files separately after completing Setup.

4. Click **This is a new appliance** and then click **Next**. The **Install License** page appears.

FIGURE 16 Setup Wizard: Install License Page



Install License

To continue Setup you will need a valid Services Director License.

○ I don't have a license yet

○ I have **not** redeemed my License Token yet

● I have redeemed my License Token

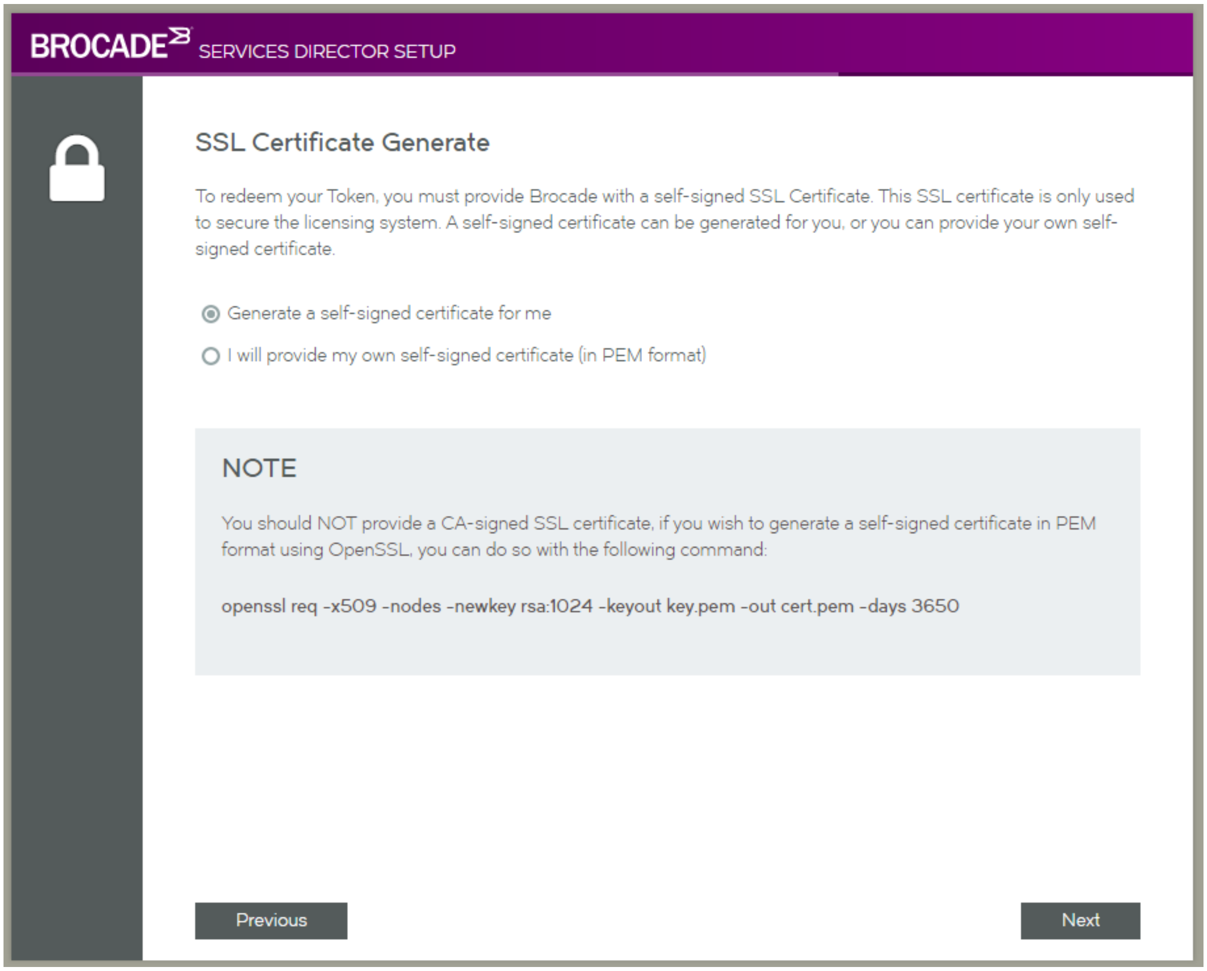
5. Select one of the following options:
   - **I have redeemed my License Token**. You can now add your licenses. Click **Next**, and continue from Adding Certificates and Licenses on page 43.
   - **I have not redeemed my License Token yet**. The Setup Wizard will guide you through this process. Click **Next**, and continue from Redeeming a License Token on page 39.
   - **I don't have a license yet**. If you have not obtained a License Token, you *cannot* proceed with the Setup Wizard at this time. Refer to Obtaining Services Director Licenses on page 17.

     Close the Setup Wizard.

Redeeming a License Token

After you indicate that you have an unredeemed license token, the **SSL Certificate Generate** page appears. An SSL certificate is required to redeem your token. You can provide your own certificate, or the system can generate one for you.

FIGURE 17 Setup Wizard: SSL Certificate Generate Page



SSL Certificate Generate

To redeem your Token, you must provide Brocade with a self-signed SSL Certificate. This SSL certificate is only used to secure the licensing system. A self-signed certificate can be generated for you, or you can provide your own self-signed certificate.

● Generate a self-signed certificate for me

○ I will provide my own self-signed certificate (in PEM format)

NOTE

You should NOT provide a CA-signed SSL certificate, if you wish to generate a self-signed certificate in PEM format using OpenSSL, you can do so with the following command:

```
openssl req -x509 -nodes -newkey rsa:1024 -keyout key.pem -out cert.pem -days 3650
```

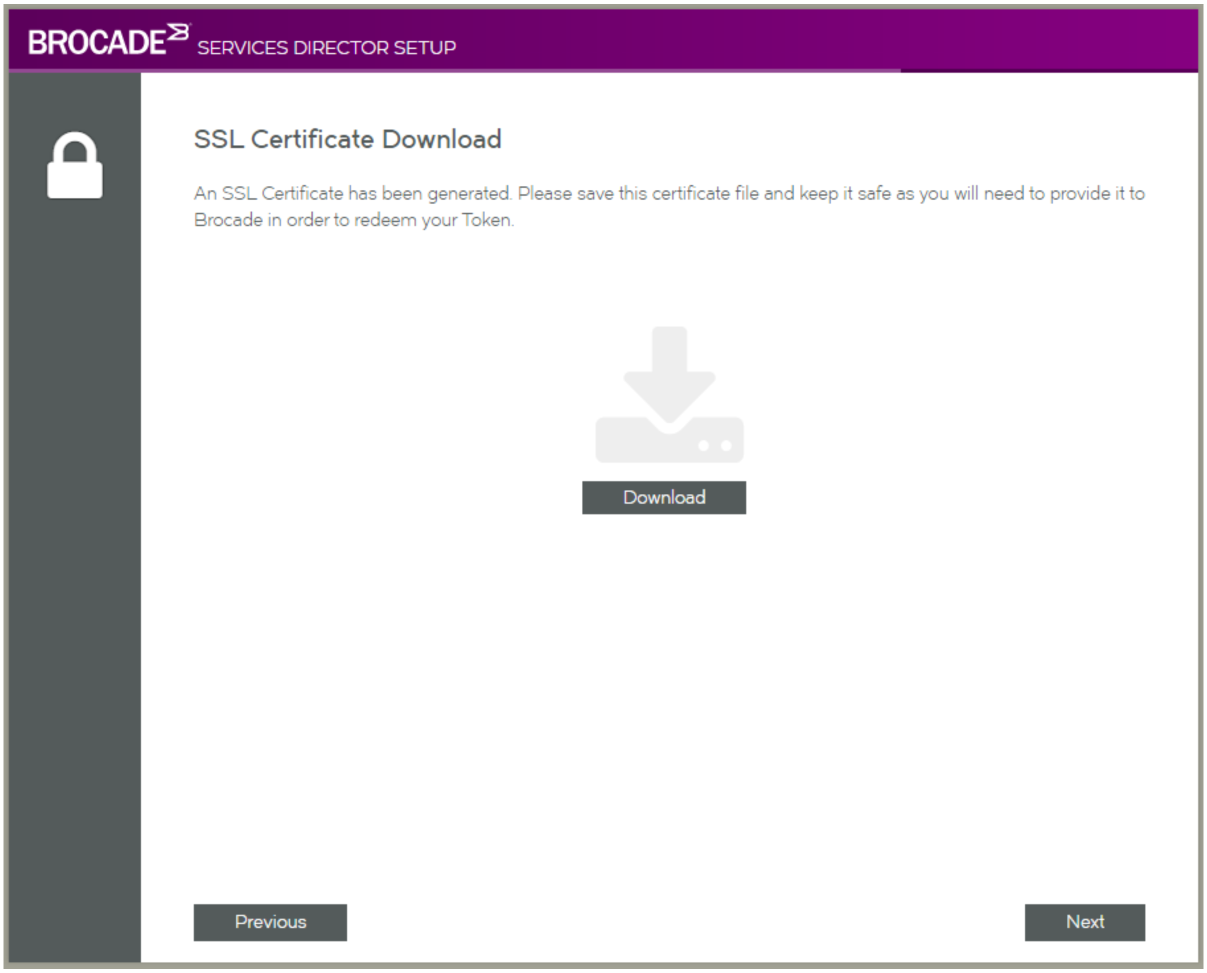
Select one of the following options:

- **Generate a signed certificate for me**. This selection will instruct the system to create a signed certificate that can be used to redeem your License Token with Brocade. Click **Next**, and continue from Generating a Self-Signed SSL Certificate on page 40.
- **I will provide my own self-signed certificate**. This selection requires you to have a self-signed SSL certificate. *You cannot use a CA-signed certificate.* Click **Next**, and continue from Adding Certificates and Licenses on page 43.

Generating a Self-Signed SSL Certificate

After you choose to have Services Director generate a self-signed SSL certificate, the **SSL Certificate Download** page appears. An SSL certificate is required to redeem your token.

FIGURE 18 Setup Wizard: SSL Certificate Download Page



SSL Certificate Download

An SSL Certificate has been generated. Please save this certificate file and keep it safe as you will need to provide it to Brocade in order to redeem your Token.

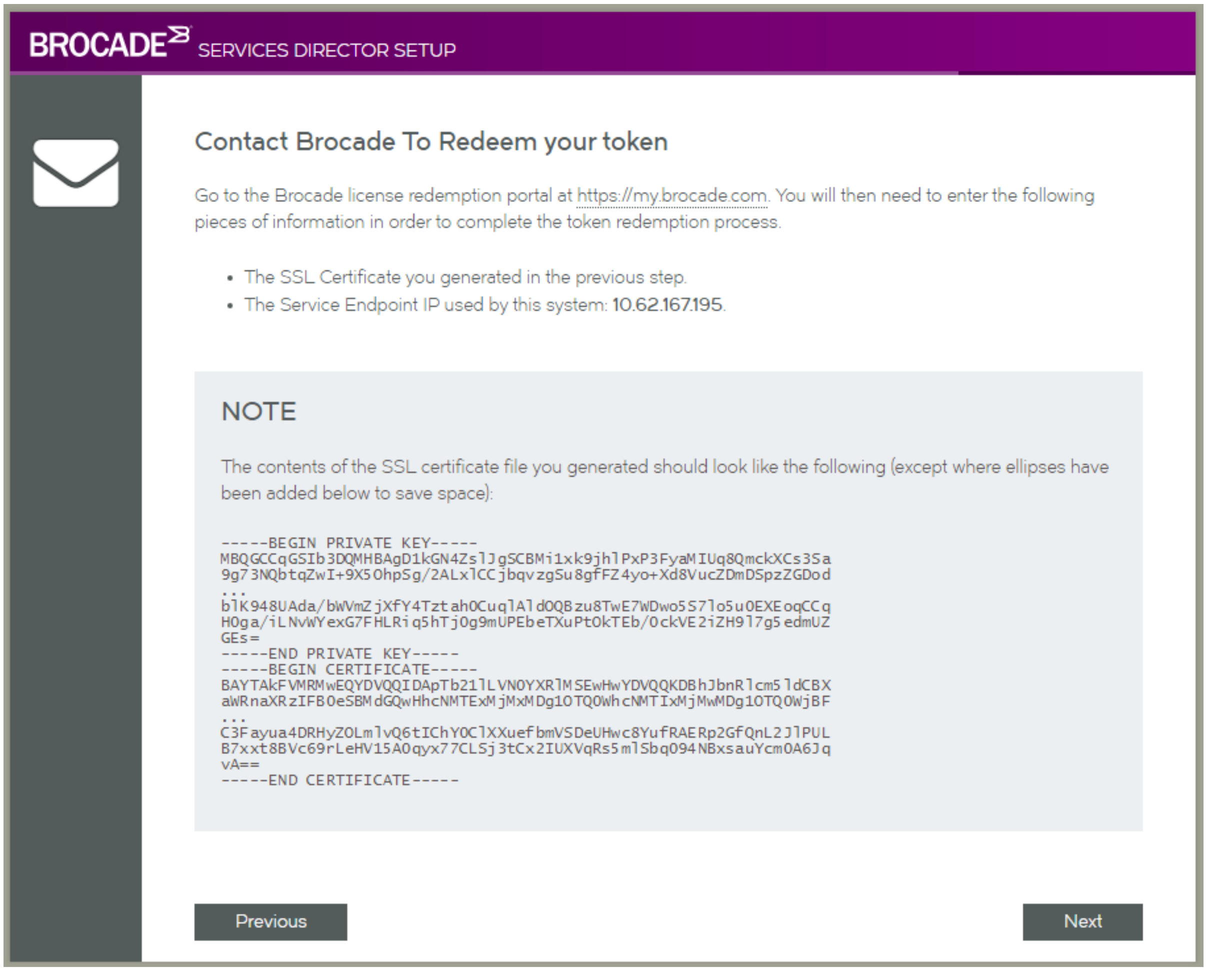
1. Click **Download** and choose a location for the file. The self-signed SSL certificate file downloads.

2. Click **Next**.

   The **Contact Brocade to Redeem Your Token** page appears. This page provides advice about how to redeem your token.

   NOTE
   You cannot proceed with the Setup Wizard until you have redeemed your token.

FIGURE 19 Setup Wizard: Contact Brocade to Redeem Your Token Page



Contact Brocade To Redeem your token

Go to the Brocade license redemption portal at https://my.brocade.com. You will then need to enter the following pieces of information in order to complete the token redemption process.

- The SSL Certificate you generated in the previous step.
- The Service Endpoint IP used by this system: 10.62.167.195.

NOTE

The contents of the SSL certificate file you generated should look like the following (except where ellipses have been added below to save space):

```
-----BEGIN PRIVATE KEY-----
MBQGCCqGSIb3DQMHBAgD1kGN4ZslJgSCBMi1xk9jhlPxP3FyaMIUq8QmckXCs3Sa
9g73NQbtqZwI+9X5OhpSg/2ALxlCCjbqvzgSu8gfFZ4yo+Xd8VucZDmDSpzZGDod
...
blK948UAda/bWVmZjXfY4TztahOCuqlAldOQBzu8TwE7WDwo5S7lo5uOEXEoqCCq
HOga/iLNvWYexG7FHLRiq5hTjOg9mUPEbeTXuPtOkTEb/OckVE2iZH9l7g5edmUZ
GEs=
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
BAYTAkFVMRMwEQYDVQQIDApTb21lLVNOYXRlMSEwHwYDVQQKDBhJbnRlcm5ldCBX
aWRnaXRzIFBOeSBMdGQwHhcNMTExMjMxMDg1OTQOWhcNMTIxMjMwMDg1OTQOWjBF
...
C3Fayua4DRHyZOLmlvQ6tIChYOClXXuefbmVSDeUHwc8YufRAERp2GfQnL2JlPUL
B7xxt8BVc69rLeHV15AOqyx77CLSj3tCx2IUXVqRs5mlSbq094NBxsauYcmOA6Jq
vA==
-----END CERTIFICATE-----
```

3. To redeem your License Token, visit the Brocade license redemption portal at `https://my.brocade.com`. You will need:

   - Your License Token.
   - Your self-generated SSL certificate.
   - The Service Endpoint Address.

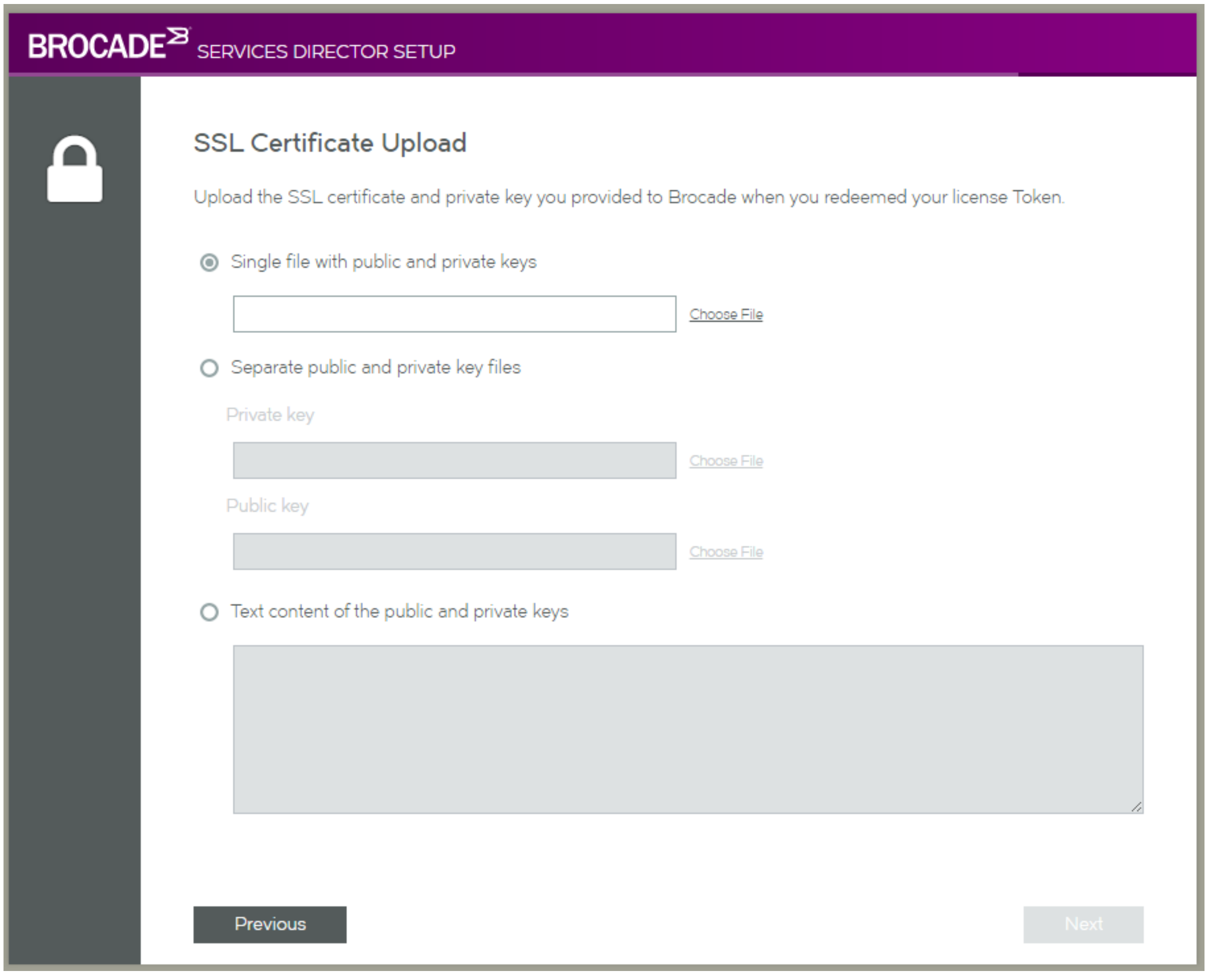
   Once you have your licenses, continue from Adding Certificates and Licenses on page 43.

Adding Certificates and Licenses

After you have redeemed your License Token, the **SSL Certificate Upload** page appears. This page enables you to input your certificate. The text of the certificate can be pasted in manually. Alternatively, you can identify individual Private/public key files, or a single combined file.

NOTE
If you previously chose to generate a self-signed certificate using the Setup Wizard, you will bypass this screen. This is because the Services Director already has the SSL certificate.

FIGURE 20 Setup Wizard: SSL Certificate Upload Page



SSL Certificate Upload

Upload the SSL certificate and private key you provided to Brocade when you redeemed your license Token.

● Single file with public and private keys

○ Separate public and private key files

Private key

Public key

○ Text content of the public and private keys

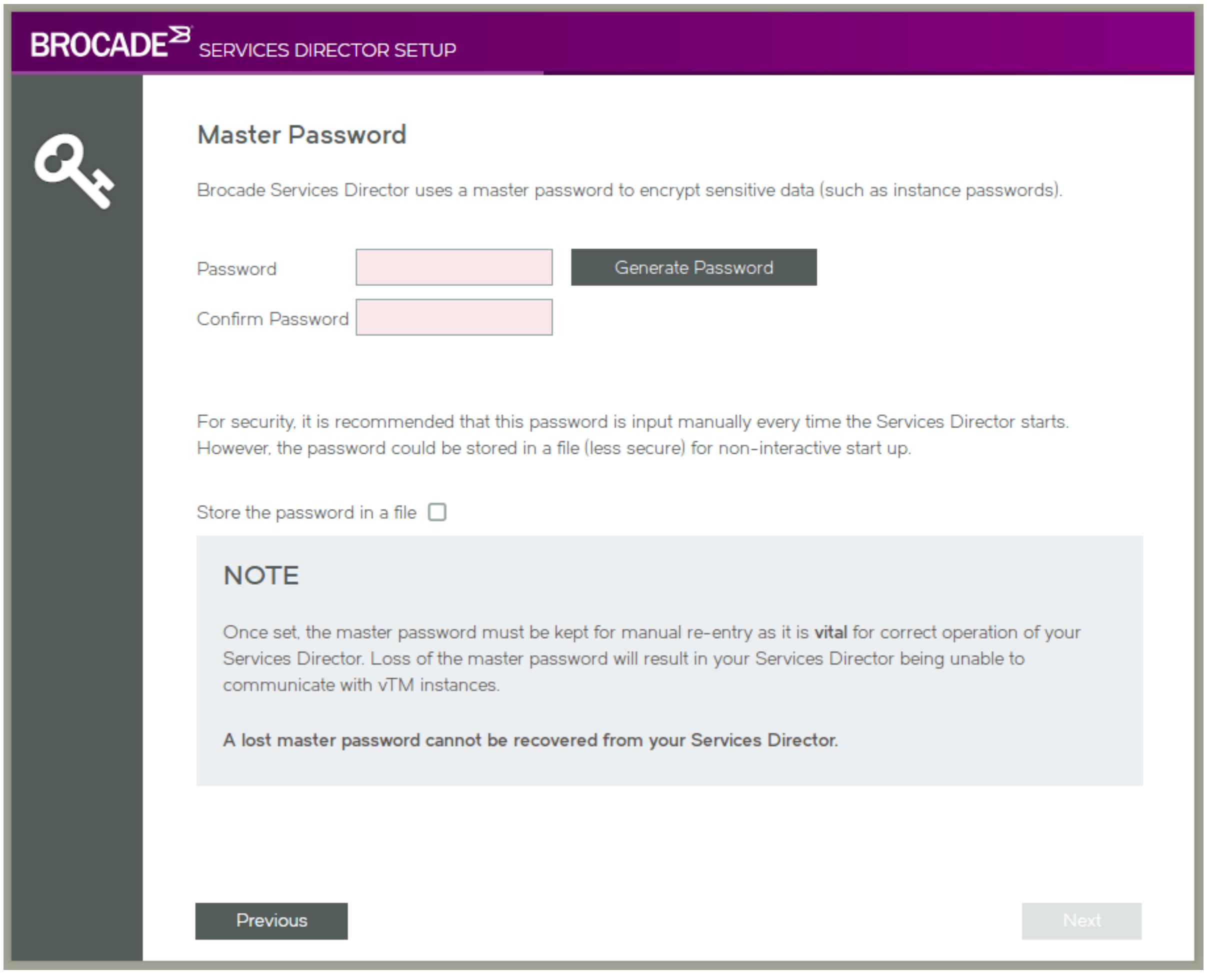
1. Select one of the following options:
   - **Single file with public and private keys**. Then, click **Choose File** to locate the certificate file.
   - **Separate public and private key files**. Then, click **Choose File** to locate each file.
   - **Text content of the public and private keys**. Then, paste the required text in.

   The selected text/file(s) are then verified. If successful, the **Next** button becomes available.

   NOTE
   The SSL certificate can be changed after the Services Director VA is operational. Refer to Updating the SSL Certificate on page 63.

2. Click **Next**. The Services Director **Master Password** page appears. This page enables you to define a master password that is required to decrypt stored password information whenever the Virtual Machine for this Services Director VA node restarts, or a backup of this node is used to restore/create a Services Director VA (refer to Recovering from a Services Director Failure on page 237).

FIGURE 21 Setup Wizard: Master Password Page



Master Password

Brocade Services Director uses a master password to encrypt sensitive data (such as instance passwords).

Password

Confirm Password

For security, it is recommended that this password is input manually every time the Services Director starts. However, the password could be stored in a file (less secure) for non-interactive start up.

Store the password in a file □

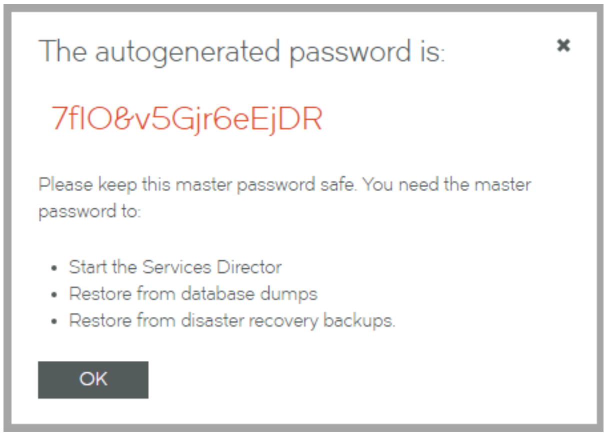
NOTE

Once set, the master password must be kept for manual re-entry as it is **vital** for correct operation of your Services Director. Loss of the master password will result in your Services Director being unable to communicate with vTM instances.

A lost master password cannot be recovered from your Services Director.

3. To set the master password, perform one of the following operations.
   - Enter a password and confirm the password.
   - Click **Generate Password**. The **Password** and **Confirm Password** fields are populated automatically and a dialog box is displayed.

   FIGURE 22 Setup Wizard: Master Password Dialog

   The autogenerated password is:

   7flO&v5Gjr6eEjDR

   Please keep this master password safe. You need the master password to:

   - Start the Services Director
   - Restore from database dumps
   - Restore from disaster recovery backups.

   Record the password, click **OK** to close the information dialog box, and confirm that you have stored the password in the next dialog box.

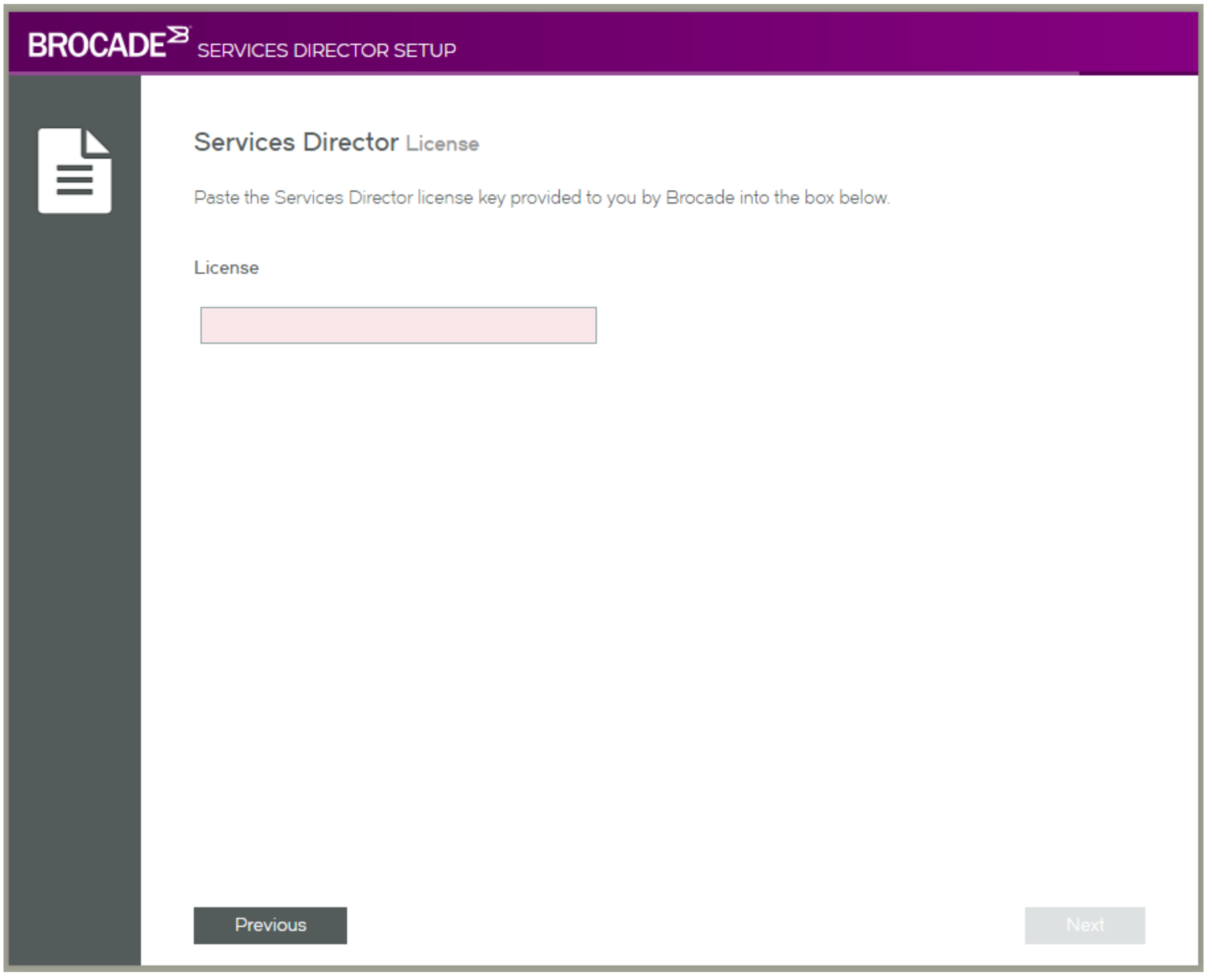
   NOTE
   It is essential that the master password (whether chosen yourself or generated automatically) is recorded and can be retrieved. Brocade recommends that this password is recorded in a secure location that is separate from the Services Director VA.

4. Choose whether to store the password internally for automatic use:
   - Select the **Store the password in a file** check box to store the master password within the Services Director VA. The password will be automatically available whenever the Virtual Machine for a Services Director VA restarts. However, you must enter the master password manually when you create a Services Director VA from a backup file.
   - Clear the **Store the password in a file** check box to not record the master password. You must to enter the master password manually whenever the Virtual Machine for a Services Director VA restarts, and when you create a Services Director VA from a backup file.

   Refer to Entering the Master Password After a Virtual Machine Restart on page 254 for details of restarting a VM.

5. Click **Next**. The Services Director **License** page appears.

FIGURE 23 Setup Wizard: Services Director License Page



Services Director License

Paste the Services Director license key provided to you by Brocade into the box below.

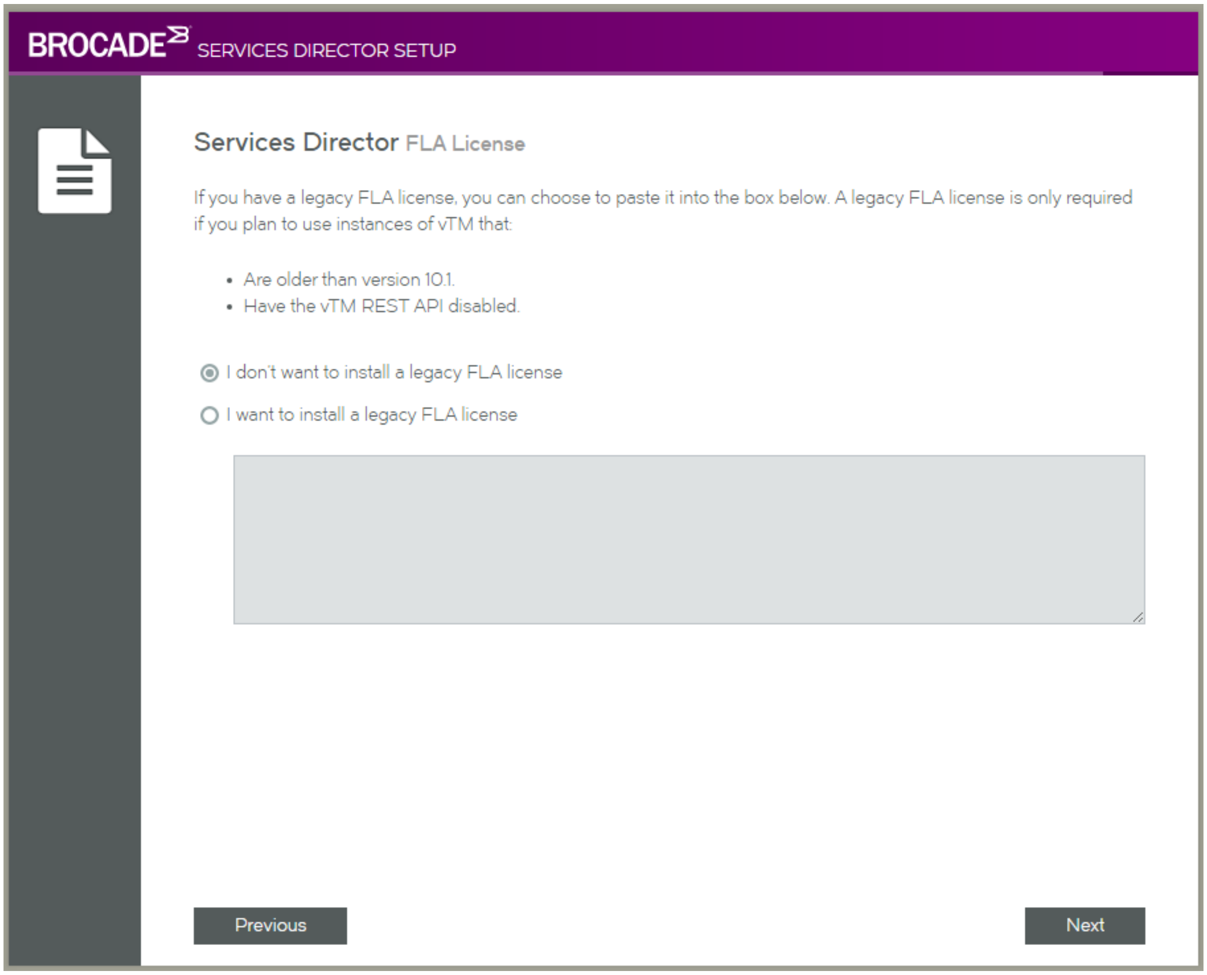
License

6. Enter the **License** text. This is validated automatically. Once validation completes, either:
   - A success message is displayed, and the **Next** button becomes available. OR
   - A failure message is displayed. You must repeat this step.

7. Click **Next**.

   The Services Director **FLA License** page appears. This page enables you to add a Legacy FLA license if you are using a Traffic Manager at version 10.0 (or earlier), or wish to disable the REST API for any of your Traffic Manager instances.

   FIGURE 24 Setup Wizard: Services Director FLA License Page



Services Director FLA License

If you have a legacy FLA license, you can choose to paste it into the box below. A legacy FLA license is only required if you plan to use instances of vTM that:

- Are older than version 10.1.
- Have the vTM REST API disabled.

● I don't want to install a legacy FLA license

○ I want to install a legacy FLA license

8. Select one of the following options:

   - **I don't want to install a legacy FLA license**. You will do this for one of the following reasons:
     - You want to use the installed Universal FLA License. To support this selection, all of your Traffic Manager instances must be running version 10.1 (or later) with the REST API enabled.
     - You do not want to install a Legacy FLA License at this time. This can be entered using the Services Director VA graphical interface after it is deployed.

   A default Feature Pack will not be created, but this can be created at a later date. Refer to Adding a Feature Pack to the Services Director on page 70.

   Continue from the next step.

   - **I want to install a legacy FLA license**. You will do this if any of your traffic managers are running at version 10.0 (or earlier) or have their REST API disabled. Paste the text of your Legacy FLA License into the box. This is validated automatically.

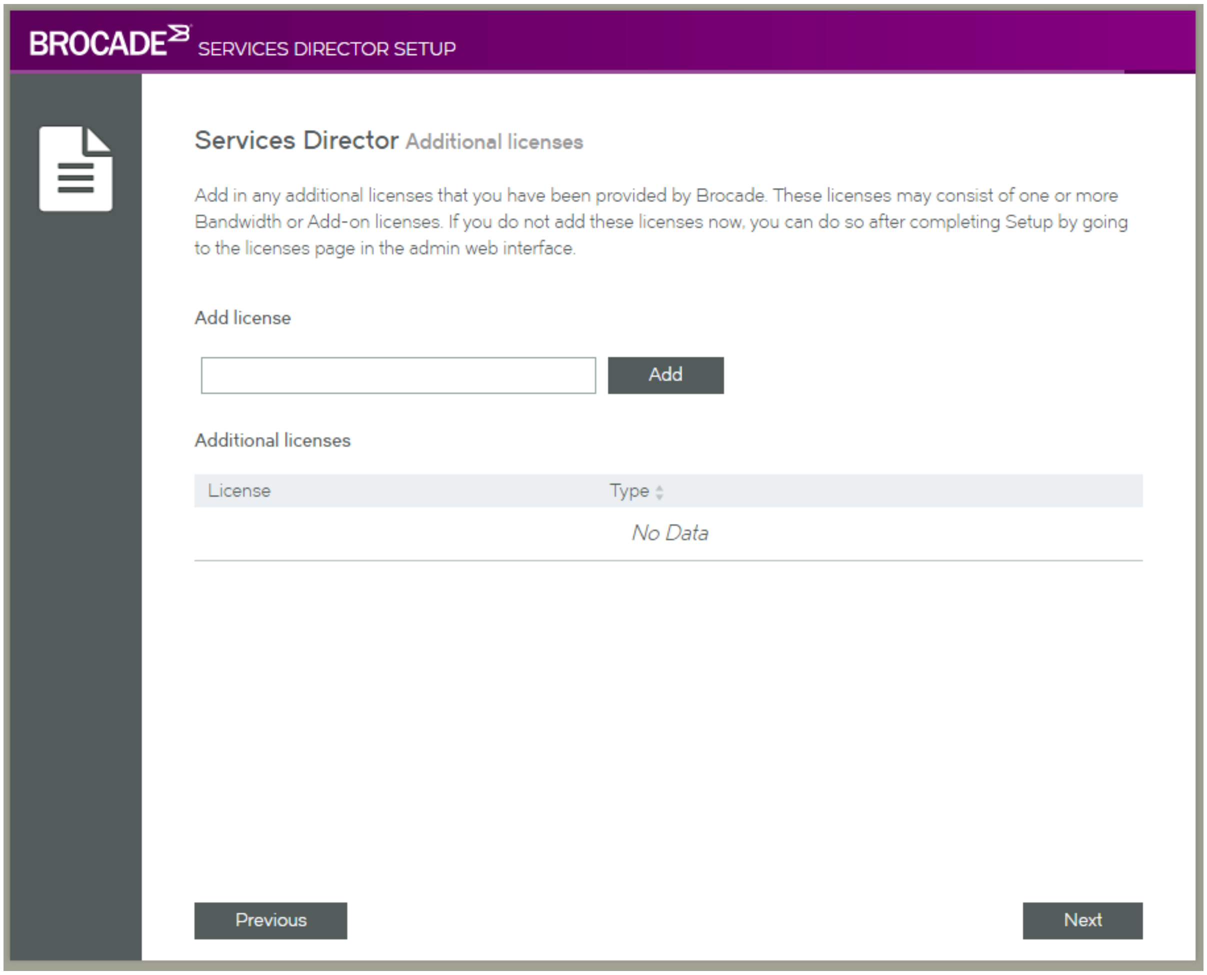
9. Click **Next**. The Services Director **Additional Licenses** page appears.

   If you have Bandwidth Licenses and Add-On Licenses, use this page to enter them.

   NOTE
   If you do not have Bandwidth Licenses and Add-On Licenses at this point, you can still continue with the Setup Wizard. You can enter these licenses using the Services Director VA after it is deployed.

   NOTE
   If you have a Cloud Services Provider (CSP) License for your Services Director, you do not require either Bandwidth Licenses or Add-On Licenses, and can ignore this page.

   FIGURE 25 Setup Wizard: Services Director Additional Licenses Page



Services Director Additional licenses

Add in any additional licenses that you have been provided by Brocade. These licenses may consist of one or more Bandwidth or Add-on licenses. If you do not add these licenses now, you can do so after completing Setup by going to the licenses page in the admin web interface.

License	Type
No Data	

10. Enter a license number and click **Add**.

    This license is validated automatically. Once validation completes, either:

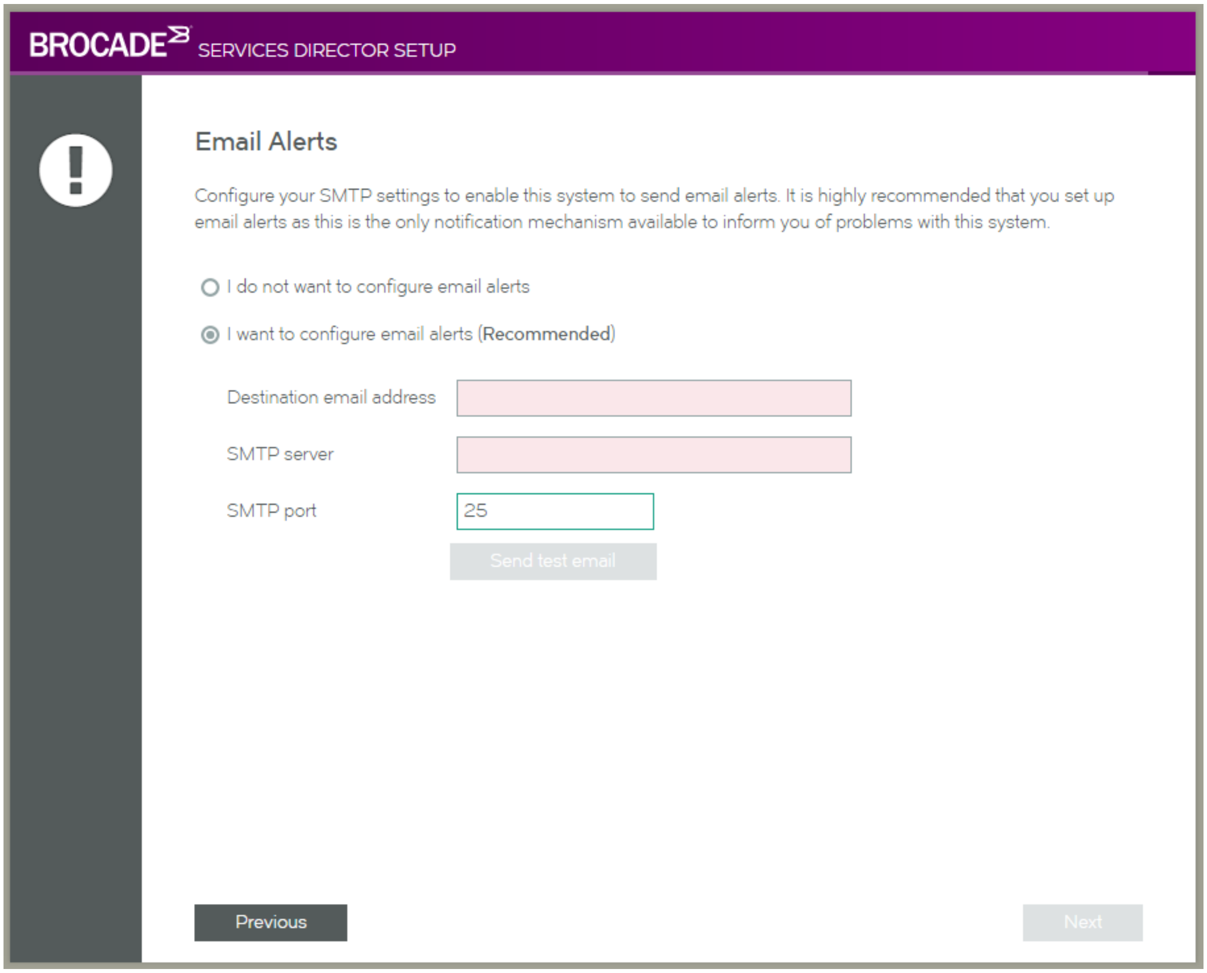
    - The retrieved information for the license is listed in the **Additional licenses** table. OR
    - A failure message is displayed.

11. Repeat the previous step to add all available licenses.

12. Click **Next**. The **Email alerts** page appears.

    This page enables you to optionally enter email notification details for your Services Director. This ensures that you receive email notifications for events and failures.
    You do not have to enter this information now. It can be entered using the Services Director VA after it is deployed. Refer to Updating Email Settings on page 62.

    FIGURE 26 Setup Wizard: Email Alerts Page



BROCADE SERVICES DIRECTOR SETUP

Email Alerts

Configure your SMTP settings to enable this system to send email alerts. It is highly recommended that you set up email alerts as this is the only notification mechanism available to inform you of problems with this system.

○ I do not want to configure email alerts

● I want to configure email alerts (**Recommended**)

Destination email address

SMTP server

SMTP port 25

13. Select one of the following options:
    - **I do not want to configure email alerts**. This option enables you to bypass this step. This information can be entered using the Services Director VA graphical interface after it is deployed. Refer to Updating Email Settings on page 62.
    - **I want to configure email alerts**. This is the recommended option. Then, provide:
      - A **Destination email address**.
      - An **SMTP server**. This is either the hostname or IP address of the SMTP server in your network.
      - An **SMTP port** number. Typically, you will use the default port number, 25.

14. Click **Send test email** to confirm these settings.

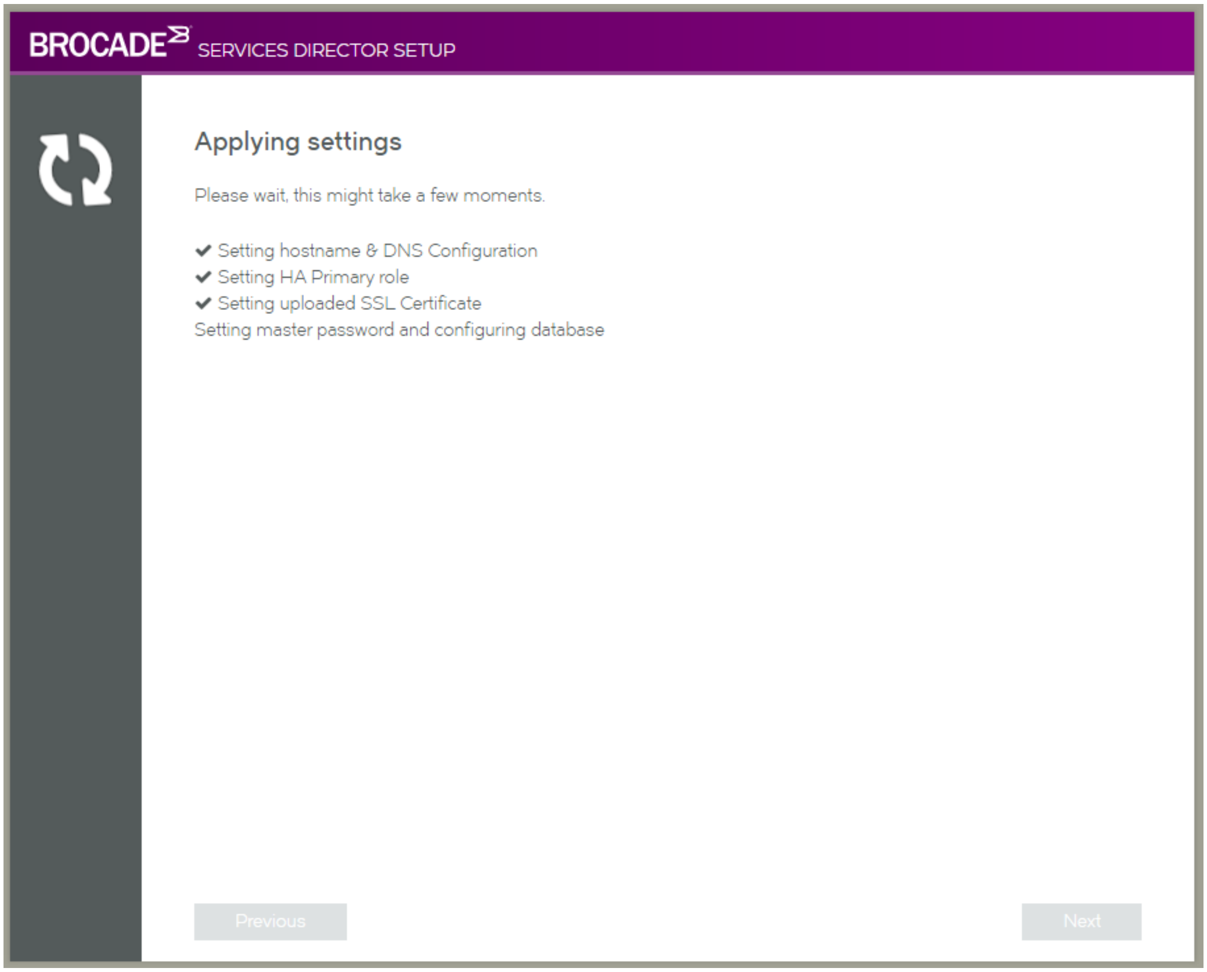
    NOTE
    You must have external access for SMTP traffic for this feature to function.

15. Click **Next**, and continue from Completing the Services Director Installation on page 51.

Completing the Services Director Installation

After all information is gathered, the **Applying Settings** page appears. This page configures the system based on collected information. For example:

FIGURE 27 Setup Wizard: Applying Settings Page



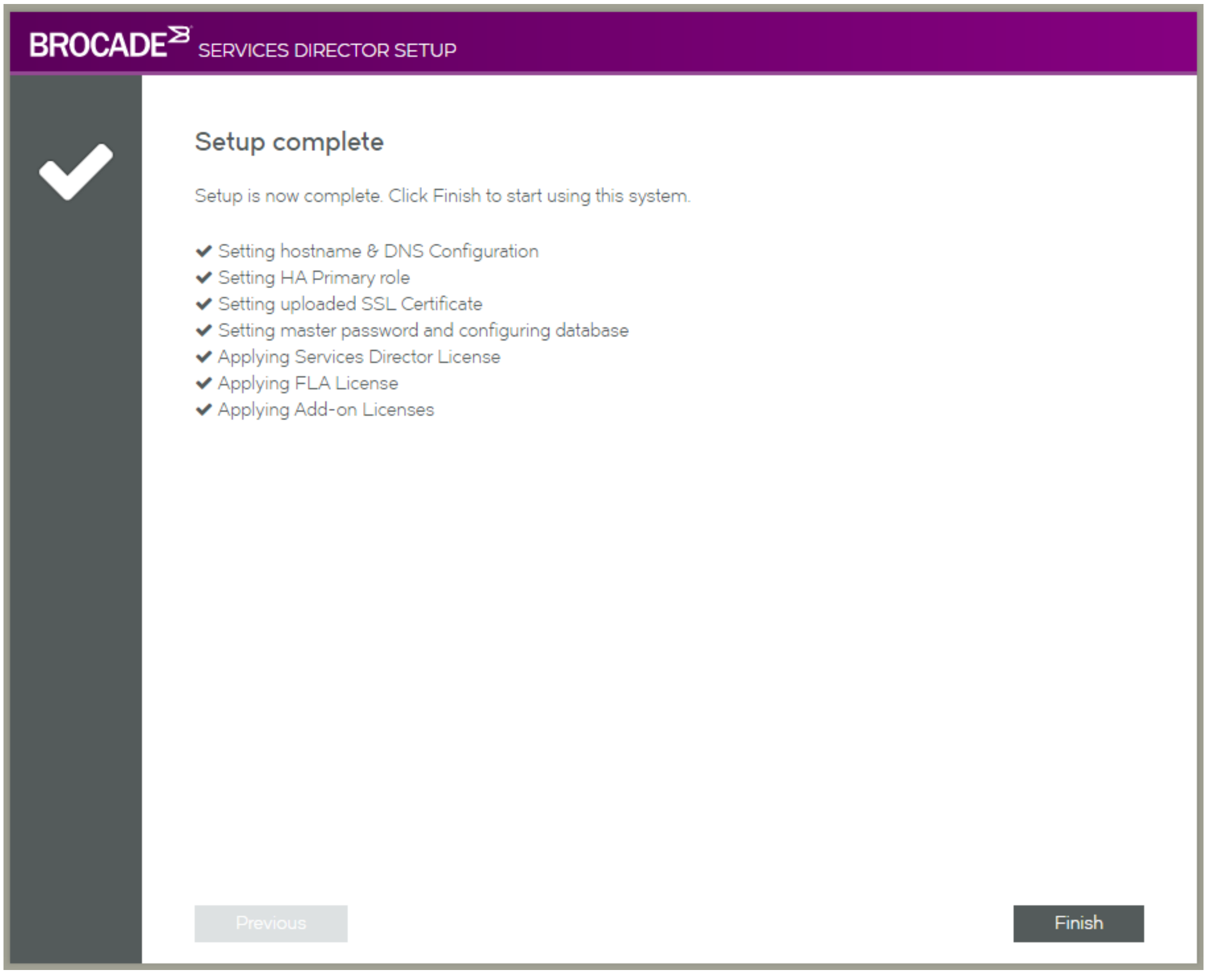
Applying settings

Please wait, this might take a few moments.

✓ Setting hostname & DNS Configuration
✓ Setting HA Primary role
✓ Setting uploaded SSL Certificate
Setting master password and configuring database

Once this is complete, the **Setup Complete** page appears.

FIGURE 28 Setup Wizard: Setup Complete Page



Setup complete

Setup is now complete. Click Finish to start using this system.

- ✓ Setting hostname & DNS Configuration
- ✓ Setting HA Primary role
- ✓ Setting uploaded SSL Certificate
- ✓ Setting master password and configuring database
- ✓ Applying Services Director License
- ✓ Applying FLA License
- ✓ Applying Add-on Licenses

Click **Finish** to close the setup wizard.

Once the setup wizard completes, your Services Director is deployed.

If required, you can now create a Secondary Services Director, and join it to the Primary Services Director. Refer to Installing and Configuring a Secondary Services Director on page 53.

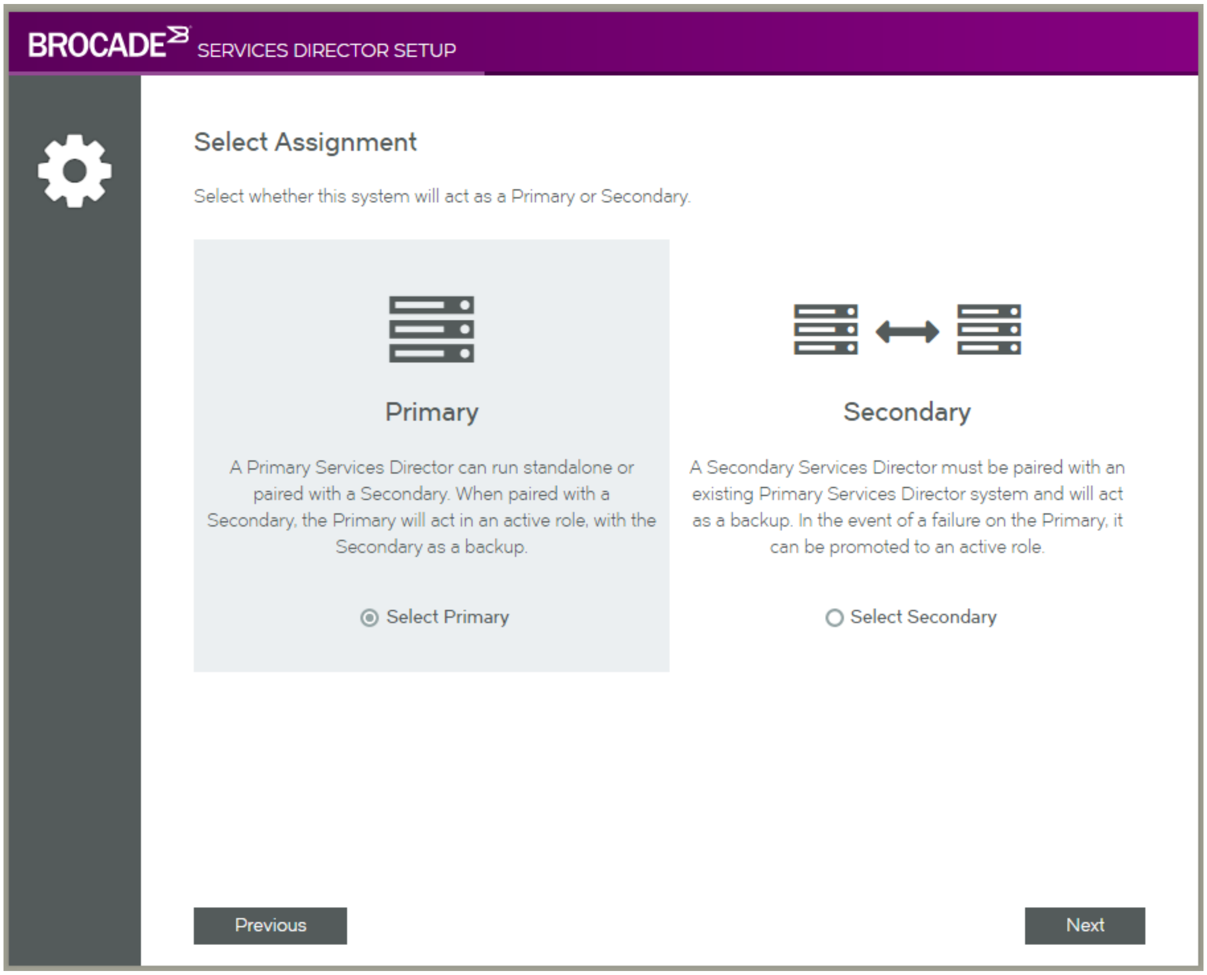
> NOTE
>
> Once the Setup Wizard completes, it cannot be rerun. Many of the options chosen in the Setup Wizard can be reconfigured from inside the Services Director VA, but others can only be reconfigured from the Command-Line Interface (CLI). Refer to *Brocade Services Director Advanced User Guide* and the *Brocade Services Director Command Reference* for full details.

Installing and Configuring a Secondary Services Director

The process for creating a Secondary Services Director is similar to the installation for a Primary Services Director.

1. Repeat the installation process for a Primary Services Director (see Starting a Services Director Installation on page 29) until you reach the following screen:

FIGURE 29 Setup Wizard: Select Assignment



Select Assignment

Select whether this system will act as a Primary or Secondary.

Primary

A Primary Services Director can run standalone or paired with a Secondary. When paired with a Secondary, the Primary will act in an active role, with the Secondary as a backup.

● Select Primary

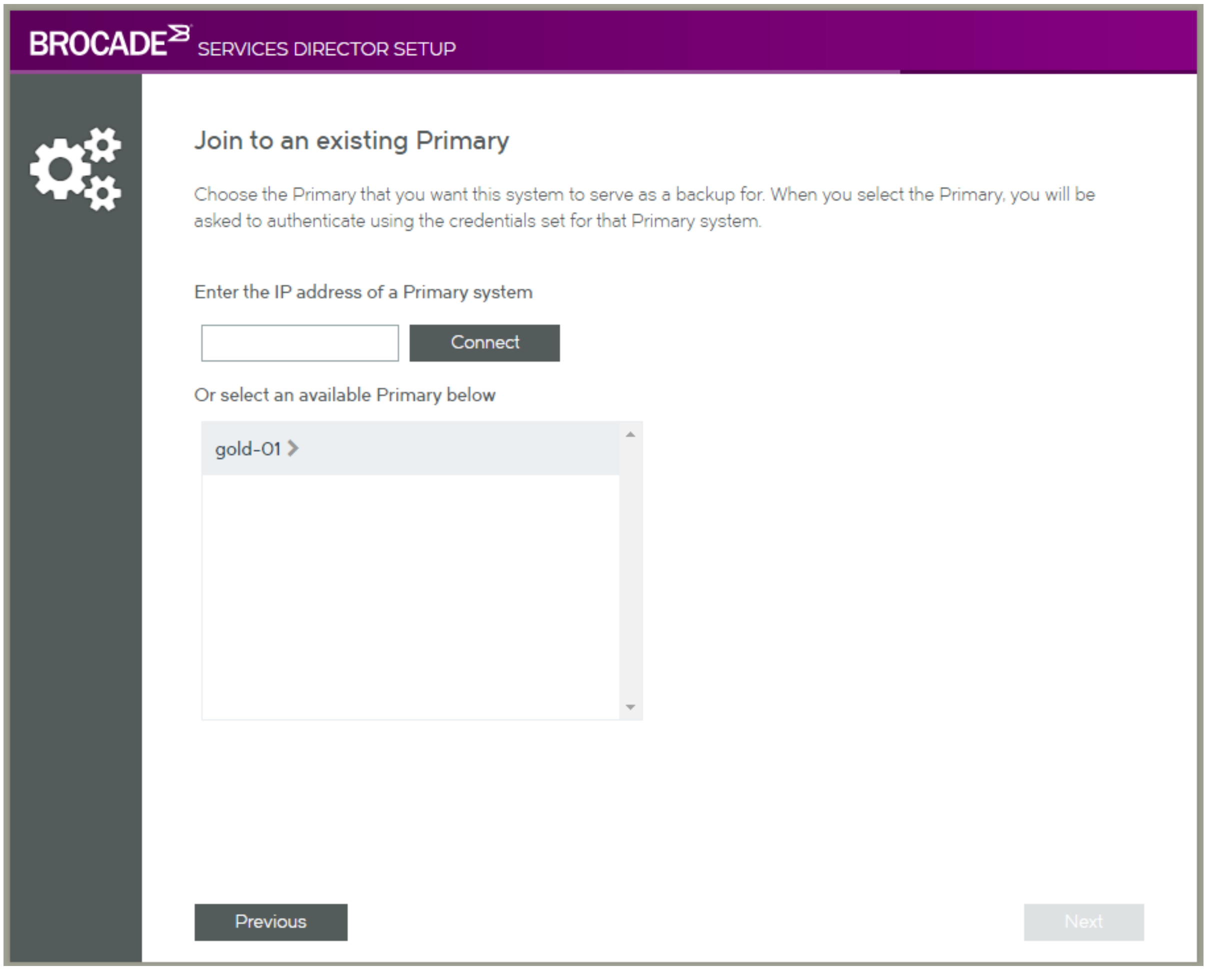
Secondary

A Secondary Services Director must be paired with an existing Primary Services Director system and will act as a backup. In the event of a failure on the Primary, it can be promoted to an active role.

○ Select Secondary

2. Click Secondary.
   The **Join to an Existing Primary** page appears.

   FIGURE 30 Setup Wizard: Join to an Existing Primary Page



Join to an existing Primary

Choose the Primary that you want this system to serve as a backup for. When you select the Primary, you will be asked to authenticate using the credentials set for that Primary system.

Enter the IP address of a Primary system

Or select an available Primary below

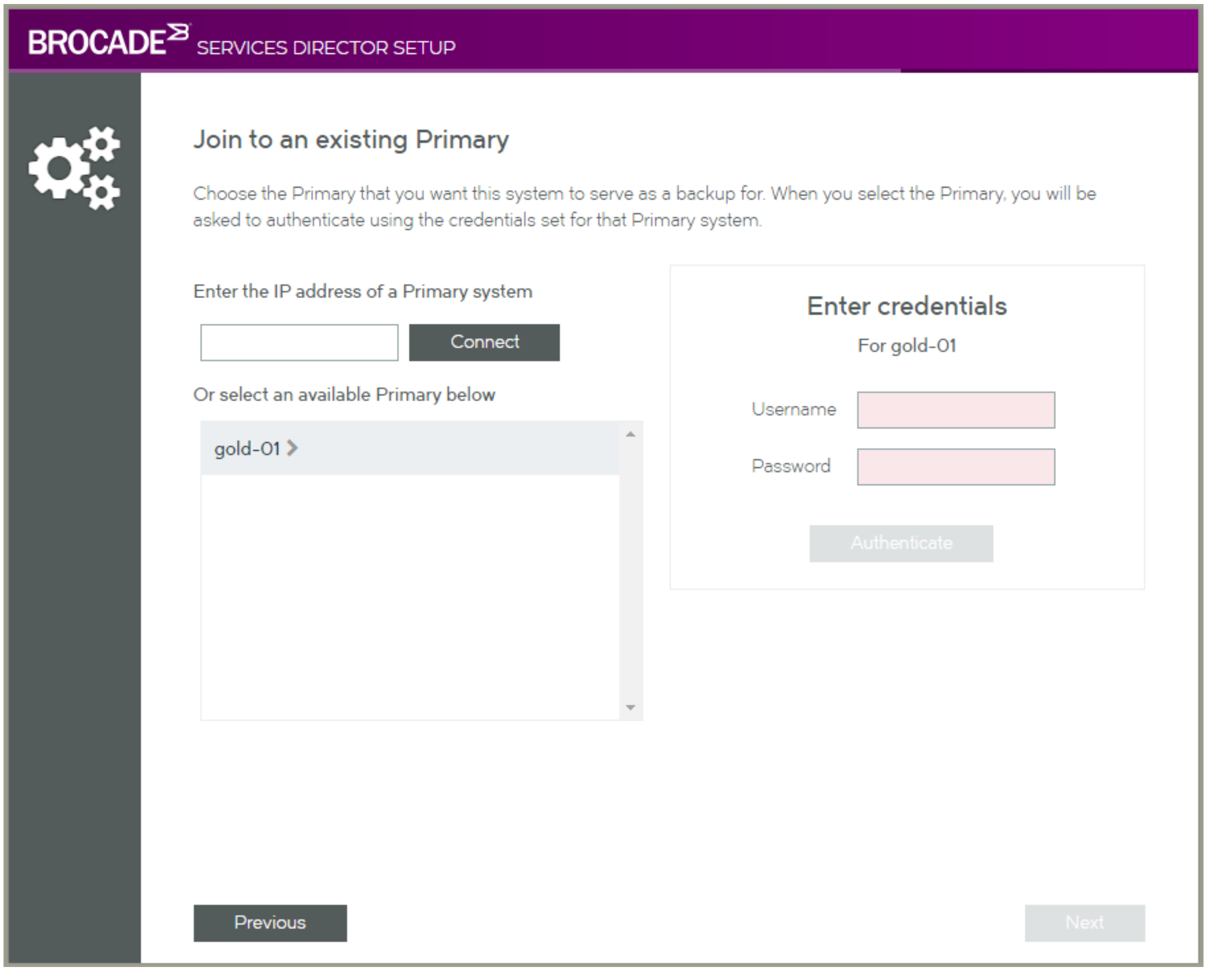
gold-01

3. To connect to an existing Primary Services Director, either:
   - Select the Primary Services Director from the list.
   - Enter the IP address of the Primary Services Director.

4. Click **Connect**.

   The page updates to include credential authentication fields.

   FIGURE 31 Setup Wizard: Join to an Existing Primary: Credentials Page



Join to an existing Primary

Choose the Primary that you want this system to serve as a backup for. When you select the Primary, you will be asked to authenticate using the credentials set for that Primary system.

Enter the IP address of a Primary system

Or select an available Primary below

Enter credentials

For gold-01

5. Enter an administration **Username** and **Password** for the Primary Services Director.

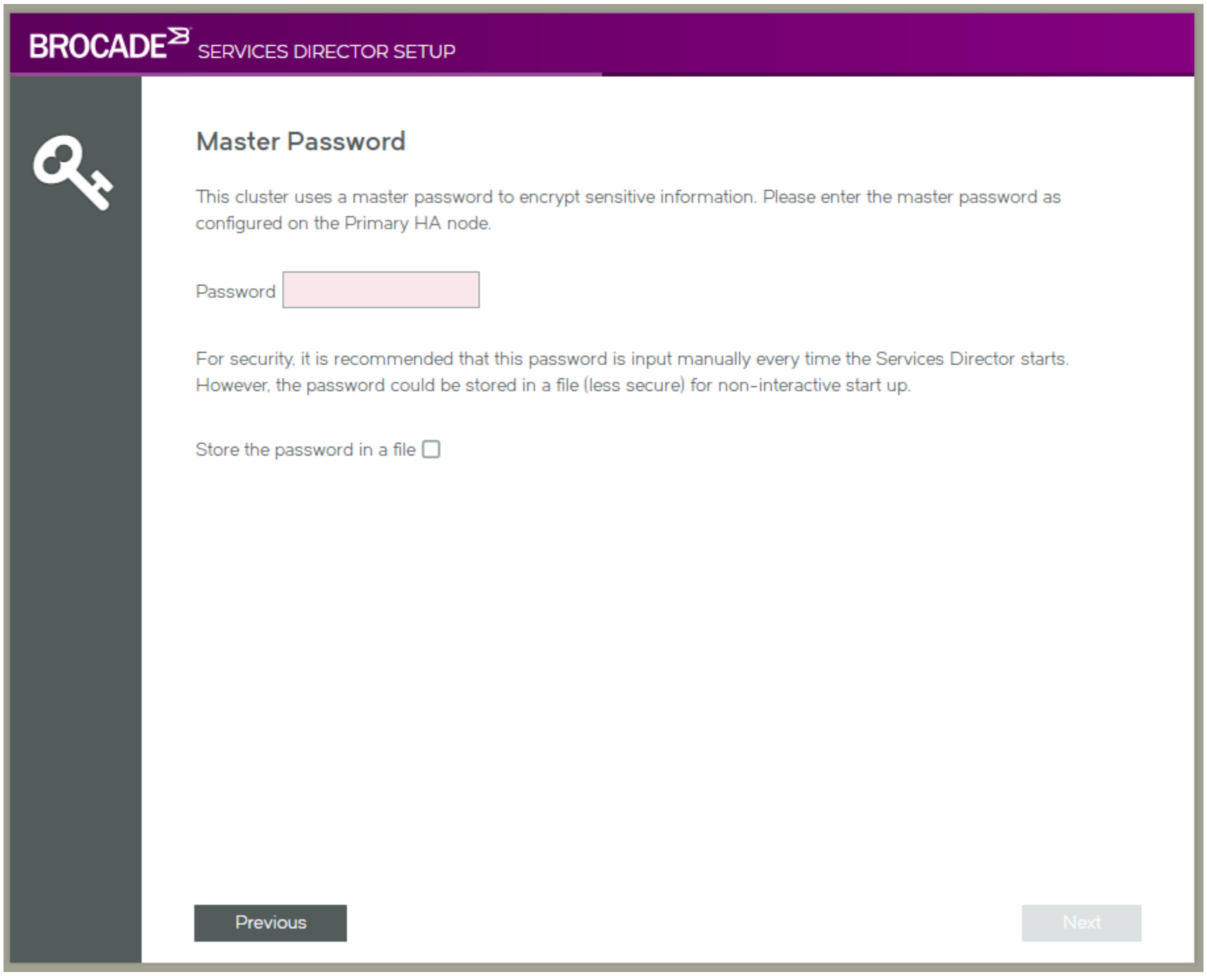
   NOTE
   The master password is not required until the next page of the wizard.

6. Click **Authenticate**.

7. Click **Next**.

   The Services Director **Master Password** page appears. This page requires you to enter the master password that you chose for the Primary Services Director VA. This is required to decrypt stored password information whenever the Virtual Machine for a Services Director VA node restarts, or a backup of this Services Director VA node is used to restore/create a Services Director VA (refer to Recovering from a Services Director Failure on page 237).

   FIGURE 32 Setup Wizard: Services Director Master Password Page



Master Password

This cluster uses a master password to encrypt sensitive information. Please enter the master password as configured on the Primary HA node.

Password

For security, it is recommended that this password is input manually every time the Services Director starts. However, the password could be stored in a file (less secure) for non-interactive start up.

Store the password in a file □

8. Enter the master password. The password is validated immediately.

   NOTE
   It is essential that the master password (whether chosen yourself or generated automatically) is recorded and can be retrieved. Brocade recommends that this password is recorded in a secure location that is separate from the Services Director VA.

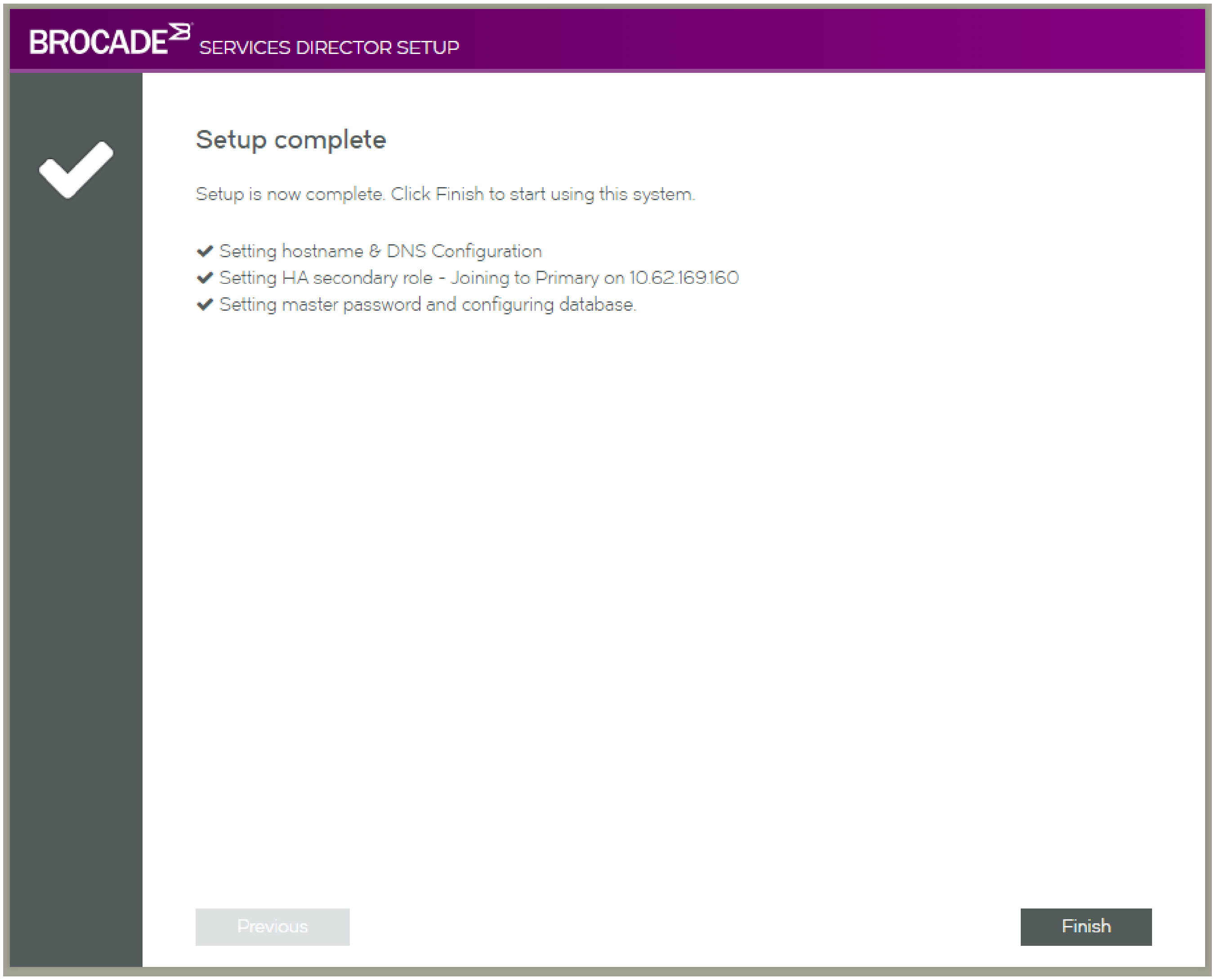
9. Choose whether to store the password internally for automatic use:
   - Select the **Store the password in a file** check box to store the master password within the Services Director VA. The password will be automatically available whenever the Virtual Machine for a Services Director VA restarts. However, you must enter the master password manually when you create a Services Director VA from a backup file.
   - Clear the **Store the password in a file** check box to not record the master password. You must to enter the master password manually whenever the Virtual Machine for a Services Director VA restarts, and when you create a Services Director VA from a backup file.

   Refer to Entering the Master Password After a Virtual Machine Restart on page 254 for details of restarting a VM.
10. Click **Next**.

    The Secondary Services Director now joins with the Primary Services Director to form a HA pair. The progress of this process appears on the **Applying Settings** page.

    Once this process completes, the **Setup Complete** page appears.

FIGURE 33 Setup Wizard: Setup Complete Page (Secondary Services Director)



Setup complete

Setup is now complete. Click Finish to start using this system.

✓ Setting hostname & DNS Configuration
✓ Setting HA secondary role - Joining to Primary on 10.62.169.160
✓ Setting master password and configuring database.

Accessing your Services Director VA

Once the Setup Wizard is complete, you can access the Services Director VA using a secure (https) URL in a browser:

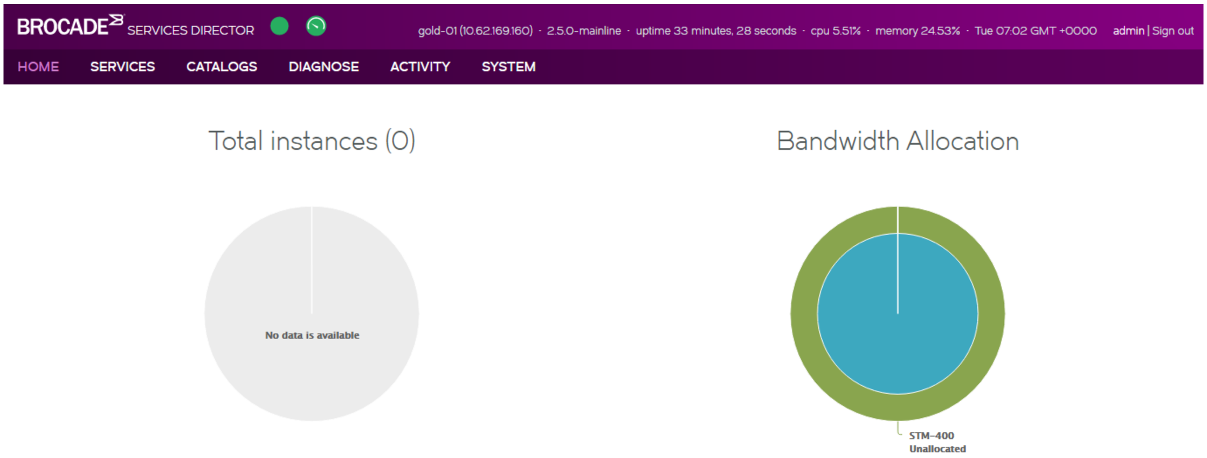
- For an HA pair, you access the active Services Director using the Service Endpoint IP address.

  NOTE
  If the Services Director HA pair is in a private network behind a NAT device, access the active Services Director using the external IP address of the Service Endpoint Address.

- You can access a standalone Services Director using its IP address or Service Endpoint IP address.
- You can access the Primary Services Director directly using its IP address.
- You can access the Secondary Services Director directly using its IP address.

Log in to the Services Director VA. The **Home** page appears:

FIGURE 34 The Home Page


BROCADE SERVICES DIRECTOR
gold-01 (10.62.169.160) · 2.5.0-mainline · uptime 33 minutes, 28 seconds · cpu 5.51% · memory 24.53% · Tue 07:02 GMT +0000
admin | Sign out
HOME
SERVICES
CATALOGS
DIAGNOSE
ACTIVITY
SYSTEM
Total instances (0)
No data is available
Bandwidth Allocation
STM-400
Unallocated

The "Brocade Services Director" header displays two coloured indicators:

- The first is an indication of system health. This includes: high availability, the Services Director license, and the availability of the service.

  A healthy system displays a green circle, and an unhealthy system displays an orange warning triangle.

- The second is an indicator for metering discrepancies for the vTMs within the estate of the Services Director VA.

  A healthy metering system results in a green meter. An unhealthy metering system displays as an orange warning meter. Refer to Processing Traffic Manager Metering Discrepancy Warnings on page 145.

At this point, no Traffic Managers are registered on the Services Director VA.

The **Home** page displays the **Bandwidth Allocation** for any a Bandwidth License that was installed during the Setup Wizard.

Optionally, you may wish to fine-tune settings for the Services Director VA. Refer to Updating Services Director VA Settings on page 59.

Otherwise, you can now proceed with the registration of Traffic Managers and additional system configuration. Refer to Adding Traffic Managers to the Services Director on page 67.

Updating Services Director VA Settings

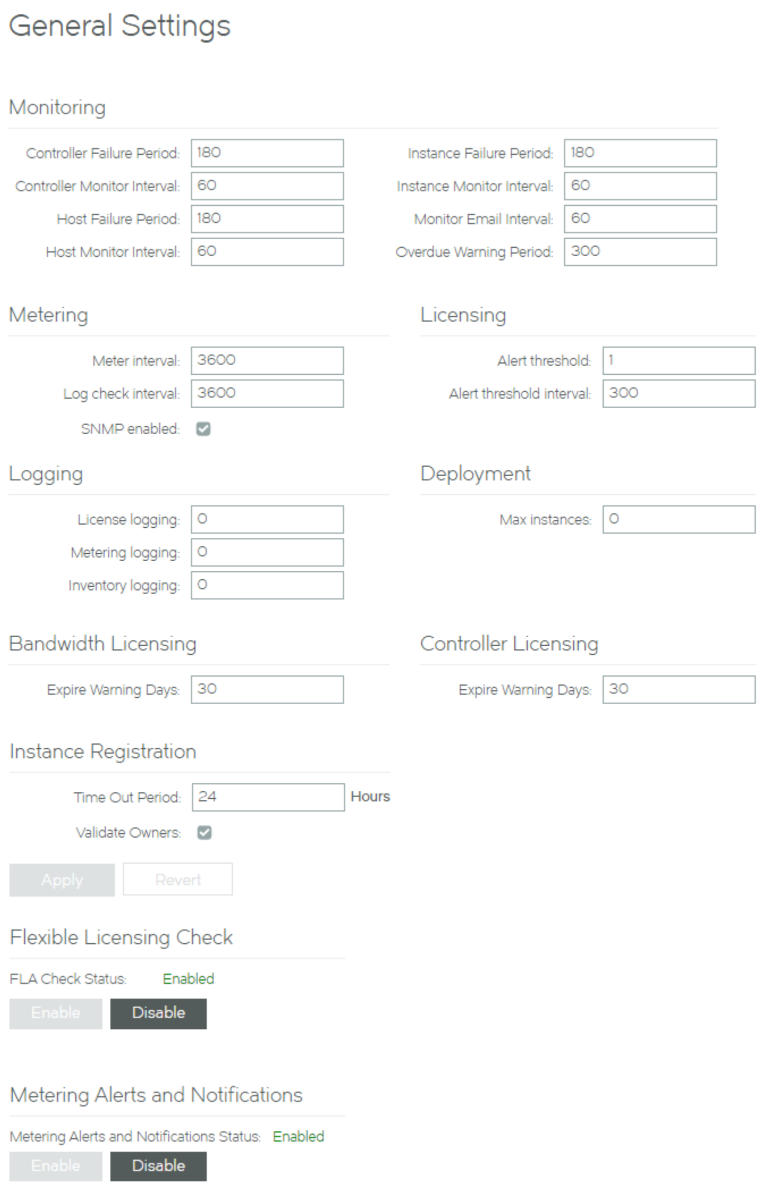
Many of the configured settings for the Services Director can be updated from the Services Director VA **System** menu.

Updating General Settings

You can change a variety of general settings for Services Director VA from the **System** > **General Settings** page. Defaults are applied automatically when the Services Director VA is created. You only need to update these settings to fine-tune the Services Director VA to your specific requirements.

Apply any changes to put them into use immediately.

FIGURE 35 General Settings Page



General Settings

Monitoring

Controller Failure Period: 180
Controller Monitor Interval: 60
Host Failure Period: 180
Host Monitor Interval: 60
Instance Failure Period: 180
Instance Monitor Interval: 60
Monitor Email Interval: 60
Overdue Warning Period: 300

Metering

Meter interval: 3600
Log check interval: 3600
SNMP enabled: ☑

Licensing

Alert threshold: 1
Alert threshold interval: 300

Logging

License logging: 0
Metering logging: 0
Inventory logging: 0

Deployment

Max instances: 0

Bandwidth Licensing

Expire Warning Days: 30

Controller Licensing

Expire Warning Days: 30

Instance Registration

Time Out Period: 24 Hours
Validate Owners: ☑

Flexible Licensing Check

FLA Check Status: Enabled

Metering Alerts and Notifications

Metering Alerts and Notifications Status: Enabled

Updating Monitoring Settings

The following settings enable you to configure monitoring.

- **Controller Failure Period** - the period of time, in seconds, after which a Services Director is considered to have failed. The default value is 180.
- **Controller Monitor Interval** - the period of time, in seconds, between monitoring the Services Director. The default value is 60.
- **Host Failure Period** - the period of time, in seconds, after which a host is considered to have failed. The default value is 180.
- **Host Monitor Interval** - the period of time, in seconds, between monitoring hosts. The default value is 60.
- **Instance Failure Period** - the period of time, in seconds, after which the instance is considered to have failed. The default value is 180.
- **Instance Monitor Interval** - the period of time, in seconds, between monitoring instances. The default value is 60.
- **Monitor Email Interval** - the period of time, in seconds, between monitoring alert emails. The default value is 60.
- **Overdue Warning Period** - the period of time, in seconds, to consider monitoring overdue. The default value is 300.

Updating Metering Settings

The following settings enable you to configure metering.

- **Meter Interval** - the period of time, in seconds, between metering actions. The range is from 1-3600. The default value is 3600 seconds (1 hour).
- **Log Check Interval** - the period of time, in seconds, between checks for log space. The range is from 1-3600. The default value is 3600 seconds (1 hour).
- **SNMP enabled** - this check box is used to enable/disable the use of SNMP. SNMP is used to gather certain types of information (such as metering) from the Traffic Managers in the estate of the Services Director.

Updating Licensing Settings

The following settings enable you to configure licensing.

- **Alert Threshold** - the number of alerts that sent. The range is from 1-3600. The default is 1.

The threshold and interval settings enable you to determine how many requests have to be received by a non-primary license server in the specified interval before an alert email is sent to the configured alert email addresses. After the threshold and interval is reached then an alert message is sent. At most, one message is sent per hour, to protect against a flood of messages being sent in the case of complete failure of the primary license server on a busy system.

- **Alert Threshold Interval** - the period of time, in seconds, between alerts. The range is from 1-3600. The default value is 3600 seconds (1 hour).

The threshold and interval settings enable you to specify the time interval before an alert email is sent to the configured alert email addresses. After the threshold and interval is reached, an alert message is sent. At most one message is sent per hour, to protect against a flood of sent messages in the case of complete failure of the primary license server on a busy system.

Updating Logging Settings

The following settings enable you to configure logging.

- **License Logging** - a license value. The range is from 0-10.
  - The default value is 0, which equals no logging.
  - A log level of 3 or higher causes responses to license server requests to be logged in full, including the feature values set by the feature pack and bandwidth associated with the instance making the request.

- **Metering Logging** - the metering logging value. The range is from 0-10.
  - The default value is 0, which equals no logging.
  - A log level of 5 or higher gives a summary of the activities of the metering thread (that is, starting metering, stopping metering, and so forth)
  - A log level of 9 or higher provides a detailed logging of each instance being metered.
- **Inventory Logging** - the metering logging value. The range is 0-10.
  - The default value is 0, which equals no logging.
  - A log level of 1 or higher will cause inventory changes to be logged (the equivalent of the audit records).
  - A log level of 3 or higher causes logging of all deployment and action commands.
  - A log level of 8 or higher causes logging of the output from all deployment and actions.

Updating Deployment Settings

The following setting enables you to configure deployment.

- **Max Instances** - the maximum number of Traffic Manager instances that can be deployed. The default value is 0, which equals no limit. Typically, this is the correct value for most deployments. Note that:
  - Instances that have been deleted do not count towards the limit.
  - Instances that have been deployed but are not active (that is, have not been started) do count towards the limit.
  - If you create a new instance in excess of this number, the instance is rejected with an error message.
  - If this property is set to a lower number than the number of currently deployed instances then there is no immediate effect but subsequent deployment requests are rejected.

Updating Bandwidth Licensing Settings

The following setting enables you to configure bandwidth licensing.

- **Expire Warning Days** - the number of days to warn you before the bandwidth license expires. The default value is 30.

Updating Controller Licensing Settings

The following setting enables you to configure controller licensing.

- **Expire Warning Days** - the number of days to warn you before the controller license expires. The default value is 30.

Updating Instance Registration Settings

The following settings enables you to configure self-registration.

- **Time Out Period** - the number of hours before a Pending self-registration request will transition automatically to Blacklisted. The default is 24.
- **Validate Owners** - enables/disables the mandatory validation of the Owner property during the automatic self-registration of vTMs.

Updating Metering Alerts and Notifications Settings

The following setting enables you to configure the reporting of metering issues.

- **Metering Alerts and Notifications** - enables/disables the reporting of metering alerts and notifications. Refer to Processing Traffic Manager Metering Discrepancy Warnings on page 145.

Configuring the FLA Checker

The Services Director VA uses an automatic FLA checker. Refer to *Brocade Services Director Advanced User Guide* for details.

To configure the global Flexible Licensing Check, click **Enable** or **Disable**.

This selection is applied automatically.

Updating Date and Time Settings

You can change the date and time settings for the Services Director VA from the **System** > **Date and Time Settings** page. Settings are in three categories:

- Basic date and time settings. To change the basic settings, set the correct **Date** and **Time**, and click **Apply**.
- Time zone settings. To change the **Time Zone** for your Services Director, select the required time zone and click **Apply**.
- NTP settings. Where NTP is active, basic date and time settings are overwritten.
  - A default set of NTP services are listed. You can enable or disable any listed service by expanding the service entry and changing its state.
  - You can add another NTP service by clicking **Add** and specifying details for the service.
  - To stop the use of the NTP service, click **Stop**. Click **Start** to restart it.

Updating Administration Credentials

You can change the administration credentials for the Services Director VA from the **System > Administration Credentials** page. These credentials are used as follows:

- To log in to the Services Director VA.
- To access a terminal session for the Services Director, such as when you wish to use the command-line user interface.
- For REST API authentication.

Apply these changes to put them into use immediately. You will be required to authenticate using the new credentials.

Updating Email Settings

You can change the email settings for the Services Director VA from the **System** > **Email Alerts** page. This page enables you to enter email notification details for your Services Director, to ensure that you receive email notifications for events and failures. You must specify:

- **SMTP Server** - This is either the hostname or IP address of the SMTP server in your network.
- **SMTP Port** - Typically, you will use the default port number, 25.
- **Notification Email** - All email from the Services Director will go to each entry in this comma-separated list of e-mail addresses.
- **From Address** - The required "from" address for all emails.

  NOTE
  You can use "$fqdn" to substitute in this appliance's fully-qualified domain name.

NOTE
Services Director VA automatically restarts the Services Director service after email changes are applied.

Updating the SSL Certificate

You can replace the SSL certificate for the Services Director VA from the **Service SSL Certificate** page. Select one of the following options:

- **Single file with public and private keys**. Then, click **Choose File** to locate the certificate file.
- **Separate public and private key files**. Then, click **Choose File** to locate each file.
- **Text content of the public and private keys**. Then, paste the required text in.

Apply these changes to put them into use immediately.

Updating the REST API Port

You can update the REST API port used by the Services Director VA from the **System** > **Service Status** page. Apply this change to put the new port number into use immediately.

You can also start, stop and restart the Services Director service from this page. Refer to Starting and Stopping the Services Director Service on page 253.

Updating Security Settings

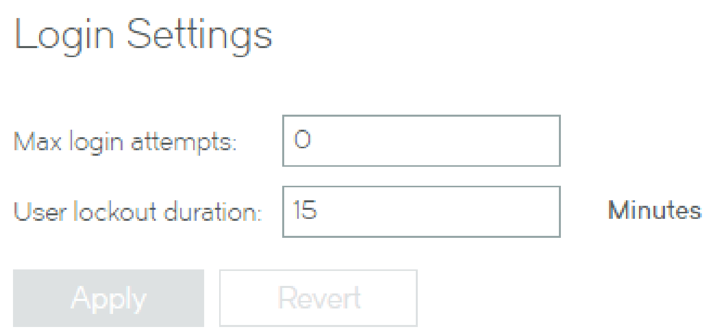
You can change the security settings for Services Director VA from the **System** > **Security Settings** page. Defaults are applied automatically when the Services Director VA is created.

This page supports the following functions:

- Changing the Master Password for your Services Director. Refer to Changing the Master Password for the Services Director VA on page 64.
- Enabling shell access for command line users of the Services Director. Refer to the *Brocade Services Director Advanced User Guide*.

You can also define the suspension criteria for failed Services Director logins.

FIGURE 36 Security Settings Page: Suspension Settings



Login Settings

Max login attempts: 0

User lockout duration: 15 Minutes

The **Max login attempts** defines the maximum number of failed Services Director login attempts for a user. Zero (the default setting) indicates that there is no maximum.

If the **Max login attempts** limit is reached, a lockout defined by the **User lockout duration** is applied. This has a default of 1 minute, and a maximum of 1440 minutes (equal to one day).

After the lockout period has ended, the same user can continue to attempt to log in.

Changing the Master Password for the Services Director VA

The master password for the Active Services Director VA can be changed from the **Security Settings** page.

> NOTE
> If you wish to *reset* the master password (that is, you do not know what the current master password is), refer to the *Brocade Services Director Advanced User Guide*.

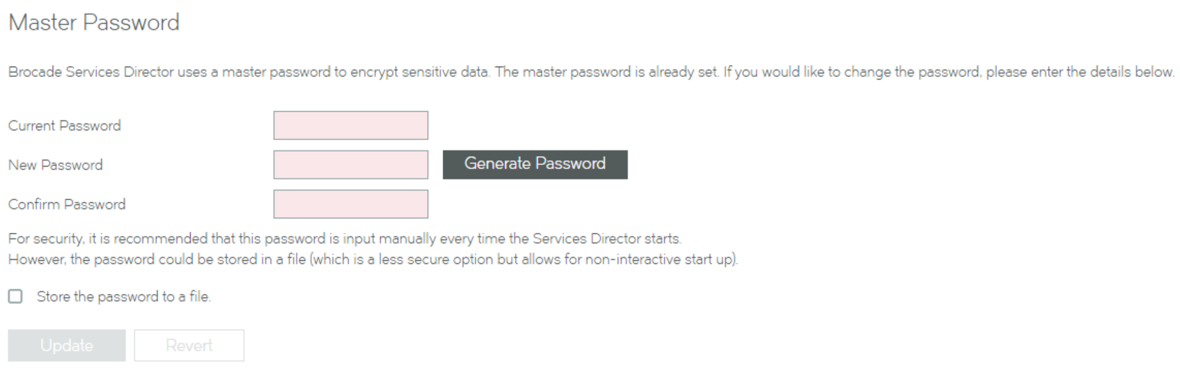
Changing the Master Password

The master password for the Active Services Director VA can be changed from the **Security Settings** page.

> NOTE
> If you wish to *reset* the master password (that is, you do not know what the current master password is), refer to the *Brocade Services Director Advanced User Guide*.

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.
3. Click the **System** Menu, then click **Security**. The **Security Settings** page appears.

FIGURE 37 Security Settings Page



Master Password

Brocade Services Director uses a master password to encrypt sensitive data. The master password is already set. If you would like to change the password, please enter the details below.

Current Password

New Password

Confirm Password

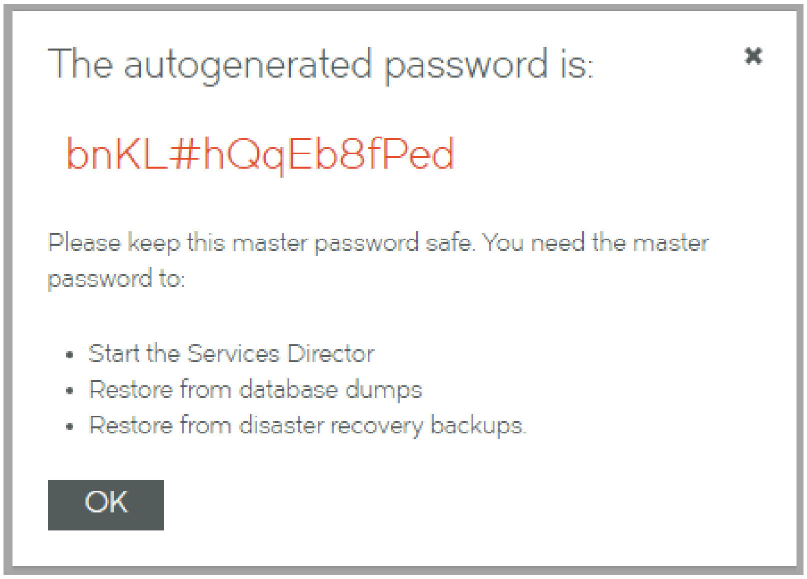
For security, it is recommended that this password is input manually every time the Services Director starts.
However, the password could be stored in a file (which is a less secure option but allows for non-interactive start up).

☐ Store the password to a file.

4. Enter the **Current Password**.

5. To change the master password, perform one of the following operations.
   - Enter a new password and confirm the password.
   - Click **Generate Password**. The **Password** and **Confirm Password** fields are populated automatically and an information dialog box is displayed.

   FIGURE 38 Autogenerated Password Dialog Box

   The autogenerated password is:

   bnKL#hQqEb8fPed

   Please keep this master password safe. You need the master password to:

   - Start the Services Director
   - Restore from database dumps
   - Restore from disaster recovery backups.

   Click **OK** to close the information dialog box after recording the password, and then confirm that you have stored the password in the next dialog box.

   > NOTE
   > It is essential that the master password (whether chosen yourself or generated automatically) is recorded and can be retrieved. Brocade recommends that this password is recorded in a secure location that is separate from the Services Director VA.

6. Choose whether to store the password internally for automatic use:
   - Select the **Store the password in a file** check box to store the master password within the Services Director VA. The password will be automatically available whenever the Virtual Machine for a Services Director VA restarts. However, you must enter the master password manually when you create a Services Director VA from a backup file.
   - Clear the **Store the password in a file** check box to not record the master password. You must to enter the master password manually whenever the Virtual Machine for a Services Director VA restarts, and when you create a Services Director VA from a backup file.

   Refer to Entering the Master Password After a Virtual Machine Restart on page 254 for details of restarting a VM.
7. Select the **Store the password to a file** check box if you want to store the master password internally for future use.

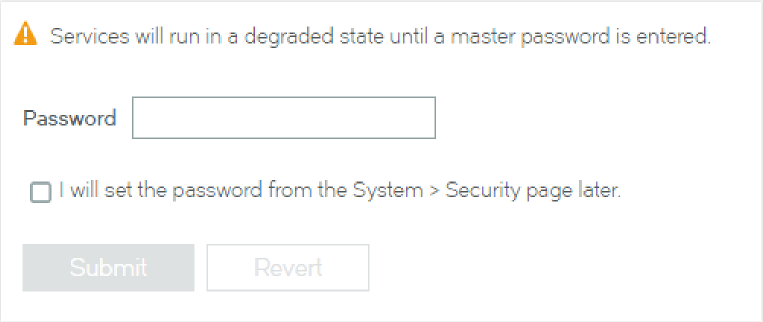
   > NOTE
   > If you do not choose to store this password, you must enter it after the Virtual Machine for this Services Director VA restarts (refer to Entering the Master Password After a Virtual Machine Restart on page 254).

8. Click **Update**. The master password is changed.

9. Access your Standby Services Director VA from a browser.
10. Log in as the administration user.

    A dialog box requesting the new master password immediately appears:

    FIGURE 39 Master Password Required



⚠ Services will run in a degraded state until a master password is entered.

Password

□ I will set the password from the System > Security page later.

NOTE

You may receive an e-mail notification of a raised **master_password_fail** alarm between you changing the master password on the Active Services Director VA and entering the new master password on the Standby Services Director VA.

11. Enter the new master password and click **Submit**.

Adding Traffic Managers to the Services Director

Overview: Adding Traffic Managers to the Services Director

The Services Director supports several methods for adding a Virtual Traffic Manager (vTM) to the estate of the Services Director:

- By registering an externally-deployed vTM from the Services Director. Refer to Registering an Externally-Deployed Traffic Manager on page 91.
- By processing a self-registration request that was received from an externally-deployed vTM by the Services Director. Refer to Self-Registering an Externally-Deployed Traffic Manager on page 107.
- By deploying a vTM from the Services Director VA using an instance host. Refer to the *Brocade Services Director Advanced User Guide* for full details.

Before you perform any of these methods, you must create any required resources, refer to Creating Resources Required For Traffic Managers on page 67.

Creating Resources Required For Traffic Managers

Before you attempt to register any Traffic Manager, you must create any required resources. The tasks required will vary according to your specific configuration.

- Create any required Feature Packs, refer to Adding a Feature Pack to the Services Director on page 70.
- Create any required Owner entries, refer to Adding an Owner to the Services Director on page 83.
- Create any required Legacy licenses, refer to Adding a Legacy FLA License to the Services Director on page 67.
- Create any required Access Profiles, refer to Creating an Access Profile (vTM User Authentication Only) on page 192.

Adding a Legacy FLA License to the Services Director

The Brocade Services Director comes with a pre-installed *Universal FLA License*. This is suitable for any Traffic Manager at version 10.1 or later with an active REST API. In all other cases, a *Legacy FLA License* is required. That is:

- The Traffic Manager version is 10.0 or earlier.
- The Traffic Manager (any version) has its REST API disabled.

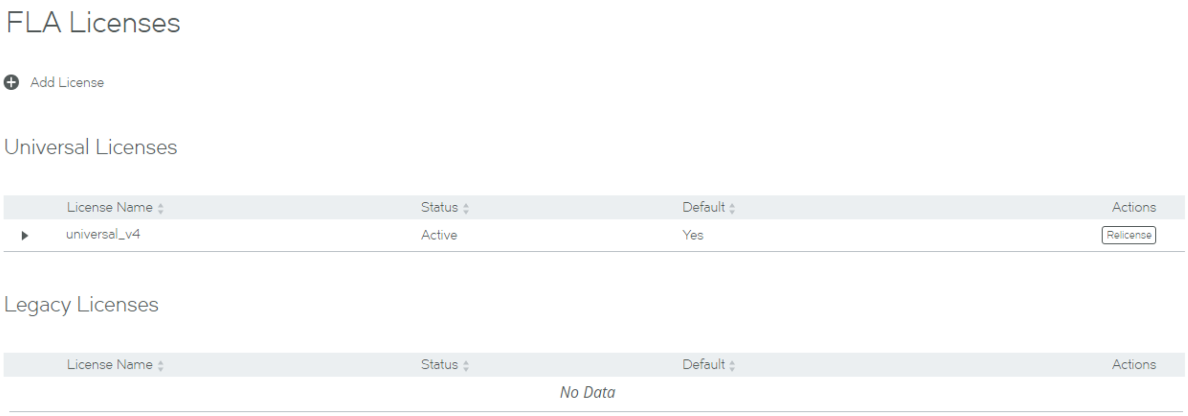
You can install a Legacy FLA License using the Services Director VA, after which you can install either of these Traffic Manager types.

This procedure can also be used to update a Legacy FLA license to a Universal FLA License.

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.
3. Click the **Catalogs** menu, and then click **Licensing: FLA Licenses**. The **Flexible Licenses** page appears.

   NOTE
   When the Services Director is first installed, only the pre-installed Universal FLA License is shown on this page; no Legacy FLA Licenses are present.

   FIGURE 40 Flexible Licenses Page: No Legacy FLA



FLA Licenses

Universal Licenses

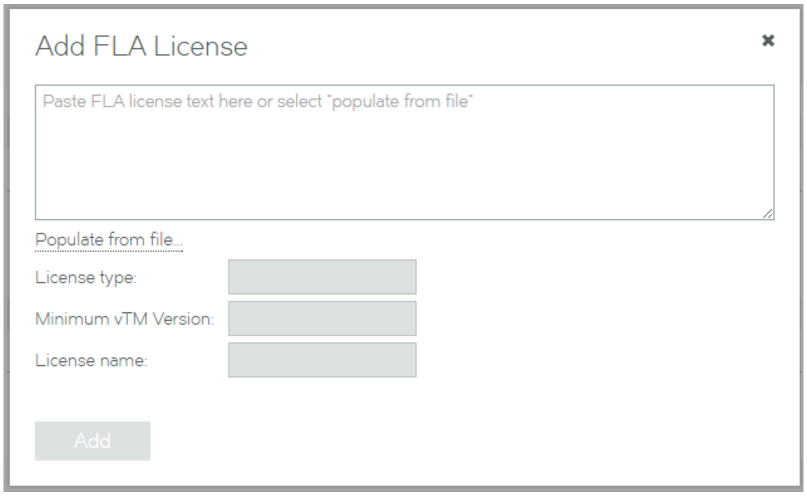
	License Name	Status	Default	Actions
▸	universal_v4	Active	Yes	Relicense

Legacy Licenses

License Name	Status	Default	Actions
No Data			

4. Click the **Add License** plus symbol. A licensing dialog box window appears.

   FIGURE 41 Add FLA License Dialog Box



Add FLA License

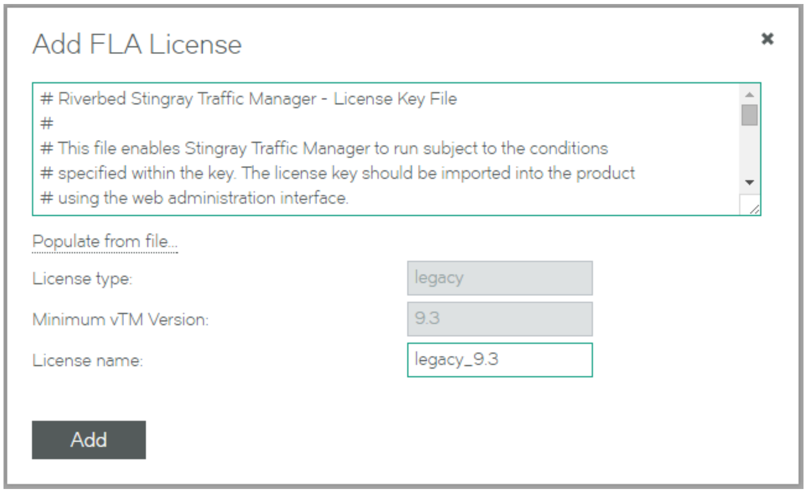
Paste FLA license text here or select "populate from file"

5. Either:

- – Paste the text of the Legacy FLA License into the text box, OR
  – Click **Populate from File**, select the file and then click **Upload**. This will populate the text box.

The remainder of the fields in the dialog box will then update to provide license information:

FIGURE 42 License Information



Add FLA License

```
# Riverbed Stingray Traffic Manager - License Key File
#
# This file enables Stingray Traffic Manager to run subject to the conditions
# specified within the key. The license key should be imported into the product
# using the web administration interface.
```

Populate from file...

License type: legacy

Minimum vTM Version: 9.3

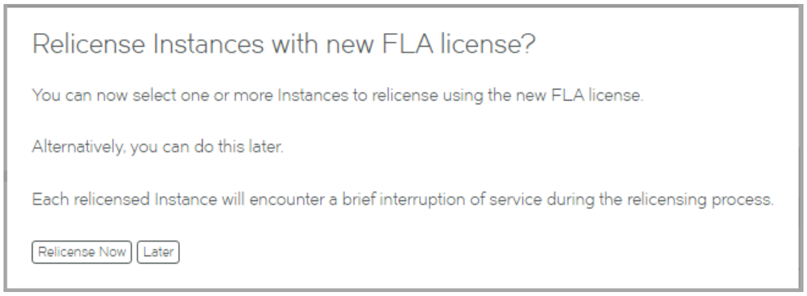
License name: legacy_9.3

6. Click **Add**.

A relicensing dialog box appears. This enables you to apply the new Legacy FLA License to Traffic Manager instances that are currently using a different Legacy FLA License.

Refer to Relicensing Traffic Managers on page 141 for details of the FLA relicensing mechanism.

FIGURE 43 Relicensing Dialog Box



Relicense Instances with new FLA license?

You can now select one or more Instances to relicense using the new FLA license.

Alternatively, you can do this later.

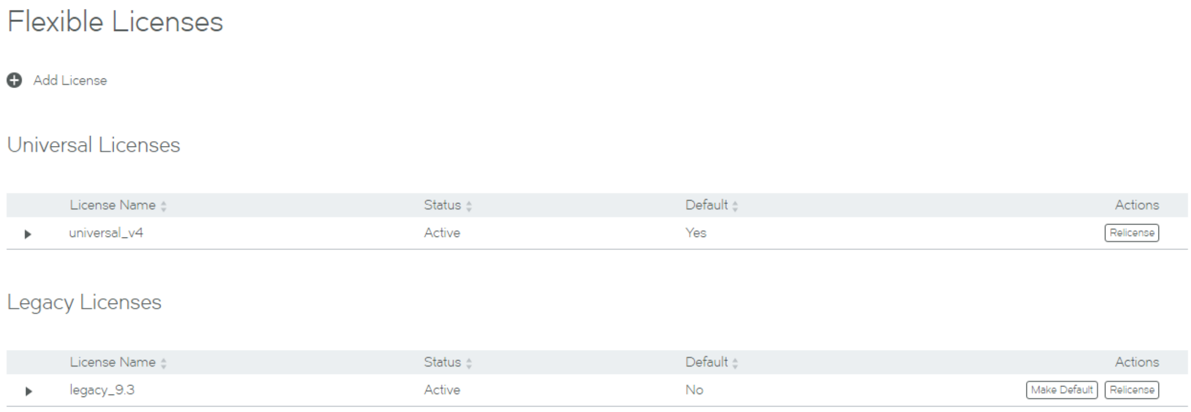
Each relicensed Instance will encounter a brief interruption of service during the relicensing process.

7. Click **Later**.

   NOTE
   You can perform relicensing operations from the **FLA Licenses** page.

   The new license is added to the **FLA Licenses** page.

   FIGURE 44 Flexible Licenses Page: Legacy FLA Added



Flexible Licenses

Universal Licenses

	License Name	Status	Default	Actions
▸	universal_v4	Active	Yes	Relicense

Legacy Licenses

	License Name	Status	Default	Actions
▸	legacy_9.3	Active	No	Make Default Relicense

8. Repeat this procedure if you require additional licenses.
9. Both Legacy FLA Licenses and Universal FLA Licenses have a default FLA. If you have more than one FLA license for either type, and want to make it the default license for that type, click **Make Default**.

Adding a Feature Pack to the Services Director

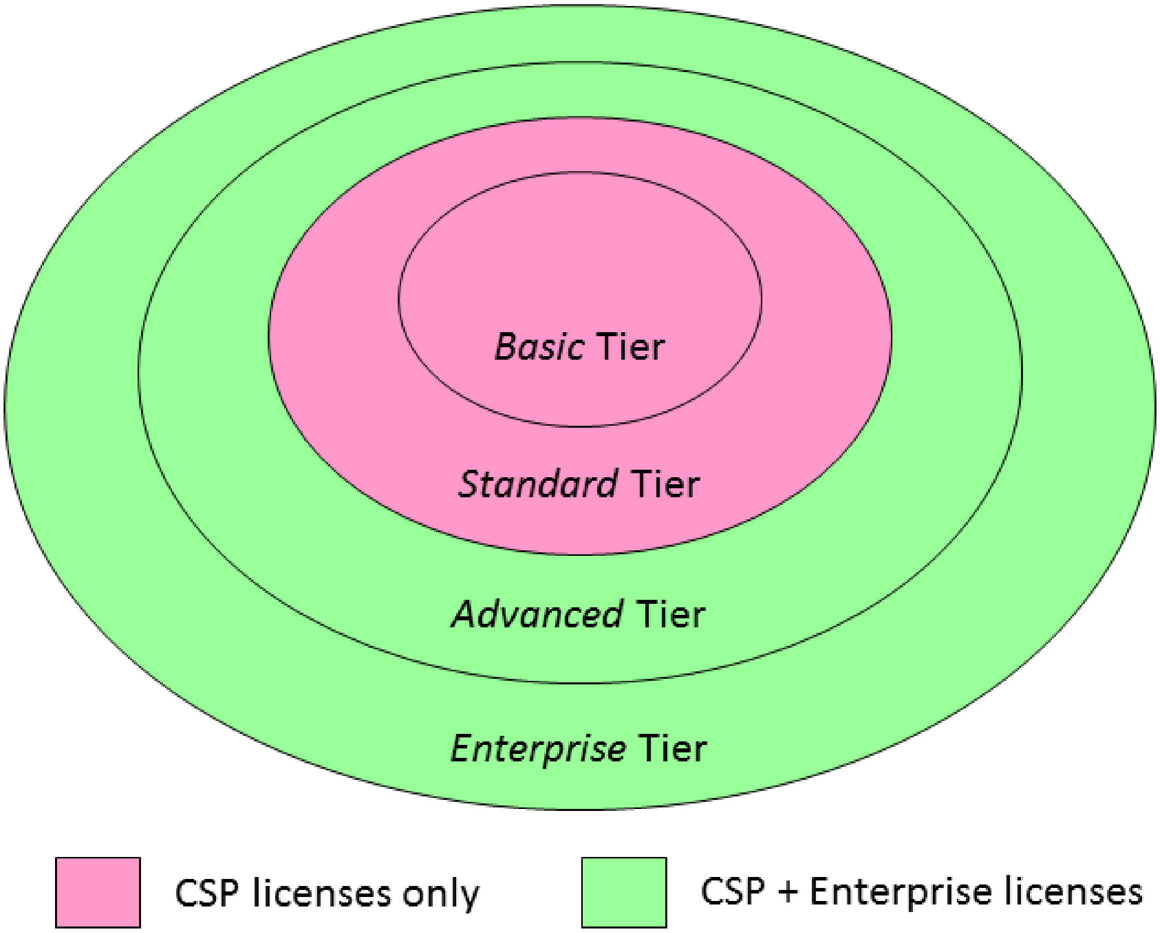
Before you register any Virtual Traffic Manager (vTM) instances, you must define one or more Feature Packs.

A Feature Pack defines the Services Director features that are available to a vTM instance once you have registered it on the Services Director.

The total set of features that are available in a Feature Pack is defined by its selected *Feature Tier*.

- Each Feature Tier is a subset of the tier above it.
- Feature Tiers include features that are relevant to your license type: Enterprise or Cloud Service Provider (CSP).
- Enterprise licenses have access to *Advanced* and *Enterprise* tiers only.
- CSP licenses have access to *Basic*, *Standard*, *Advanced* and *Enterprise* tiers.

FIGURE 45 Features Tiers for Enterprise and CSP licenses



NOTE

The *Enterprise* feature tier should not be confused with the Enterprise customer/license type.

For CSP licenses only, a Feature Pack also requires:

- A bandwidth, expressed as either Mbps or Gbps.
- A pricing model - *Fixed Price Monthly*, *Fixed Price Weekly*, or *Hourly plus Data Transfer*.

Once all Feature Pack properties are defined, the system is able to identify the required Stock-Keeping Unit (SKU) for the Feature Pack.

Once a SKU is identified for your Feature Pack, you can exclude any of the SKU's features from the Feature Pack.

NOTE

A list of features for a SKU can be seen on the expanded view of a SKU in the **SKUS and Feature Packs** page.

A default Feature Pack (typically a SKU with no exclusions) is created automatically when you install the Services Director VA based on an Enterprise license.

The procedure for creating a Feature Pack is dependent on your license type.

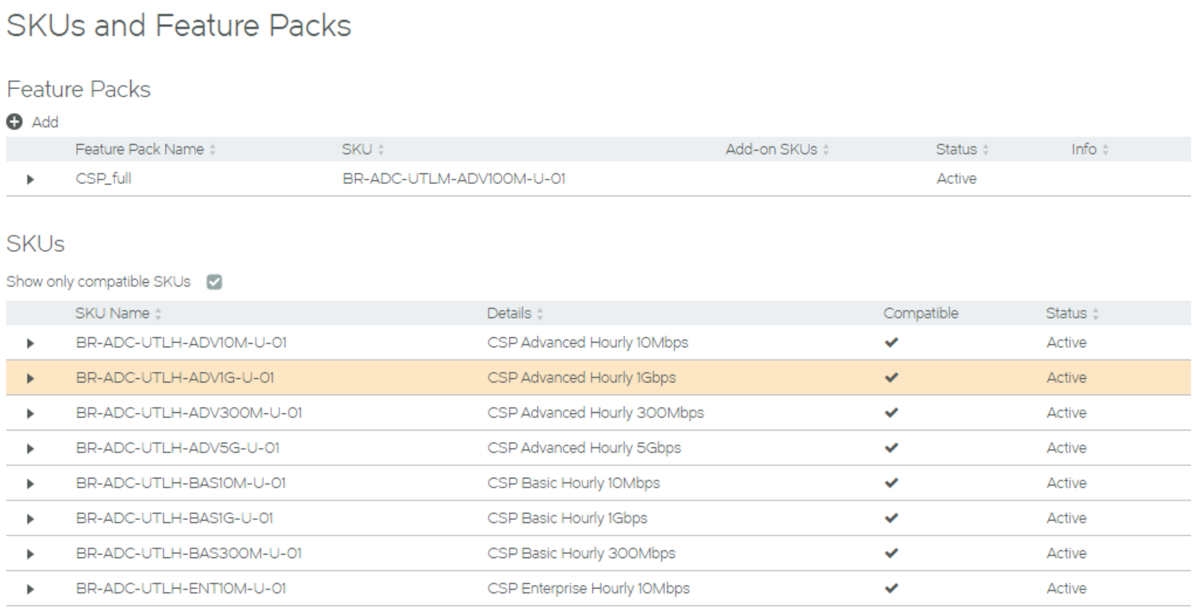
- For current Enterprise licenses, see Adding a Feature Pack for an Enterprise License on page 75.

- For current Cloud Service Provider (CSP) licenses, see Adding a Feature Pack for a CSP License on page 72.
- For older Enterprise/CSP licenses, see Adding a Feature Pack for an Older License on page 79.

Adding a Feature Pack for a CSP License

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.
3. Click the **Catalogs** menu, and then click **SKUS and Feature Packs**.
   The **SKUS and Feature Packs** page appears.

   FIGURE 46 SKUS and Feature Packs Page: CSP



SKUs and Feature Packs

Feature Packs

⊕ Add

	Feature Pack Name	SKU	Add-on SKUs	Status	Info
▸	CSP_full	BR-ADC-UTLM-ADV100M-U-01		Active	

SKUs

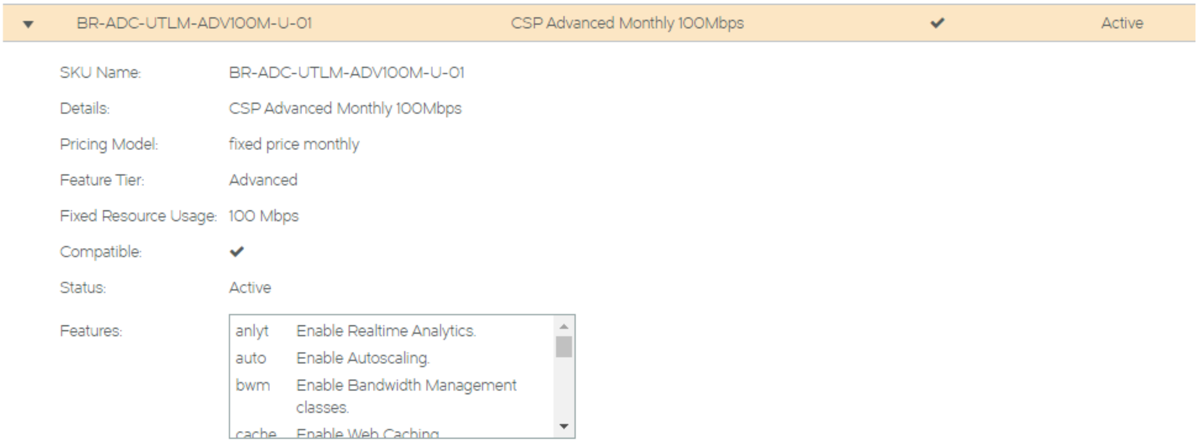
Show only compatible SKUs ☑

	SKU Name	Details	Compatible	Status
▸	BR-ADC-UTLH-ADV10M-U-01	CSP Advanced Hourly 10Mbps	✓	Active
▸	BR-ADC-UTLH-ADV1G-U-01	CSP Advanced Hourly 1Gbps	✓	Active
▸	BR-ADC-UTLH-ADV300M-U-01	CSP Advanced Hourly 300Mbps	✓	Active
▸	BR-ADC-UTLH-ADV5G-U-01	CSP Advanced Hourly 5Gbps	✓	Active
▸	BR-ADC-UTLH-BAS10M-U-01	CSP Basic Hourly 10Mbps	✓	Active
▸	BR-ADC-UTLH-BAS1G-U-01	CSP Basic Hourly 1Gbps	✓	Active
▸	BR-ADC-UTLH-BAS300M-U-01	CSP Basic Hourly 300Mbps	✓	Active
▸	BR-ADC-UTLH-ENT10M-U-01	CSP Enterprise Hourly 10Mbps	✓	Active

4. Select the **Show only compatible SKUs** check box to ensure that only SKUs that are compatible with your license are displayed.
5. In the table of SKUs, locate the SKU from which you wish to create a Feature Pack.

6. Expand this SKU to view its supported features. For example, the BR-ADC-UTLM-ADV100M-U-01 SKU:

FIGURE 47 SKUS and Feature Packs Page: Expanded SKU



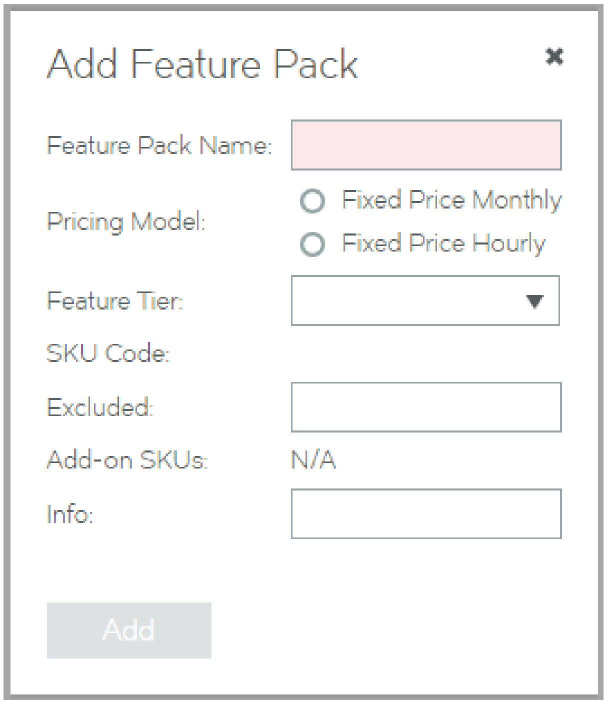
▾	BR-ADC-UTLM-ADV100M-U-01	CSP Advanced Monthly 100Mbps	✓	Active

SKU Name:	BR-ADC-UTLM-ADV100M-U-01
Details:	CSP Advanced Monthly 100Mbps
Pricing Model:	fixed price monthly
Feature Tier:	Advanced
Fixed Resource Usage:	100 Mbps
Compatible:	✓
Status:	Active
Features:	anlyt Enable Realtime Analytics. auto Enable Autoscaling. bwm Enable Bandwidth Management classes. cache Enable Web Caching

7. Locate the features(s) that you wish to exclude, and make a note of the feature name. For example, the auto (Autoscaling) feature. That is, this Feature Pack will not support the Autoscaling feature. All other features will still be supported.
8. Collapse the SKU in the table.
9. Click the **Add** button above the table of feature packs.

   The **Add Feature Pack** dialog box appears.

FIGURE 48 SKUS and Feature Packs Page: Add Feature Pack



Add Feature Pack ✖

Feature Pack Name:	
Pricing Model:	○ Fixed Price Monthly ○ Fixed Price Hourly
Feature Tier:	▼
SKU Code:	
Excluded:	
Add-on SKUs:	N/A
Info:	

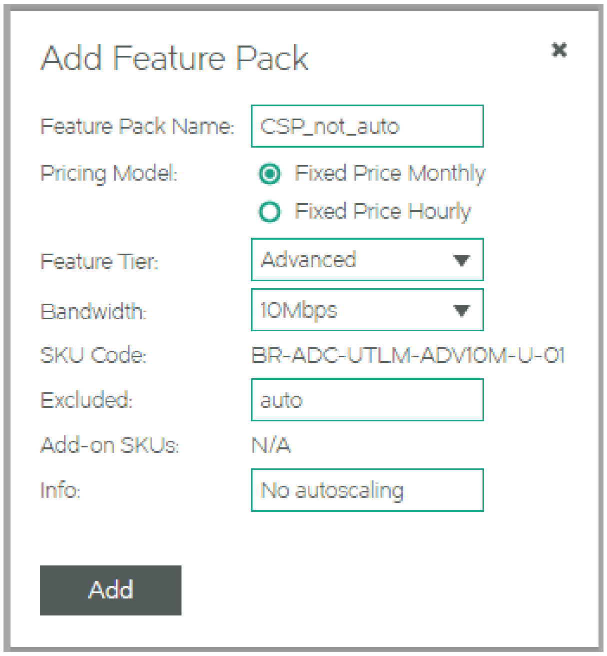
10. Enter a **Feature Pack Name**.

    This name will appear in the table of Feature Packs.

11. Select a **Pricing Model**.
12. Select the required **Feature Tier**.
13. Select a **Bandwidth**.
    The displayed SKU Code updates automatically to reflect your choices.
14. Enter a space-separated list of **Excluded** features.
15. Enter a description for the Feature pack as **Info**.

    This name will appear in the table of Feature Packs.

    FIGURE 49 SKUS and Feature Packs Page: Specify New Feature Pack



Add Feature Pack

Feature Pack Name: CSP_not_auto

Pricing Model: ● Fixed Price Monthly ○ Fixed Price Hourly

Feature Tier: Advanced

Bandwidth: 10Mbps

SKU Code: BR-ADC-UTLM-ADV10M-U-01

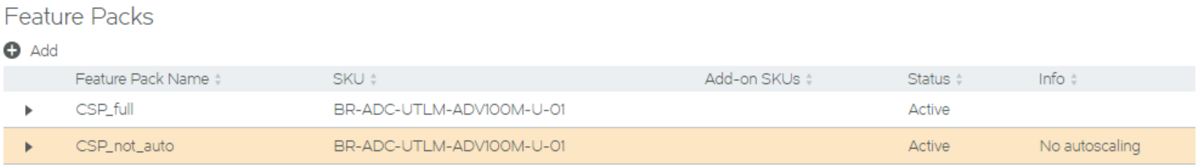
Excluded: auto

Add-on SKUs: N/A

Info: No autoscaling

16. Click **Add**. The new Feature Pack is added to the table of Feature Packs.

    FIGURE 50 SKUS and Feature Packs Page: New Feature Pack Added

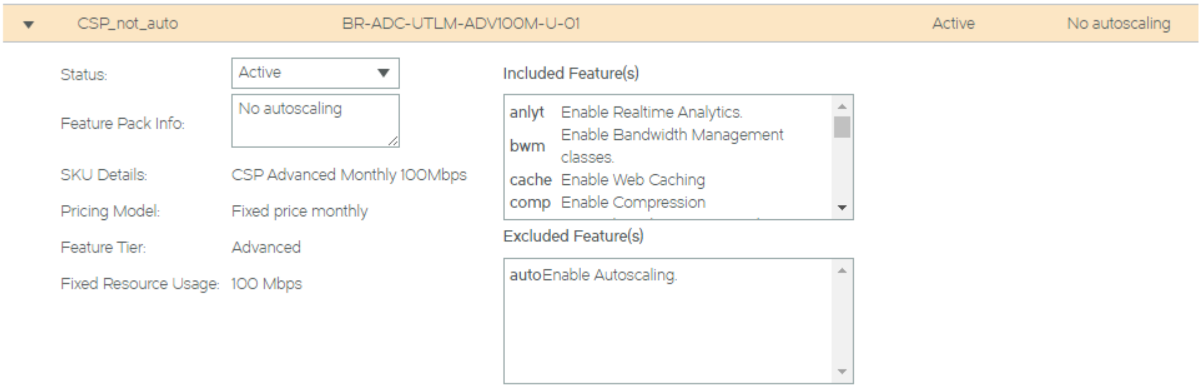


Feature Packs

	Feature Pack Name	SKU	Add-on SKUs	Status	Info
▸	CSP_full	BR-ADC-UTLM-ADV100M-U-01		Active	
▸	CSP_not_auto	BR-ADC-UTLM-ADV100M-U-01		Active	No autoscaling

17. Expand the Feature Pack to view its full details.

FIGURE 51 SKUS and Feature Packs Page: Full Details



CSP_not_auto	BR-ADC-UTLM-ADV100M-U-01	Active	No autoscaling

Status:	Active
Feature Pack Info:	No autoscaling
SKU Details:	CSP Advanced Monthly 100Mbps
Pricing Model:	Fixed price monthly
Feature Tier:	Advanced
Fixed Resource Usage:	100 Mbps

Included Feature(s)

anlyt	Enable Realtime Analytics.
bwm	Enable Bandwidth Management classes.
cache	Enable Web Caching
comp	Enable Compression

Excluded Feature(s)

auto	Enable Autoscaling.

18. Repeat this process to create all required Feature Packs.

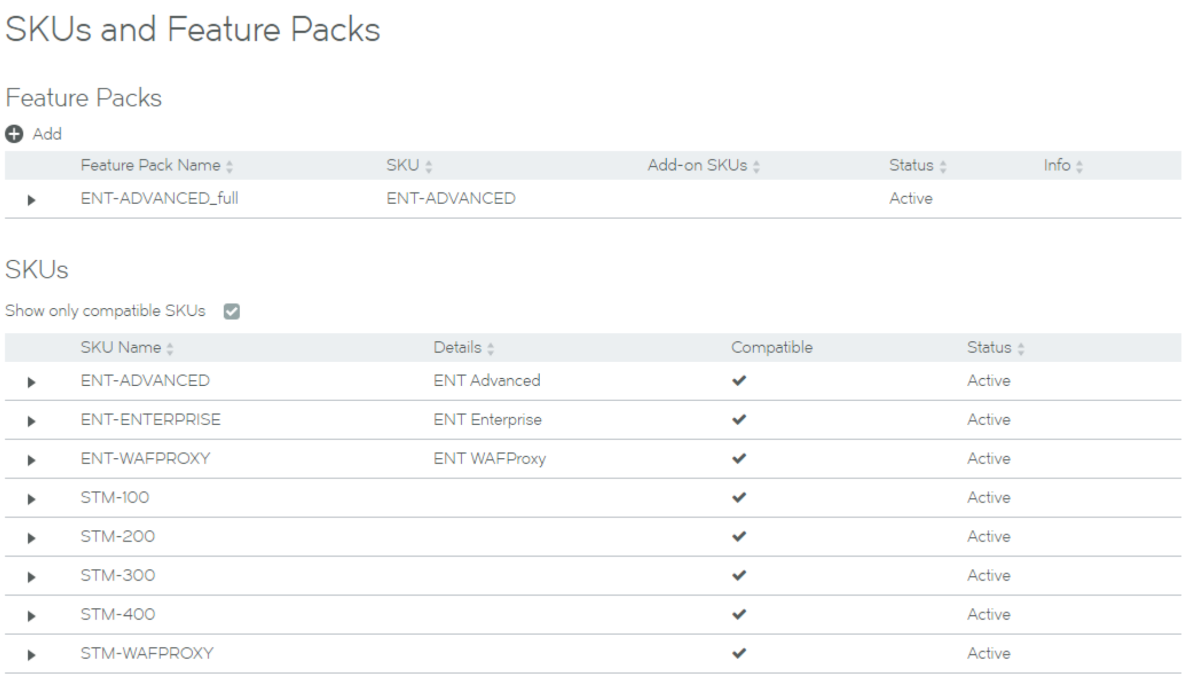
    Once you have created all required Feature Packs, you can use these to register and deploy Traffic Manager instances.

Adding a Feature Pack for an Enterprise License

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.

3. Click the **Catalogs** menu, and then click **SKUS and Feature Packs**.
   The **SKUS and Feature Packs** page appears.

   FIGURE 52 SKUS and Feature Packs Page: Enterprise



SKUs and Feature Packs

Feature Packs

Add

	Feature Pack Name	SKU	Add-on SKUs	Status	Info
▸	ENT-ADVANCED_full	ENT-ADVANCED		Active	

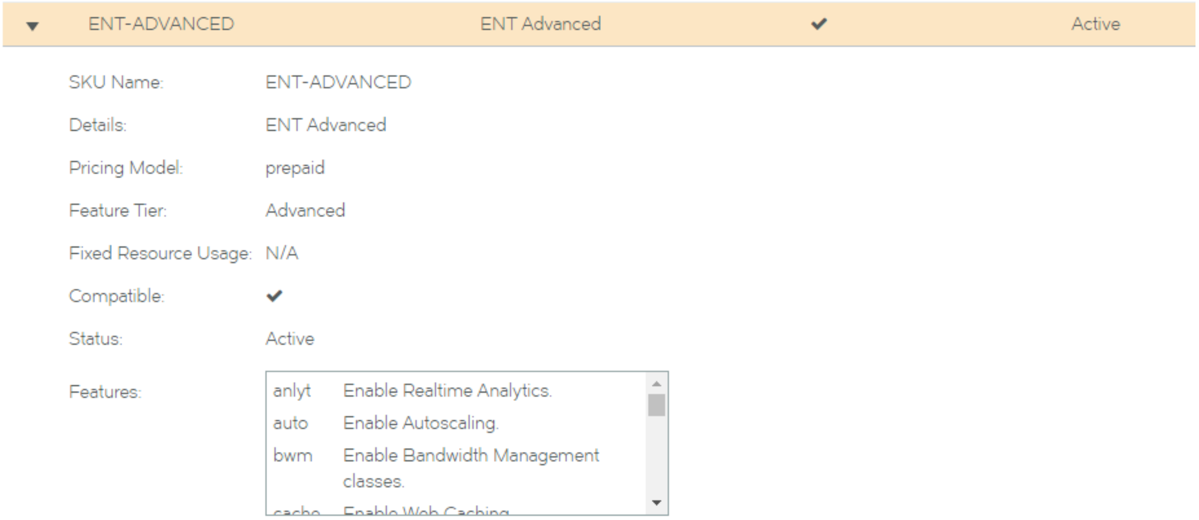
SKUs

Show only compatible SKUs ☑

	SKU Name	Details	Compatible	Status
▸	ENT-ADVANCED	ENT Advanced	✓	Active
▸	ENT-ENTERPRISE	ENT Enterprise	✓	Active
▸	ENT-WAFPROXY	ENT WAFProxy	✓	Active
▸	STM-100		✓	Active
▸	STM-200		✓	Active
▸	STM-300		✓	Active
▸	STM-400		✓	Active
▸	STM-WAFPROXY		✓	Active

4. Select the **Show only compatible SKUs** check box to ensure that only SKUs that are compatible with your license are displayed.
5. In the table of SKUs, locate the SKU from which you wish to create a Feature Pack.
6. Expand this SKU to view its supported features. For example, the ENT-ADVANCED SKU:

   FIGURE 53 SKUS and Feature Packs Page: Expanded SKU



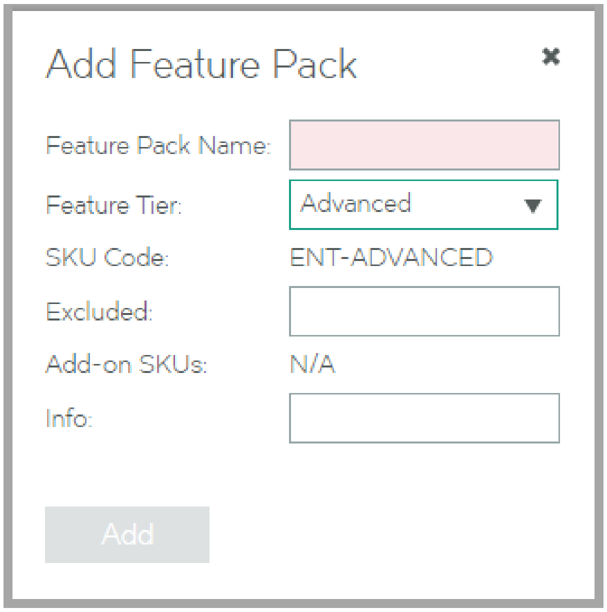
▾	ENT-ADVANCED	ENT Advanced	✓	Active

SKU Name:	ENT-ADVANCED
Details:	ENT Advanced
Pricing Model:	prepaid
Feature Tier:	Advanced
Fixed Resource Usage:	N/A
Compatible:	✓
Status:	Active
Features:	anlyt Enable Realtime Analytics. auto Enable Autoscaling. bwm Enable Bandwidth Management classes. cache Enable Web Caching

7. Locate the features(s) that you wish to exclude, and make a note of the feature name. For example, the cache (Web Caching) feature. That is, this Feature Pack will not support the Web Caching feature. All other features will still be supported.
8. Collapse the SKU in the table.
9. Click the **Add** button above the table of feature packs.

   The **Add Feature Pack** dialog box appears.

   FIGURE 54 SKUS and Feature Packs Page: Add Feature Pack



Add Feature Pack

Feature Pack Name:

Feature Tier: Advanced

SKU Code: ENT-ADVANCED

Excluded:

Add-on SKUs: N/A

Info:

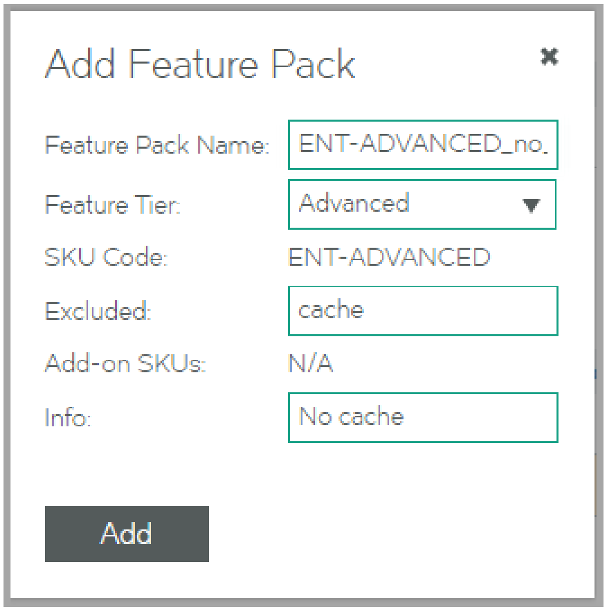
10. Enter a **Feature Pack Name**.

    This name will appear in the table of Feature Packs.
11. Select the required **Feature Tier**.
12. Enter a space-separated list of **Excluded** features.

13. Enter a description for the Feature pack as **Info**.

    This name will appear in the table of Feature Packs.

    FIGURE 55 SKUS and Feature Packs Page: Specify New Feature Pack

    Add Feature Pack

    Feature Pack Name: ENT-ADVANCED_no_

    Feature Tier: Advanced

    SKU Code: ENT-ADVANCED

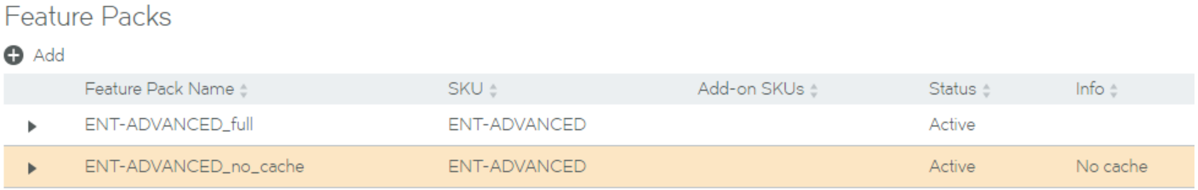
    Excluded: cache

    Add-on SKUs: N/A

    Info: No cache

14. Click **Add**. The new Feature Pack is added to the table of Feature Packs.

    FIGURE 56 SKUS and Feature Packs Page: New Feature Pack Added

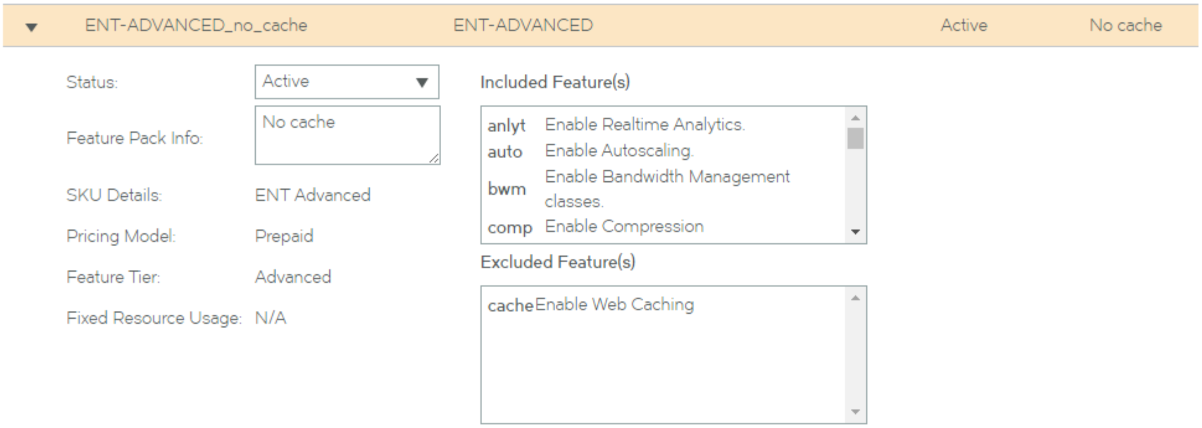
    

    Feature Packs

	Feature Pack Name	SKU	Add-on SKUs	Status	Info
▸	ENT-ADVANCED_full	ENT-ADVANCED		Active	
▸	ENT-ADVANCED_no_cache	ENT-ADVANCED		Active	No cache

15. Expand the Feature Pack to view its full details.

FIGURE 57 SKUS and Feature Packs Page: Full Details



ENT-ADVANCED_no_cache	ENT-ADVANCED	Active	No cache

Status: Active

Feature Pack Info: No cache

SKU Details: ENT Advanced

Pricing Model: Prepaid

Feature Tier: Advanced

Fixed Resource Usage: N/A

Included Feature(s)

anlyt	Enable Realtime Analytics.
auto	Enable Autoscaling.
bwm	Enable Bandwidth Management classes.
comp	Enable Compression

Excluded Feature(s)

cache	Enable Web Caching

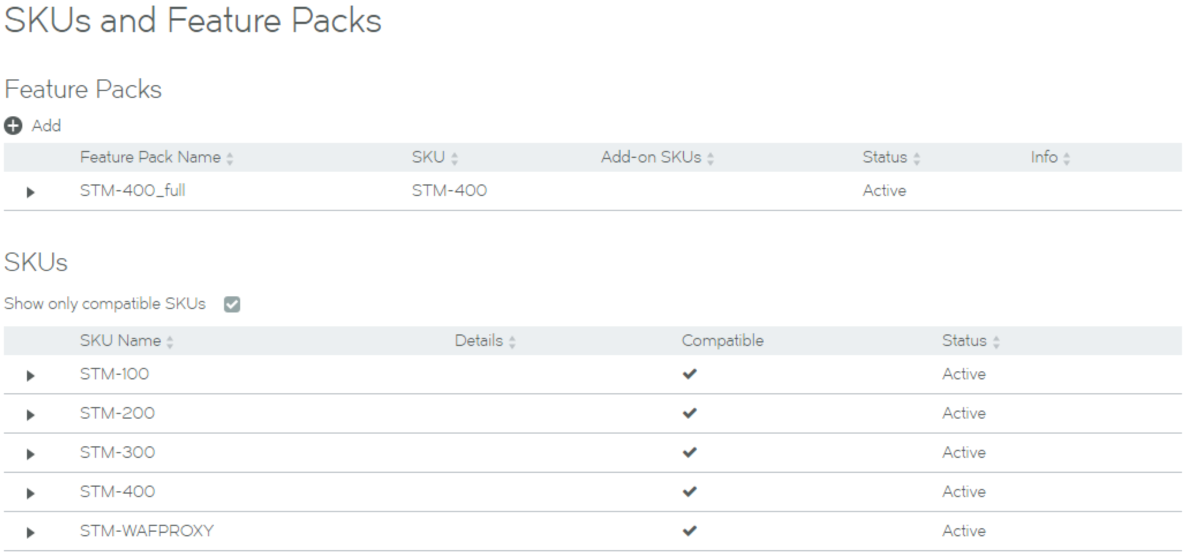
16. Repeat this process to create all required Feature Packs.

    Once you have created all required Feature Packs, you can use these to register and deploy Traffic Manager instances.

Adding a Feature Pack for an Older License

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.
3. Click the **Catalogs** menu, and then click **SKUS and Feature Packs**.
   The **SKUS and Feature Packs** page appears.

FIGURE 58 SKUS and Feature Packs Page



SKUs and Feature Packs

Feature Packs

Feature Pack Name	SKU	Add-on SKUs	Status	Info
STM-400_full	STM-400		Active	

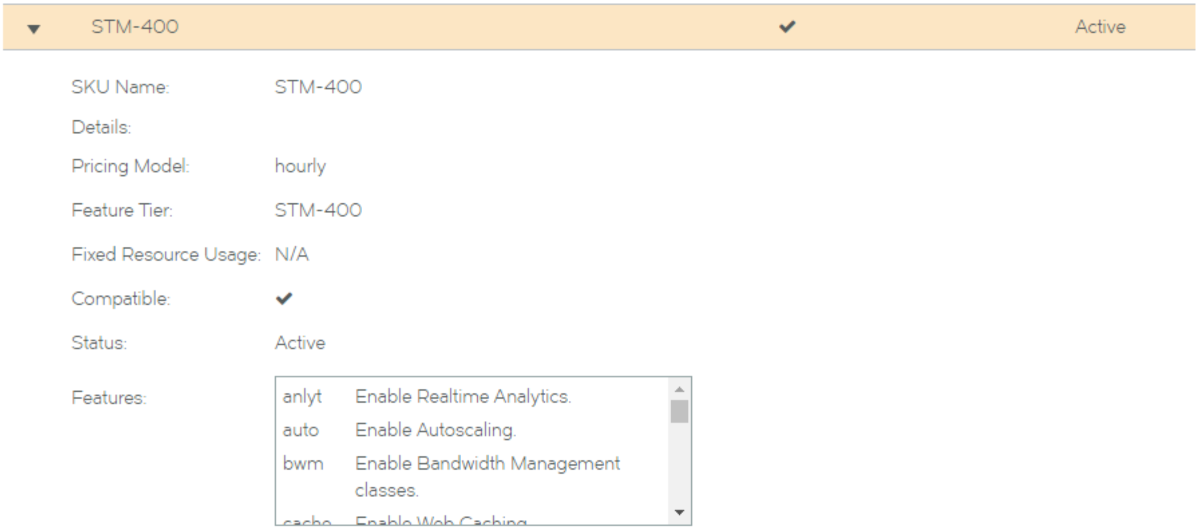
SKUs

Show only compatible SKUs ☑

SKU Name	Details	Compatible	Status
STM-100		✓	Active
STM-200		✓	Active
STM-300		✓	Active
STM-400		✓	Active
STM-WAFPROXY		✓	Active

4. Select the **Show only compatible SKUs** check box to ensure that only SKUs that are compatible with your license are displayed.
5. In the table of SKUs, locate the SKU from which you wish to create a Feature Pack.
6. Expand this SKU to view its supported features. For example, the STM-400 SKU:

FIGURE 59 SKUS and Feature Packs Page: Expanded SKU



▾ STM-400 ✓ Active

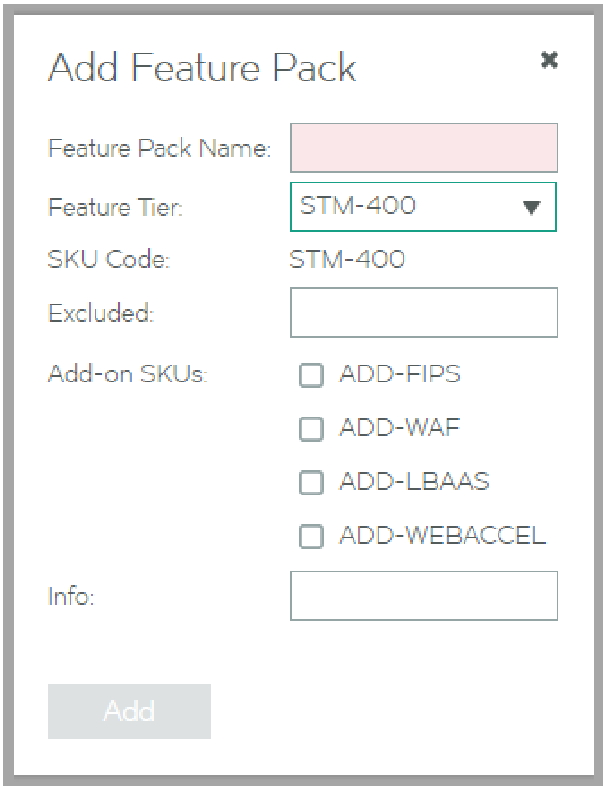
SKU Name:	STM-400
Details:	
Pricing Model:	hourly
Feature Tier:	STM-400
Fixed Resource Usage:	N/A
Compatible:	✓
Status:	Active
Features:	anlyt Enable Realtime Analytics. auto Enable Autoscaling. bwm Enable Bandwidth Management classes. cache Enable Web Caching

7. Locate the feature(s) that you wish to exclude, and make a note of the feature name. For example, the Lbrnd (Random Load Balancing) feature. That is, this Feature Pack will not support the Random load balancing feature. Other load balancing features, such as Round Robin, will still be supported.
8. Collapse the SKU in the table.

9. Click the **Add** button above the table of feature packs.

   The **Add Feature Pack** dialog box appears.

   FIGURE 60 SKUS and Feature Packs Page: Add Feature Pack



Add Feature Pack ✖

Feature Pack Name:

Feature Tier: STM-400 ▼

SKU Code: STM-400

Excluded:

Add-on SKUs: □ ADD-FIPS □ ADD-WAF □ ADD-LBAAS □ ADD-WEBACCEL

Info:

10. Enter a **Feature Pack Name**.

    This name will appear in the table of Feature Packs.

11. Select the required **Feature Tier**.

    This list is defined by the bandwidth packs added to the Services Director.

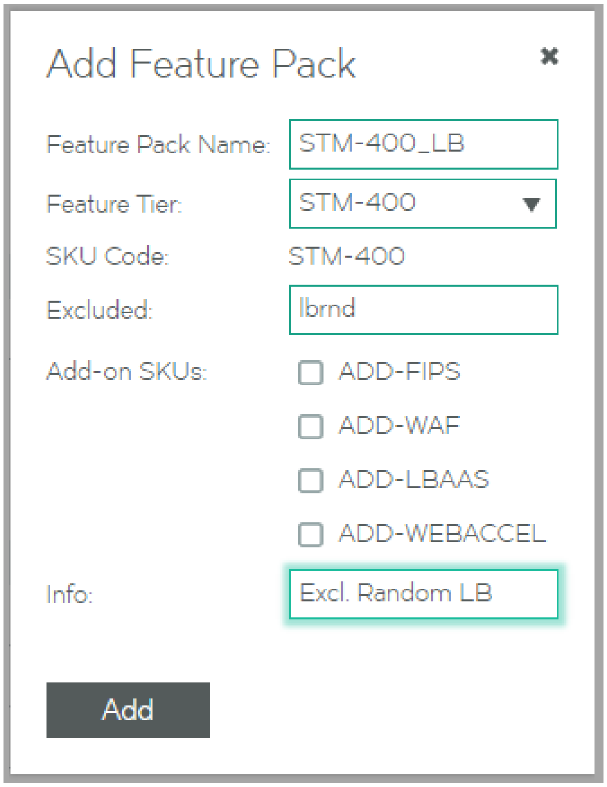
12. Enter a space-separated list of **Excluded** features.

13. Select any required **Add-on SKUs**.

14. Enter a description for the Feature pack as **Info**.

    This description will appear in the table of Feature Packs.

FIGURE 61 SKUS and Feature Packs Page: Specify New Feature Pack



Add Feature Pack

Feature Pack Name: STM-400_LB

Feature Tier: STM-400

SKU Code: STM-400

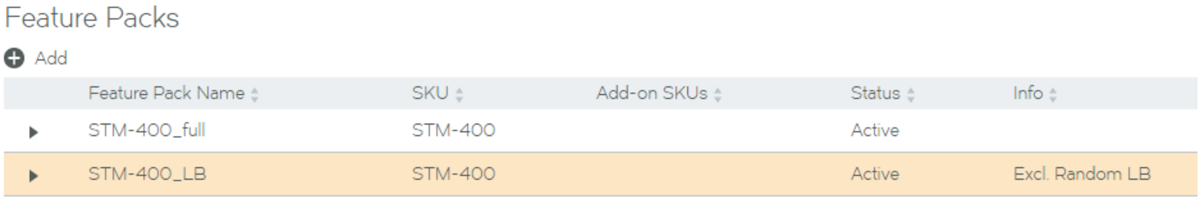
Excluded: lbrnd

Add-on SKUs: □ ADD-FIPS □ ADD-WAF □ ADD-LBAAS □ ADD-WEBACCEL

Info: Excl. Random LB

15. Click **Add**. The new Feature Pack is added to the table of Feature Packs.

FIGURE 62 SKUS and Feature Packs Page: New Feature Pack Added

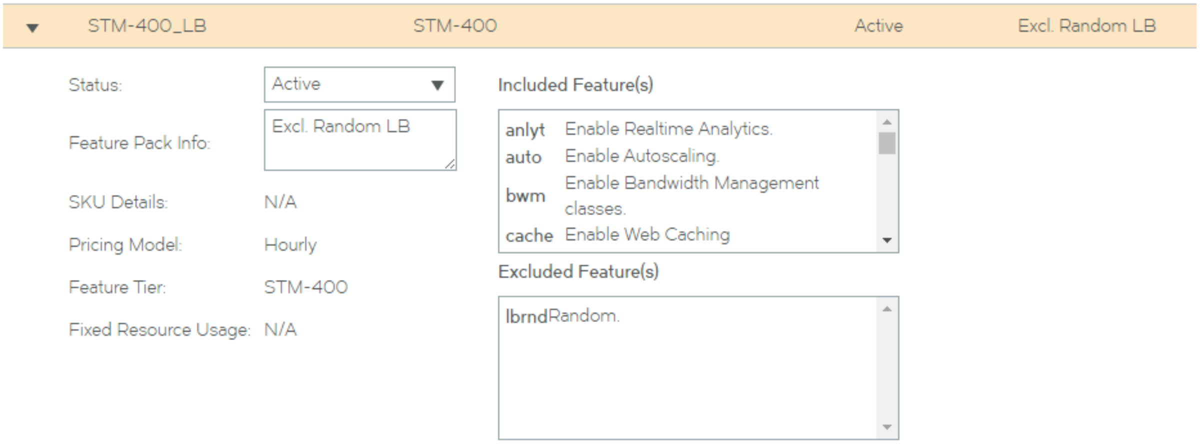


Feature Packs

	Feature Pack Name	SKU	Add-on SKUs	Status	Info
▸	STM-400_full	STM-400		Active	
▸	STM-400_LB	STM-400		Active	Excl. Random LB

16. Expand the Feature Pack to view its full details.

FIGURE 63 SKUS and Feature Packs Page: Full Details



STM-400_LB STM-400 Active Excl. Random LB

Status: Active

Feature Pack Info: Excl. Random LB

SKU Details: N/A

Pricing Model: Hourly

Feature Tier: STM-400

Fixed Resource Usage: N/A

Included Feature(s)

anlyt	Enable Realtime Analytics.
auto	Enable Autoscaling.
bwm	Enable Bandwidth Management classes.
cache	Enable Web Caching

Excluded Feature(s)

lbrndRandom.

17. Repeat this process to create all required Feature Packs.

    Once you have created all required Feature Packs, you can use these to register and deploy Traffic Manager instances.

Adding an Owner to the Services Director

There are several Services Director resources that require an *owner*. This property identifies a person or organisation that is associated with a resource, and optionally includes contact information.

For example, a single owner entry can be used for all resources owned by a Enterprise customer. Alternatively, an owner entry can be created to identify individual customers for resources supplied by a Cloud Service Provider.

The following resources require an owner:

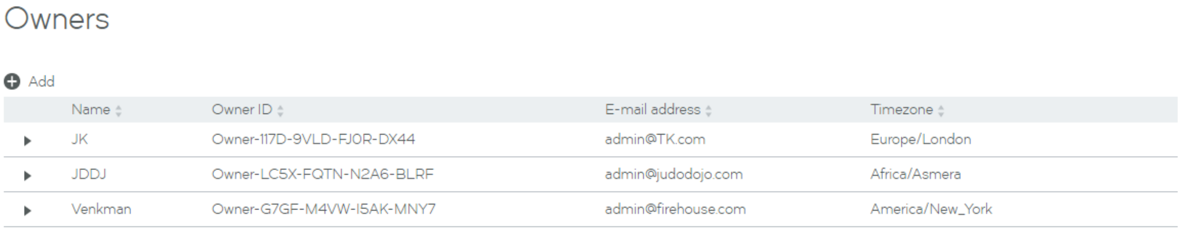
- An externally-deployed vTM Traffic Manager instance. Refer to Registering an Externally-Deployed Traffic Manager on page 91.
- A vTM Traffic Manager instance that is deployed using an instance host. Refer to the *Brocade Services Director Advanced User Guide*.
- A vTM Cluster. Refer to Creating a Traffic Manager Cluster on page 154.

Creating an Owner

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.

3. Click the **Catalogs** menu, and then click **Owners**. The **Owners** page appears.

FIGURE 64 Owners Page

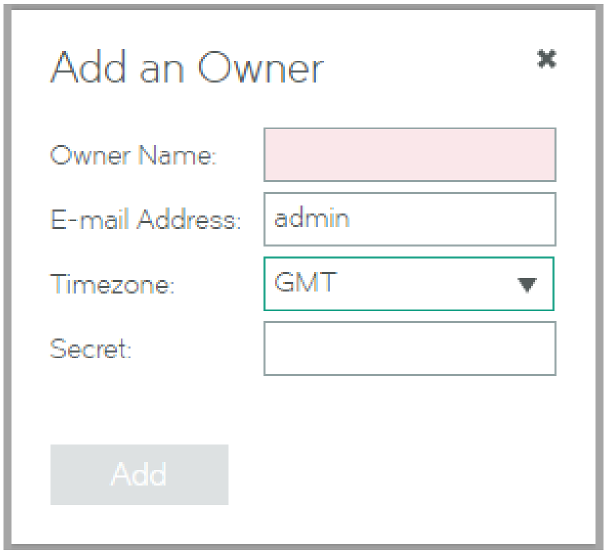


Owners

	Name	Owner ID	E-mail address	Timezone
▸	JK	Owner-117D-9VLD-FJ0R-DX44	admin@TK.com	Europe/London
▸	JDDJ	Owner-LC5X-FQTN-N2A6-BLRF	admin@judodojo.com	Africa/Asmera
▸	Venkman	Owner-G7GF-M4VW-I5AK-MNY7	admin@firehouse.com	America/New_York

4. Click the **Add** button above the table of Owners. A popup appears.

FIGURE 65 Owners Page: Adding an Owner



Add an Owner

Owner Name:

E-mail Address: admin

Timezone: GMT

Secret:

5. Enter an **Owner Name** for the new entry.
6. (Optional) Enter an **E-mail Address** for the owner.
7. Select the required timezone for the owner.
8. (Optional) Enter a **Secret** password for the owner. This is used during self-registration.
9. Click **Add**. The new Owner is added to the table of Owners.
10. Expand an Owner to view its full details, refer to Viewing Full Details for an Owner on page 84.
11. Repeat this process to create all required Owners.

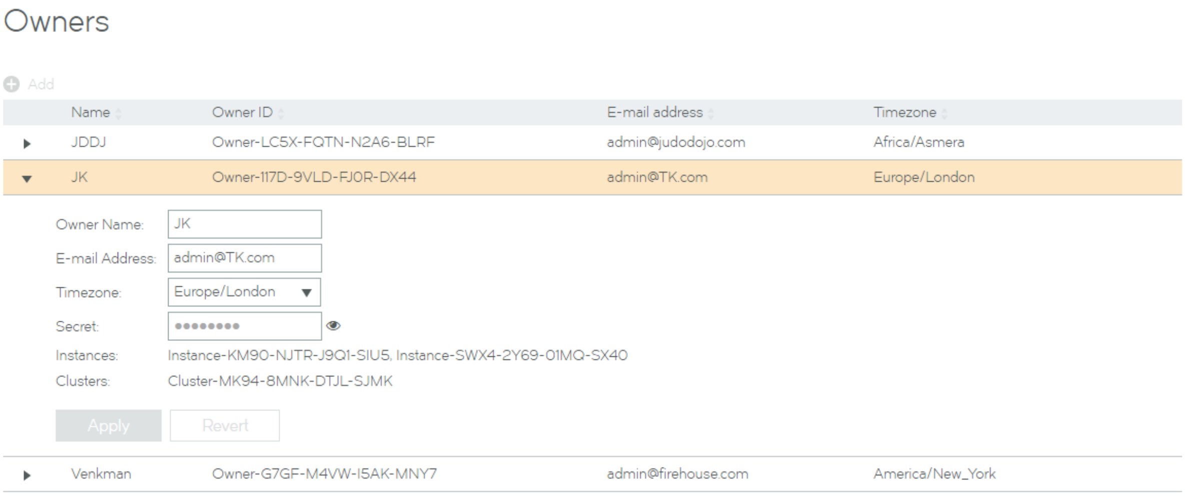
    Once you have created all required Owners, you can use these to register and deploy Traffic Managers and vTM clusters.

Viewing Full Details for an Owner

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.

3. Click the **Catalogs** menu, and then click **Owners**. The **Owners** page appears.
4. Locate and expand an Owner to view its full details. For example:

FIGURE 66 Owners Page: Displaying Full Details for an Owner



Owners

	Name	Owner ID	E-mail address	Timezone
▶	JDDJ	Owner-LC5X-FQTN-N2A6-BLRF	admin@judodojo.com	Africa/Asmera
▼	JK	Owner-117D-9VLD-FJ0R-DX44	admin@TK.com	Europe/London

Owner Name: JK
E-mail Address: admin@TK.com
Timezone: Europe/London
Secret: ••••••••
Instances: Instance-KM90-NJTR-J9Q1-SIU5, Instance-SWX4-2Y69-01MQ-SX40
Clusters: Cluster-MK94-8MNK-DTJL-SJMK

	Name	Owner ID	E-mail address	Timezone
▶	Venkman	Owner-G7GF-M4VW-I5AK-MNY7	admin@firehouse.com	America/New_York

The properties of the Owner are as follows:

- **Owner Name**: The name of the Owner.
- **E-mail Address**: (Optional) The e-mail address for a point of contact (typically, the admin user) for the Owner.
- **Timezone**: The selected timezone for the Owner.
- **Secret**: (Optional) The password for the Owner. This is used during self-registration.
- **Instances**: A list of vTM instances that are associated with the Owner. This can be empty if the Owner is not in use.
- **Clusters**: A list of vTM clusters that are associated with the Owner. This can be empty if the Owner is not in use.

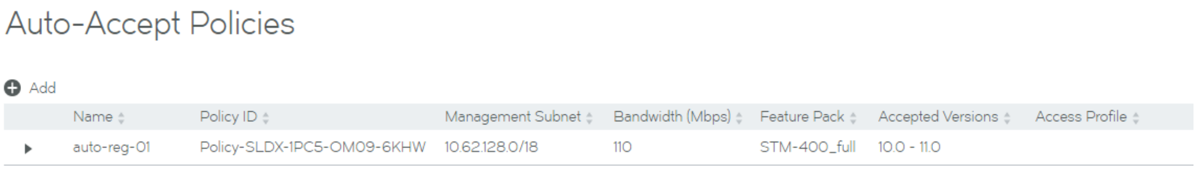
5. (Optional) Change the Owner's properties and click **Apply** to update the Owner.

Adding an Auto-Accept Policy to the Services Director

If you want to configure vTMs for automatic self-registration, you will need to create one or more auto-accept policies.

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.
3. Click the **Catalogs** menu, and then click **Auto-Accept Policies**. The **Auto-Accept Policies** page appears.

FIGURE 67 Registration Policies Page

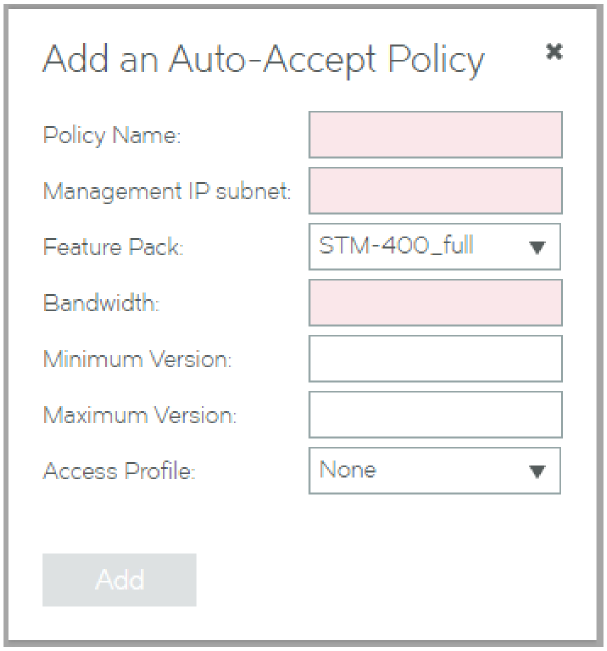


Auto-Accept Policies

	Name	Policy ID	Management Subnet	Bandwidth (Mbps)	Feature Pack	Accepted Versions	Access Profile
▶	auto-reg-01	Policy-SLDX-1PC5-OM09-6KHW	10.62.128.0/18	110	STM-400_full	10.0 - 11.0	

4. Click the **Add** button above the table of auto-accept policies. A popup appears.

FIGURE 68 Owners Page: Adding an Auto-Accept Policy



Add an Auto-Accept Policy

Policy Name:	
Management IP subnet:	
Feature Pack:	STM-400_full ▼
Bandwidth:	
Minimum Version:	
Maximum Version:	
Access Profile:	None ▼

5. Enter a unique **Policy Name** for the auto-accept policy.
6. Enter a **Management IP subnet** for the auto-accept policy. This identifies the subnet to which a vTM must belong to be accepted by this policy.
   If a vTM that is evaluated by this policy is from outside this subnetwork, the auto-acceptance of the vTM is rejected by the auto-accept policy.
7. Select a **Feature Pack** for the auto-accept policy. This is the feature pack that will be assigned to a vTM that is successfully evaluated using this policy.

   NOTE
   This is not an acceptance condition, but the evaluation of the **Bandwidth** property refers to this property.

8. Enter the **Bandwidth** for the auto-accept policy. This is the required bandwidth for a vTM that is evaluated using this policy.
   If there is insufficient bandwidth in the specified **Feature Pack** for a vTM, the auto-acceptance of the vTM is rejected by the auto-accept policy.
9. (Optional) Select a **Minimum Version** for the vTM software. This takes the form X.Y. Examples: 10.0, 10.3.

   R1 releases are included automatically for any base version. For example, 10.0 includes 10.0r1.

   If a vTM that is evaluated by this policy does not meet this condition, the auto-acceptance of the vTM is rejected by the auto-accept policy.

   NOTE
   Where a **Minimum Version** is not specified for a policy, the version will be displayed as "Any" in the **Accepted Versions** property in the table of policies.

10. (Optional) Select a **Maximum Version** for the vTM software. This takes the form X.Y. Examples: 10.4, 11.0.

    R1 releases are included automatically for any base version. For example, 10.3 includes 10.3r1.

    If a vTM that is evaluated by this policy does not meet this condition, the auto-acceptance of the vTM is rejected by the auto-accept policy.

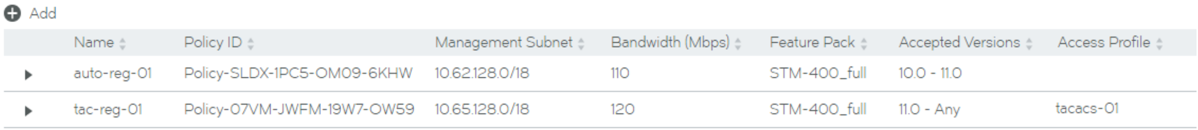
    NOTE
    Where a **Maximum Version** is not specified for a policy, the version will be displayed as "Any" in the **Accepted Versions** property in the table of policies.

11. (Optional) Select an **Access Profile**.

    This access profile identifies the authenticator and permission groups required for the user authentication on this vTM. If selected, these will be applied to the vTM once it is accepted. All cluster members are affected by this change. Refer to Working with User Authentication on page 179.

12. Click **Add**. The new auto-accept policy is added to the table of policies. For example:

    FIGURE 69 Owners Page: Auto-Accept Policy Added



	Name	Policy ID	Management Subnet	Bandwidth (Mbps)	Feature Pack	Accepted Versions	Access Profile
▶	auto-reg-01	Policy-SLDX-1PC5-OM09-6KHW	10.62.128.0/18	110	STM-400_full	10.0 - 11.0	
▶	tac-reg-01	Policy-07VM-JWFM-19W7-OW59	10.65.128.0/18	120	STM-400_full	11.0 - Any	tacacs-01

    This includes:

    - **Policy ID** - the UUID of the auto-accept policy.
    - **Accepted Versions** - a ranged version of the **Minimum Version** and **Maximum Version** properties.

13. Expand an auto-accept policy to view its full details.
14. Repeat this process to create all required auto-accept policies.

    Once you have created all required auto-accept policies, you can use these to automatically register vTMs, refer to Requesting Self-Registration During vTM Installation on page 109.

Adding a Cloud Registration Resource to the Services Director

If you want to create a cloud-based vTM that will self-register automatically on the Services Director, you must first create a Cloud Registration resource on the Services Director.

Before you create a Cloud Registration resource, you must also create:

- The required Owner on the Services Director, refer to Adding an Owner to the Services Director on page 83.
- The required Auto-Accept Policy on the Services Director, refer to Adding an Auto-Accept Policy to the Services Director on page 85.

NOTE
You can create a Cloud Registration resource without either an Owner or a Self-Registration Policy property, but the resulting vTM will not contain sufficient information to register automatically on the Services Director. When this happens, you must process the self-registration manually, refer to Processing Self-Registration Requests Manually on page 119.

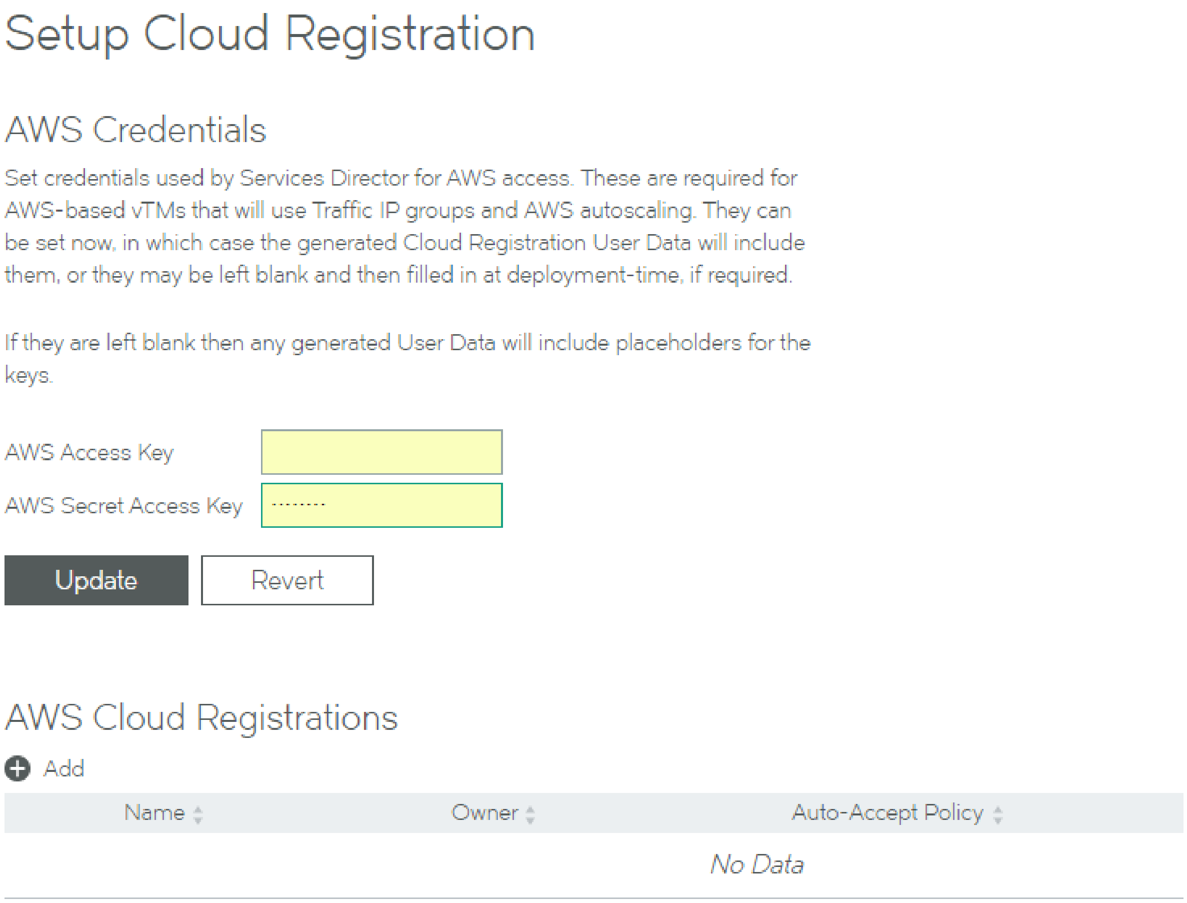
Once you have created a Cloud Registration resource, you can:

- View the user data text block that is required for the creation of the first cloud-based vTM in a cluster, refer to Viewing User Data Text for a Cloud Registration Resource on page 90.
- Create the first cloud-based vTM in a cluster, refer to Creating a Cloud-Based Traffic Manager on page 126.

Adding a Cloud Registration Resource

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.
3. Click the **Catalogs** menu, and then click **Cloud Registration**. The **Setup Cloud Registration** page appears.

FIGURE 70 Cloud Registration Page



Setup Cloud Registration

AWS Credentials

Set credentials used by Services Director for AWS access. These are required for AWS-based vTMs that will use Traffic IP groups and AWS autoscaling. They can be set now, in which case the generated Cloud Registration User Data will include them, or they may be left blank and then filled in at deployment-time, if required.

If they are left blank then any generated User Data will include placeholders for the keys.

AWS Access Key	
AWS Secret Access Key	········

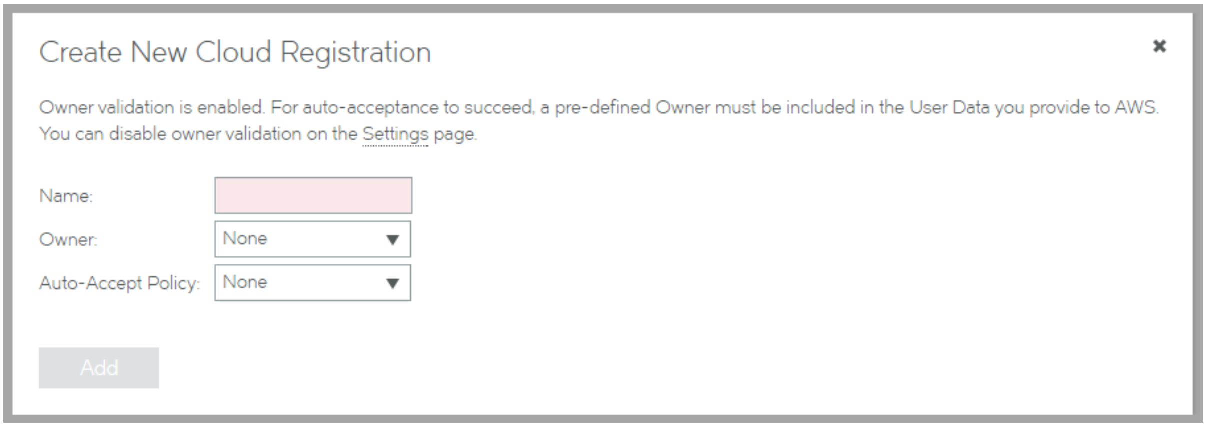
AWS Cloud Registrations

Name	Owner	Auto-Accept Policy
	No Data	

4. Specify your AWS credentials as **AWS Access Key** and **AWS Secret Access Key**, and then click **Update**.

5. Click the **Add** button above the table of Cloud Registration resources. A popup appears.

FIGURE 71 Cloud Registration Page: Adding a Cloud Registration



Create New Cloud Registration

Owner validation is enabled. For auto-acceptance to succeed, a pre-defined Owner must be included in the User Data you provide to AWS. You can disable owner validation on the Settings page.

Name:

Owner: None ▼

Auto-Accept Policy: None ▼

6. Enter a unique **Name** for the Cloud Registration resource.
7. (Optional) Select an **Owner** for the Cloud Registration resource.

   NOTE
   If you do not specify an owner before registration, you cannot perform an automatic self-registration of the cloud-based vTM. However, this information can be added in the AWS system before registration.

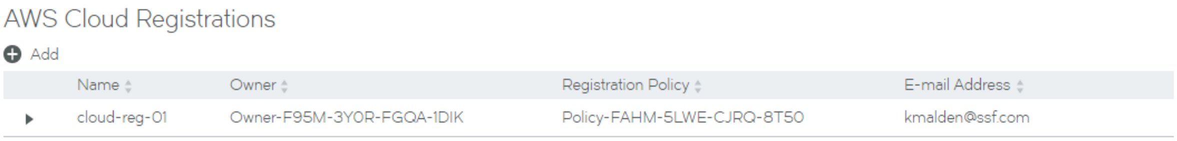
   NOTE
   You can disable the mandatory validation of this property from the **General Settings** page, refer to Updating Instance Registration Settings on page 61.

8. (Optional) Select an **Auto-Accept Policy** for the Cloud Registration resource. This is the auto-accept policy that will be used during the evaluation of a cloud-based vTM's self-registration.

   NOTE
   If you do not specify an auto-accept policy before registration, you cannot perform an automatic self-registration of the cloud-based vTM. However, this information can be added in the AWS system before registration.

9. Click **Add**. The new Cloud Registration resource is added to the table of Cloud Registration resources. For example:

FIGURE 72 Cloud Registration Page: Cloud Registration Added



AWS Cloud Registrations

	Name	Owner	Registration Policy	E-mail Address
▸	cloud-reg-01	Owner-F95M-3Y0R-FGQA-1DIK	Policy-FAHM-5LWE-CJRQ-8T50	kmalden@ssf.com

10. Expand a Cloud Registration resource to view the user data text block that is required for cloud-based registration, refer to Viewing User Data Text for a Cloud Registration Resource on page 90.

11. Repeat this process to create all required Cloud Registration resources.

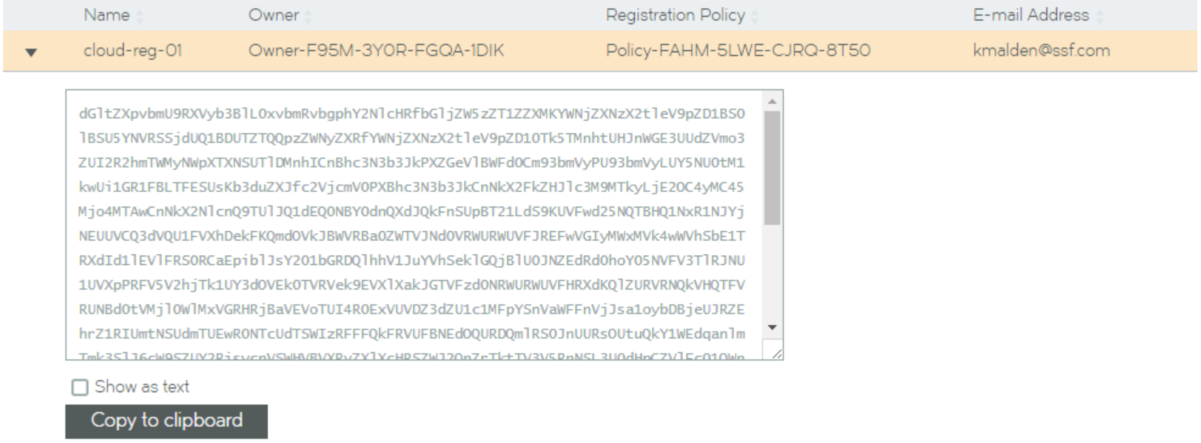
    Once you have created a required Cloud Registration resource, you can use it to create the first cloud-based vTM in a cluster, refer to Creating a Cloud-Based Traffic Manager on page 126.

Viewing User Data Text for a Cloud Registration Resource

The Cloud Registrations page enables you to view and copy the user data text block for individual Cloud Registration resources. This text is required when creating a cloud-based vTM, refer to Creating a Cloud-Based Traffic Manager on page 126.

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.
3. Click the **Catalogs** menu, and then click **Cloud Registration**. The **Setup Cloud Registration** page appears.
4. In the table of AWS Cloud Registrations, locate the required Cloud Registration resource.
5. Expand the Cloud Registration resource to view the user data text block. By default, this uses base64 encoding. For example:

FIGURE 73 User Data Text Block: Base64 Format



	Name	Owner	Registration Policy	E-mail Address
▼	cloud-reg-01	Owner-F95M-3Y0R-FGQA-1DIK	Policy-FAHM-5LWE-CJRQ-8T50	kmalden@ssf.com

```
dGltZXpvbmU9RXVyb3BlL0xvbmRvbgphY2NlcHRfbGljZW5zZT1ZZXMKYWNjZXNzX2tleV9pZD1BS0
lBSU5YNVRSSjdUQ1BDUTZTQQpzZWNyZXRfYWNjZXNzX2tleV9pZD10Tk5TMnhtUHJnWGE3UUdZVmo3
ZUI2R2hmTWMyNWpXTXNSUTlDMnhICnBhc3N3b3JkPXZGeVlBWFd0Cm93bmVyPU93bmVyLUY5NU0tM1
kwUi1GR1FBLTFESUsKb3duZXJfc2VjcmV0PXBhc3N3b3JkCnNkX2FkZHJlc3M9MTkyLjE2OC4yMC45
Mjo4MTAwCnNkX2NlcnQ9TUlJQ1dEQ0NBY0dnQXdJQkFnSUpBT21LdS9KUVFwd25NQTBHQ1NxR1NJYj
NEUUVCQ3dVQU1FVXhDekFKQmdOVkJBWVRBa0ZWTVJNd0VRWURWUVFJREFwVGIyMWxMVk4wWVhSbE1T
RXdId1lEVlFRS0RCaEpibl JsY201bGRDQlhhV1JuYVhSeklGQjBlU0JNZEdRd0hoY05NVFV3TlRJNU
1UVXpPRFV5V2hjTk1UY3dOVEk0TVRVek9EVXlXakJGTVFzd0NRWURWUVFHRXdKQlZURVRNQkVHQTFV
RUNBd0tVMjl0WlMxVGRHRjBaVEVoTUI4R0ExVUVDZ3dZU1c1MFpYSnVaWFFnVjJsa1oybDBjeUJRZE
hrZ1RIUmtNSUdmTUEwR0NTcUdTSWIzRFFFQkFRVUFBNEdOQURDQmlRS0JnUURsOUtuQkY1WEdqanlm
```

□ Show as text

Copy to clipboard

NOTE
This is displayed as plain text if any of the information required for the AWS user data block are unspecified. For example, if the Owner or Auto-Accept Policy is unspecified. In these cases, the lines relating to the unspecified Owner or the unspecified Auto-Accept Policy are included with placeholder text that you can complete manually in the AWS system, refer to Creating the First vTM in a Cluster on page 126.

6. If you intend to make any changes to the user data, disable the **Show as text** check box. This ensures it is displayed as plain text rather than base64-encoded text.
7. Click **Copy to Clipboard** to copy the displayed user data text block.
   Once you have copied the user data text block, you can paste it directly into the AWS creation wizard, refer to Creating a Cloud-Based Traffic Manager on page 126.

Registering an Externally-Deployed Traffic Manager

The Services Director VA enables you to register one or more externally-deployed Traffic Manager. This adds the Traffic Manager to the estate of the Services Director, from where it can be licensed, monitored and metered.

You can register/license a Traffic Manager that is in a cluster. This process does not register other Traffic Managers in the cluster, nor does it license them; you must independently register and license each node in a cluster.

Before you register an externally-deployed Traffic Manager, ensure that all required objects exist:

- The required Feature Pack. This lists the functions supported by the Traffic Manager, refer to Adding a Feature Pack to the Services Director on page 70.
- The required Owner. This identifies the customer/owner for the Traffic Manager, refer to Adding an Owner to the Services Director on page 83.
- The required Access Profile (optional). This identifies the authentication mechanism for the Traffic Manager, refer to Creating an Access Profile (vTM User Authentication Only) on page 192.

NOTE
The Services Director VA also enables you to deploy Traffic Manager. Each is deployed into an container using an existing instance host. The Services Director VA can then manage the lifecycle states of these Traffic Managers, which is not supported for externally-deployed Traffic Managers. For details, refer to the *Brocade Services Director Advanced User Guide*.

Preparing to Register a Traffic Manager (Universal FLA)

After you have completed the initial configuration of a Services Directors HA pair (refer to Installing the Brocade Services Director VA on page 13, you can begin to add externally-deployed Traffic Managers to the estate of the Services Director.

One method for achieving this is by registration of the vTMs. Typically, these will use a Universal FLA License.

You can register an externally-deployed Traffic Manager using a Universal FLA when:

- The Traffic Manager is installed and running.
- The Traffic Manager is at version 10.1 or later.
- You know the Traffic Manager's hostname (in DNS-enabled networks) or IP address.
- The Traffic Manager's REST API is enabled.

If any Traffic Manager is running an earlier version of the Traffic Manager software, or has its REST API disabled, you must manually install a Legacy FLA License onto the Services Director. Refer to Preparing to Register a Traffic Manager (Legacy FLA License) on page 97.

NOTE
To minimize delays in licensing, ensure that the clocks of your Services Directors and your Traffic Managers are aligned.

Registering a Traffic Manager (Universal FLA)

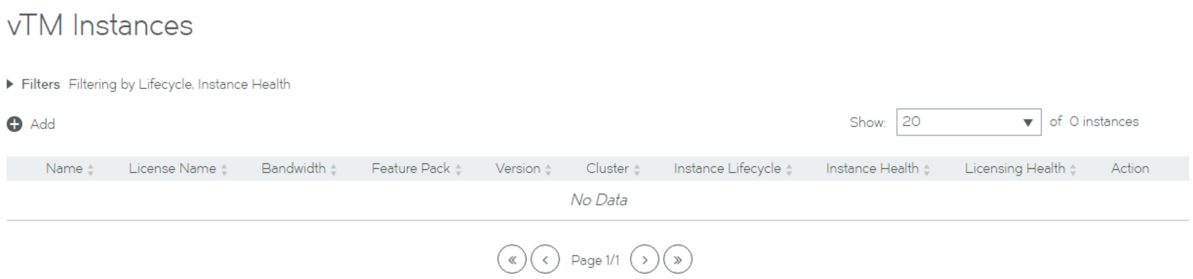
The Services Director VA supports the registration and management of Traffic Manager instances from its **vTM Instances** page. After you have completed all initial setup operations, no Traffic Manager instances are registered.

If you wish to register a Traffic Manager whose REST API is disabled, refer to Registering a Traffic Manager (Inactive REST API) on page 98.

NOTE
To minimize delays in licensing, ensure that the clocks of your Services Director(s) and your Traffic Manager instances are aligned.

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.
3. Click the **Services** menu, and then click **Services Controller: vTM Instances**. The **vTM Instances** page appears. After you have completed the Setup Wizard, this page contains no entries.

FIGURE 74 The vTM Instances Page: Before vTM Registrations



vTM Instances

▸ **Filters** Filtering by Lifecycle, Instance Health

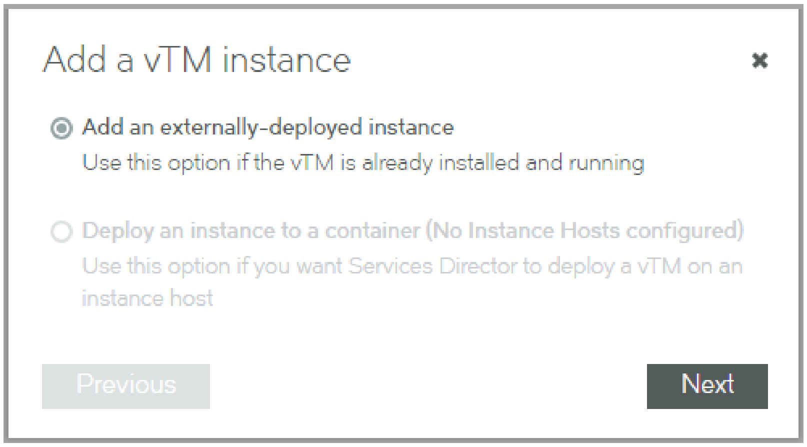
⊕ Add

Show: 20 ▾ of 0 instances

Name	License Name	Bandwidth	Feature Pack	Version	Cluster	Instance Lifecycle	Instance Health	Licensing Health	Action
No Data									

4. Click the plus symbol above the empty table. A dialog box appears:

FIGURE 75 Adding an Instance Method



Add a vTM instance

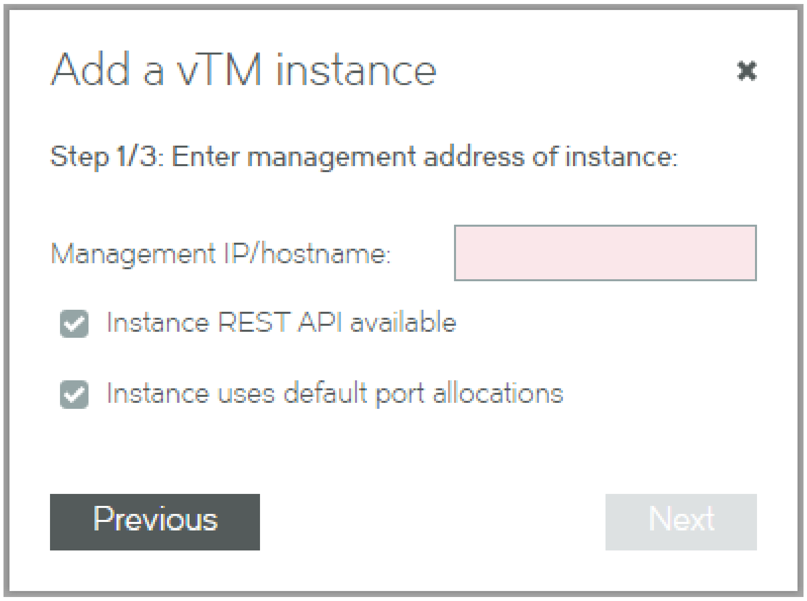
● Add an externally-deployed instance
Use this option if the vTM is already installed and running

○ Deploy an instance to a container (No Instance Hosts configured)
Use this option if you want Services Director to deploy a vTM on an instance host

5. Click **Add an externally-deployed instance**.

6. Click **Next**. A registration wizard appears:

FIGURE 76 Registration Wizard (1 of 3)



Add a vTM instance ✖

Step 1/3: Enter management address of instance:

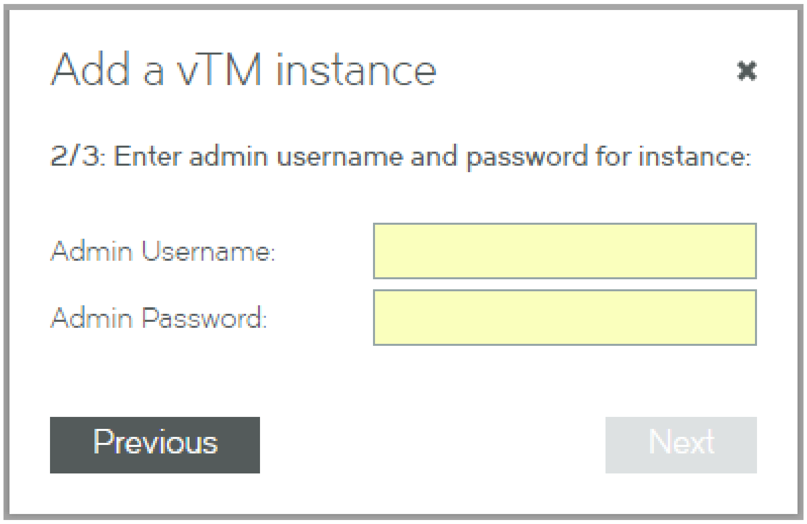
Management IP/hostname:

☑ Instance REST API available

☑ Instance uses default port allocations

7. Enter the hostname or IP address for the instance, and click **Next**. The next page of the wizard appears.

FIGURE 77 Registration Wizard (2 of 3)



Add a vTM instance ✖

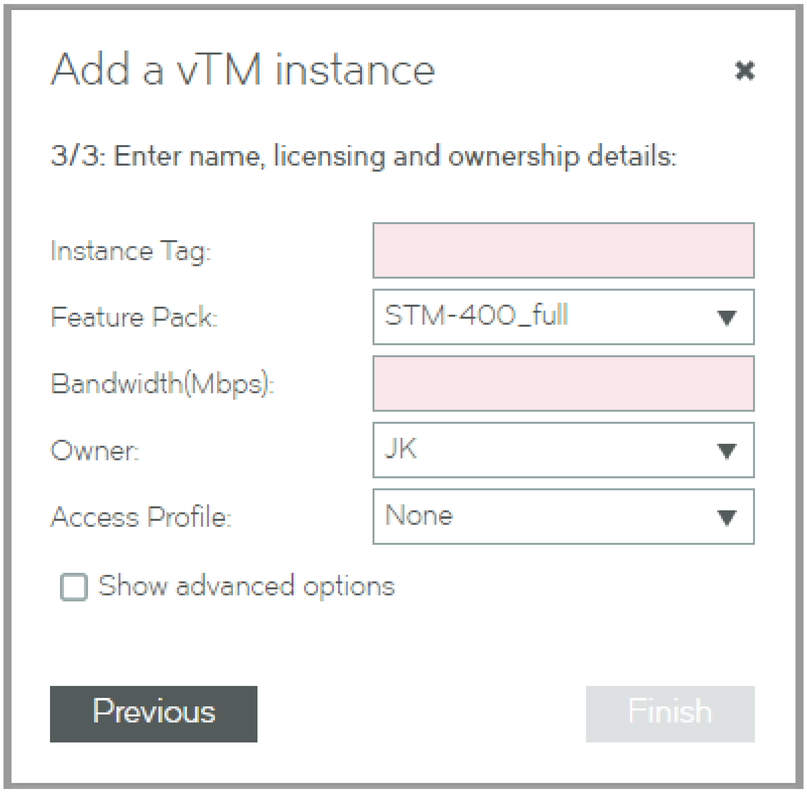
2/3: Enter admin username and password for instance:

Admin Username:

Admin Password:

8. Enter the administration username and password, and click **Next**. The next page of the wizard appears.

FIGURE 78 Registration Wizard (3 of 3)



Add a vTM instance

3/3: Enter name, licensing and ownership details:

Instance Tag:

Feature Pack: STM-400_full

Bandwidth(Mbps):

Owner: JK

Access Profile: None

□ Show advanced options

9. Enter an **Instance Tag** for the Traffic Manager instance.

   This is a user-facing name for the instance that will be used throughout the Services Director VA user interface. This tag can be changed at any time. It must be unique among non-deleted Traffic Manager instances registered on the Services Director, but can be reused as required.

   That is, if an instance is deleted, its tag can be reused for a different instance.

10. Select a **Feature Pack** for the Traffic Manager instance.

    This feature pack must be supported by your Services Director's License.

    If the required Feature Pack is not defined on your Services Director, refer to Adding a Feature Pack to the Services Director on page 70.

11. Enter a numeric **Bandwidth** (in Mbps) for the Traffic Manager instance.

    This bandwidth must be available within your Services Director's Bandwidth License.

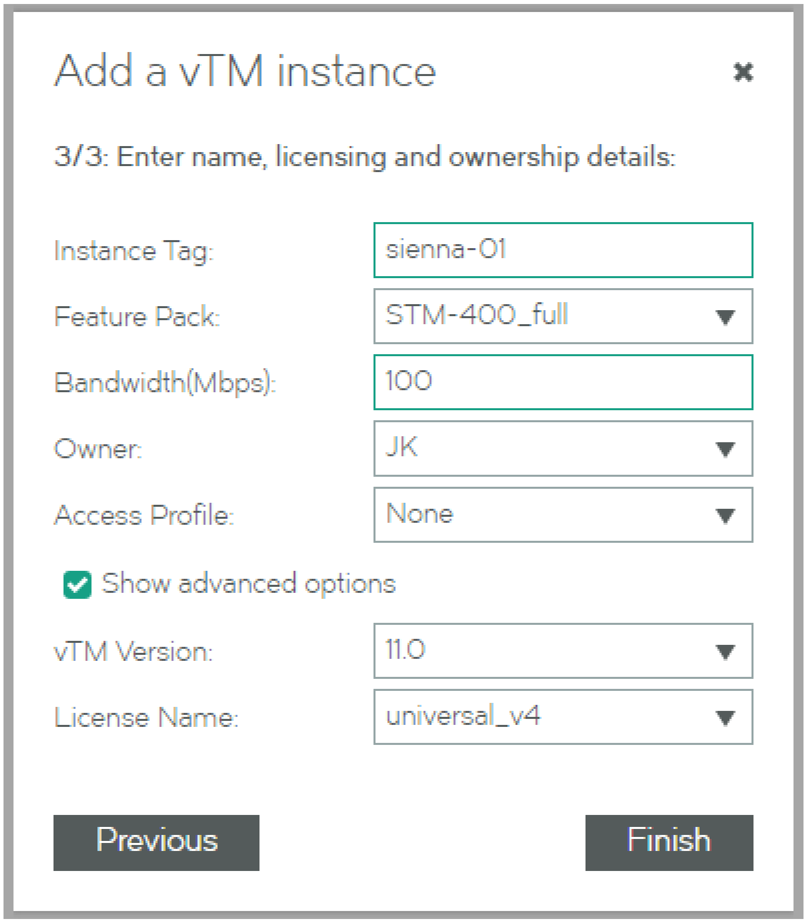
12. Select an **Owner** for the Traffic Manager instance. Refer to Adding an Owner to the Services Director on page 83. Alternatively, select *<create new>* from the **Owner** list, and type the name of a new owner. The Services Director will create a new Owner resource automatically when the registration completes. You can fully populate the Owner resource afterwards, refer to Viewing Full Details for an Owner on page 84.

13. (Optional) Select an **Access Profile**.

    This access profile identifies the authenticator and permission groups required for the user authentication on this Traffic Manager instance. If selected, these will be applied to the Traffic Manager. All cluster members are affected. Refer to Working with User Authentication on page 179.

14. Click **Show advanced options** to view additional settings.

FIGURE 79 Registration Wizard (3 of 3)



Add a vTM instance

3/3: Enter name, licensing and ownership details:

Instance Tag: sienna-01

Feature Pack: STM-400_full

Bandwidth(Mbps): 100

Owner: JK

Access Profile: None

☑ Show advanced options

vTM Version: 11.0

License Name: universal_v4

NOTE
The **vTM Version** will automatically be the software version of your Traffic Manager.

15. Select the **License Name** of your Universal FLA License.

16. Click **Finish**.

    The Traffic Manager is added to the **vTM Instances** table.

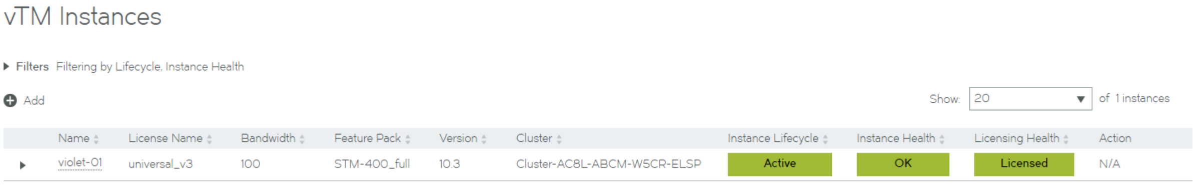
    If this Traffic Manager is at version 10.1, no cluster information is displayed.

    If this Traffic Manager is at version 10.2 or later, its cluster is considered:

    - If the Traffic Manager is in a cluster, the cluster is displayed as a Discovered cluster. The other Traffic Managers in the cluster remain unregistered and unlicensed; you must independently register and license each node in a cluster.
    - If this Traffic Manager is not in a cluster, a new cluster is created. This cluster has an automatically-generated name, and is a Discovered cluster.

    Refer to Working with Traffic Manager Clusters on page 149.

    FIGURE 80 First Added Traffic Manager Instance



vTM Instances

▸ Filters Filtering by Lifecycle, Instance Health

⊕ Add

Show: 20 ▾ of 1 instances

	Name	License Name	Bandwidth	Feature Pack	Version	Cluster	Instance Lifecycle	Instance Health	Licensing Health	Action
▸	violet-01	universal_v3	100	STM-400_full	10.3	Cluster-AC8L-ABCM-W5CR-ELSP	Active	OK	Licensed	N/A

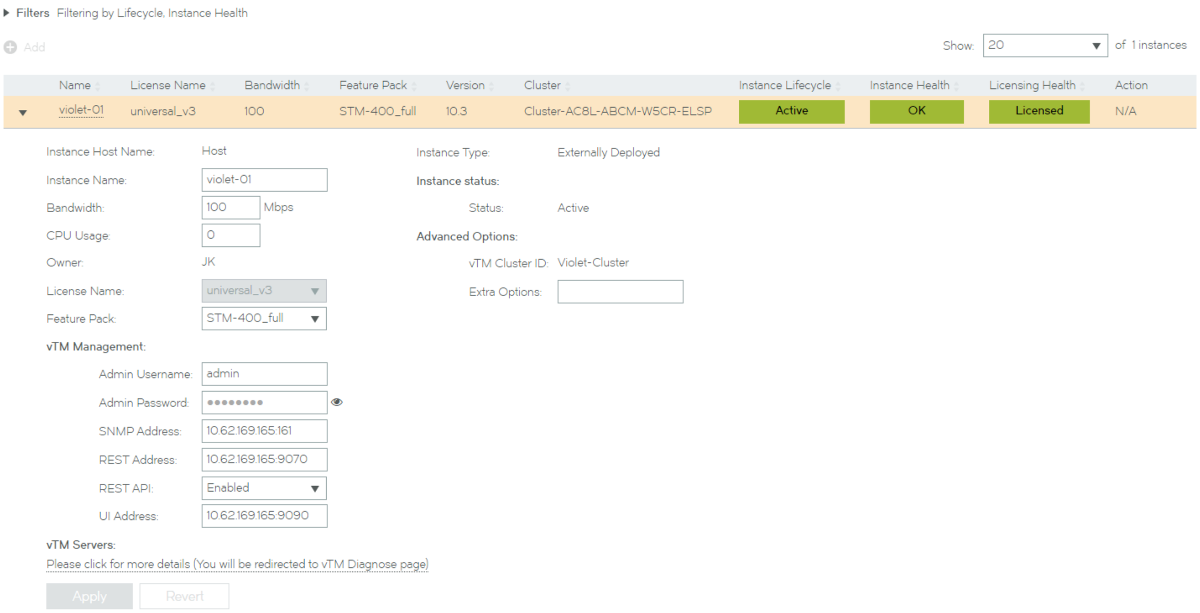
    This new entry shows basic details for the Traffic Manager instance. This includes a color-coded **Instance Lifecycle** status, **Instance Health** status, and **License Health** status. Refer to Viewing Traffic Managers on page 131.

    The **Instance Health** status is supported on all Traffic Managers at version 10.3 or later with a REST API enabled. Where it is not supported, it will be shown as N/A.

    The **License Health** status will be Pending (blue) until the licensing is confirmed. This then changes to Licensed (green).

17. Click the arrow to the left of the entry. The entry then expands to show the full details of the Traffic Manager instance.

FIGURE 81 Full Details for a Traffic Manager



▸ **Filters** Filtering by Lifecycle, Instance Health

⊕ Add

Show: 20 ▾ of 1 instances

	Name	License Name	Bandwidth	Feature Pack	Version	Cluster	Instance Lifecycle	Instance Health	Licensing Health	Action
▾	violet-01	universal_v3	100	STM-400_full	10.3	Cluster-AC8L-ABCM-W5CR-ELSP	Active	OK	Licensed	N/A

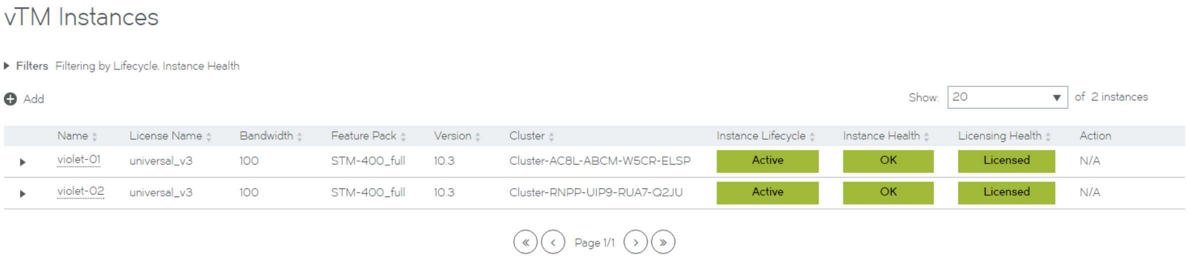
Instance Host Name: Host
Instance Name: violet-01
Bandwidth: 100 Mbps
CPU Usage: 0
Owner: JK
License Name: universal_v3
Feature Pack: STM-400_full
vTM Management:
Admin Username: admin
Admin Password: ••••••••
SNMP Address: 10.62.169.165:161
REST Address: 10.62.169.165:9070
REST API: Enabled
UI Address: 10.62.169.165:9090
vTM Servers:
Please click for more details (You will be redirected to vTM Diagnose page)

Instance Type: Externally Deployed
Instance status:
Status: Active
Advanced Options:
vTM Cluster ID: Violet-Cluster
Extra Options:

NOTE
The **Extra Options** property lists advanced settings. For more information, refer to Configuration Options (**config_options**) in the *Brocade Services Director Advanced User Guide*.

18. Repeat this procedure to add other Traffic Manager instances.

FIGURE 82 Second Added Traffic Manager Instance



vTM Instances

▸ **Filters** Filtering by Lifecycle, Instance Health

⊕ Add

Show: 20 ▾ of 2 instances

	Name	License Name	Bandwidth	Feature Pack	Version	Cluster	Instance Lifecycle	Instance Health	Licensing Health	Action
▸	violet-01	universal_v3	100	STM-400_full	10.3	Cluster-AC8L-ABCM-W5CR-ELSP	Active	OK	Licensed	N/A
▸	violet-02	universal_v3	100	STM-400_full	10.3	Cluster-RNPP-UIP9-RUA7-Q2JU	Active	OK	Licensed	N/A

Preparing to Register a Traffic Manager (Legacy FLA License)

When you register an externally-deployed Traffic Manager, typically it is at version 10.1 (or later) and its REST API is enabled. Refer to Registering a Traffic Manager (Universal FLA) on page 91.

However, you can also add a Traffic Manager that has:

- A disabled REST API. Refer to Registering a Traffic Manager (Inactive REST API) on page 98.
- A software version of 10.0 (or earlier). Refer to Registering a Traffic Manager (Pre-10.1 vTM Software Version) on page 102.

You can register these Traffic Manager instances when:

- The Traffic Manager is installed and running.
- You know the management address for the Traffic Manager. The management address that you specify when registering the Traffic Manager should always match the hostname of the Traffic Manager being registered. That is:
  - If the Traffic Manager has been configured with a resolvable hostname, that same hostname should be used as the management address when registering.
  - If the Traffic Manager has been configured without a resolvable hostname (and an IP address used instead), that IP address should be used as the management address when registering.

  NOTE
  Where no DNS-system is configured, the use of hostnames should be avoided in the product.

- You have already installed a Legacy FLA License onto the Services Director. Refer to Adding a Legacy FLA License to the Services Director on page 67.
- You have manually installed a Legacy FLA License onto the Traffic Manager. Refer to the manuals for the Brocade Virtual Traffic Manager. This is not required when the REST API is active.

Brocade recommends that you use vTM 10.1 or later and universal licensing wherever possible.

Registering a Traffic Manager (Inactive REST API)

The Services Director VA supports the registration and management of Traffic Managers from its **vTM Instances** page. This process requires:

- A valid Legacy FLA License, keyed to the Service Endpoint Address of your Services Directors. If you do not have this, refer to Adding a Legacy FLA License to the Services Director on page 67.
- A Feature Pack that identifies the supported features for the Traffic Manager. If you do not have this, refer to Adding a Feature Pack to the Services Director on page 70.

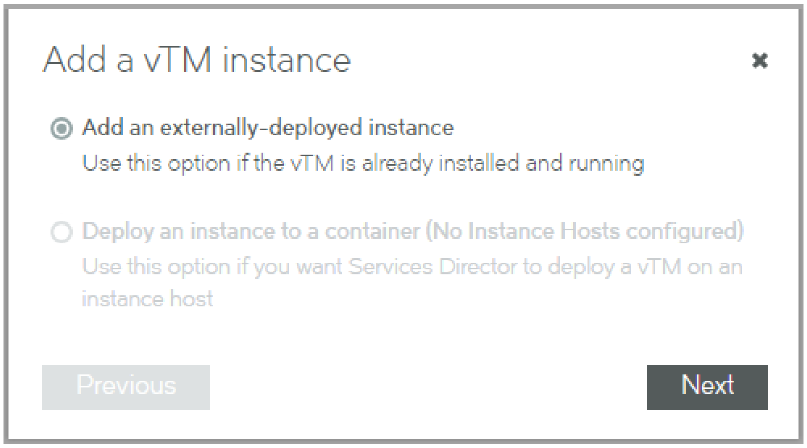
  NOTE
  You cannot specify an access profile for a Traffic Manager when its REST API is disabled.

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.
3. Click the **Services** menu, and then click **Services Controller: vTM Instances**.

   The **vTM Instances** page appears.

4. Click the plus symbol above the empty table. A dialog box appears:

FIGURE 83 Adding an Instance Method



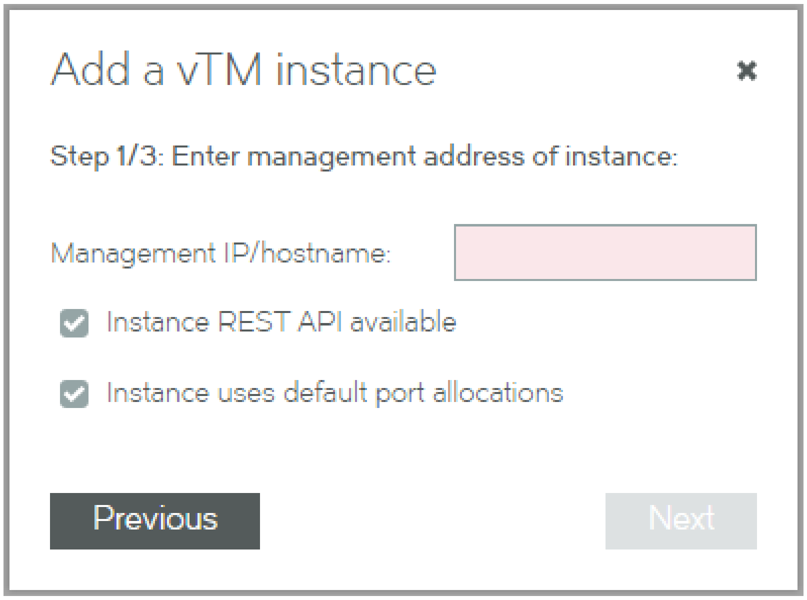
Add a vTM instance

● Add an externally-deployed instance
Use this option if the vTM is already installed and running

○ Deploy an instance to a container (No Instance Hosts configured)
Use this option if you want Services Director to deploy a vTM on an instance host

5. Click **Add an externally-deployed instance**.
6. Click **Next**. A registration wizard appears:

FIGURE 84 Registration Wizard (1 of 3)



Add a vTM instance

Step 1/3: Enter management address of instance:

Management IP/hostname:

☑ Instance REST API available

☑ Instance uses default port allocations

7. Enter the management address for the Traffic Manager.

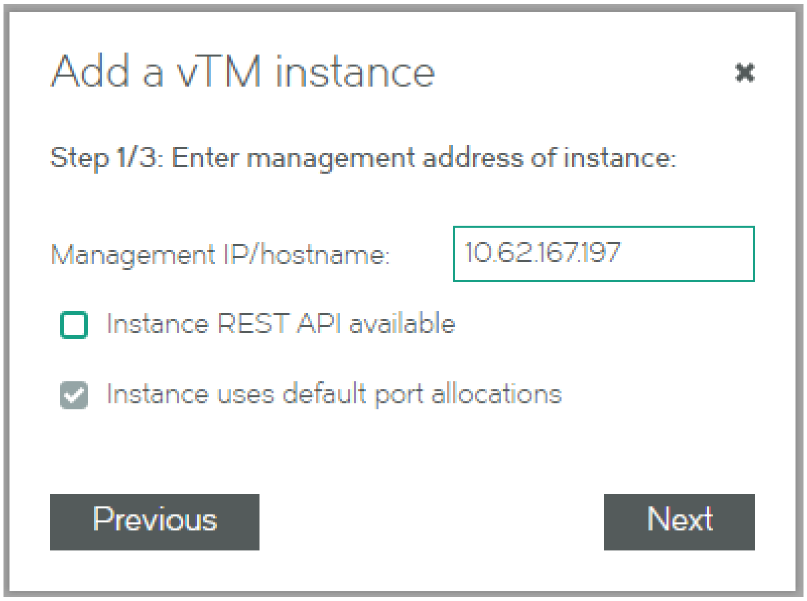
   The management address that you specify when registering the Traffic Manager should always match the hostname of the Traffic Manager being registered. That is:

   - If the Traffic Manager has been configured with a resolvable hostname, that same hostname should be used as the management address when registering.
   - If the Traffic Manager has been configured without a resolvable hostname (and an IP address used instead), that IP address should be used as the management address when registering.

     NOTE
     Where no DNS-system is configured, the use of hostnames should be avoided in the product.

8. Clear the **Instance REST API available** check box.

FIGURE 85 Clearing the Instance REST API Available Check Box



Add a vTM instance

Step 1/3: Enter management address of instance:

Management IP/hostname: 10.62.167.197

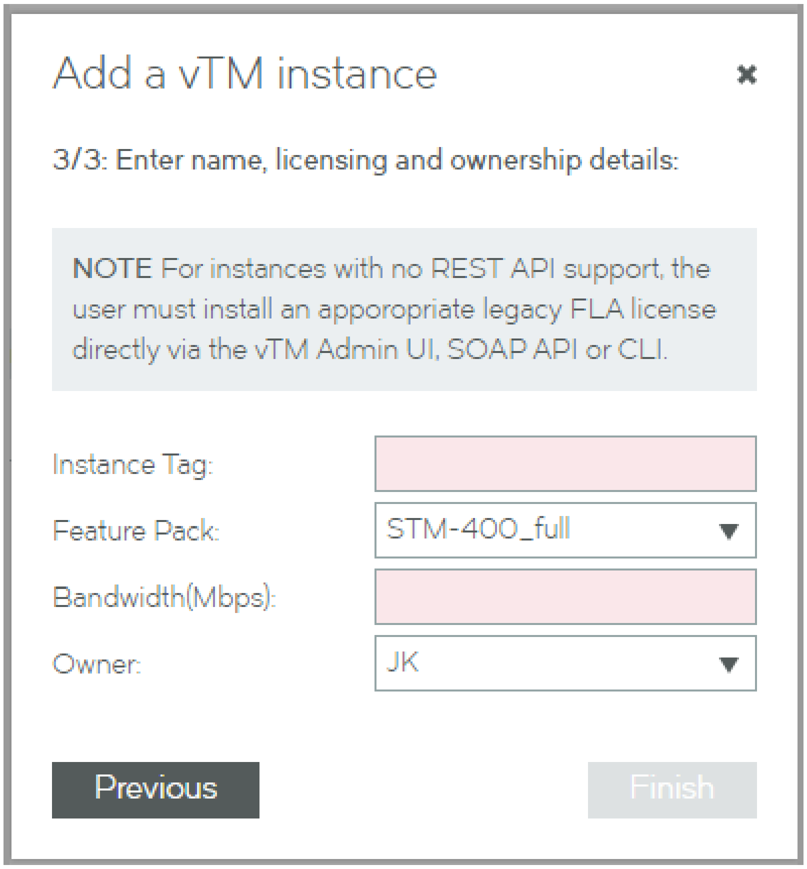
□ Instance REST API available

☑ Instance uses default port allocations

9. Click **Next**.

   This option bypasses the second page of the wizard, and delivers you directly to the final page.

   FIGURE 86 Registration Wizard (3 of 3)

   Add a vTM instance

   3/3: Enter name, licensing and ownership details:

   NOTE For instances with no REST API support, the user must install an apporopriate legacy FLA license directly via the vTM Admin UI, SOAP API or CLI.

   Instance Tag:

   Feature Pack: STM-400_full

   Bandwidth(Mbps):

   Owner: JK

10. Enter an **Instance Tag** for the Traffic Manager instance.

    This is a user-facing name for the instance that will be used throughout the Services Director VA user interface. This tag can be changed at any time. It must be unique among non-deleted Traffic Manager instances registered on the Services Director, but can be reused as required.

    That is, if an instance is deleted, its tag can be reused for a different instance.

11. Select a **Feature Pack** for the Traffic Manager instance.

    This feature pack must be supported by your Services Director's License.

    If the required Feature Pack is not defined on your Services Director, refer to Adding a Feature Pack to the Services Director on page 70.

12. Enter a numeric **Bandwidth** (in Mbps) for the Traffic Manager instance.

    This bandwidth must be available within your Services Director's Bandwidth License.

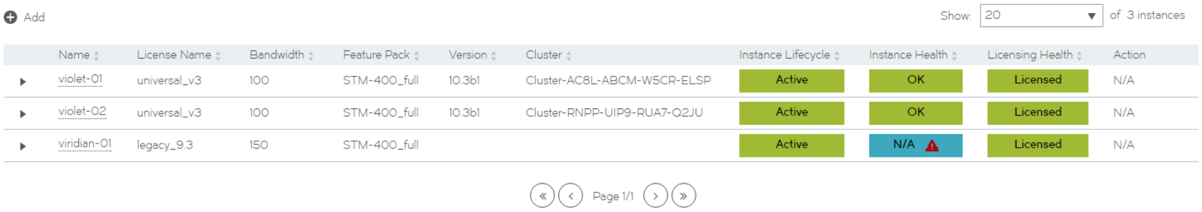
13. Select an **Owner** for the Traffic Manager instance. Refer to Adding an Owner to the Services Director on page 83. Alternatively, select *<create new>* from the **Owner** list, and type the name of a new owner. The Services Director will create a new Owner resource automatically when the registration completes. You can fully populate the Owner resource afterwards, refer to Viewing Full Details for an Owner on page 84.
14. Click **Finish**.

    The Traffic Manager is added to the **vTM Instances** table.

    The **Cluster** and software **Version** for this Traffic Manager are not shown, as the REST API is required to retrieve this information from the Traffic Manager.

    If this Traffic Manager is not already in a cluster (and is at version 10.2 or later with the REST API enabled), a new cluster is created. This cluster has an automatically-generated name, and is a Discovered cluster. Refer to Working with Traffic Manager Clusters on page 149.

    FIGURE 87 Traffic Manager Instance: Inactive REST API)



⊕ Add

Show: 20 ▼ of 3 instances

	Name	License Name	Bandwidth	Feature Pack	Version	Cluster	Instance Lifecycle	Instance Health	Licensing Health	Action
▸	violet-01	universal_v3	100	STM-400_full	10.3b1	Cluster-AC8L-ABCM-W5CR-ELSP	Active	OK	Licensed	N/A
▸	violet-02	universal_v3	100	STM-400_full	10.3b1	Cluster-RNPP-UIP9-RUA7-Q2JU	Active	OK	Licensed	N/A
▸	viridian-01	legacy_9.3	150	STM-400_full			Active	N/A ⚠	Licensed	N/A

    This new entry shows basic details for the Traffic Manager instance. This includes a color-coded **Instance Lifecycle** status, **Instance Health** status, and **License Health** status. Refer to Viewing Traffic Managers on page 131.

    The **Instance Health** status is always N/A for Traffic Managers using a Legacy FLA. This feature is only supported on Traffic Managers at version 10.3 or later with a REST API enabled.

    The **License Health** status will be Pending (blue) until the licensing is confirmed. This then changes to Licensed (green).

> NOTE
> If the Pending status does not clear after a few minutes, log in to the affected Traffic Manager and investigate further.

Registering a Traffic Manager (Pre-10.1 vTM Software Version)

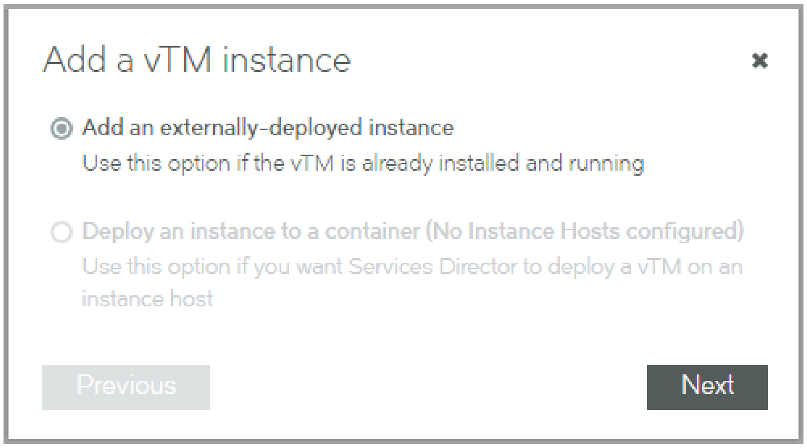
The Services Director VA supports the registration and management of Traffic Manager instances from its **vTM Instances** page. This process requires:

- A valid Legacy FLA License, keyed to the Service Endpoint Address of your Services Director instances. If you do not have this, refer to Adding a Legacy FLA License to the Services Director on page 67.
- A Feature Pack that identifies the supported features for the Traffic Manager. If you do not have this, refer to Adding a Feature Pack to the Services Director on page 70.

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears:
3. Click the **Services** menu, and then click **Services Controller: vTM Instances**. The **vTM Instances** page appears.

4. Click the plus symbol above the Traffic Manager table. A dialog box appears:

FIGURE 88 Adding an Instance Method



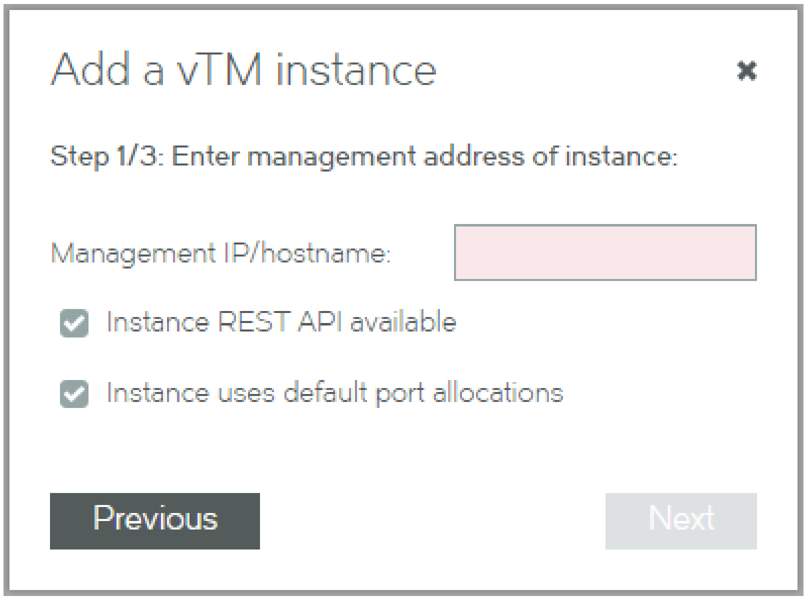
Add a vTM instance

● Add an externally-deployed instance
Use this option if the vTM is already installed and running

○ Deploy an instance to a container (No Instance Hosts configured)
Use this option if you want Services Director to deploy a vTM on an instance host

5. Click **Add an externally-deployed instance**.
6. Click **Next**. A registration wizard appears:

FIGURE 89 Registration Wizard (1 of 3)



Add a vTM instance

Step 1/3: Enter management address of instance:

Management IP/hostname:

☑ Instance REST API available

☑ Instance uses default port allocations

7. Enter the management address for the Traffic Manager.

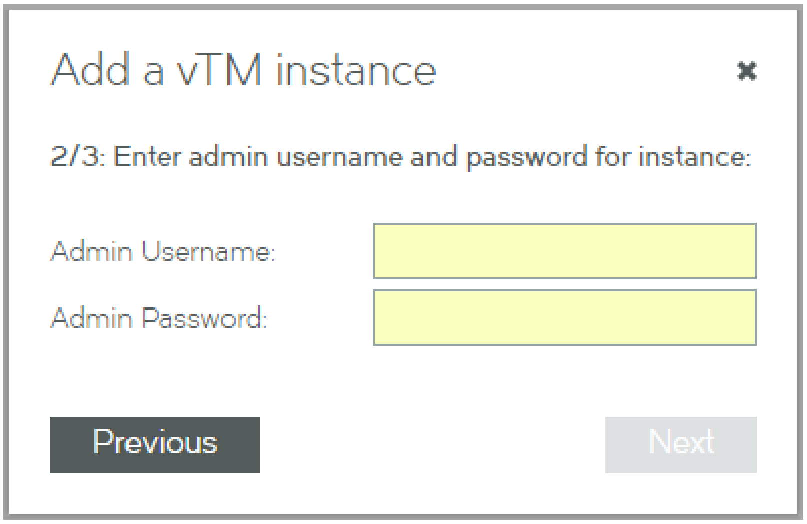
   The management address that you specify when registering the Traffic Manager should always match the hostname of the Traffic Manager being registered. That is:

   - If the Traffic Manager has been configured with a resolvable hostname, that same hostname should be used as the management address when registering.
   - If the Traffic Manager has been configured without a resolvable hostname (and an IP address used instead), that IP address should be used as the management address when registering.

     NOTE
     Where no DNS-system is configured, the use of hostnames should be avoided in the product.

8. Click **Next**. The next page of the wizard appears.

   FIGURE 90 Registration Wizard (2 of 3)



Add a vTM instance

2/3: Enter admin username and password for instance:

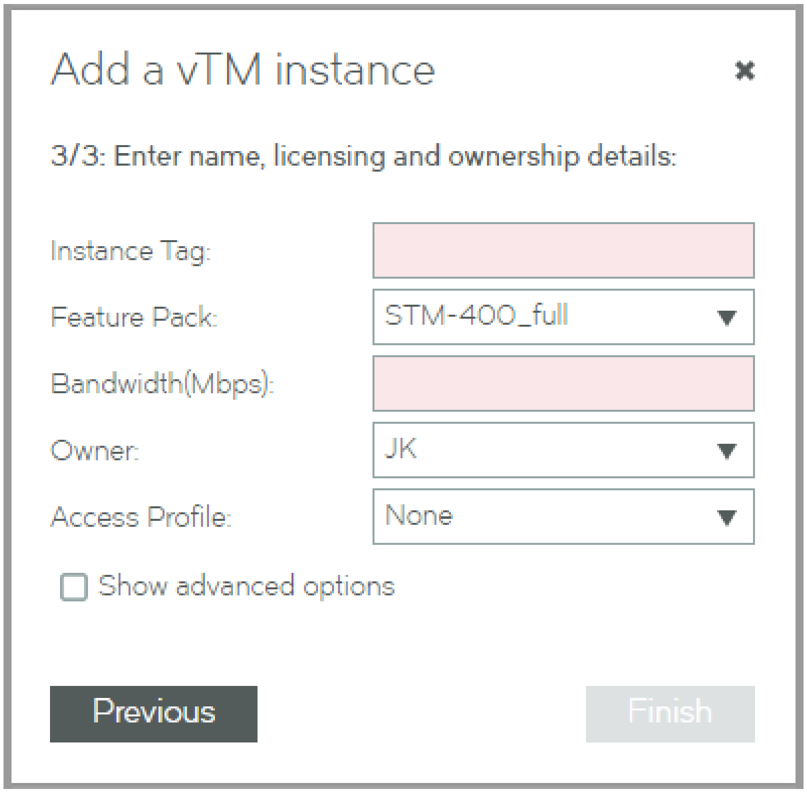
Admin Username:

Admin Password:

9. Enter the administration username and password.

10. Click **Next**. The next page of the wizard appears.

FIGURE 91 Registration Wizard (3 of 3)



Add a vTM instance

3/3: Enter name, licensing and ownership details:

Instance Tag:

Feature Pack: STM-400_full

Bandwidth(Mbps):

Owner: JK

Access Profile: None

□ Show advanced options

11. Enter an **Instance Tag** for the Traffic Manager instance.

    This is a user-facing name for the instance that will be used throughout the Services Director VA user interface. This tag can be changed at any time. It must be unique among non-deleted Traffic Manager instances registered on the Services Director, but can be reused as required.

    That is, if an instance is deleted, its tag can be reused for a different instance.

12. Select a **Feature Pack** for the Traffic Manager instance.

    This feature pack must be supported by your Services Director's License.

    If the required Feature Pack is not defined on your Services Director, refer to Adding a Feature Pack to the Services Director on page 70.

13. Enter a numeric **Bandwidth** (in Mbps) for the Traffic Manager instance.

    This bandwidth must be available within your Services Director's Bandwidth License.

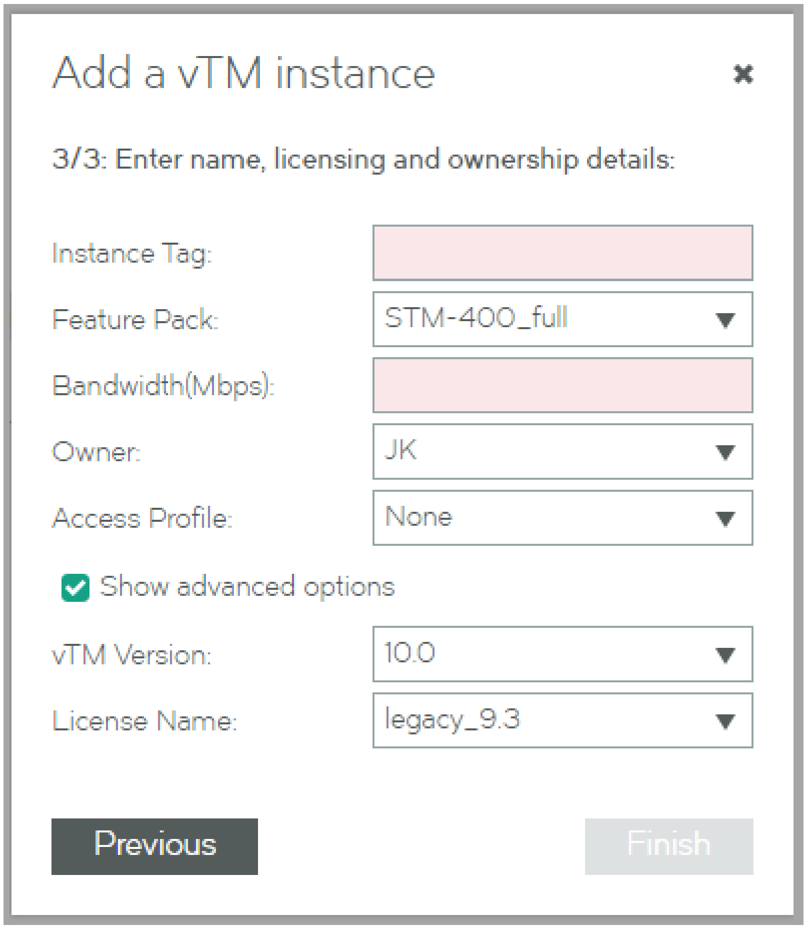
14. Select an **Owner** for the Traffic Manager instance. Refer to Adding an Owner to the Services Director on page 83. Alternatively, select *<create new>* from the **Owner** list, and type the name of a new owner. The Services Director will create a new Owner resource automatically when the registration completes. You can fully populate the Owner resource afterwards, refer to Viewing Full Details for an Owner on page 84.

15. (Optional) Select an **Access Profile**.

    This access profile identifies the authenticator and permission groups required for the user authentication on this Traffic Manager instance. If selected, these will be applied to the Traffic Manager. All cluster members are affected. Refer to Working with User Authentication on page 179.

16. Click **Show advanced options** to view additional settings.

    FIGURE 92 Registration Wizard (3 of 3)

    Add a vTM instance

    3/3: Enter name, licensing and ownership details:

    Instance Tag:

    Feature Pack: STM-400_full

    Bandwidth(Mbps):

    Owner: JK

    Access Profile: None

    ☑ Show advanced options

    vTM Version: 10.0

    License Name: legacy_9.3

    The **vTM Version** will automatically be the software version of your Traffic Manager.

17. Select the **License Name** for your Legacy FLA License.

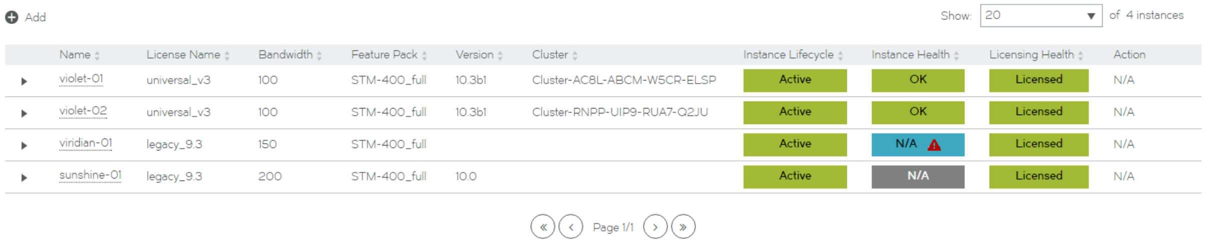
    If the required Legacy FLA License is not listed, you must add it before you can register this Traffic Manager. Refer to Adding a Legacy FLA License to the Services Director on page 67.

18. Click **Finish**.

The Traffic Manager is added to the **vTM Instances** table.

The **Cluster** and software **Version** for this Traffic Manager are not shown, as version 10.2 and an active REST API are required to retrieve this information from the Traffic Manager.

FIGURE 93 Traffic Manager Instance: Pre-10.1 vTM Software Version



	Name	License Name	Bandwidth	Feature Pack	Version	Cluster	Instance Lifecycle	Instance Health	Licensing Health	Action
▸	violet-01	universal_v3	100	STM-400_full	10.3b1	Cluster-AC8L-ABCM-W5CR-ELSP	Active	OK	Licensed	N/A
▸	violet-02	universal_v3	100	STM-400_full	10.3b1	Cluster-RNPP-UIP9-RUA7-Q2JU	Active	OK	Licensed	N/A
▸	viridian-01	legacy_9.3	150	STM-400_full			Active	N/A ⚠	Licensed	N/A
▸	sunshine-01	legacy_9.3	200	STM-400_full	10.0		Active	N/A	Licensed	N/A

This new entry shows basic details for the Traffic Manager instance. This includes a color-coded **Instance Lifecycle** status, **Instance Health** status and a **License Health** status. Refer to Viewing Traffic Managers on page 131.

The **Instance Health** status is always N/A for Traffic Managers using a Legacy FLA. This feature is only supported on Traffic Managers at version 10.3 or later with a REST API enabled.

The **License Health** status will be Pending (blue) until the licensing is confirmed. This then changes to Licensed (green).

NOTE
If the Pending status does not clear after a few minutes, log in to the affected Traffic Manager and investigate further.

Self-Registering an Externally-Deployed Traffic Manager

The Services Director VA supports the self-registration of externally-deployed Virtual Traffic Managers (vTM). This adds vTMs to the estate of the Services Director, from where it can be licensed, monitored and metered.

This section describes the principles of vTM self-registration, and outlines the processing of self-registration requests on the Services Director.

NOTE
Self-registration is not supported for vTMs that are in a private network behind a NAT.

Overview: vTM Self-Registration (VMware)

After you have completed the initial configuration of the Services Director, you can begin to add externally-deployed Virtual Traffic Managers (vTMs) to the estate of the Services Director.

One method for achieving this is by self-registration of the vTMs.

NOTE
Self-registration on the Services Director VA is also supported for cloud-based vTMs on AWS installations, refer to Overview: vTM Self-Registration (Cloud) on page 123.

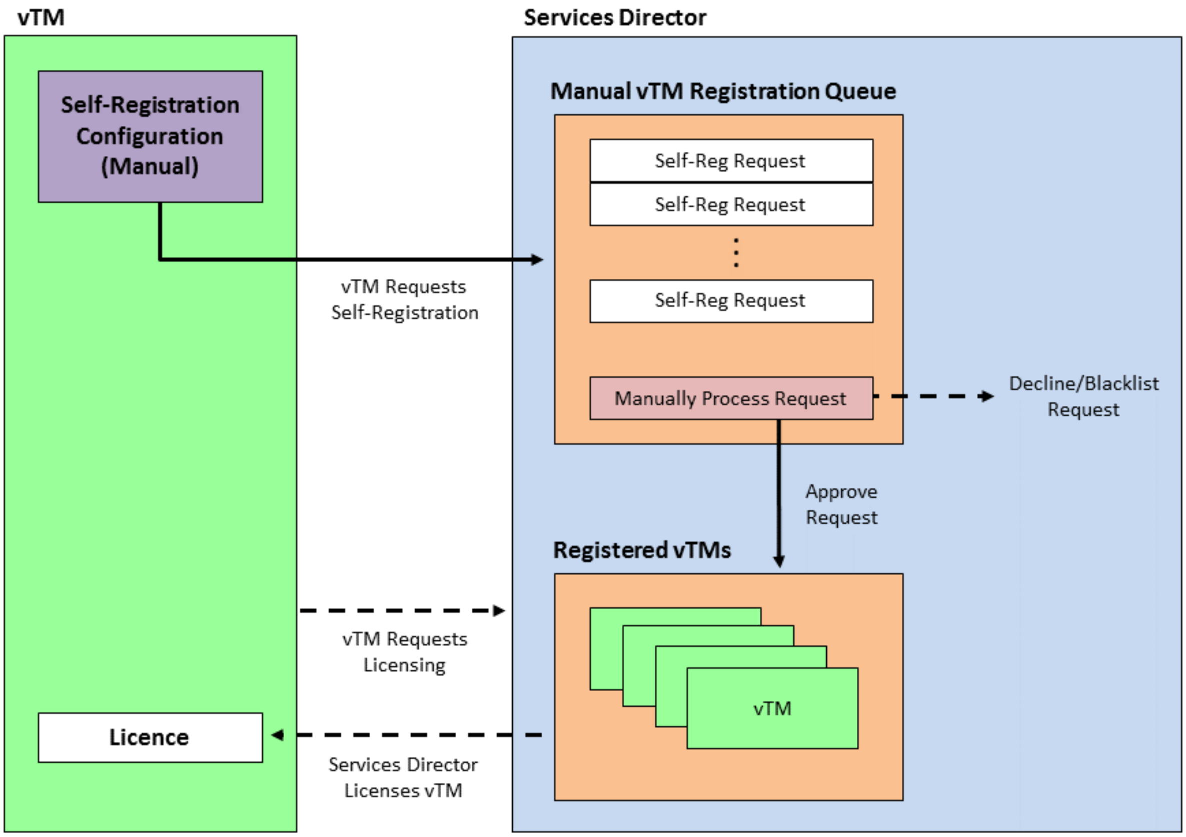
NOTE
Self-registration is not supported for vTMs that are in a private network behind a NAT.

Self-registration is initially configured from the vTM user interface. An Administrator configures the vTM so that it will request self-registration on a specified Services Director. Typically, this is done during the installation wizard for the vTM, refer to Requesting Self-Registration During vTM Installation on page 109. However, this can also be done during later configuration of the vTM. Refer to Requesting Self Registration on a Configured vTM on page 115.

Self-registration can be either manual or automatic:

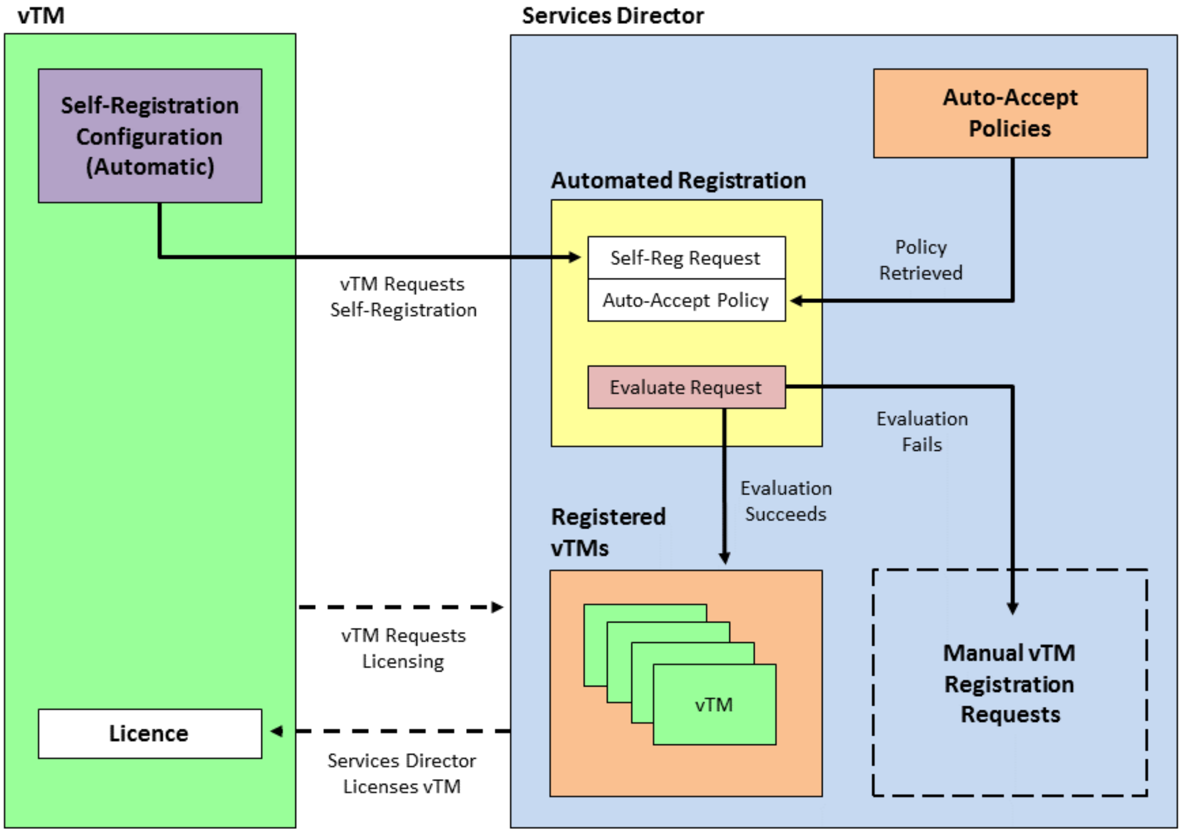
- Manual self-registration requires configuration of the vTM so that it requests self-registration on the Services Director. When the request is received, the Services Director adds it to a queue of self-registration requests. The Administrator processes these manually as required, and can accept, decline or blacklist a request (refer to Processing Self-Registration Requests Manually on page 119). Once a request is accepted, the vTM is added to the list of vTMs known to the Services Director. Licensing of the vTM can then occur as a separate process.

FIGURE 94 Manual Self-Registration of a vTM


vTM
Services Director
Self-Registration Configuration (Manual)
Manual vTM Registration Queue
Self-Reg Request
Self-Reg Request
Self-Reg Request
vTM Requests Self-Registration
Manually Process Request
Decline/Blacklist Request
Approve Request
Registered vTMs
vTM Requests Licensing
vTM
Licence
Services Director Licenses vTM

- Automatic self-registration requires configuration on both the vTM and the Services Director. An auto-accept policy must exist on the Services Director. This policy (one of many, potentially) defines the acceptance conditions and some fixed values for vTMs that use the policy. A policy must be referenced during the configuration of self-registration on the vTM. When the request is received, the Services Director evaluates the request against the specified auto-accept policy, and will either accept or reject the vTM automatically. Once accepted, the vTM is added to the list of vTMs known to the Services Director, and licensing of the vTM can then occur as a separate process. When rejected (for example, when there is insufficient bandwidth remaining, or the vTM is from outside the subnetwork), the vTM is added to the queue for manual self-registration requests instead, and the Administrator can process this in the usual way (see above).

FIGURE 95 Automatic Self-Registration of a vTM



NOTE
Once a vTM is configured for self-registration, it will make a self-registration request every time it restarts. The Services Director will assess this request, but will not process it if the vTM is already registered, blacklisted, or there is a pending self-registration request for the vTM.

NOTE
Once a self-registration request is received by the Services Director from a vTM, you must not change the cluster to which the vTM belongs until the registration request is accepted.

Requesting Self-Registration During vTM Installation

When you install the Virtual Traffic Manager VA, you can configure it for self-registration on the Services Director VA. Both manual and automatic self-registrations are supported.

NOTE
Once self-registration is requested by the vTM to the Services Director, you must not change the cluster to which a vTM belongs until the registration request is accepted.

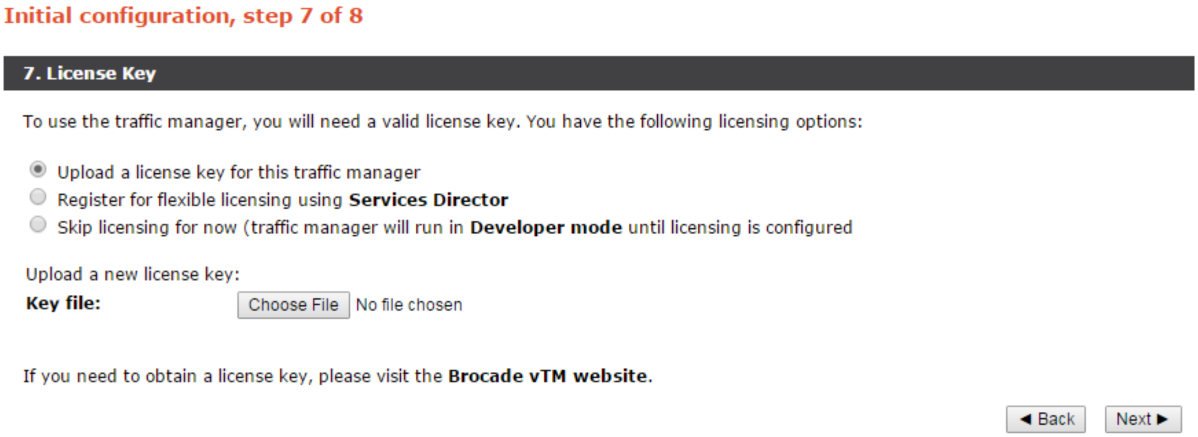
Requesting Manual Self-Registration During the Installation of a vTM

This procedure enables you to configure a vTM for manual self-registration.

NOTE
For automatic self-registration, refer to Requesting Automatic Self-Registration During the Installation of a vTM on page 112.

1. Install the Virtual Traffic Manager VA.
2. Log in to the vTM VA to start its installation wizard.
3. Progress through the Setup Wizard until the following page appears:

FIGURE 96 vTM Installation Wizard: License Key Page



Initial configuration, step 7 of 8

7. License Key

To use the traffic manager, you will need a valid license key. You have the following licensing options:

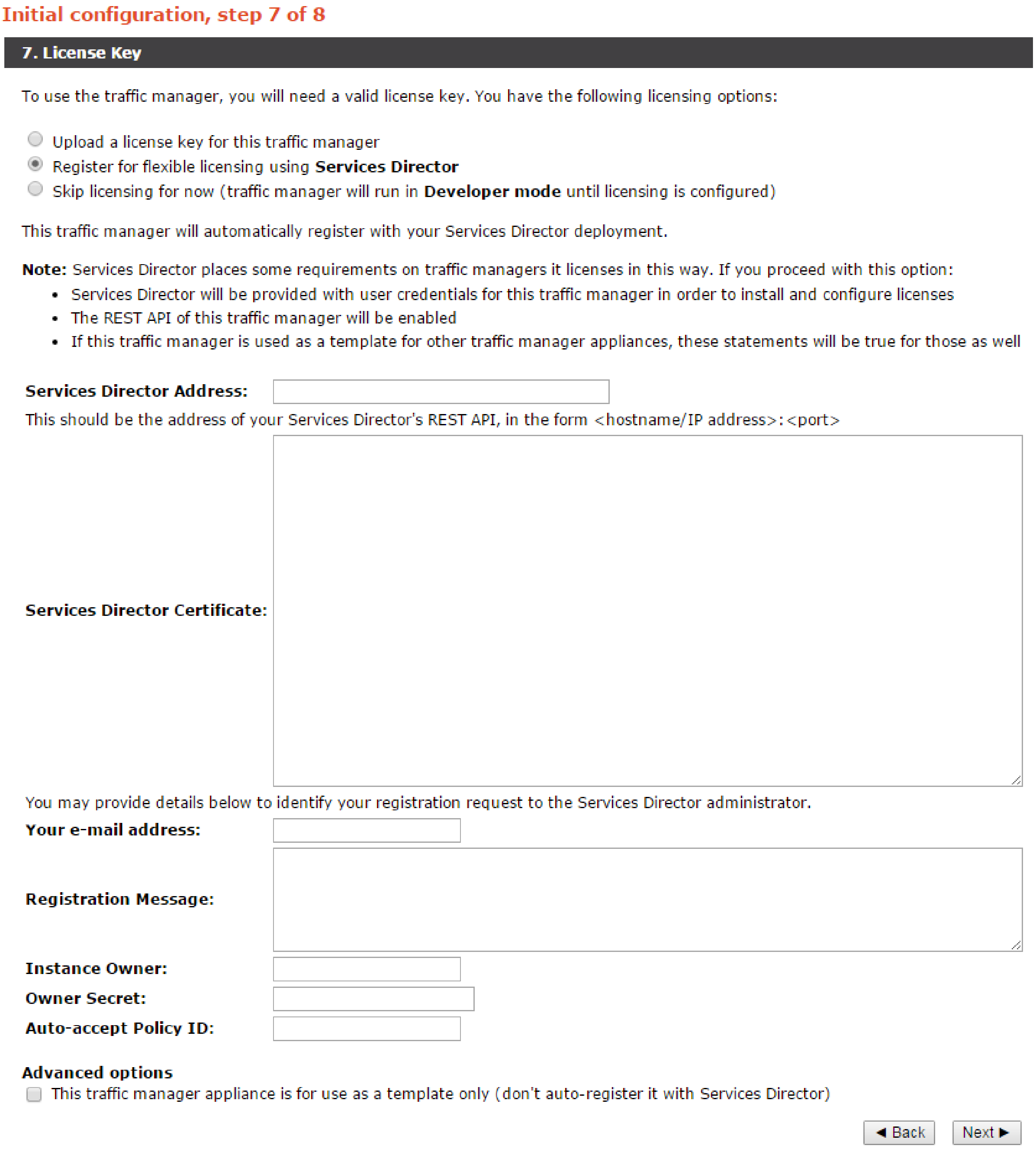
● Upload a license key for this traffic manager
○ Register for flexible licensing using **Services Director**
○ Skip licensing for now (traffic manager will run in **Developer mode** until licensing is configured

Upload a new license key:
Key file: Choose File No file chosen

If you need to obtain a license key, please visit the **Brocade vTM website**.

4. Select **Register for flexible licensing using Services Director**. The page updates to include fields for self-registration:

FIGURE 97 vTM Installation Wizard: Requesting Self-Registration



Initial configuration, step 7 of 8

7. License Key

To use the traffic manager, you will need a valid license key. You have the following licensing options:

○ Upload a license key for this traffic manager
● Register for flexible licensing using **Services Director**
○ Skip licensing for now (traffic manager will run in **Developer mode** until licensing is configured)

This traffic manager will automatically register with your Services Director deployment.

Note: Services Director places some requirements on traffic managers it licenses in this way. If you proceed with this option:

- Services Director will be provided with user credentials for this traffic manager in order to install and configure licenses
- The REST API of this traffic manager will be enabled
- If this traffic manager is used as a template for other traffic manager appliances, these statements will be true for those as well

Services Director Address:
This should be the address of your Services Director's REST API, in the form <hostname/IP address>:<port>

Services Director Certificate:

You may provide details below to identify your registration request to the Services Director administrator.

Your e-mail address:

Registration Message:

Instance Owner:

Owner Secret:

Auto-accept Policy ID:

Advanced options
□ This traffic manager appliance is for use as a template only (don't auto-register it with Services Director)

5. Specify the **Services Director Address**. This is the management address of the REST API port for the Services Director, as an <ip_address/host>:<port> pair.

6. Paste the Services Director's REST API SSL certificate as the **Services Director Certificate**. Contact the Services Director Administrator to obtain this.

7. (Optional) Specify **Your e-mail address**. If you provide this, the Services Director Administrator will receive a notification email when the self-registration request is received by the Services Director.
8. (Optional) Specify a **Registration Message**. This is seen by the Services Director Administrator when they view the self-registration request.
9. (Optional) Select an **Owner** for the vTM instance.

   NOTE
   The owner entry was created in the Services Director, refer to Adding an Owner to the Services Director on page 83.

10. Where you have selected an **Owner**, enter the **Owner Secret** password.

    NOTE
    The password for the owner was created in the Services Director, refer to Adding an Owner to the Services Director on page 83.

11. Do not enter an **Auto-accept Policy ID**. This is required for automatic self-registration only.
12. Ensure that the **Advanced Options** check box is clear. This is only required when creating a template vTM, refer to Working with vTM Templates on page 197.
13. Click **Next** to go to the final wizard page and complete the wizard.

    After the wizard completes, the vTM restarts.

    The Services Director will receive a self-registration request from the vTM after the vTM restarts. The request is added to the queue of vTM self-registration requests, and can then be processed manually, refer to Accepting a Pending Self-Registration Request on page 119.

    NOTE
    Once a vTM is configured for self-registration, it will make a self-registration request every time it restarts. The Services Director will assess this request, but will not process it if the vTM is already registered, or there is a Pending self-registration request for the vTM.

    NOTE
    Once a self-registration request is received by the Services Director from a vTM, you must not change the cluster to which the vTM belongs until the registration request is accepted.

Requesting Automatic Self-Registration During the Installation of a vTM

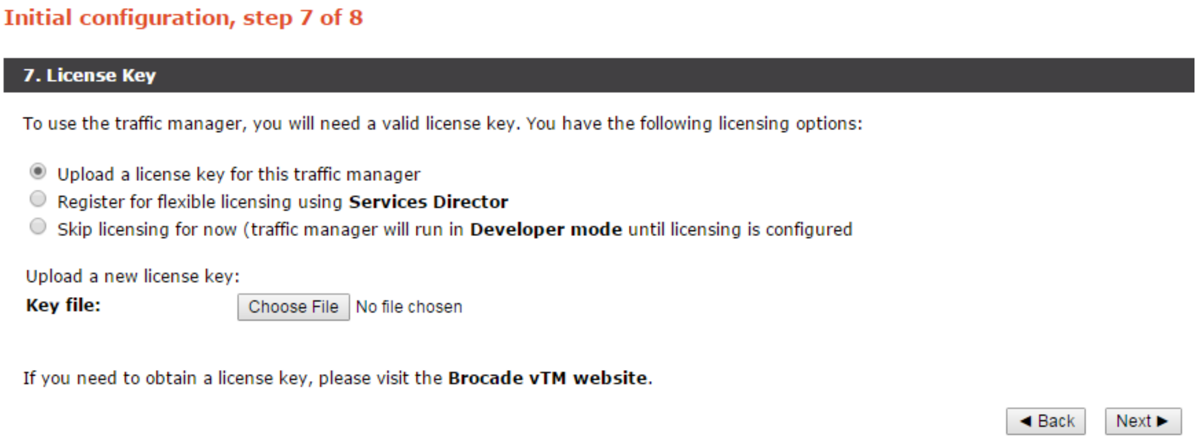
This procedure enables you to configure a vTM for automatic self-registration.

NOTE
For manual self-registration, refer to Requesting Manual Self-Registration During the Installation of a vTM on page 110.

1. Install the Virtual Traffic Manager VA.
2. Log in to the vTM VA to start its installation wizard.

3. Progress through the Setup Wizard until the following page appears:

FIGURE 98 vTM Installation Wizard: License Key Page



Initial configuration, step 7 of 8

7. License Key

To use the traffic manager, you will need a valid license key. You have the following licensing options:

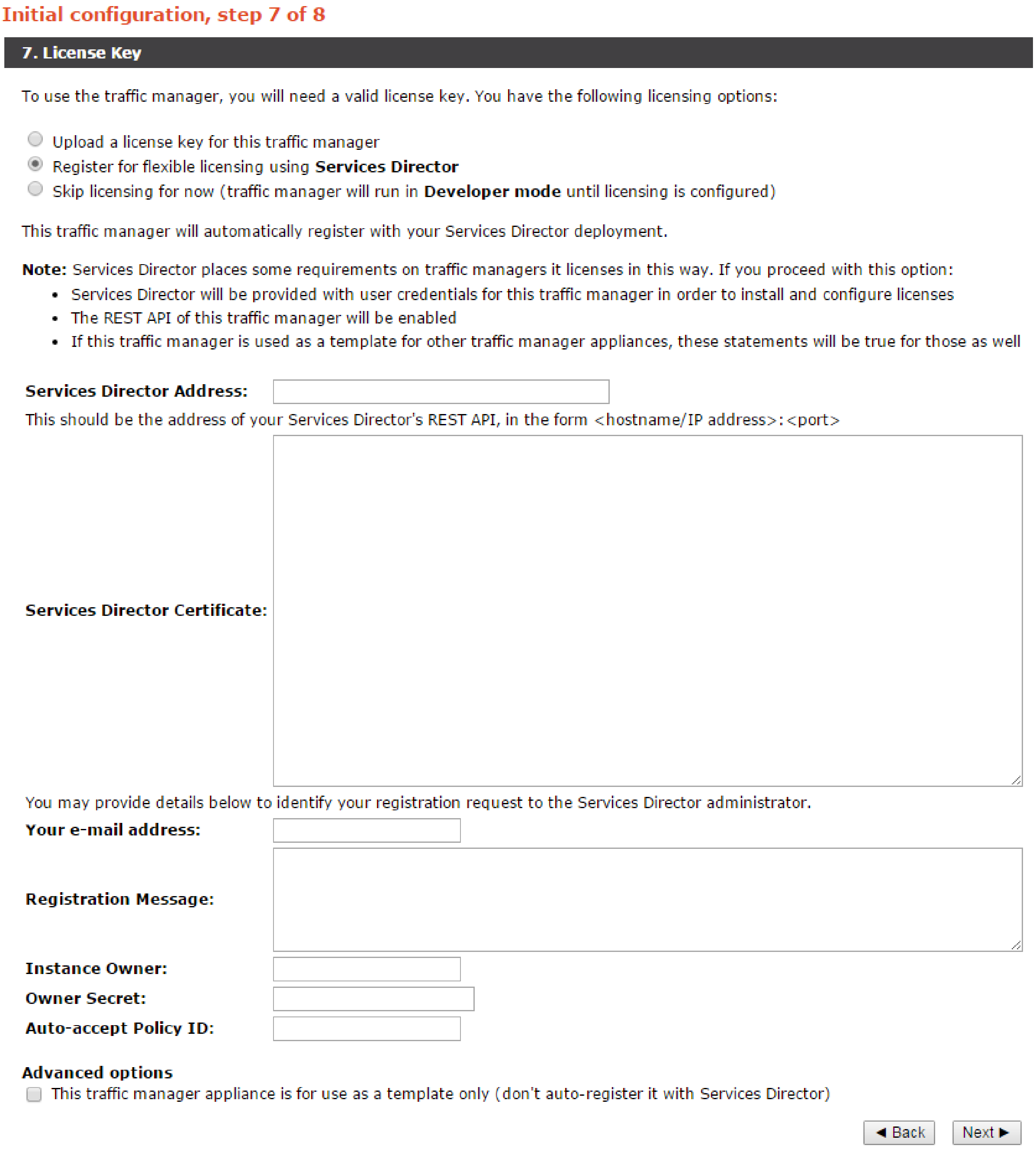
● Upload a license key for this traffic manager
○ Register for flexible licensing using **Services Director**
○ Skip licensing for now (traffic manager will run in **Developer mode** until licensing is configured

Upload a new license key:
Key file: Choose File No file chosen

If you need to obtain a license key, please visit the **Brocade vTM website**.

4. Select **Register for flexible licensing using Services Director**. The page updates to include fields for self-registration:

FIGURE 99 vTM Installation Wizard: Requesting Self-Registration



Initial configuration, step 7 of 8

7. License Key

To use the traffic manager, you will need a valid license key. You have the following licensing options:

○ Upload a license key for this traffic manager
● Register for flexible licensing using **Services Director**
○ Skip licensing for now (traffic manager will run in **Developer mode** until licensing is configured)

This traffic manager will automatically register with your Services Director deployment.

Note: Services Director places some requirements on traffic managers it licenses in this way. If you proceed with this option:

- Services Director will be provided with user credentials for this traffic manager in order to install and configure licenses
- The REST API of this traffic manager will be enabled
- If this traffic manager is used as a template for other traffic manager appliances, these statements will be true for those as well

Services Director Address:

This should be the address of your Services Director's REST API, in the form <hostname/IP address>:<port>

Services Director Certificate:

You may provide details below to identify your registration request to the Services Director administrator.

Your e-mail address:

Registration Message:

Instance Owner:

Owner Secret:

Auto-accept Policy ID:

Advanced options

□ This traffic manager appliance is for use as a template only (don't auto-register it with Services Director)

5. Specify the **Services Director Address**. This is the management address of the REST API port for the Services Director, as an <ip_address/host>:<port> pair.

6. Paste the Services Director's REST API SSL certificate as the **Services Director Certificate**. Contact the Services Director Administrator to obtain this.

7. (Optional) Specify **Your e-mail address**. If you provide this, the Services Director Administrator will receive a notification email when the self-registration request is received by the Services Director.
8. (Optional) Specify a **Registration Message**. This is seen by the Services Director Administrator when they view the self-registration request.
9. Select an **Owner** for the vTM instance.

   NOTE
   The owner entry was created in the Services Director, refer to Adding an Owner to the Services Director on page 83.

10. Enter the **Owner Secret** password for the selected **Owner**.

    NOTE
    The password for the owner was created in the Services Director, refer to Adding an Owner to the Services Director on page 83.

11. Enter the **Auto-accept Policy ID** of the auto-accept policy required for this vTM instance.

    NOTE
    The auto-accept policy was created in the Services Director, refer to Adding an Auto-Accept Policy to the Services Director on page 85.

12. Ensure that the **Advanced Options** check box is clear. This is only required when creating a template vTM, refer to Working with vTM Templates on page 197.
13. Click **Next** to go to the final wizard page and complete the wizard.

    After the wizard completes, the vTM restarts.

    The Services Director will receive a request for automatic self-registration the vTM after the vTM restarts. Either:

    - If the request can be processed automatically using the specified auto-accept policy, the vTM is added to the estate of the Services Director immediately, and subsequently licensed.
    - If the request cannot be processed automatically using the specified auto-accept policy, the request is added to the queue of vTM self-registration requests, and can then be processed manually, refer to Accepting a Pending Self-Registration Request on page 119.

    NOTE
    Once a vTM is configured for self-registration, it will make a self-registration request every time it restarts. The Services Director will assess this request, but will not process it if the vTM is already registered, or there is a Pending self-registration request for the vTM.

    NOTE
    Once a self-registration request is received by the Services Director from a vTM, you must not change the cluster to which the vTM belongs until the registration request is accepted.

Requesting Self Registration on a Configured vTM

You can configure an established vTM to request self-registration.

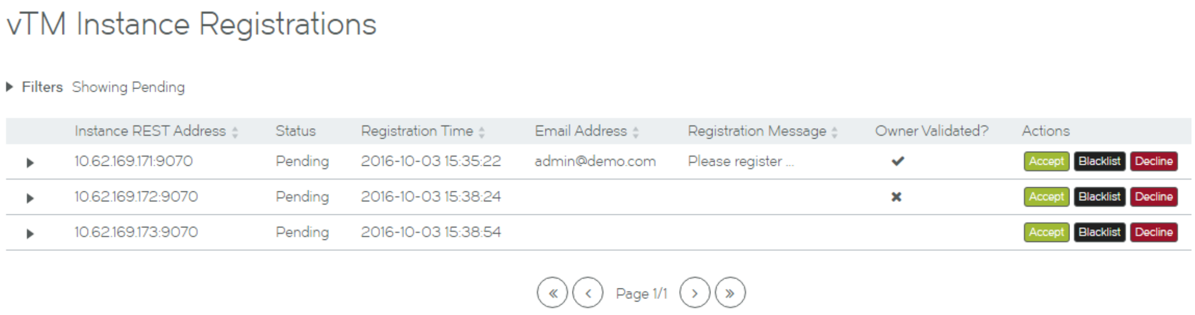
This process is performed entirely in the vTM user interface, under **System** > **Licenses** > **Services Director Registration**.

Refer to the Virtual Traffic Manager documentation for full details of the vTM VA software.

Viewing vTM Instance Registration Requests

The **vTM Instance Registrations** page lists all self-registration requests (both manual and automatic) that have been received by the Services Director from vTMs.

FIGURE 100 The vTM Instance Registration Page



vTM Instance Registrations

▸ Filters Showing Pending

	Instance REST Address	Status	Registration Time	Email Address	Registration Message	Owner Validated?	Actions
▸	10.62.169.171:9070	Pending	2016-10-03 15:35:22	admin@demo.com	Please register ...	✓	Accept Blacklist Decline
▸	10.62.169.172:9070	Pending	2016-10-03 15:38:24			✗	Accept Blacklist Decline
▸	10.62.169.173:9070	Pending	2016-10-03 15:38:54				Accept Blacklist Decline

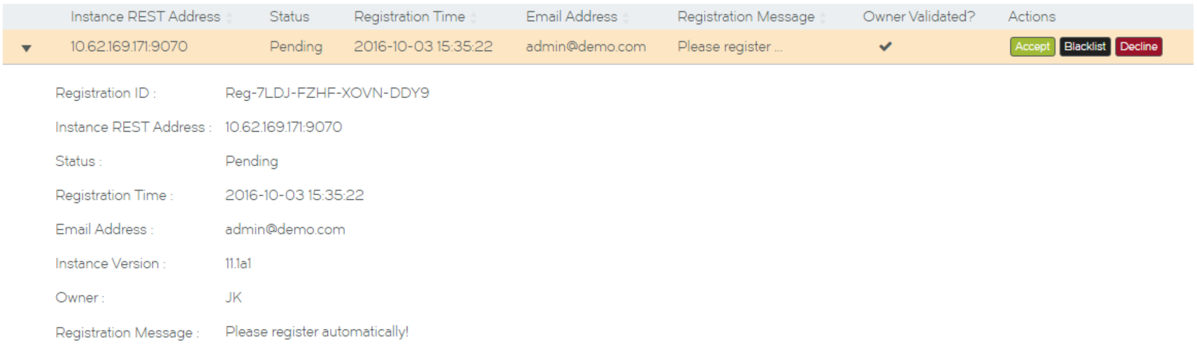
« ‹ Page 1/1 › »

Refer to Understanding vTM Registration Requests on page 117 for details of the headings.

You can **Accept**, **Blacklist** and **Decline** individual registrations from this list, refer to Processing Self-Registration Requests Manually on page 119.

Expand a registration request to view its full details. For example:

FIGURE 101 vTM Instance Registration: Detailed View



	Instance REST Address	Status	Registration Time	Email Address	Registration Message	Owner Validated?	Actions
▾	10.62.169.171:9070	Pending	2016-10-03 15:35:22	admin@demo.com	Please register ...	✓	Accept Blacklist Decline

Registration ID :	Reg-7LDJ-FZHF-XOVN-DDY9
Instance REST Address :	10.62.169.171:9070
Status :	Pending
Registration Time :	2016-10-03 15:35:22
Email Address :	admin@demo.com
Instance Version :	11.1a1
Owner :	JK
Registration Message :	Please register automatically!

This page also includes:

- A collapsed list of filters. These filters control which request state categories are displayed. Refer to Filtering Self-Registration Requests on page 118. Typically, you will view Pending requests only.

  NOTE
  To view all requests for automatic self-registration, ensure you set the filter to include Accepted registrations.

- Paging controls for when there are larger numbers of registration requests.

Understanding vTM Registration Requests

Each entry in the table of vTM registration requests shows properties for a single self-registration request. Both automatic and manual self-registration requests are included. To view successful automatic self-registration requests, ensure that you have Accepted requests included, refer to Filtering Self-Registration Requests on page 118.

Property	Description
Instance Rest Address	Instance Rest Address
Status	The current state of the self-registration request. This determines the **Actions** that are supported for the request. Refer to Understanding Registration Status on page 117.
Registration Time	The time at which the Services Director received the self-registration request.
Email Address	The e-mail address of the administrator who configured the self-registration request on the vTM.
Registration Message	A text field. Typically, this will provide information for the Administrator who will process the self-registration request.
Owner Validated?	Indicates whether owner information was received from the vTM, and whether it was valid: • A tick indicates that owner/password information was received from the vTM, and that these have been validated against the Services Director's known owners. • A cross indicates that owner/password information was received from the vTM, but that it failed validation. • A blank column indicates that no owner/password information was received from the vTM.
Actions	A list of state transition actions that are valid from the current state. Refer to Understanding Registration Status on page 117.

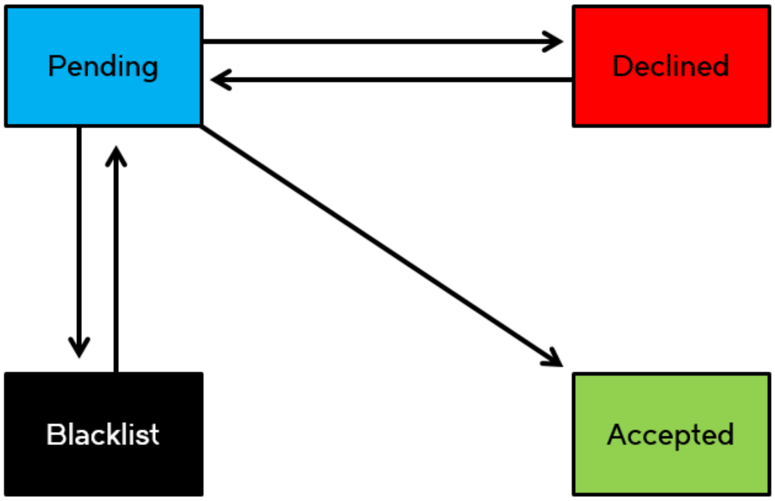
Understanding Registration Status

The status of each self-registration request is displayed in the **vTM Instance Registration** page. Refer to Viewing vTM Instance Registration Requests on page 116.

> NOTE
> Once self-registration is requested by the vTM to the Services Director, you must not change the cluster to which a vTM belongs until the registration request is accepted.

The lifecycle of a self-registration request is as follows:

FIGURE 102 State Model: Self-Registration Requests



When a self-registration request is received, it is given a Pending status.

For an automatic self-registration request, the auto-accept policy is then evaluated. Either:

- The evaluation of the auto-accept policy is successful. The request transitions automatically to Accepted, and the vTM is registered.
- The evaluation of the auto-accept policy is unsuccessful. The request retains its Pending status, and must then be resolved manually (see below).

For manual self-registration requests, you can transition it to:

- Accepted. You can manually transition a Pending request to Accepted, which completes the registration. Refer to Accepting a Pending Self-Registration Request on page 119.
- Declined. You can manually transition a Pending request to Declined if you do not wish to accept the request. Refer to Declining a Pending Self-Registration Request on page 121. You can transition a Declined request back to Pending if required.
- Blacklisted. You can manually transition a Pending request to Blacklisted if you do not wish to accept the request. Refer to Blacklisting a Pending Self-Registration Request on page 122. You can transition a Blacklisted request back to Pending if required.

  NOTE
  A Pending request will transition to Blacklisted automatically after a defined timeout period. This defaults to 24 hours. Refer to Updating Instance Registration Settings on page 61.

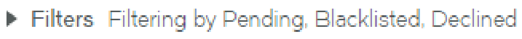
The displayed states are subject to a status filter. By default, only Pending requests are shown. Refer to Filtering Self-Registration Requests on page 118.

To view automatic self-registration requests, you will need the Accepted requests to be visible.

Filtering Self-Registration Requests

You can filter the self-registration requests that are included on the **vTM Instance Registration** page. By default, only Pending requests are shown. When the filters are collapsed, a summary of the filter settings is shown:

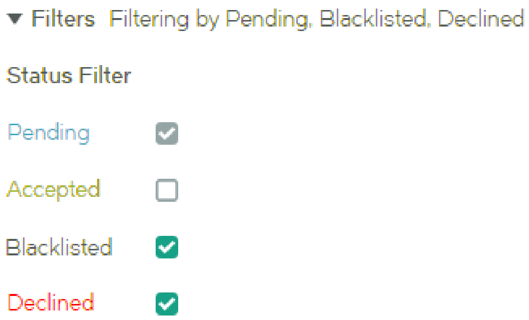
FIGURE 103 vTM Self Registration Filters: Collapsed



▶ Filters Filtering by Pending, Blacklisted, Declined

Click the arrow on the left side of the filters to expand the **Status Filter** list.

FIGURE 104 vTM Self Registration Filters: Expanded



▼ Filters Filtering by Pending, Blacklisted, Declined

Status Filter

Pending	☑
Accepted	□
Blacklisted	☑
Declined	☑

To view automatic self-registration requests that have been processed, the Accepted requests must be visible.

1. Click the **Catalogs** menu, and then click **Licensing: Instance Registrations**.
   The **vTM Instance Registration** page appears.
2. Click the left arrow next to Filters to expand the **Status Filter** list.
3. Under **Status Filter**, select the check box for each required self-registration state.
   Any state that is ticked is included in the table of self-registration requests.

Processing Self-Registration Requests Manually

All manual self-registrations and all failed automatic self-registrations are initially given a status of Pending. Each Pending request must be processed manually:

- Accepting a Pending Self-Registration Request on page 119.
- Declining a Pending Self-Registration Request on page 121.
- Blacklisting a Pending Self-Registration Request on page 122.
- Returning a Declined/Blacklisted Self-Registration Request to Pending on page 123.

Accepting a Pending Self-Registration Request

You can manually transition a Pending self-registration request to Accepted. You have the opportunity to review, change and confirm registration details before completing the process.

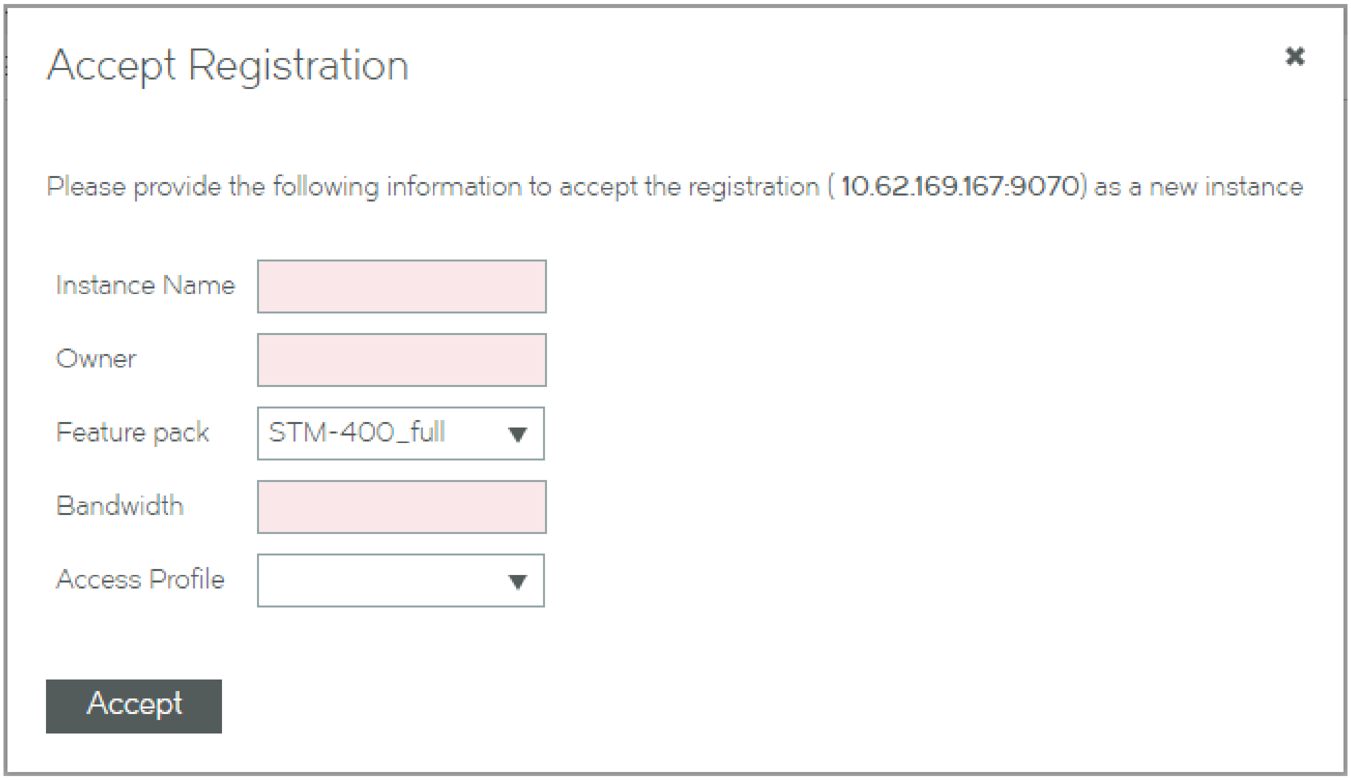
> NOTE
> Once a vTM is registered, you cannot change the Accepted state of self-registration request.

1. Access your Active Services Director VA user interface from a browser, using the Service Endpoint Address of your Services Director.
2. Log in as the admin user. The **Home** page appears.

3. Click the **Catalogs** menu, and then click **Licensing: Instance Registrations**.
   The **vTM Instance Registration** page appears.
4. Expand the filters, and ensure that Pending requests are included.
5. Locate the required Pending request.
6. Examine the information presented for the request, refer to Understanding vTM Registration Requests on page 117.
   If additional information is required, expand the entry to view all details for the request, refer to Viewing vTM Instance Registration Requests on page 116.
7. In the **Actions** column for the request, click **Accept**.

   The **Accept Registration** dialog box appears:

   FIGURE 105 Accepting a Pending Request



Accept Registration

Please provide the following information to accept the registration (10.62.169.167:9070) as a new instance

Instance Name

Owner

Feature pack: STM-400_full

Bandwidth

Access Profile

8. Enter an **Instance Name** for the vTM.

   This is a user-facing name for the vTM that will be used throughout the Services Director VA user interface. This tag can be changed at any time. It must be unique among non-deleted vTM instances registered on the Services Director, but can be reused as required.

   That is, if an instance is deleted, its tag can be reused for a different instance.
9. Enter an **Owner** for the vTM.
10. Select a **Feature Pack** for the vTM.
    This feature pack must be supported by your Services Director's License. If the required Feature Pack is not defined on your Services Director, refer to Adding a Feature Pack to the Services Director on page 70.

11. Enter a numeric **Bandwidth** (in Mbps) for the vTM.
    This bandwidth must be available within your Services Director's Bandwidth License.
12. (Optional) Select an **Access Profile**.
    This access profile identifies the authenticator and permission groups required for the user authentication on this vTM. Refer to Working with User Authentication on page 179.
13. Click **Accept**.

    The state of the request changes to Accepted. The authenticator and permission groups in the access profile are applied to the vTM. Existing authenticators and permission groups may be overwritten, but none will be deleted. All members of a cluster are affected.

    The vTM then appears as a registered vTM on the **vTM Instances page**.

Declining a Pending Self-Registration Request

You can manually transition a Pending self-registration request to Declined. You can provide a reason for this decision if required.

You can exclude Declined requests from the **vTM Instance Registration** page if required by changing the Status Filter. Refer to Filtering Self-Registration Requests on page 118.

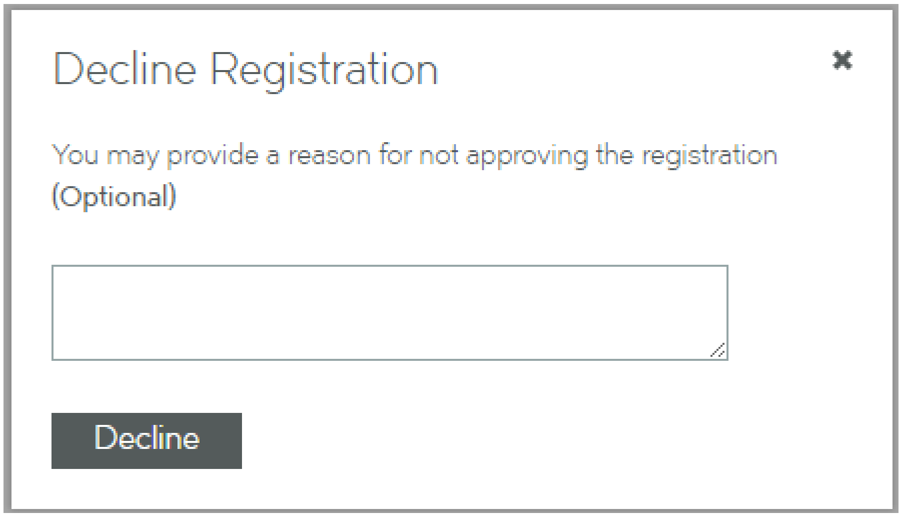
> NOTE
> You can transition a Declined self-registration request back to Pending. Refer to Returning a Declined/Blacklisted Self-Registration Request to Pending on page 123.

1. Active Services Director VA user interface from a browser, using the Service Endpoint Address of your Services Director.
2. Log in as the admin user. The **Home** page appears.
3. Click the **Catalogs** menu, and then click **Licensing: Instance Registrations**.
   The **vTM Instance Registration** page appears.
4. Expand the filters, and ensure that Pending requests are included.
5. Locate the required Pending request.
6. Examine the information presented for the request, refer to Understanding vTM Registration Requests on page 117.
   If additional information is required, expand the entry to view all details for the request, refer to Viewing vTM Instance Registration Requests on page 116.

7. In the **Actions** column for the request, click **Decline**.

   The **Decline Registration** dialog box appears.

   FIGURE 106 Declining a Pending Request



Decline Registration

You may provide a reason for not approving the registration (Optional)

8. (Optional) Enter your reasons for declining the request.
   This information will be accessible to the vTM's Administrator.
9. Click **Decline** to close the dialog box.
   The state of the request changes to Declined.

Blacklisting a Pending Self-Registration Request

You can manually transition a Pending self-registration request to Blacklisted.

You can exclude Blacklisted requests from the **vTM Instance Registration** page if required by changing the Status Filter, refer to Filtering Self-Registration Requests on page 118.

NOTE
A Pending request will transition to Blacklisted automatically after a defined timeout period. This defaults to 24 hours. Refer to Updating Instance Registration Settings on page 61.

NOTE
You can transition a Blacklisted self-registration request back to Pending. Refer to Returning a Declined/Blacklisted Self-Registration Request to Pending on page 123.

1. Active the Services Director VA user interface from a browser, using the Service Endpoint Address of your Services Director.
2. Log in as the admin user.
   The **Home** page appears.
3. Click the **Catalogs** menu, and then click **Licensing: Instance Registrations**.
   The **vTM Instance Registration** page appears.
4. Expand the filters, and ensure that Pending requests are included.
5. Locate the required Pending request.

6. Examine the information presented for the request, refer to Understanding vTM Registration Requests on page 117.
   If additional information is required, expand the entry to view all details for the request, refer to Viewing vTM Instance Registration Requests on page 116.
7. In the **Actions** column for the request, click **Blacklist**.
   The state of the request changes to Blacklisted.

Returning a Declined/Blacklisted Self-Registration Request to Pending

You can transition a Declined/Blacklisted self-registration request back to Pending. For example, you can choose to do this after an issue with a Declined request is resolved, or when a request that was Blacklisted automatically (refer to Updating Instance Registration Settings on page 61) still needs to be processed.

1. Active the Services Director VA user interface from a browser, using the Service Endpoint Address of your Services Director.
2. Log in as the admin user.
   The **Home** page appears.
3. Click the **Catalogs** menu, and then click **Licensing: Instance Registrations**.
   The **vTM Instance Registration** page appears.
4. Expand the filters, and ensure that Declined/Blacklisted requests are included.
5. Locate the required request.
6. In the **Actions** column for the request, click **Set to Pending**.
   The state of the request changes to Pending.

Requesting Re-Registration of a vTM

After you have successfully self-registered a vTM, you may need to re-register it. For example, if the authorisation credentials on the vTM change.

This process is performed entirely in the vTM user interface, under **System** > **Licenses** > **Services Director Registration**.

To force re-registration, update the registration details as required. Then, enable the **Force Re-Registration** check box and click **Save and Register**.

Refer to the Virtual Traffic Manager documentation for full details of the vTM VA software.

Self-Registering a Cloud-Based Traffic Manager

The Services Director VA supports the automatic self-registration of cloud-based Virtual Traffic Manager (vTM) instances. This adds cloud-based vTMs to the estate of the Services Director, from where it can be licensed, monitored and metered.

This section describes the principles of automatic self-registration for cloud-based vTMs.

> NOTE
> Self-registration of cloud-based vTMs is not supported where the Services Director is in a private network behind a NAT.

Overview: vTM Self-Registration (Cloud)

After you have completed the initial configuration of theServices Director, you can begin to add externally-deployed Virtual Traffic Managers (vTMs) to the estate of the Services Director.

One method for achieving this is by automatic self-registration a cloud-based vTM.

> **NOTE**
> Currently, cloud-based vTMs are supported on the Amazon Web Services (AWS) EC2 platform.

> **NOTE**
> Self-registration of cloud-based vTMs is not supported where the Services Director is in a private network behind a NAT.

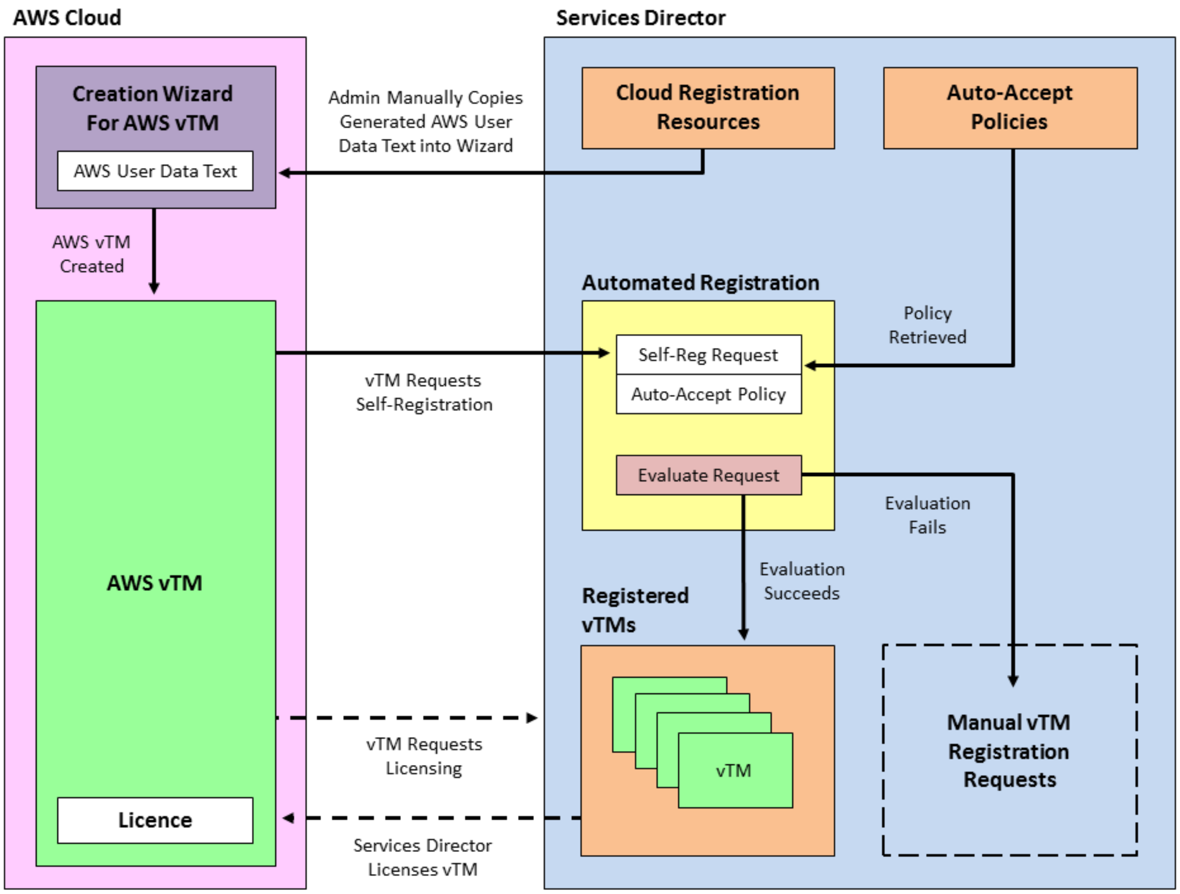
Cloud-based automatic registration begins on the Services Director, where a Cloud Registration resource must be created for one or more required deployments, refer to Adding a Cloud Registration Resource to the Services Director on page 87. This resource identifies a number of properties that will be used by a cloud-based vTM, such as its Owner and the Self-Registration Policy that the Services Director will use to evaluate it.

Once a Cloud Registration resource has been created, a block of automatically-generated text becomes available on the Services Director. This text encapsulates the user data required by the AWS system to create the first cloud-based vTM in a cluster, and this vTM can automatically self-register on the Services Director. To do this, the administrator first manually copies this text into the AWS vTM creation wizard. Then, after the administrator specifies all other required network-specific details, the cloud-based AWS vTM is created. This process is described in Creating the First vTM in a Cluster on page 126.

Self-registration of a cloud-based vTMs is intended to be automatic. The vTM makes a self-registration request to the Services Director. When the self-registration request is received, the Services Director evaluates the request against the specified self-registration policy, and will either accept or reject the vTM automatically.

When accepted, the vTM is added to the list of vTMs known to the Services Director. When rejected (for example, when there is insufficient bandwidth remaining, or the self-generated text does not include both an Owner and a Self-Registration Policy), the vTM is added to the queue of manual self-registration requests instead, and the Administrator can process manually, refer to Processing Self-Registration Requests Manually on page 119.

FIGURE 107 Automatic Self-Registration of a Cloud-Based vTM



Refer to Creating a Cloud-Based Traffic Manager on page 126 for a full description of this process.

If you want to create additional cloud-based vTMs in the same cluster, you replace the user data text block for the Cloud Registration resource with the user data text block from the vTM's cluster, refer to Creating the Second vTM in a Cluster on page 127.

Once a self-registered vTM is known to the Services Director, the Services Director will respond to valid licensing requests by licensing the vTM, in the same way as for any other registered vTM.

NOTE
Once a vTM is configured for self-registration, it will make a self-registration request every time it restarts. The Services Director will assess this request, but will not process it if the vTM is already registered, blacklisted, or there is a pending self-registration request for the vTM.

NOTE
Once a self-registration request is received by the Services Director from a vTM, you must not change the cluster to which the vTM belongs until the registration request is accepted.

NOTE
A detailed description of the creation of an AWS cloud-based vTM can be found in the Virtual Traffic Manager documentation, refer to *Brocade Virtual Traffic Manager Cloud Services Installation and Getting Started Guide*.

Creating a Cloud-Based Traffic Manager

You create one or more cloud-based Virtual Traffic Manager (vTM) instances from the Amazon Web Services (AWS) system. To do this, you use a block of user data text that is created automatically by the Services Director, refer to Overview: vTM Self-Registration (Cloud) on page 123 for details.

You must create each cloud-based instance individually. There are separate processes for:

- Creating the first cloud-based vTM in a cluster, refer to Creating the First vTM in a Cluster on page 126.
- Creating the second cloud-based vTM in a cluster, refer to Creating the Second vTM in a Cluster on page 127.
- All subsequent cloud-based vTMs in a cluster, refer to Creating Subsequent vTMs in a Cluster on page 128.

Creating the First vTM in a Cluster

The creation of a cloud-based vTM that is the first in a cluster is described below as a high-level process. Specific implementation choices will depend on your network configuration.

> NOTE
> Before you perform this process, you must:
>
> - Create the required Cloud Registration resource, refer to Adding a Cloud Registration Resource to the Services Director on page 87.
> - Have the user data text block for this resource in your clipboard, refer to Viewing User Data Text for a Cloud Registration Resource on page 90.

1. On the Services Director, access the required Cloud Registration resource, and copy its user data text block to the clipboard. Refer to Viewing User Data Text for a Cloud Registration Resource on page 90.
2. Access the Amazon Web Services (AWS) system and log in using your AWS credentials.
3. Access the EC2 dashboard.
4. Launch the process to create a new instance.
   This starts a wizard that will lead you through the creation process.
5. On page 1 of the wizard (Choose AMI), locate and select the Amazon Machine Image (AMI) for the vTM from the AWS Marketplace.
6. On page 2 of the wizard (Choose Instance Type), select the required instance type.
7. On page 3 of the wizard (Configure Instance):
   - Ensure the number of instances is 1. You can add more cloud-based instances to the cluster later, refer to Creating the Second vTM in a Cluster on page 127.
   - Select your network and subnetwork.
   - You can choose to automatically assign a public IP for the new instance if required. By default, a public IP address is not assigned to a new instance. Your need to do this will depend on your specific networking configuration.
   - Expand the advanced details, and paste in the AWS user data from your Cloud Registration resource.
   - If your user data is plain text, add any incomplete properties, such as owner or auto-accept policy. If these are not specified, automatic self-registration will be unable to complete.

     > NOTE
     > If you do not intend to complete the owner or auto-accept policy properties, you must remove the incomplete entries from the pasted user data text block before continuing.

   - Configure all other settings to your requirement.

8. On page 4 of the wizard (Add Storage), configure settings to match your network and requirement.
9. On page 5 of the wizard (Tag Instance), enter a name for your instance.
10. On page 6 of the wizard (Configure Security Group), either create a new security group, or select an existing one.
11. On page 7 of the wizard (Review):
    - Review your choices and confirm. This effectively closes the wizard, but further configuration information is required.
    - Create a new key pair. This key pair is used for this instance and all others that join its cluster.
    - Download the key pair and save it in a safe location for future reference and use.
    - Launch the instance.

    The wizard closes and you are informed that the instance is being created.

    Once the instance is created, it appears on the list of instances that is accessible from the EC2 dashboard.

    When the Services Director receives the auto-registration request from the new cloud-based vTM, it will process the request:

    - If automatic self-registration succeeds, the vTM will appear on the **vTM Instances** page, refer to Viewing Traffic Managers on page 131. The vTM uses a new Discovered cluster. The name of the vTM is the private IP assigned by AWS to the vTM.
    - If automatic self-registration is unable to complete (for example, because of a missing owner or auto-accept policy), the registration request will appear as a Pending self-registration request on the **Instance Registrations** page. From there, you can manually process the request, refer to Processing Self-Registration Requests Manually on page 119. Once you have accepted this self-registration request, you can create a second cloud-based vTM to the cluster, refer to Creating the Second vTM in a Cluster on page 127.

Creating the Second vTM in a Cluster

The creation of a cloud-based vTM that is the second in a cluster is described below as a high-level process. Specific implementation choices will depend on your network configuration.

NOTE
Before you perform this process, you must create the first vTM in a cluster (refer to Creating the First vTM in a Cluster on page 126), and then access the user data text block from its vTM Cluster resource. This user data text block replaces the one that was used to create the first cloud-based vTM.

1. On the Services Director, access the vTM Cluster for the first vTM instance in the cluster, and copy its cluster text block to the clipboard. Refer to Understanding Traffic Manager Cluster Details on page 150.
2. Access the Amazon Web Services (AWS) system and log in using your AWS credentials.
3. Access the EC2 dashboard.
4. Launch the process to create a new instance.
   This starts a wizard that will lead you through the creation process.
5. On page 1 of the wizard (Choose AMI), locate and select the Amazon Machine Image (AMI) for the vTM from the AWS Marketplace.
6. On page 2 of the wizard (Choose Instance Type), select the required instance type.

7. On page 3 of the wizard (Configure Instance):
   - Ensure the number of instances is 1. You can add more cloud-based instances to the cluster later, refer to Creating Subsequent vTMs in a Cluster on page 128.
   - Select your network and subnetwork.
   - You can choose to automatically assign a public IP for the new instance if required. By default, a public IP address is not assigned to a new instance. Your need to do this will depend on your specific networking configuration.
   - Expand the advanced details, and paste in the AWS user data from your vTM cluster.
   - Configure all other settings to your requirement.
8. On page 4 of the wizard (Add Storage), configure settings to match your network and requirement.
9. On page 5 of the wizard (Tag Instance), enter a name for your instance.
10. On page 6 of the wizard (Configure Security Group), select the existing security group that you used for the first instance in the cluster.
11. On page 7 of the wizard (Review):
    - Review your choices and confirm. This effectively closes the wizard, but further configuration information is required.
    - Select the key pair that you created for the first vTM in the cluster. This key pair is used for all instances in the cluster.
    - Launch the instance.

    The wizard closes and you are informed that the instance is being created.

    Once the instance is created, it appears on the list of instances that is accessible from the EC2 dashboard.

    When the Services Director receives the auto-registration request from the new cloud-based vTM, it will process the request:
    - If successful, the vTM will appear on the **vTM Instances** page, refer to Viewing Traffic Managers on page 131. This vTM shares its Discovered cluster with the first vTM in the cluster. The name of the vTM is the private IP assigned by AWS to the vTM.
    - If unsuccessful, the registration request will appear as a Pending self-registration request on the **Instance Registrations** page. From there, you can manually process the request, refer to Processing Self-Registration Requests Manually on page 119. Once you have accepted this self-registration request, you can create additional cloud-based vTMs in the cluster, refer to Creating Subsequent vTMs in a Cluster on page 128,

Creating Subsequent vTMs in a Cluster

Once you have created the first and second cloud-based vTMs in a cluster, creating additional vTMs in the cluster can be performed by duplicating the second vTM from the EC2 dashboard.

> NOTE
> You do not need to access and copy any user data text blocks during this process.

The creation of additional cloud-based vTMs in a cluster is described below as a high-level process. Specific implementation choices will depend on your network configuration.

1. Access the Amazon Web Services (AWS) system and log in using your AWS credentials.
2. Access the EC2 dashboard and view your instances.
3. Select the second instance in the cluster and issue a new action to create another instance like the one selected.
   The instance creation wizard starts, and you are taken to page 7.

4. On page 7 of the wizard (Review):

   - Edit the tag for the new instance, so that it is unique. By default, it uses the same tag name as the duplicated instance.
   - Review your choices and confirm. This effectively closes the wizard, but further configuration information is required.
   - Select the key pair that you created for the first vTM in the cluster. This key pair is used for all instances in the cluster.
   - Launch the instance.

   The wizard closes and you are informed that the instance is being created.

   Once the instance is created, it appears on the list of instances that is accessible from the EC2 dashboard.

   When the Services Director receives the auto-registration request from the new cloud-based vTM, it will process the request:

   - If successful, the vTM will appear on the **vTM Instances** page, refer to Viewing Traffic Managers on page 131. This vTM shares its Discovered cluster with the first vTM in the cluster. The name of the vTM is the private IP assigned by AWS to the vTM.
   - If unsuccessful, the registration request will appear as a Pending self-registration request on the **Instance Registrations** page. From there, you can manually process the request, refer to Processing Self-Registration Requests Manually on page 119.

Working with Traffic Managers

Overview: Working with Traffic Managers

Once you have installed your Brocade Virtual Traffic Managers, you manage them from the **vTM Instances** page of the Services Director VA. From this page, you can:

- View the basic status details for each Traffic Manager, including:
  - The lifecycle state of each Traffic Manager.
  - The instance health of each Traffic Manager.
  - The licensing health for each Traffic Manager.
- Show full details for each Traffic Manager.
- Change the order in which Traffic Managers are displayed.
- Update the details for each Traffic Manager.
- Delete a Traffic Manager.
- Filter Traffic Managers based on lifecycle state, instance health and licensing health.
- Change the lifecycle status for Traffic Managers deployed from the Services Director.

NOTE
To register an externally-deployed Traffic Manager, refer to Adding Traffic Managers to the Services Director on page 67.

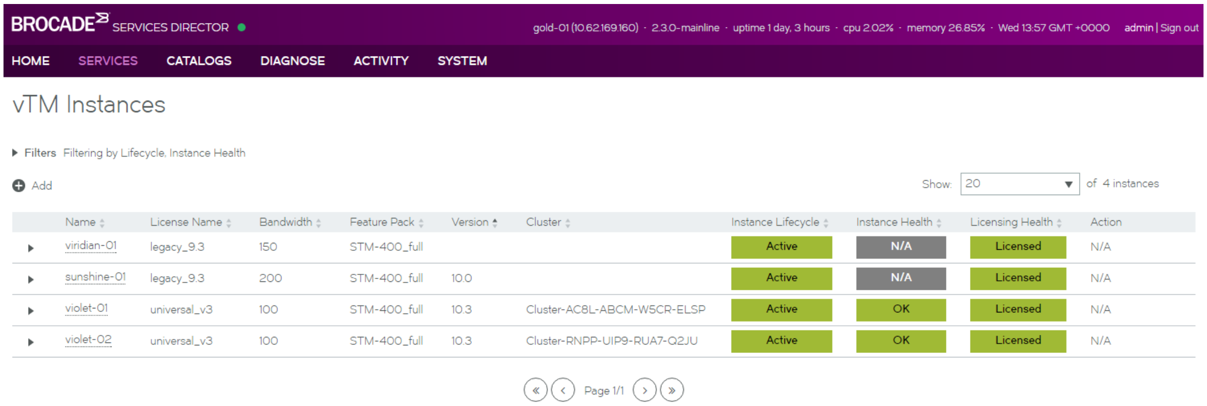
NOTE
The operation of Traffic Management and Load Balancing on individual Traffic Managers is not addressed by the Services Director product. This requires use of the Brocade Virtual Traffic Manager software for each Traffic Manager.

Viewing Traffic Managers

The **vTM Instances** page shows a table of all Traffic Manager instances known by the Services Director. This page also includes:

- A collapsed list of filters. These filters control which categories of Traffic Manager instances are displayed. Refer to Filtering Traffic Managers on page 137.
- A count of instances.
- Paging controls for when there are larger numbers of Traffic Manager instances.

FIGURE 108 The vTM Instances Page


BROCADE SERVICES DIRECTOR
gold-01 (10.62.169.160) · 2.3.0-mainline · uptime 1 day, 3 hours · cpu 2.02% · memory 26.85% · Wed 13:57 GMT +0000
admin | Sign out
HOME
SERVICES
CATALOGS
DIAGNOSE
ACTIVITY
SYSTEM
Add
Page 1/1

vTM Instances

Filters Filtering by Lifecycle, Instance Health

Show: 20 of 4 instances

Name	License Name	Bandwidth	Feature Pack	Version	Cluster	Instance Lifecycle	Instance Health	Licensing Health	Action
viridian-01	legacy_9.3	150	STM-400_full			Active	N/A	Licensed	N/A
sunshine-01	legacy_9.3	200	STM-400_full	10.0		Active	N/A	Licensed	N/A
violet-01	universal_v3	100	STM-400_full	10.3	Cluster-AC8L-ABCM-W5CR-ELSP	Active	OK	Licensed	N/A
violet-02	universal_v3	100	STM-400_full	10.3	Cluster-RNPP-UIP9-RUA7-Q2JU	Active	OK	Licensed	N/A

Understanding Basic Details of a Traffic Manager

Each entry in the table of Traffic Manager instances shows basic details for the Traffic Manager.

Name	Description
Name	The chosen name for the Traffic Manager. Names can be edited, and reused after a Traffic Manager is deleted if required.
License Name	The name of the FLA License for the Traffic Manager. This will either be a Universal FLA or a Legacy FLA, depending on the Traffic Manager settings.
Bandwidth	The maximum permitted bandwidth for this Traffic Manager (in Mbps).
Feature Pack	The chosen Feature Pack for the Traffic Manager.
Version	The software version for the Traffic Manager. Where the Traffic Manager's REST API is unavailable, this is blank.
Cluster	The current cluster for the Traffic Manager. This is supported when: The Traffic Manager is deployed by the Services Director. The Traffic Manager is at version 10.2 or later with a REST API enabled.
Instance Lifecycle	A colored indicator (green, blue, orange, red, black) and description of the Traffic Manager's lifecycle status. Refer to Understanding Lifecycle Status (Externally-Deployed Traffic Managers) on page 133.
Instance Health	A colored indicator (green, blue, orange, red, black) and description of the Traffic Manager's current health status, which reflects the health of the cluster to which it belongs. Refer to Understanding the Instance Health of a Traffic Manager on page 134.
License Health	A colored indicator (green, blue, orange, red, black) and description of the Traffic Manager's current licensing health status. Refer to Understanding the Instance Health of a Traffic Manager on page 134.
Action	*Actions are only available for* Traffic Manager *'s deployed by the* Services Director . • When a Traffic Manager is Active, a **Stop** button is displayed. This enables you to stop the Traffic Manager, changing its status to Idle. A status of Stopping is displayed during this process.

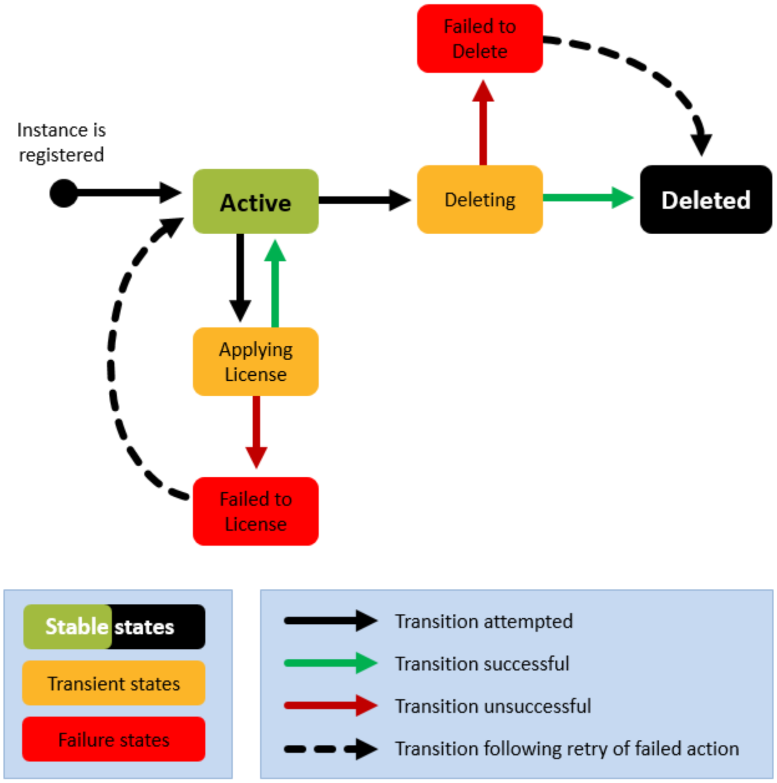
Name	Description
	- When a Traffic Manager is Idle, a **Start** button is displayed. This enables you to start the Traffic Manager, changing its status to Active. A status of Starting is displayed during this process.

Understanding Lifecycle Status (Externally-Deployed Traffic Managers)

The **Instance Lifecycle** state of each Traffic Manager is displayed in the **vTM Instances** page.

When you register an externally-deployed Traffic Manager, the lifecycle operations supported by the Services Director VA are as follows:

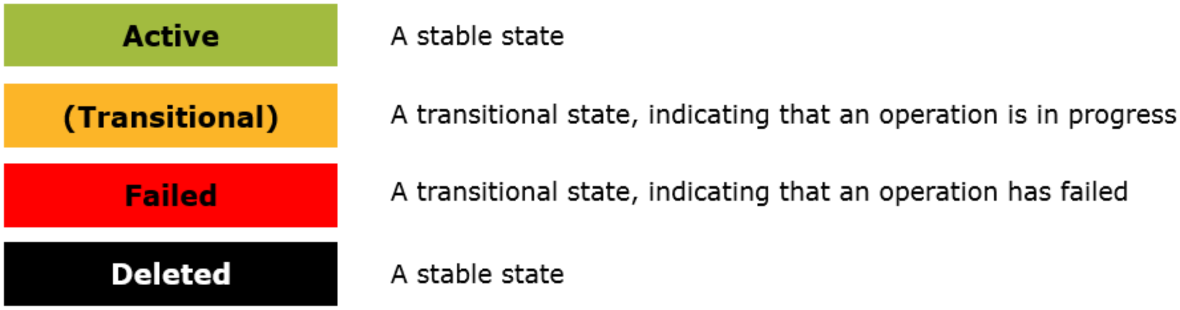
FIGURE 109 Lifecycle States: Externally-Deployed Traffic Managers



For most externally-deployed Traffic Managers, the **Instance Lifecycle** state will remain Active until the Traffic Manager is deleted.

NOTE
The **Lifecycle Status** column for an externally-deployed Traffic Manager does *not* display a live monitoring status. As a result, if a Traffic Manager fails independently, this will not be indicated.

FIGURE 110 Lifecycle Status Column: Externally-Deployed Traffic Managers



Active	A stable state
(Transitional)	A transitional state, indicating that an operation is in progress
Failed	A transitional state, indicating that an operation has failed
Deleted	A stable state

Note that:

- Where additional information is available, a red triangle is displayed next to the text of the status. Pause over this with your pointer to read the additional information in a dialog box.
- The displayed states are subject to the **Instance Status** filter. Refer to Filtering Traffic Managers on page 137.

You can affect the **Lifecycle Status** of an externally-deployed Traffic Manager as follows:

- By deleting a Traffic Manager from its entry in the Traffic Manager table. Refer to Deleting a Traffic Manager on page 140.
- Other states are visible during relicensing.

Understanding Lifecycle Status (Deployed Traffic Managers)

The **Instance Lifecycle** state of each Traffic Manager is displayed in the **vTM Instances** page.

When you deploy a Traffic Manager from the Services Director VA, it is deployed into a *container* on an instance host. This container enables full control of lifecycle operations for the Traffic Manager.

Refer to the *Brocade Services Director Advanced User Guide* for full details.

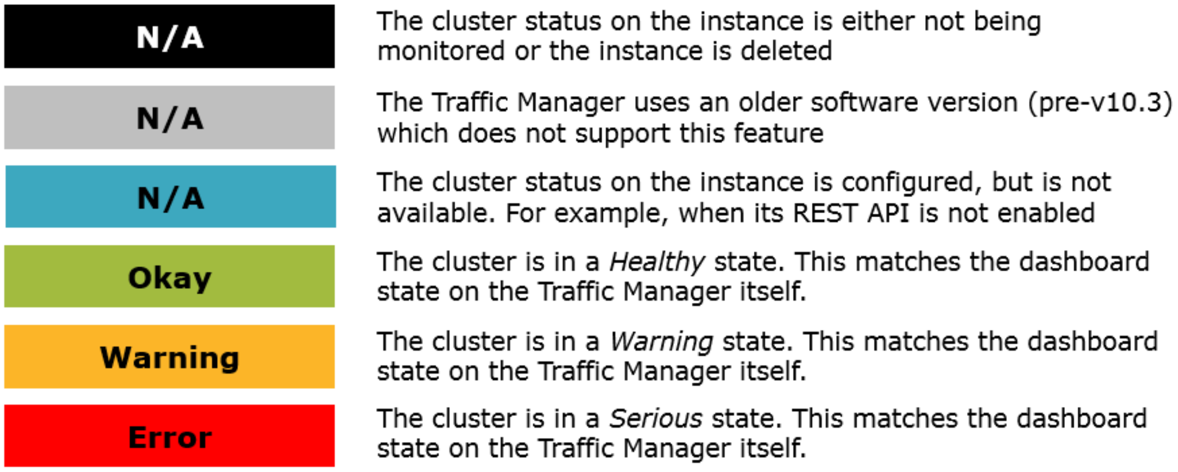
Understanding the Instance Health of a Traffic Manager

The **Instance Health** of each Traffic Manager is displayed in the **vTM Instances** page.

The displayed **Instance Health** of a Traffic Manager is a summary status that reflects the health of the *cluster* to which the Traffic Manager belongs. As a result, where cluster health is an issue, all Traffic Managers in a cluster will typically display the same status.

Instance Health is reported as follows:

FIGURE 111 Instance Health Column



N/A	The cluster status on the instance is either not being monitored or the instance is deleted
N/A	The Traffic Manager uses an older software version (pre-v10.3) which does not support this feature
N/A	The cluster status on the instance is configured, but is not available. For example, when its REST API is not enabled
Okay	The cluster is in a *Healthy* state. This matches the dashboard state on the Traffic Manager itself.
Warning	The cluster is in a *Warning* state. This matches the dashboard state on the Traffic Manager itself.
Error	The cluster is in a *Serious* state. This matches the dashboard state on the Traffic Manager itself.

Note that:

- Instance health checks are only performed for Traffic Managers at version 10.3 or later with an active REST API. For all other cases, the **Instance Health** is reported as N/A.
- Where additional information is available, a red triangle is displayed next to the text of the status. Pause over this with your pointer to read the additional information in a dialog box.
- The displayed states are subject to the **Instance Health** filter, refer to Filtering Traffic Managers on page 137.

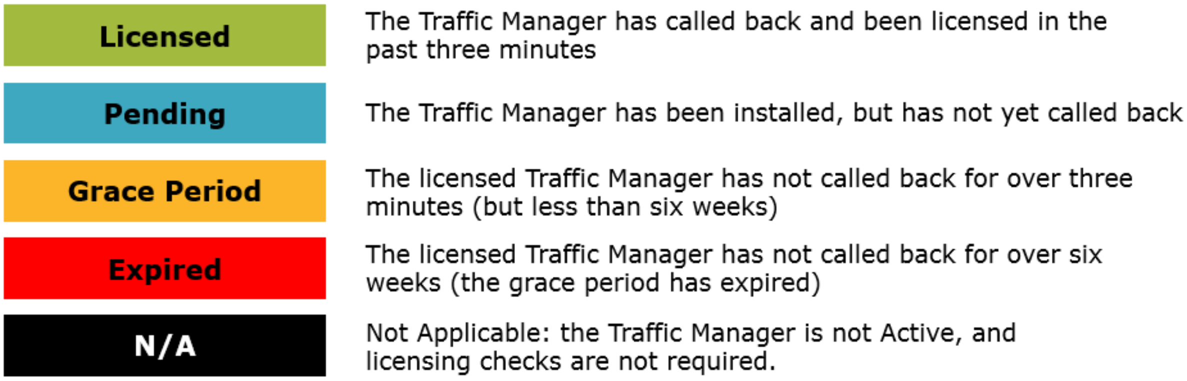
Understanding the Licensing Health of a Traffic Manager

The **Licensing Health** of each Traffic Manager is displayed in the **vTM Instances** page.

The displayed **Licensing Health** of a Traffic Manager is a summary status, based on a number of licensing checks. Licensing is requested every three minutes using a callback mechanism. The method varies, depending on whether a Universal FLA or Legacy FLA License is in use on a Traffic Manager.

Licensing Health is reported as follows:

FIGURE 112 Licensing Health Column



Licensed	The Traffic Manager has called back and been licensed in the past three minutes
Pending	The Traffic Manager has been installed, but has not yet called back
Grace Period	The licensed Traffic Manager has not called back for over three minutes (but less than six weeks)
Expired	The licensed Traffic Manager has not called back for over six weeks (the grace period has expired)
N/A	Not Applicable: the Traffic Manager is not Active, and licensing checks are not required.

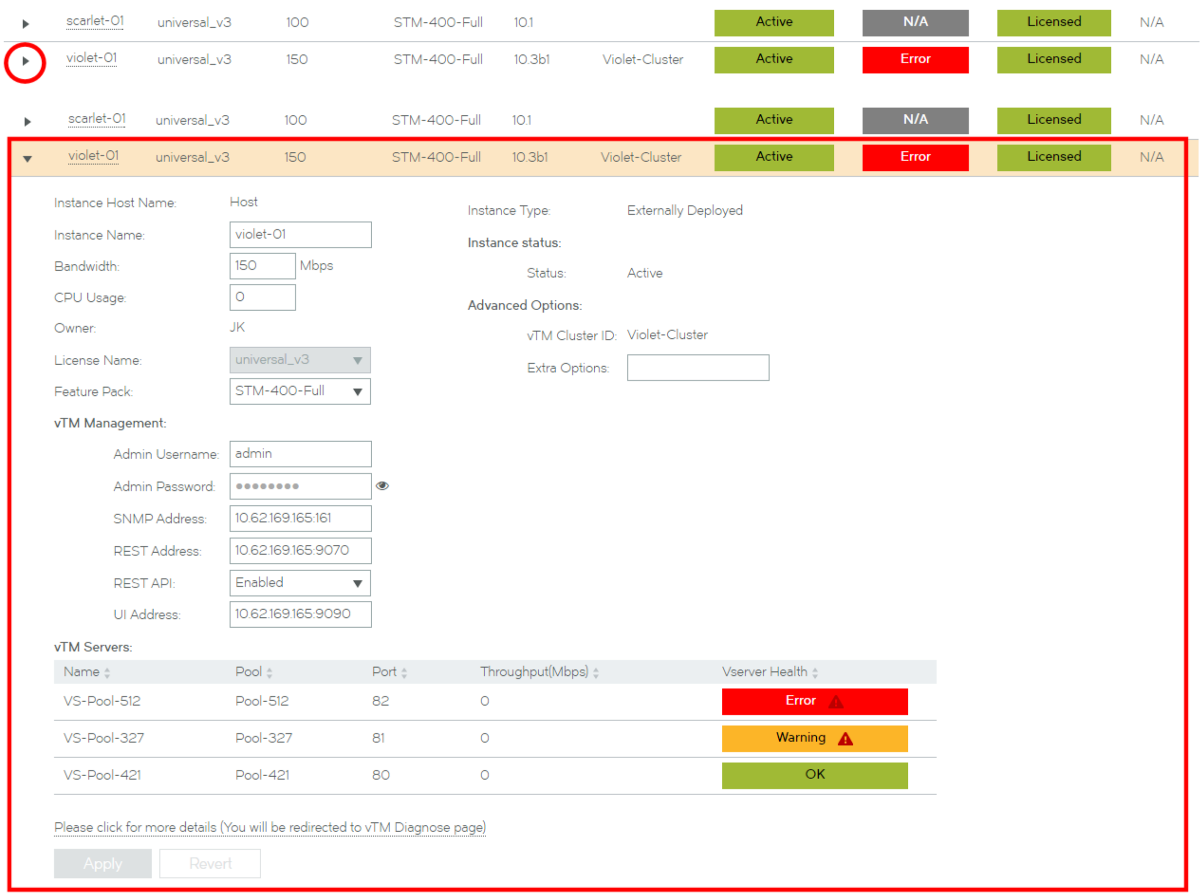
Note that:

- License checks are only performed for Traffic Managers with an Active **Lifecycle Status**. For all other lifecycle states, the **Licensing Health** is reported as N/A.
- Where additional information is available, a red triangle is displayed next to the text of the status. Pause over this with your pointer to read the additional information in a dialog box.
- The displayed states are subject to the **Licensing Health** filter, refer to Filtering Traffic Managers on page 137.

Viewing Full Details for a Traffic Manager

The **vTM Instances** page shows a table of basic details for all Traffic Manager instances. To view full details for a Traffic Manager, click the arrow on the left side of the Traffic Manager's entry.

FIGURE 113 Viewing Full Details for a Traffic Manager Instance



▸	scarlet-01	universal_v3	100	STM-400-Full	10.1		Active	N/A	Licensed	N/A
▸	violet-01	universal_v3	150	STM-400-Full	10.3b1	Violet-Cluster	Active	Error	Licensed	N/A

▸	scarlet-01	universal_v3	100	STM-400-Full	10.1		Active	N/A	Licensed	N/A
▾	violet-01	universal_v3	150	STM-400-Full	10.3b1	Violet-Cluster	Active	Error	Licensed	N/A

Instance Host Name: Host

Instance Name: violet-01

Bandwidth: 150 Mbps

CPU Usage: 0

Owner: JK

License Name: universal_v3

Feature Pack: STM-400-Full

vTM Management:

Admin Username: admin

Admin Password: ••••••••

SNMP Address: 10.62.169.165:161

REST Address: 10.62.169.165:9070

REST API: Enabled

UI Address: 10.62.169.165:9090

Instance Type: Externally Deployed

Instance status:

Status: Active

Advanced Options:

vTM Cluster ID: Violet-Cluster

Extra Options:

vTM Servers:

Name	Pool	Port	Throughput(Mbps)	Vserver Health
VS-Pool-512	Pool-512	82	0	Error ⚠
VS-Pool-327	Pool-327	81	0	Warning ⚠
VS-Pool-421	Pool-421	80	0	OK

Please click for more details (You will be redirected to vTM Diagnose page)

NOTE

The administration password for the Traffic Manager is not displayed by default. To reveal the administration password, click the eye icon next to the **Password** field.

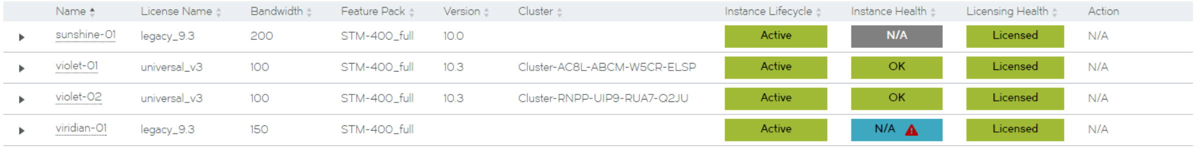
This view shows full details for the Traffic Manager, and includes a list of vServers with a status for each. Refer to Understanding vServer Status on page 139.

Changing the Display Order of Traffic Managers

The **vTM Instances** page shows a table of all Traffic Managers known by the Services Director.

The table of Traffic Managers can be sorted according to any of the basic details, including **Lifecycle Status** and **Licensing Health** (refer to Understanding Basic Details of a Traffic Manager on page 132). For example, the table is sorted by default by ascending **Name**.

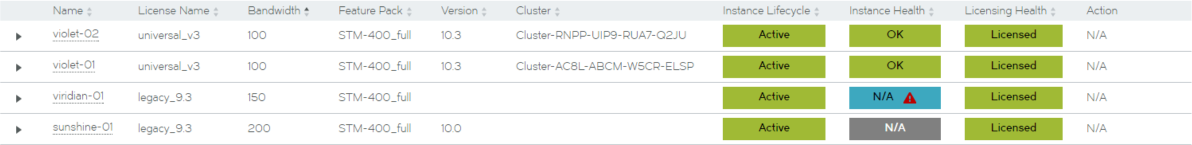
FIGURE 114 vTM Table Sorted By Ascending Name



	Name	License Name	Bandwidth	Feature Pack	Version	Cluster	Instance Lifecycle	Instance Health	Licensing Health	Action
▸	sunshine-01	legacy_9.3	200	STM-400_full	10.0		Active	N/A	Licensed	N/A
▸	violet-01	universal_v3	100	STM-400_full	10.3	Cluster-AC8L-ABCM-W5CR-ELSP	Active	OK	Licensed	N/A
▸	violet-02	universal_v3	100	STM-400_full	10.3	Cluster-RNPP-UIP9-RUA7-Q2JU	Active	OK	Licensed	N/A
▸	viridian-01	legacy_9.3	150	STM-400_full			Active	N/A ⚠	Licensed	N/A

To sort the table based on *ascending* values of any of the basic details, click the relevant column heading. For example, after clicking the **Bandwidth** heading, the same table is now sorted according to ascending **Bandwidth**.

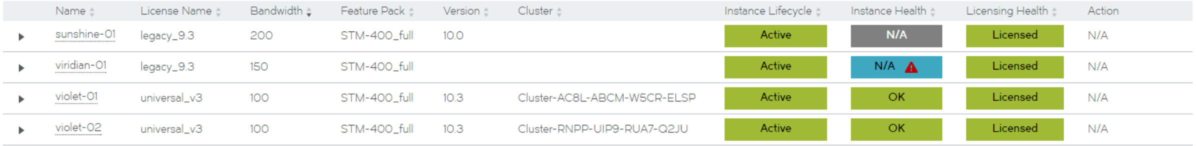
FIGURE 115 vTM Table Sorted By Ascending Bandwidth



	Name	License Name	Bandwidth	Feature Pack	Version	Cluster	Instance Lifecycle	Instance Health	Licensing Health	Action
▸	violet-02	universal_v3	100	STM-400_full	10.3	Cluster-RNPP-UIP9-RUA7-Q2JU	Active	OK	Licensed	N/A
▸	violet-01	universal_v3	100	STM-400_full	10.3	Cluster-AC8L-ABCM-W5CR-ELSP	Active	OK	Licensed	N/A
▸	viridian-01	legacy_9.3	150	STM-400_full			Active	N/A ⚠	Licensed	N/A
▸	sunshine-01	legacy_9.3	200	STM-400_full	10.0		Active	N/A	Licensed	N/A

Clicking the column heading again will sort the table according to a *descending* view of the same basic detail. For example, after clicking the **Bandwidth** heading again, the same table is now sorted according to a descending value of **Bandwidth**.

FIGURE 116 vTM Table Sorted By Descending Bandwidth



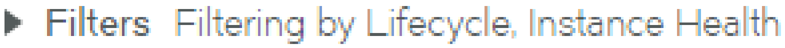
	Name	License Name	Bandwidth	Feature Pack	Version	Cluster	Instance Lifecycle	Instance Health	Licensing Health	Action
▸	sunshine-01	legacy_9.3	200	STM-400_full	10.0		Active	N/A	Licensed	N/A
▸	viridian-01	legacy_9.3	150	STM-400_full			Active	N/A ⚠	Licensed	N/A
▸	violet-01	universal_v3	100	STM-400_full	10.3	Cluster-AC8L-ABCM-W5CR-ELSP	Active	OK	Licensed	N/A
▸	violet-02	universal_v3	100	STM-400_full	10.3	Cluster-RNPP-UIP9-RUA7-Q2JU	Active	OK	Licensed	N/A

Filtering Traffic Managers

You can filter the Traffic Manager instances that are included on the **vTM Instances** page.

By default, the filters are collapsed, and a summary of filters is shown:

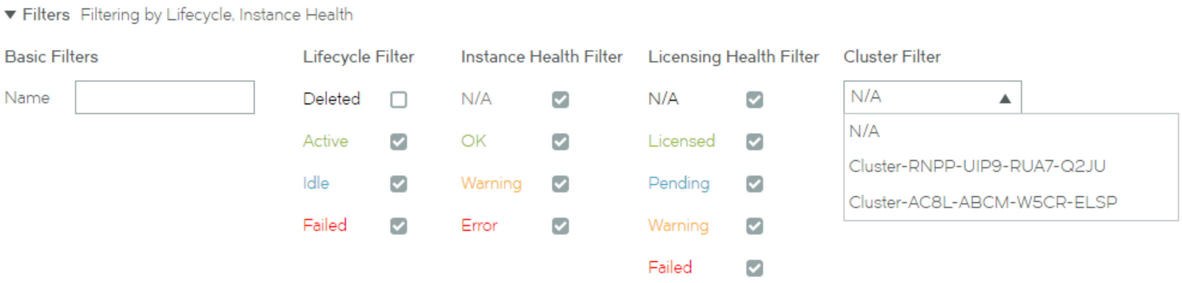
FIGURE 117 vTM Instance Filters: Collapsed



▸ Filters Filtering by Lifecycle, Instance Health

You can expand this to show the filters list.

FIGURE 118 vTM Instance Filters: Expanded



▼ Filters Filtering by Lifecycle, Instance Health

Basic Filters
Name

Lifecycle Filter
Deleted □
Active ☑
Idle ☑
Failed ☑

Instance Health Filter
N/A ☑
OK ☑
Warning ☑
Error ☑

Licensing Health Filter
N/A ☑
Licensed ☑
Pending ☑
Warning ☑
Failed ☑

Cluster Filter
N/A ▲
N/A
Cluster-RNPP-UIP9-RUA7-Q2JU
Cluster-AC8L-ABCM-W5CR-ELSP

The following filters are supported, which can be used in combination:

- **Basic Filters** - this filters Traffic Managers by name. This supports *regular expressions* for search purposes.
- **Lifecycle Filter** - this filters Traffic Managers by instance lifecycle status. Any of the four lifecycle states can be included/excluded. That is: Active, Idle, Failed, Deleted. You cannot filter using any of the (orange) supported transitional states.

  NOTE
  Traffic Managers with the Deleted instance lifecycle state are not included by default.

- **Instance Health Filter** - this filters Traffic Managers by license health. Any of the four licensing states can be included/excluded. That is: Error, Warning, OK or N/A.
- **Licensing Health Filter** - this filters Traffic Managers by license health. Any of the five licensing states can be included/excluded. That is: Licensed, Pending, Warning, Failed or N/A.
- **Cluster Filter** - this filters Traffic Managers using a single selected cluster. The list of clusters includes both Discovered and User Created clusters, refer to Working with Traffic Manager Clusters on page 149.

1. Click the **Services** menu, and then click Services Director**: vTM Instances**.

   The **vTM Instances** page appears.

2. Under **Basic Filters**, type a **Name** if required. This supports *regular expressions* for search purposes. This filter is applied automatically as you type.

   When a **Name** filter is set the summary of filters includes "Name".

3. Under **Lifecycle Status**, select the check box for each required instance lifecycle state.

   Any state that is ticked is included in the table of Traffic Managers.

   NOTE
   Deleted Traffic Managers are not included by default. To include these, select the **Deleted** check box.

4. Under **Instance Health**, select the check box for any required instance health states.

   Any state that is ticked is included in the table of Traffic Managers.

5. Under **License Health**, select the check box for any required licensing health states.

   Any state that is ticked is included in the table of Traffic Managers.

6. Under **Cluster**, select the required cluster from the drop-down list.

   The table of Traffic Managers is limited to Traffic Managers that are in the selected cluster.

Updating Details for a Traffic Manager

You can update many of the details of a Traffic Manager from the **vTM Instances** page.

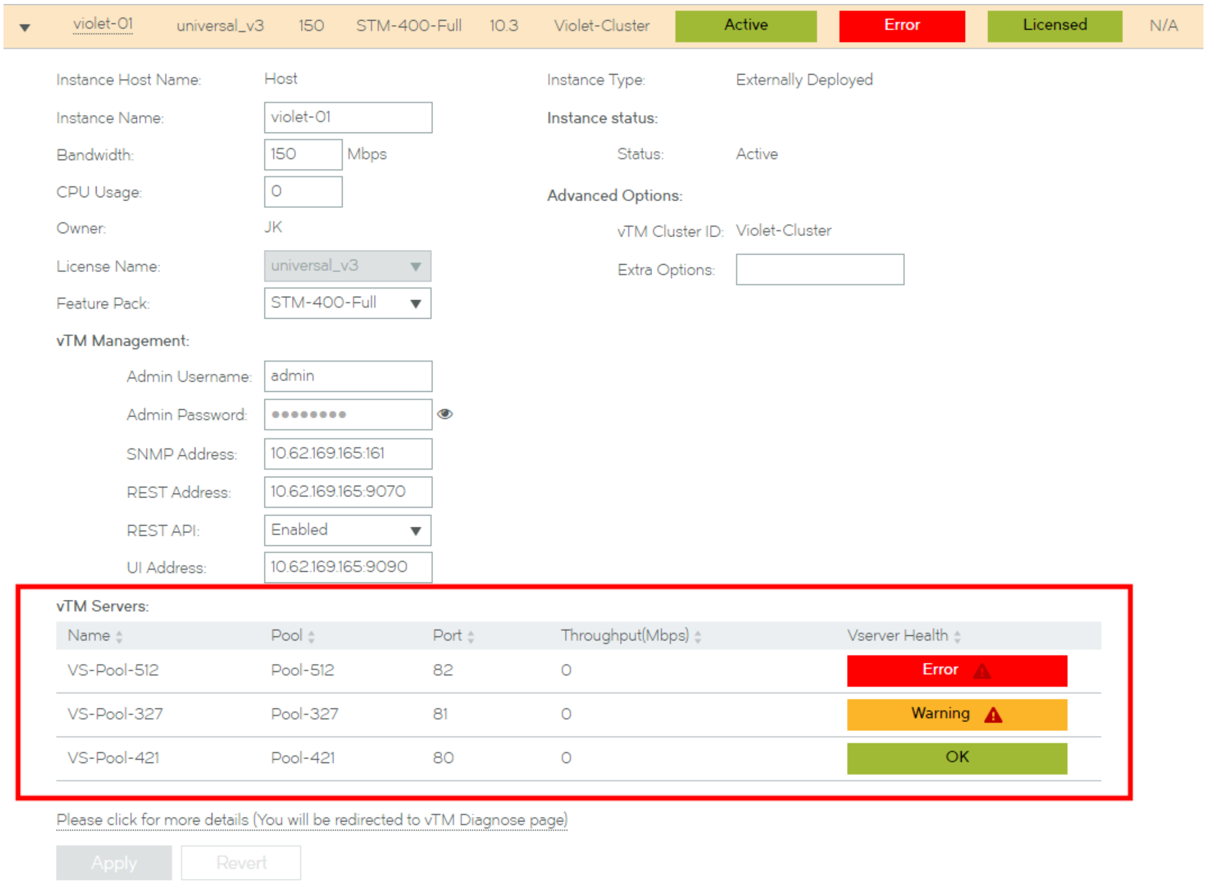
1. Click the **Services** menu, and then click **Services Director: vTM Instances**. The **vTM Instances** page appears.
2. Locate the Traffic Manager's entry in the table of Traffic Managers.
3. Click the arrow on the left side of the Traffic Manager's entry. The entry expands to show full details for the Traffic Manager.
4. Make the required changes to the Traffic Manager's details.
5. Click **Apply**.

Understanding vServer Status

Each Traffic Manager will have one or more vServers. Each vServer is responsible for balancing incoming traffic across a pool of nodes, as configured on the Brocade Virtual Traffic Manager itself.

A list of vServers is included in the Traffic Manager detailed view on the **vTM Instances** page. The Traffic Manager must be at version 10.3 or later with the REST API available. For example:

FIGURE 119 Traffic Manager Details: vServers



▼	violet-01	universal_v3	150	STM-400-Full	10.3	Violet-Cluster	Active	Error	Licensed	N/A

Instance Host Name: Host

Instance Name: violet-01

Bandwidth: 150 Mbps

CPU Usage: 0

Owner: JK

License Name: universal_v3

Feature Pack: STM-400-Full

vTM Management:

Admin Username: admin

Admin Password: ●●●●●●●●

SNMP Address: 10.62.169.165:161

REST Address: 10.62.169.165:9070

REST API: Enabled

UI Address: 10.62.169.165:9090

Instance Type: Externally Deployed

Instance status:

Status: Active

Advanced Options:

vTM Cluster ID: Violet-Cluster

Extra Options:

vTM Servers:

Name	Pool	Port	Throughput(Mbps)	Vserver Health
VS-Pool-512	Pool-512	82	0	Error ⚠
VS-Pool-327	Pool-327	81	0	Warning ⚠
VS-Pool-421	Pool-421	80	0	OK

Please click for more details (You will be redirected to vTM Diagnose page)

In this example, the **vTM Servers** list shows three vServers:

- VS-Pool-512 is in an Error state. This indicates that all of its nodes are in error. Pausing the pointer over the warning triangle will list failed pool nodes.
- VS-Pool-327 is in a Warning state. This indicates that some (but not all) of its nodes are in error. Pausing the pointer over the warning triangle will list failed pool nodes.
- VS-Pool-421 is in an OK state. This indicates that all of the vServer's pool nodes are working.

The **vTM Servers** list is limited to ten vServers, but by default this list displays in descending order of severity. That is, vServers showing an Error at the top, then vServers showing warnings, then vServers with no errors.

> NOTE
> To investigate any listed errors, click the **Please click for more details** control. You will be redirected to **vTM Diagnose** page on the Traffic Manager software, outside of the Services Director VA.

Deleting a Traffic Manager

You can delete a Traffic Manager from the **vTM Instances** page.

When you delete an externally-deployed Traffic Manager:

- the Traffic Manager itself is not actually deleted. It continues to exist, and remains registered. However, monitoring, metering and licensing checks for the Traffic Manager are halted.
- The **Lifecycle Status** of the Traffic Manager changes to Deleted.
- The **Licensing Health** of the Traffic Manager changes to N/A.
- The **Name** of a Deleted Traffic Manager can be reused by a different Traffic Manager.

> NOTE
> Traffic Managers with the Deleted state are not included in the default filter settings for the **vTM Instances** page. To include these Traffic Managers in the **vTM Instances** page, refer to Filtering Traffic Managers on page 137.

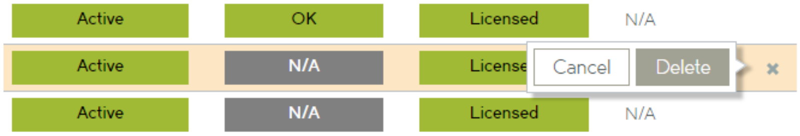
When you delete a Traffic Manager that was deployed by the Services Director VA:

- the Traffic Manager must be in an Idle state.
- the Traffic Manager itself is deleted.
- the Traffic Manager's container is deleted.
- The **Lifecycle Status** of the Traffic Manager changes to Deleted.
- The **Instance Health** of the Traffic Manager changes to N/A.
- The **Licensing Health** of the Traffic Manager changes to N/A.
- The **Name** of a Deleted Traffic Manager can be reused by a different Traffic Manager.

1. Click the **Services** menu, and then click Services Director**: vTM Instances**. The **vTM Instances** page appears.
2. Locate the Traffic Manager's entry in the table of Traffic Managers.

3. To the right of the Traffic Manager's entry, click the **X** control. A popup confirmation control appears.

FIGURE 120 The Delete Confirmation Control



4. Click **Delete**.

Relicensing Traffic Managers

Under a number of circumstances, you may need to relicense a Traffic Manager. For example:

- A Legacy FLA License is about to expire.
- The Service Endpoint Address of your Services Director changes. This affects Traffic Managers that are licensed using either Universal FLA or Legacy FLA Licensing.
- A Traffic Manager is updated from version 10.0 (or earlier) to version 10.1 (or later). You can replace the Legacy FLA licensing with Universal FLA licensing.

  NOTE
  Refer to Preparing to Relicense a Traffic Manager from Legacy FLA to Universal FLA on page 141 before starting this process.

- A new version of the Universal FLA License is released.
- The existing FLA License has been damaged in some way.

  NOTE
  If you are applying a new license to Traffic Manager that has no active REST API, you will need to add the Legacy FLA License to the Traffic Manager directly; this cannot be achieved through the Services Director.

Preparing to Relicense a Traffic Manager from Legacy FLA to Universal FLA

You may have a Traffic Manager that you used on an earlier release of the Services Director, which is now at version 10.1 or later. You can change its current Legacy FLA Licensing to Universal FLA Licensing. Before you can do this, you must enable its REST API setting.

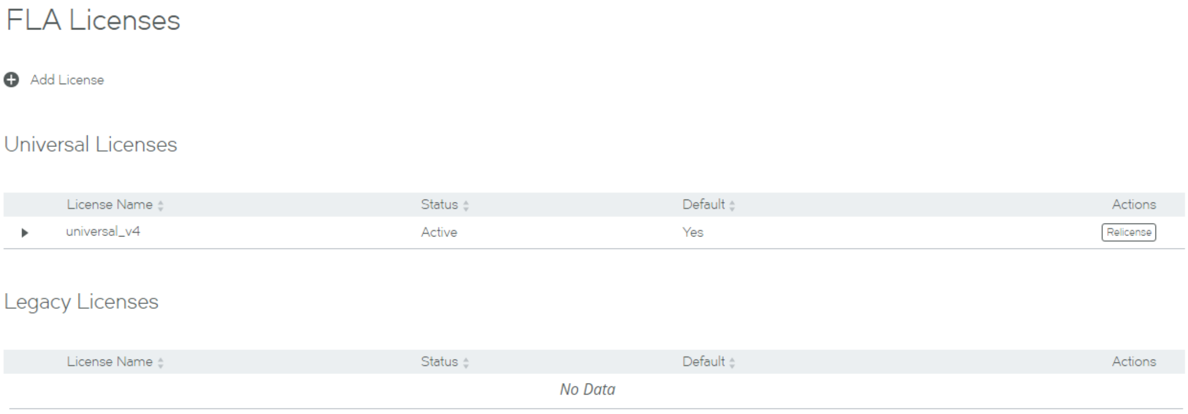
1. Click the **Services** menu, and then click Services Director**: vTM Instances**. The **vTM Instances** page appears.
2. Locate the Traffic Manager's entry in the table of Traffic Managers.
3. Click the arrow on the left side of the Traffic Manager's entry to show its details.
4. Under **vTM Management**, change **Rest API** to Enabled.
5. Click **Apply** to confirm the change.

   You can then continue with the relicensing process.

Relicensing a Traffic Manager Instance

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.
3. Click the **Catalogs** menu, and then click **Licensing: FLA Licenses**. The **FLA Licenses** page appears.

FIGURE 121 FLA Licenses Page



FLA Licenses

⊕ Add License

Universal Licenses

	License Name	Status	Default	Actions
▸	universal_v4	Active	Yes	Relicense

Legacy Licenses

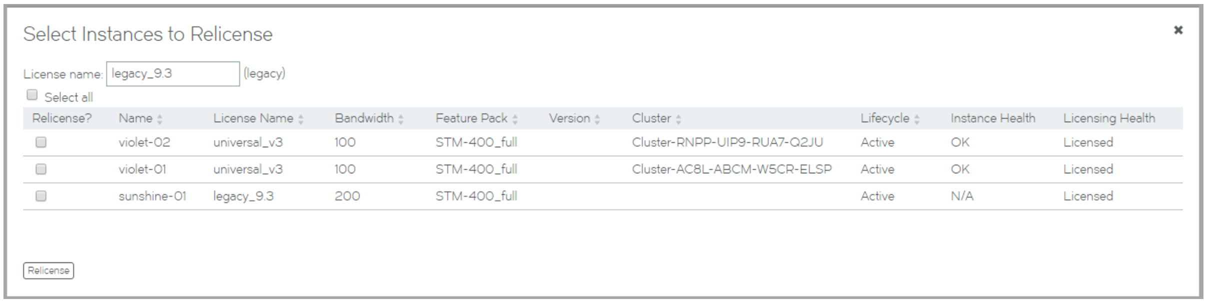
License Name	Status	Default	Actions
No Data			

4. (Optional) Add any new flexible licenses. Refer to Adding a Legacy FLA License to the Services Director on page 67.
5. Locate the license you wish to use.

   This can be either a Universal FLA License or a Legacy FLA License.
6. For this license, click **Relicense**.

   The **Select Instances To Relicense** dialog box appears. This indicates the selected FLA License, and lists all current Traffic Managers with an enabled REST API. For example:

FIGURE 122 FLA Licenses Page: Traffic Manager List



Select Instances to Relicense

License name: legacy_9.3 (legacy)

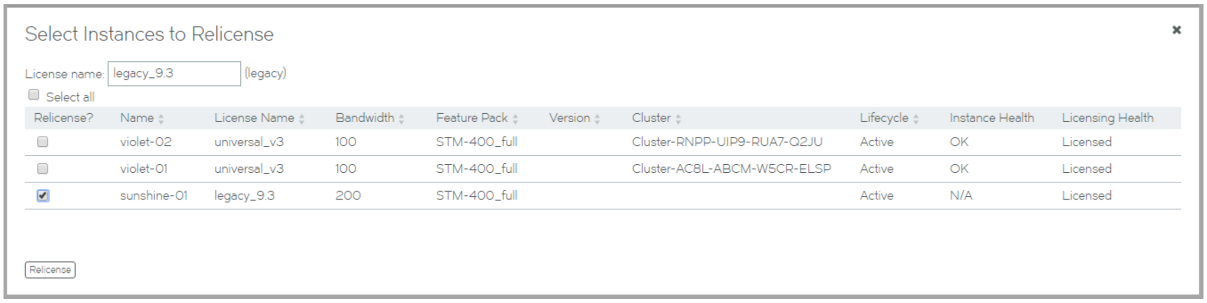
□ Select all

Relicense?	Name	License Name	Bandwidth	Feature Pack	Version	Cluster	Lifecycle	Instance Health	Licensing Health
□	violet-02	universal_v3	100	STM-400_full		Cluster-RNPP-UIP9-RUA7-Q2JU	Active	OK	Licensed
□	violet-01	universal_v3	100	STM-400_full		Cluster-AC8L-ABCM-W5CR-ELSP	Active	OK	Licensed
□	sunshine-01	legacy_9.3	200	STM-400_full			Active	N/A	Licensed

Relicense

7. Select the required Traffic Managers for the selected FLA License. For example:

FIGURE 123 Flexible Licenses Page: Traffic Manager Selections



Select Instances to Relicense

License name: legacy_9.3 (legacy)

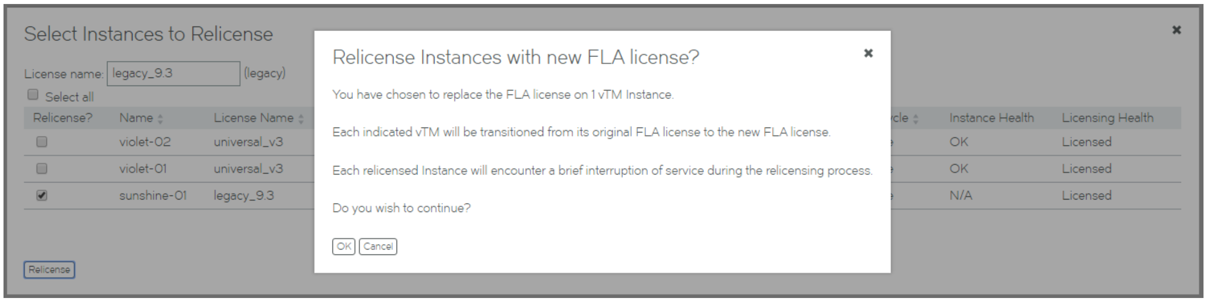
□ Select all

Relicense?	Name	License Name	Bandwidth	Feature Pack	Version	Cluster	Lifecycle	Instance Health	Licensing Health
□	violet-02	universal_v3	100	STM-400_full		Cluster-RNPP-UIP9-RUA7-Q2JU	Active	OK	Licensed
□	violet-01	universal_v3	100	STM-400_full		Cluster-AC8L-ABCM-W5CR-ELSP	Active	OK	Licensed
☑	sunshine-01	legacy_9.3	200	STM-400_full			Active	N/A	Licensed

NOTE
You may have a Traffic Manager that you used on an earlier release of the Services Director, which is now at version 10.1 or later. You can change its current Legacy FLA Licensing to Universal FLA Licensing. Refer to Preparing to Relicense a Traffic Manager from Legacy FLA to Universal FLA on page 141.

8. Click **Relicense**. A confirmation dialog box appears.

FIGURE 124 FLA Licenses Page: Traffic Manager Confirmations



Relicense Instances with new FLA license?

You have chosen to replace the FLA license on 1 vTM Instance.

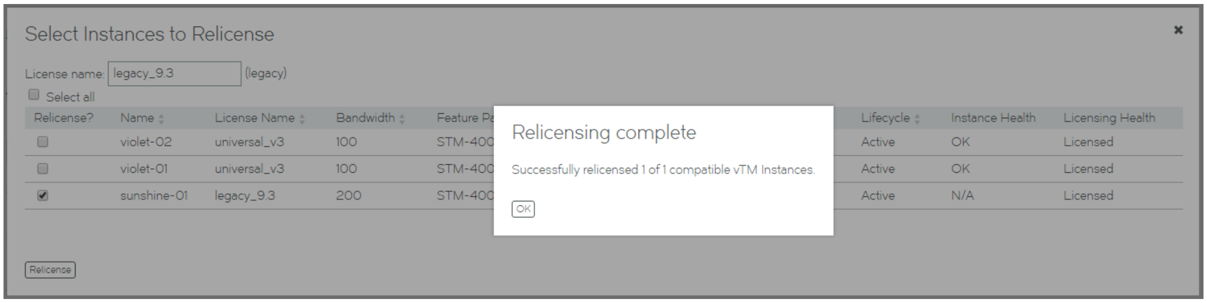
Each indicated vTM will be transitioned from its original FLA license to the new FLA license.

Each relicensed Instance will encounter a brief interruption of service during the relicensing process.

Do you wish to continue?

9. Click **OK**. The relicensing process begins, and displays progress. There are two possible outcomes:
   - The process completes successfully.

FIGURE 125 FLA Licenses Page: Traffic Manager Relicensing Succeeds



Select Instances to Relicense

License name: legacy_9.3 (legacy)

□ Select all

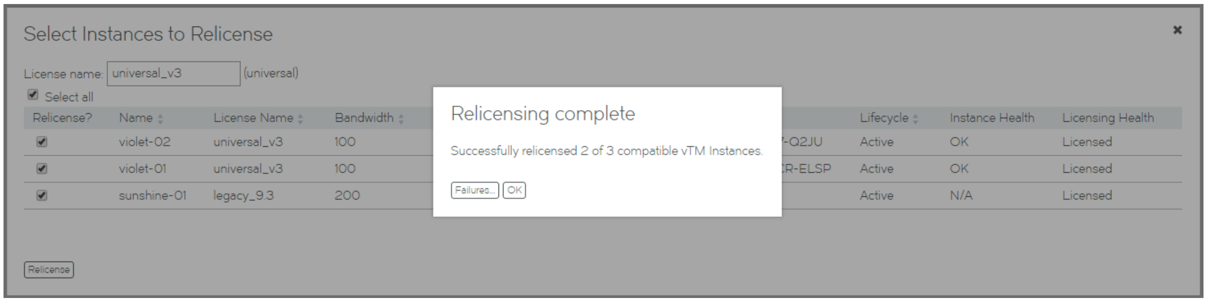
Relicense?	Name	License Name	Bandwidth	Feature Pa	Lifecycle	Instance Health	Licensing Health
□	violet-02	universal_v3	100	STM-400	Active	OK	Licensed
□	violet-01	universal_v3	100	STM-400	Active	OK	Licensed
☑	sunshine-01	legacy_9.3	200	STM-400	Active	N/A	Licensed

Relicensing complete

Successfully relicensed 1 of 1 compatible vTM Instances.

   - The process completes, but is only partially successful. Using a different example:

FIGURE 126 FLA Licenses Page: Traffic Manager Relicensing Partial Completion



Select Instances to Relicense

License name: universal_v3 (universal)

☑ Select all

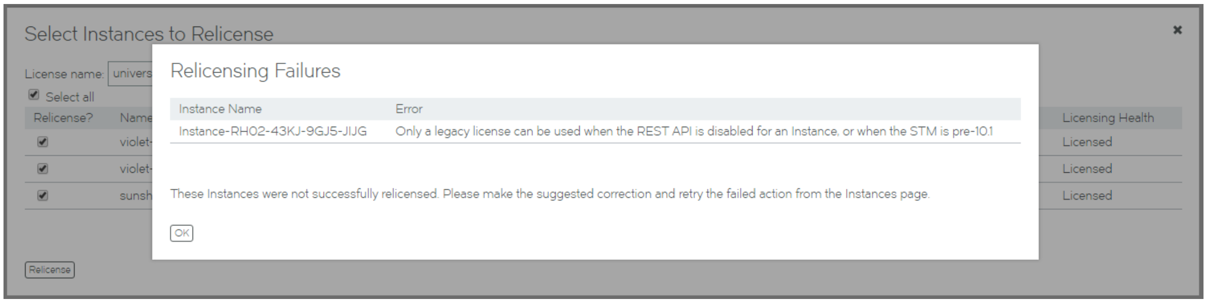
Relicense?	Name	License Name	Bandwidth		Lifecycle	Instance Health	Licensing Health
☑	violet-02	universal_v3	100	-Q2JU	Active	OK	Licensed
☑	violet-01	universal_v3	100	R-ELSP	Active	OK	Licensed
☑	sunshine-01	legacy_9.3	200		Active	N/A	Licensed

Relicensing complete

Successfully relicensed 2 of 3 compatible vTM Instances.

Click **Failures** to list the Traffic Managers that could not be relicensed. You may need to investigate the licensing of these Traffic Managers further.

FIGURE 127 FLA Licenses Page: Traffic Manager Relicensing Failures



Select Instances to Relicense

License name: univers

☑ Select all

Relicense?	Name	Licensing Health
☑	violet-	Licensed
☑	violet-	Licensed
☑	sunsh	Licensed

Relicensing Failures

Instance Name	Error
Instance-RH02-43KJ-9GJ5-JIJG	Only a legacy license can be used when the REST API is disabled for an Instance, or when the STM is pre-10.1

These Instances were not successfully relicensed. Please make the suggested correction and retry the failed action from the Instances page.

10. Click **OK** to finish this process.

Processing Traffic Manager Metering Discrepancy Warnings

The accurate billing for Cloud Service Provider customers relies on:

- Accurate record-keeping for registered Virtual Traffic Managers (vTMs).
- Availability of metering information from each vTM.

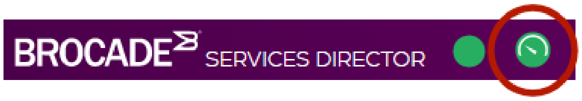
The Services Director monitors the operation of each vTM to detect scenarios that may give rise to billing discrepancies.

For example:

- A vTM was registered with the Services Director, but then decommissioned later without marking the vTM as "Deleted". In this case, the decommissioned vTM will still be being charged on an uptime basis. This will result in over-accounting of uptime and a larger CSP bill than should have been charged.
- A vTM was registered with the Services Director, but the Services Director has been unable to retrieve metered throughput metrics from the vTM using its REST API or SNMP. In this case, the vTM will not have been charged for throughput at all. This is likely to result in under-metering and a smaller CSP bill than should have been charged.

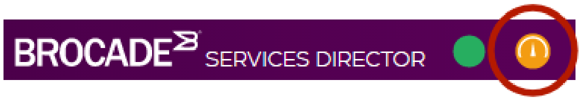
Where no metering discrepancies are detected, the Services Director VA displays a green metering symbol in the header:

FIGURE 128 No Metering Discrepancies Detected



Where metering discrepancies are detected, the Services Director VA displays an orange metering warning symbol in the header:

FIGURE 129 Metering Discrepancy Warning



You can then inspect any metering warnings in the Services Director VA and resolve them. Refer to Understanding Metering Discrepancy Warnings on page 145.

> **NOTE**
> Monitoring that gives rise to metering alerts and notifications is enabled by default. You can change this setting if required from the **System** > **General Settings** page, refer to Updating Metering Alerts and Notifications Settings on page 61.

Understanding Metering Discrepancy Warnings

Traffic Manager metering discrepancy warnings are displayed as a table in the **Metering Warnings** page.

To access this page, click the metering warning symbol in the header, see Processing Traffic Manager Metering Discrepancy Warnings on page 145.

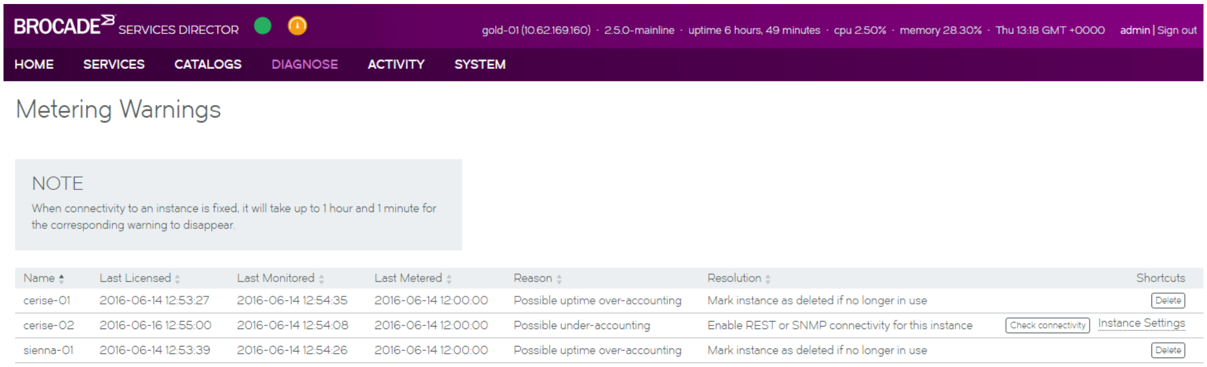
Alternatively, click the **Diagnose** menu and then click **Metering Warnings**.

In the **Metering Warnings** page, each line of the metering warnings table shows a potential billing discrepancy for a vTM. This includes:

- Timestamps for metering, licensing and monitoring.
- A summary reason for its inclusion.
- A potential solution, and the controls to access the solution.

For example:

FIGURE 130 Metering Warnings Page



BROCADE SERVICES DIRECTOR
gold-01 (10.62.169.160) · 2.5.0-mainline · uptime 6 hours, 49 minutes · cpu 2.50% · memory 28.30% · Thu 13:18 GMT +0000
admin | Sign out
HOME
SERVICES
CATALOGS
DIAGNOSE
ACTIVITY
SYSTEM

Metering Warnings

NOTE

When connectivity to an instance is fixed, it will take up to 1 hour and 1 minute for the corresponding warning to disappear.

Name	Last Licensed	Last Monitored	Last Metered	Reason	Resolution	Shortcuts
cerise-01	2016-06-14 12:53:27	2016-06-14 12:54:35	2016-06-14 12:00:00	Possible uptime over-accounting	Mark instance as deleted if no longer in use	Delete
cerise-02	2016-06-16 12:55:00	2016-06-14 12:54:08	2016-06-14 12:00:00	Possible under-accounting	Enable REST or SNMP connectivity for this instance	Check connectivity Instance Settings
sienna-01	2016-06-14 12:53:39	2016-06-14 12:54:26	2016-06-14 12:00:00	Possible uptime over-accounting	Mark instance as deleted if no longer in use	Delete

In this example:

- There are two vTMs that are flagged as potentially being *over-billed*.

  If a vTM is no longer in use, it is likely that it has not requested FLA licensing for over 24 hours, and cannot be contacted using REST API or SNMP. In this case, you can delete it to prevent over-billing for uptime. Refer to Processing Potentially Over-Accounted Traffic Managers on page 147.
- There is a vTM that is flagged as potentially being *under-billed*.

  It is likely that this vTM is still requesting FLA licensing, but is uncontactable using REST API or SNMP. If you enable the REST API or SNMP for this vTM, this will re-enable metering and prevent under-billing for its use. Refer to Processing Potentially Under-Accounted Traffic Managers on page 147.

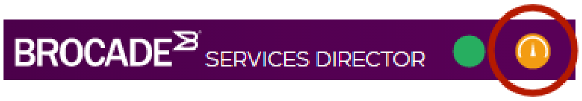
  NOTE
  Once these situations are resolved, the warnings and the warning symbol remain in place until the Services Director re-evaluates them. This may take up to one hour and one minute, and cannot be triggered from the interface.

Processing Potentially Over-Accounted Traffic Managers

If you are no longer using a vTM, but have not yet deleted it from the estate of the Services Director VA, you may see a metering discrepancy warning. This warning indicates that there is a possibility of the billing for the vTM being over-accounted. You can resolve this by deleting the vTM from the estate of the Services Director VA.

1. In the header for the Services Director VA, click the metering warning symbol.

   FIGURE 131 FLA Licenses Page

   Alternatively, click the **Diagnose** menu and then click **Metering Warnings**.

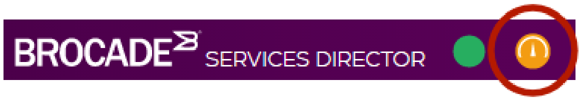
   The **Metering Warnings** page appears. This displays a table, with an entry for each vTM for which there is a metering discrepancy warning (refer to Understanding Metering Discrepancy Warnings on page 145).
2. Locate the entry for the required vTM.
3. Examine the registered details for the vTM.
   To do this, visit the **vTM Instances** page and/or examine the user interface of the vTM itself.
4. If you decide to delete the vTM, click **Delete** in the **Shortcuts** column.
   The entry is marked as Deleted in the **Shortcuts** column. Then, after a short time, the entry is removed from the table.

Processing Potentially Under-Accounted Traffic Managers

The Services Director VA uses the REST API to collect metering information. If the REST API is not enabled, SNMP is then attempted if your configuration supports it. If you are using a vTM without either its REST API or SNMP active, you may see a metering discrepancy warning. This warning indicates that there is a possibility of the billing for the vTM being under-accounted. You can resolve this by enabling the REST API or SNMP for the vTM.

1. In the header for the Services Director VA, click the metering warning symbol.

   FIGURE 132 FLA Licenses Page

   Alternatively, click the **Diagnose** menu and then click **Metering Warnings**.

   The **Metering Warnings** page appears. This displays a table, with an entry for each vTM for which there is a metering discrepancy warning (refer to Understanding Metering Discrepancy Warnings on page 145).
2. Locate the entry for the required vTM.
3. Click **Instance Setting** for the entry.
   The **vTM Instances** page appears.
4. In the table of vTMs on the **vTM Instances** page, expand the vTM to show its detailed view.
5. Check the **REST API**, **REST Address** and **SNMP Address** settings in the detailed view.

6. If the **REST API** is Disabled, the REST API has been disabled from the Services Director VA. Set this to Enabled and **Apply** the change.

   NOTE
   Once the REST API for the vTM shows as Enabled on the **Metering Warnings** page, it is not guaranteed that the REST API is enabled on the vTM itself. You must continue with this procedure to the end to ensure its operation.

7. In the detail view for the vTM, click **Please click for more details**.
   You are redirected to the vTM's login page.
8. If you want to use the REST API to gather metering information, enable it on the vTM. Refer to the Virtual Traffic Manager documentation for details.
9. If you want to use SNMP to gather metering information, enable it on the vTM. Refer to the Virtual Traffic Manager documentation for details.
10. Return to the **Metering Warnings** page on the Services Director VA.
11. For the required vTM, click **Check connectivity**.
    The connectivity between the Services Director VA and the vTM is tested. If this test succeeds, Check successful appears.

    NOTE
    The vTM entry is not removed from the table immediately. This can take up to one hour and one minute.

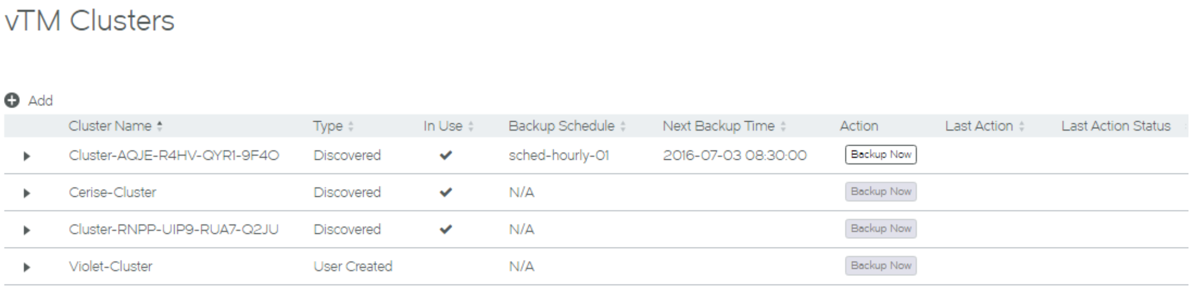
Working with Traffic Manager Clusters

Overview: Working with Traffic Manager Clusters

The **vTM Cluster** page displays a list of all clusters known to the Services Director VA.

The **vTM Cluster** page also enables you to assign a backup schedule to each cluster, and to inspect the details of the cluster backups taken.

FIGURE 133 vTM Cluster Page



vTM Clusters

	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status
▸	Cluster-AQJE-R4HV-QYR1-9F4O	Discovered	✓	sched-hourly-01	2016-07-03 08:30:00	Backup Now		
▸	Cerise-Cluster	Discovered	✓	N/A		Backup Now		
▸	Cluster-RNPP-UIP9-RUA7-Q2JU	Discovered	✓	N/A		Backup Now		
▸	Violet-Cluster	User Created		N/A		Backup Now		

There are two types of clusters used by the Services Director VA:

- Discovered - this is a cluster present on one or more externally-deployed Traffic Managers. When an externally-deployed Traffic Manager is registered, a cluster name is displayed automatically.

  NOTE
  Registering a clustered Traffic Manager does not register other Traffic Managers in the cluster, nor does it license them; you must independently register and license each node in a cluster.

  NOTE
  You cannot create a Discovered cluster from the **vTM Clusters** page.

  NOTE
  Services Director's awareness of Discovered clusters is limited to Traffic Managers at version 10.2 or later with an enabled REST API.

- User Created - this is a cluster that you create manually on the **vTM Clusters** page. This cluster type can *only* be used for Traffic Managers that you deploy from the Services Director VA. Refer to the *Brocade Services Director Advanced User Guide* for details.

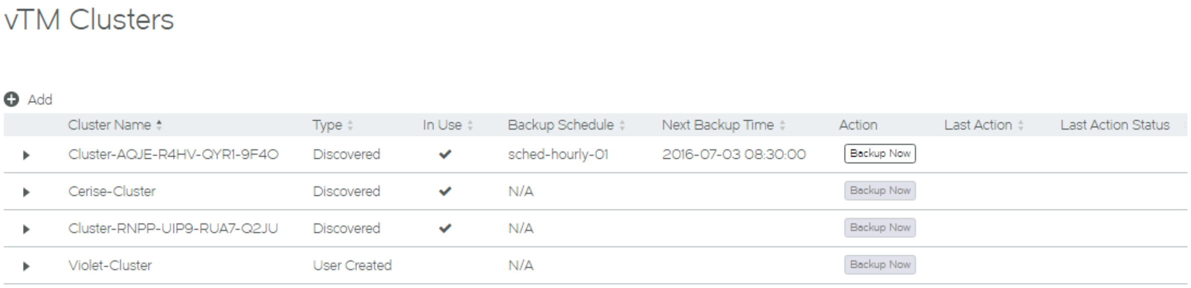
You can rename a cluster of either type from the **vTM Clusters** page, refer to Updating a Traffic Manager Cluster on page 155.

Services Director supports backup and restore for cluster configurations, refer to Working with Traffic Manager Cluster Backups on page 156.

Understanding Traffic Manager Cluster Details

The **vTM Cluster** page displays a table of clusters known to the Services Director VA.

FIGURE 134 vTM Cluster Page



vTM Clusters

	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status
▸	Cluster-AQJE-R4HV-QYR1-9F4O	Discovered	✓	sched-hourly-01	2016-07-03 08:30:00	Backup Now		
▸	Cerise-Cluster	Discovered	✓	N/A		Backup Now		
▸	Cluster-RNPP-UIP9-RUA7-Q2JU	Discovered	✓	N/A		Backup Now		
▸	Violet-Cluster	User Created		N/A		Backup Now		

Each entry in the table of clusters on the **vTM Clusters** page shows basic details for each cluster, and provides controls for backup operations where supported by the cluster.

Name	Description
Cluster Name	The unique name of the cluster. If required, you can rename a cluster. Refer to Updating a Traffic Manager Cluster on page 155.
Type	There are two cluster types used by the Services Director: • *Discovered* - this is a cluster present on one or more externally-deployed Traffic Managers. When an externally-deployed Traffic Manager is registered (version 10.2 or later with an active REST API), a cluster name is displayed automatically. NOTE Registering a clustered Traffic Manager does not register other Traffic Managers in the cluster, nor does it license them; you must independently register and license each node in a cluster. NOTE You cannot create a Discovered cluster from the **vTM Clusters** page. NOTE Services Director's awareness of Discovered clusters is limited to Traffic Managers at version 10.2 or later with an enabled REST API. • *User Created* - this is a cluster that you create manually on the **vTM Clusters** page. This cluster type can *only* be used for Traffic Managers that are deployed from the Services Director VA. Refer to the *Brocade Services Director Advanced User Guide* for details.
In Use	This indicates whether any Traffic Managers are currently in the cluster.

Name	Description
Backup Schedule	(Optional) The selected schedule for the cluster backup. The configured number of backups for this cluster and the most recent backups are displayed in the detail view for the cluster. Refer to Creating a Cluster Backup Schedule on page 158. NOTE Where no **Backup Schedule** is selected, this property is displayed as N/A. NOTE This column is only supported on vTMs at version 11.0 and later. NOTE The number of backups for this cluster is visible in the detail view for the cluster.
Next Backup Time	The time of the next scheduled cluster backup. NOTE Where no **Backup Schedule** is selected, this property is blank. NOTE This column is only supported on vTMs at version 11.0 and later. This column is blank for all other vTMs.
Action	This column displays buttons that activate (or report on) supported cluster backup activities. This includes: • **Backup Now**. When clicked, a backup is performed immediately. • **Retry**. This appears after a user-triggered **Backup Now** action fails. When clicked, the **Backup Now** action is re-attempted. Refer to Retrying An Immediate Backup After a Failure on page 166. • **Clear Failed Action**. This appears after a user-triggered **Backup Now** action fails. When clicked, both the named **Last Action** and the Failed **Last Action Status** are removed. Refer to Retrying An Immediate Backup After a Failure on page 166. NOTE This column is only supported on vTMs at version 11.0 and later. Where the vTM does not support backups, the **Backup Now** button is displayed but remains unavailable.
Last Action	The most recent manually-performed **Action** for a cluster backup (see above). This can be: • Backup Now. This appears after a **Backup Now** action is attempted (see above). • Restore. This appears after a restore operation is attempted for a listed cluster backup. Refer to Restoring a Backup to a Cluster on page 169. • Upload. This appears after an upload operation is attempted for a listed cluster backup. Refer to Uploading a Cluster Backup to a Traffic Manager on page 172. The result of the displayed action is shown in the **Last Action Status** column (see below). Scheduled backups are not included in this column.

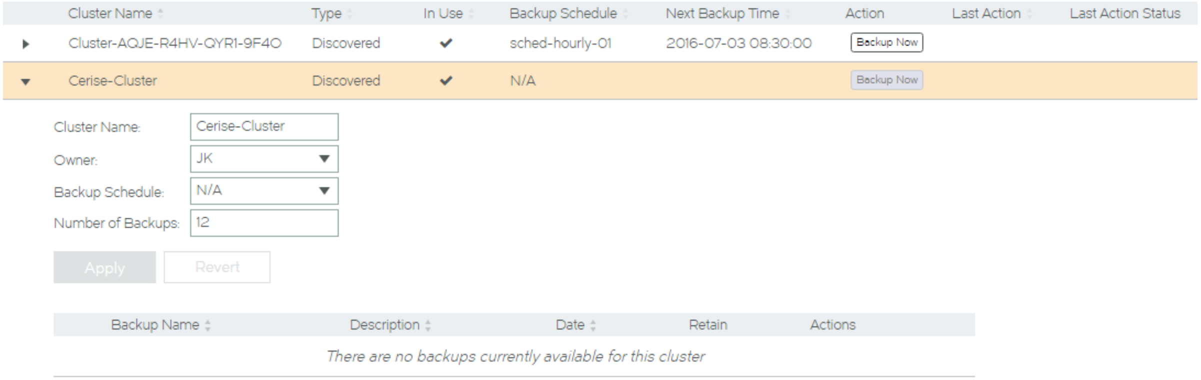
Name	Description
	NOTE This column is only supported on vTMs at version 11.0 and later. This column is blank for all other vTMs.
Last Action Status	The outcome of the **Last Action** operation (see above). This is blank, In Progress (blue), Complete or Failed (red). The results of scheduled backups are not included in this column. NOTE A failed flag can be cleared from the **Action** column (see above). NOTE This column is only supported on vTMs at version 11.0 and later. This column is blank for all other vTMs.

To view the full details for a cluster, expand the required cluster. This includes:

- a **Cluster Name** that you can update, refer to Updating a Traffic Manager Cluster on page 155.
- an **Owner** for the cluster.
- the **Backup Schedule** and **Number of Backups** that define the backup schedule for the cluster, where one is used. Refer to Overview: Cluster Backups on page 157.

For example, when no cluster backup is in use:

FIGURE 135 Cluster Detailed View: No Backups Present



	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status
▸	Cluster-AQJE-R4HV-QYR1-9F4O	Discovered	✓	sched-hourly-01	2016-07-03 08:30:00	Backup Now		
▾	Cerise-Cluster	Discovered	✓	N/A		Backup Now		

Cluster Name: Cerise-Cluster

Owner: JK

Backup Schedule: N/A

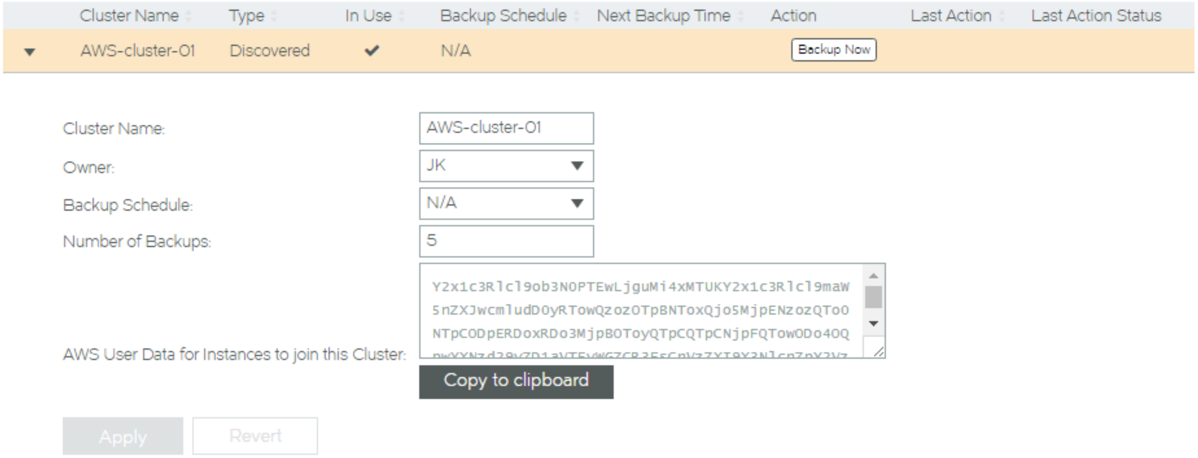
Number of Backups: 12

Backup Name	Description	Date	Retain	Actions

There are no backups currently available for this cluster

NOTE
Where a cluster was created for a cloud-based vTM, an additional field containing an AWS user data block is included.

FIGURE 136 Cluster Detailed View: Cluster for Cloud-Based vTMs



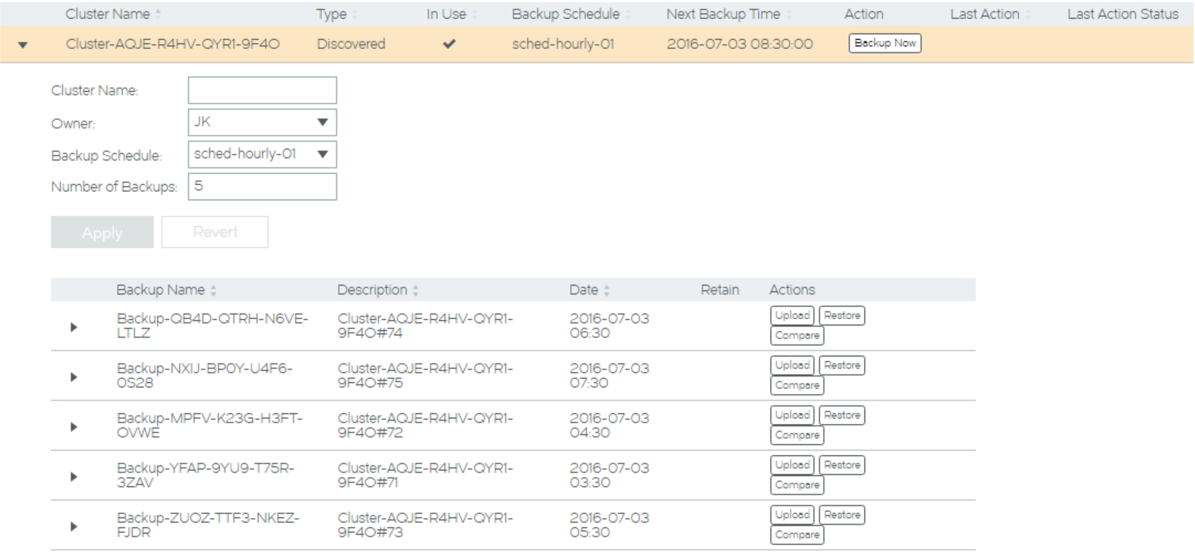
	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status
▼	AWS-cluster-01	Discovered	✓	N/A		Backup Now		

Cluster Name:	AWS-cluster-01
Owner:	JK
Backup Schedule:	N/A
Number of Backups:	5
AWS User Data for Instances to join this Cluster:	Y2x1c3Rlcl9ob3N0PTEwLjguMi4xMTUKY2x1c3Rlcl9maW 5nZXJwcmludD0yRTowQzozOTpBNToxQjo5MjpENzozQToO NTpCODpERDoxRDo3MjpBOToyQTpCQTpCNjpFQTowODo4OQ

This AWS user data text block is required when you create additional cloud-based vTM cluster members, refer to Creating the Second vTM in a Cluster on page 127.
Use **Copy to clipboard** before performing this task.

Where a backup schedule for the cluster is in use, a list of backups is included. For example:

FIGURE 137 Cluster Detailed View: Backups Present



	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status
▼	Cluster-AQJE-R4HV-QYR1-9F4O	Discovered	✓	sched-hourly-01	2016-07-03 08:30:00	Backup Now		

Cluster Name:	
Owner:	JK
Backup Schedule:	sched-hourly-01
Number of Backups:	5

	Backup Name	Description	Date	Retain	Actions
▶	Backup-QB4D-QTRH-N6VE-LTLZ	Cluster-AQJE-R4HV-QYR1-9F4O#74	2016-07-03 06:30		Upload Restore Compare
▶	Backup-NXIJ-BP0Y-U4F6-OS28	Cluster-AQJE-R4HV-QYR1-9F4O#75	2016-07-03 07:30		Upload Restore Compare
▶	Backup-MPFV-K23G-H3FT-OVWE	Cluster-AQJE-R4HV-QYR1-9F4O#72	2016-07-03 04:30		Upload Restore Compare
▶	Backup-YFAP-9YU9-T75R-3ZAV	Cluster-AQJE-R4HV-QYR1-9F4O#71	2016-07-03 03:30		Upload Restore Compare
▶	Backup-ZUOZ-TTF3-NKEZ-FJDR	Cluster-AQJE-R4HV-QYR1-9F4O#73	2016-07-03 05:30		Upload Restore Compare

To make use of any listed backups, refer to Working with Traffic Manager Cluster Backups on page 156.

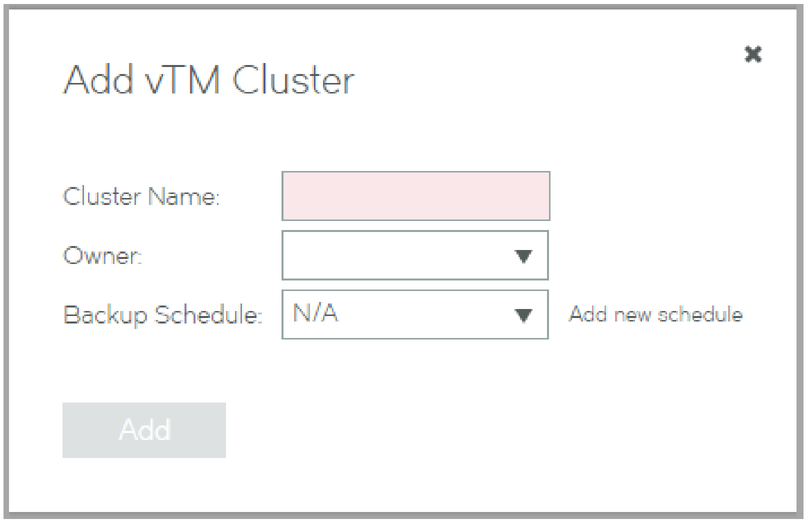
Creating a Traffic Manager Cluster

You can create a *User Created* Traffic Manager cluster from the **vTM Clusters** page.

> NOTE
> You cannot create a *Discovered* cluster using the Services Director.

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.
3. Click the **Services** menu, and then click **Services Director: vTM Clusters**. The **vTM Clusters** page appears.
4. Click the plus symbol above the vTM cluster table.
   The **Add vTM Cluster** dialog box appears.

   FIGURE 138 Adding a vTM Cluster

   Add vTM Cluster

   Cluster Name:

   Owner:

   Backup Schedule: N/A

5. Specify the following:
   - **Cluster Name** - specify the unique name for the cluster.
   - **Owner** - select an owner for the cluster.

     > NOTE
     > If there are no owner entries, refer to Adding an Owner to the Services Director on page 83.

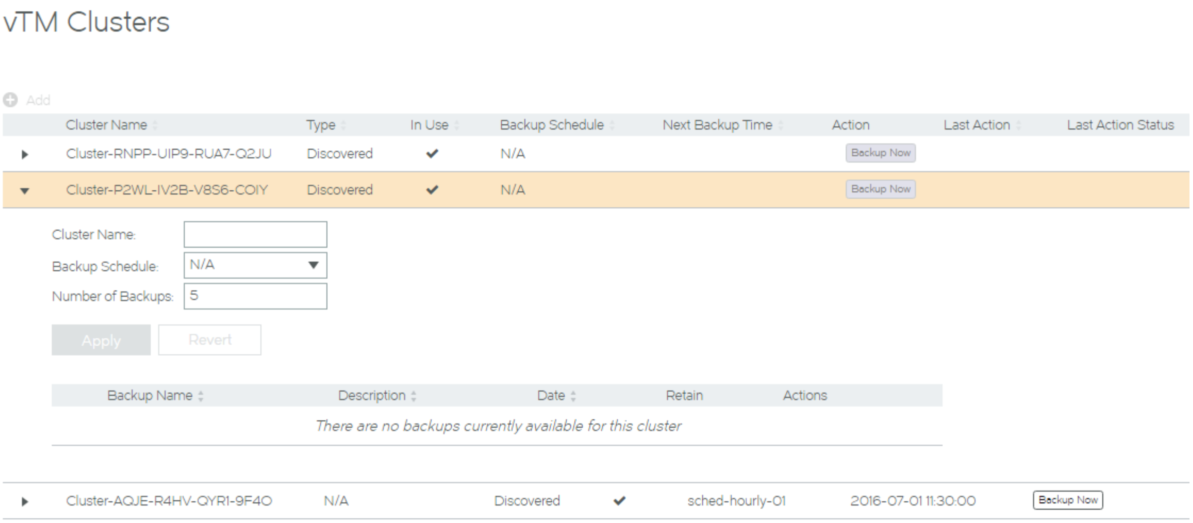
   - **Cluster Port Offset** - (Optional) Specify a port offset for the cluster.
   - **Backup Schedule** - (Optional) Select an existing backup schedule. If you want to create a new schedule, click **Add new schedule**. When you do this, this page is replaced by the **Instances Backup Schedule** page. Refer to Creating a Cluster Backup Schedule on page 158.
6. Click **Add**.
   The *User Created* cluster is added to the table of clusters.

Updating a Traffic Manager Cluster

You can update a Traffic Manager cluster from the **vTM Clusters** page.

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.
3. Click the **Services** menu, and then click **Services Director: vTM Clusters**. The **vTM Clusters** page appears.
4. Expand the required cluster.

FIGURE 139 Updating a vTM Cluster



vTM Clusters

⊕ Add

	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status
▸	Cluster-RNPP-UIP9-RUA7-Q2JU	Discovered	✓	N/A		Backup Now		
▾	Cluster-P2WL-IV2B-V8S6-COIY	Discovered	✓	N/A		Backup Now		

Cluster Name:
Backup Schedule: N/A ▾
Number of Backups: 5

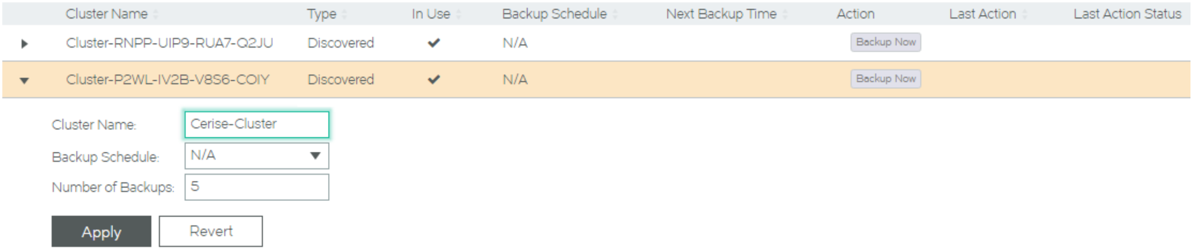
Apply Revert

Backup Name	Description	Date	Retain	Actions
There are no backups currently available for this cluster				

	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status
▸	Cluster-AQJE-R4HV-QYR1-9F4O	N/A		Discovered ✓	sched-hourly-01	2016-07-01 11:30:00		Backup Now

5. Update the **Cluster Name**. For example:

FIGURE 140 Specifying a New Name For a vTM Cluster



	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status
▸	Cluster-RNPP-UIP9-RUA7-Q2JU	Discovered	✓	N/A		Backup Now		
▾	Cluster-P2WL-IV2B-V8S6-COIY	Discovered	✓	N/A		Backup Now		

Cluster Name: Cerise-Cluster
Backup Schedule: N/A ▾
Number of Backups: 5

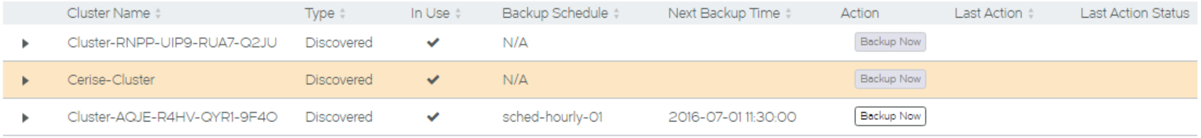
Apply Revert

6. (Optional) Select both a new **Backup Schedule** and a **Number of Backups**. Refer to Working with Traffic Manager Cluster Backups on page 156.

   NOTE
   The **Number of Backups** property is only used when there is a **Backup Schedule** selected.

7. Click **Apply**. The cluster is updated.

FIGURE 141 vTM Cluster Page: Updated (Renamed) Cluster

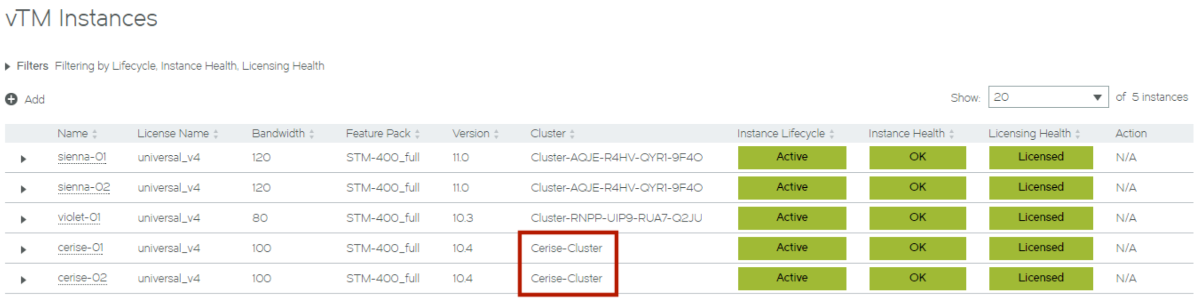


	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status
▸	Cluster-RNPP-UIP9-RUA7-Q2JU	Discovered	✓	N/A		Backup Now		
▸	Cerise-Cluster	Discovered	✓	N/A		Backup Now		
▸	Cluster-AQJE-R4HV-QYR1-9F4O	Discovered	✓	sched-hourly-01	2016-07-01 11:30:00	Backup Now		

To view updated **Backup Schedule** and **Number of Backups** settings, expand the cluster.

You can also confirm the name change from the **vTM Instances** page. For example:

FIGURE 142 Confirming an Updated vTM Cluster



vTM Instances

▸ Filters Filtering by Lifecycle, Instance Health, Licensing Health

⊕ Add

Show: 20 ▼ of 5 instances

	Name	License Name	Bandwidth	Feature Pack	Version	Cluster	Instance Lifecycle	Instance Health	Licensing Health	Action
▸	sienna-01	universal_v4	120	STM-400_full	11.0	Cluster-AQJE-R4HV-QYR1-9F4O	Active	OK	Licensed	N/A
▸	sienna-02	universal_v4	120	STM-400_full	11.0	Cluster-AQJE-R4HV-QYR1-9F4O	Active	OK	Licensed	N/A
▸	violet-01	universal_v4	80	STM-400_full	10.3	Cluster-RNPP-UIP9-RUA7-Q2JU	Active	OK	Licensed	N/A
▸	cerise-01	universal_v4	100	STM-400_full	10.4	Cerise-Cluster	Active	OK	Licensed	N/A
▸	cerise-02	universal_v4	100	STM-400_full	10.4	Cerise-Cluster	Active	OK	Licensed	N/A

In this example, the *Cerise-Cluster* name is shown for both Traffic Managers that are in the cluster.

Working with Traffic Manager Cluster Backups

All of the Virtual Traffic Managers (vTMs) in a cluster share a cluster configuration. To ensure that the cluster configuration is preserved, you can schedule a regular cluster backup for each cluster. This preserves the cluster configuration only, and not the individual configuration of each vTM. This section includes the following topics:

- Overview: Cluster Backups on page 157.
- Creating a Cluster Backup Schedule on page 158.
- Updating a Cluster Backup Schedule on page 160.
- Adding a Backup Schedule to a Cluster on page 161.
- Viewing Backups for a Cluster on page 162.
- Performing an Immediate Backup for a Cluster on page 165.
- Comparing Two Cluster Backups on page 167.
- Restoring a Backup to a Cluster on page 169.
- Uploading a Cluster Backup to a Traffic Manager on page 172.
- Deleting a Cluster Backup on page 176.

NOTE
Cluster Backups are not the same as Services Director backups. Services Director backups enable you to recover from a Services Director failure, refer to Recovering from a Services Director Failure on page 237.

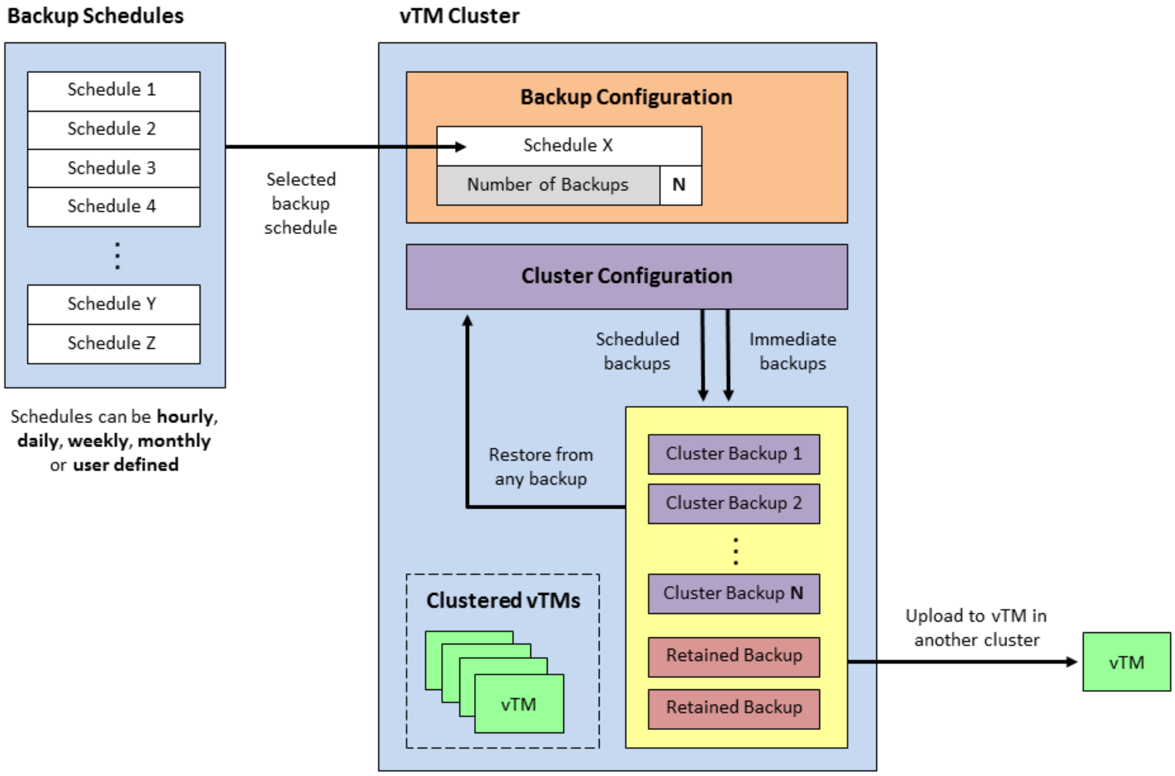
Overview: Cluster Backups

A Traffic Manager cluster gathers Virtual Traffic Managers (vTMs) together and operates them under a shared cluster configuration.

The configuration of the cluster can be backed up automatically on a regular basis according to a backup schedule.

The following provides an overview of automatic cluster backup operations.

FIGURE 143 Overview of Cluster Backups



Before you set up automatic backups for a cluster's configuration, you must create one or more backup schedules, refer to Creating a Cluster Backup Schedule on page 158. Backup schedules define the frequency and times at which a backup will be taken. Each can be applied to one or more clusters.

Once you have backup schedules, you can configure the cluster to create backups automatically using a backup schedule. To do this, you select a backup schedule for the cluster, and indicate the number of backups that you want the cluster to store, refer to Adding a Backup Schedule to a Cluster on page 161.

Once the cluster has an assigned cluster backup schedule, the cluster accumulates scheduled backups automatically. You can also manually request an immediate backup at any time. Refer to Performing an Immediate Backup for a Cluster on page 165.

NOTE
You can also request an immediate backup when there is no assigned backup schedule.

Once the maximum number of cluster backups is reached, older cluster backups are deleted automatically whenever newer cluster backups are created.

You can also choose to *retain* one or more backups if required, refer to Updating Details for a Cluster Backup on page 164. Retained backups do not count towards the maximum number of backups for the cluster, and are not deleted automatically.

The cluster's configuration can be restored from an existing backup at any time, refer to Restoring a Backup to a Cluster on page 169.

To support the selection of the correct cluster backup, you can compare any two cluster backups to identify the differences, refer to Comparing Two Cluster Backups on page 167.

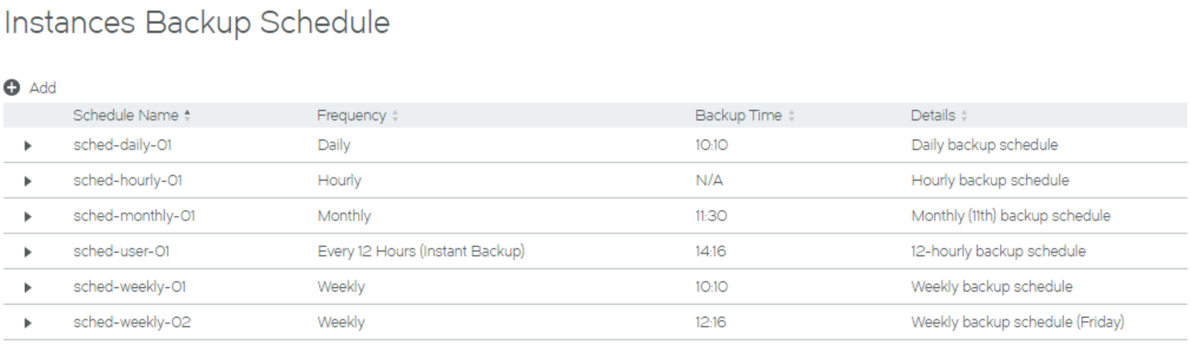
Also, you can upload a cluster backup to any vTM known to the Services Director, refer to Uploading a Cluster Backup to a Traffic Manager on page 172. The uploaded configuration file is stored by the vTM, but not restored. This enables you to perform additional analysis and comparison using the Virtual Traffic Manager's graphical user interface.

Creating a Cluster Backup Schedule

A cluster backup schedule is a definition of when a cluster backup will be created. This includes general frequency (hourly, daily, weekly, monthly, and instant backups) and information to specify an exact backup time.

Defined schedules are displayed in the **Instances Backup Schedule** page. For example:

FIGURE 144 The Instances Backup Schedule Page



Instances Backup Schedule

	Schedule Name	Frequency	Backup Time	Details
▸	sched-daily-01	Daily	10:10	Daily backup schedule
▸	sched-hourly-01	Hourly	N/A	Hourly backup schedule
▸	sched-monthly-01	Monthly	11:30	Monthly (11th) backup schedule
▸	sched-user-01	Every 12 Hours (Instant Backup)	14:16	12-hourly backup schedule
▸	sched-weekly-01	Weekly	10:10	Weekly backup schedule
▸	sched-weekly-02	Weekly	12:16	Weekly backup schedule (Friday)

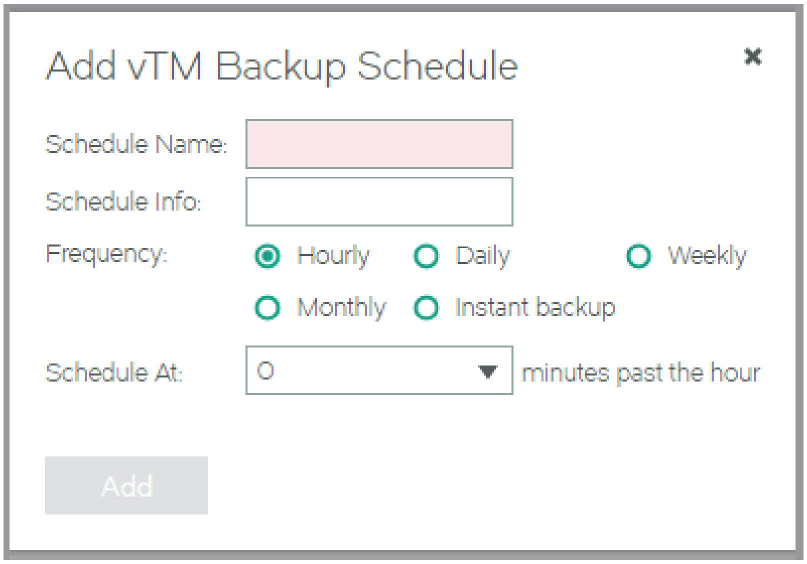
Once you have created a schedule, it can be applied to any clusters that require the specified backup schedule, refer to Adding a Backup Schedule to a Cluster on page 161.

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.
3. Click the **Services** menu, and then click **Services Director: vTM Backup Schedules**. The **Instances Backup Schedule** page appears.

4. Click the plus sign above the table of backup schedules.

   The **Add vTM Backup Schedule** dialog box appears.

   FIGURE 145 Creating a Cluster Backup Schedule

   Add vTM Backup Schedule ✖

   Schedule Name:

   Schedule Info:

   Frequency: ● Hourly ○ Daily ○ Weekly ○ Monthly ○ Instant backup

   Schedule At: 0 ▼ minutes past the hour

5. Specify the required **Schedule Name** for the backup schedule.
6. (Optional) Enter a description for the backup schedule as its **Schedule Info**.

   NOTE

   This will be displayed as **Details** in the table of schedules.

7. Select the required **Frequency** for the backup schedule:
   - **Hourly** - this schedule will be performed once every hour. By default, this is on the hour. You can also choose to **Schedule At** 15, 30 and 45 minutes past the hour.
   - **Daily** - this schedule will be performed once per day. By default, this is at midnight. Alternatively, you choose to **Schedule At** a specific time (hh:mm).
   - **Weekly** - this schedule will be performed once per week. By default, this is on Monday at midnight. Alternatively, you choose to **Schedule On** the required day (Monday - Sunday) and **Schedule At** a specific time (hh:mm).
   - **Monthly** - this schedule will be performed once per month. By default, this is on Monday at midnight. Alternatively, you choose to **Schedule On** the required day (typically, 1-28) and **Schedule At** a specific time (hh:mm).
   - **Instant Backup** - this schedule will be performed at a custom frequency. Instead of specifying an exact time, the first backup will be taken immediately when the schedule is applied to a cluster, and then at the defined **Schedule Every** frequency: every 15 minutes, hourly, every 12 hours, every week, every month).
8. Click **Add**.

   The new schedule is added to the table of backup schedules.

   Once you have created a schedule, it can be applied to any clusters that require the specified backup schedule, refer to Adding a Backup Schedule to a Cluster on page 161.

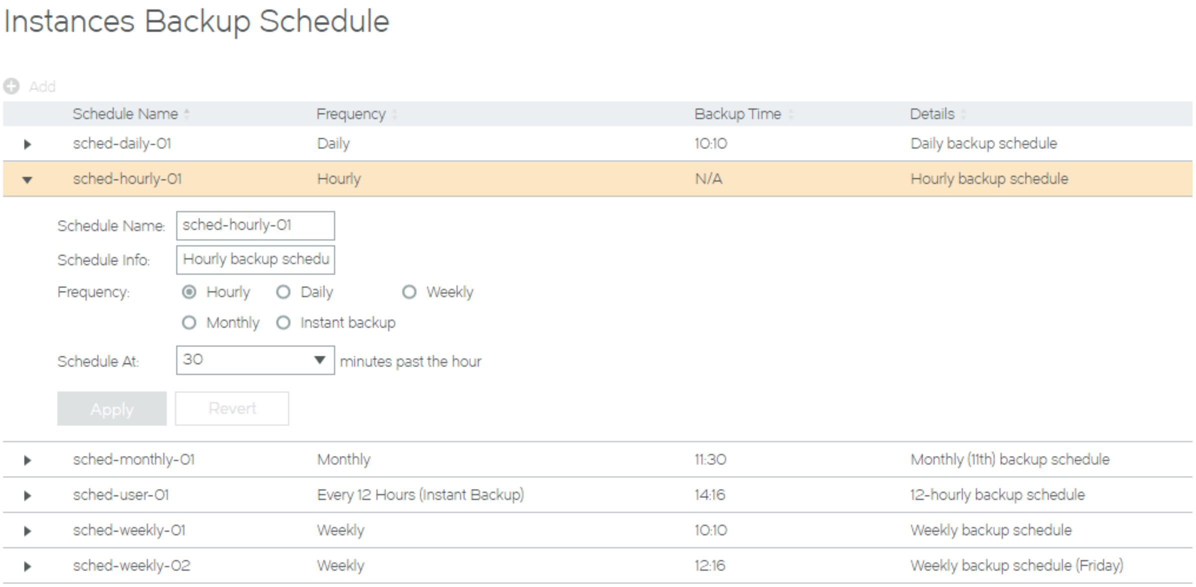
Updating a Cluster Backup Schedule

Once a cluster backup schedule is created, you can change it at any time. The schedule can be renamed, and any of the schedule details can be changed.

Any cluster that uses the backup schedule will automatically make use of the revised updated schedule.

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.
3. Click the **Services** menu, and then click **Services Director: vTM Backup Schedules**. The **Instances Backup Schedule** page appears.
4. Expand the required cluster backup schedule. For example:

FIGURE 146 Updating a Cluster Backup Schedule



Instances Backup Schedule

	Schedule Name	Frequency	Backup Time	Details
▸	sched-daily-01	Daily	10:10	Daily backup schedule
▾	sched-hourly-01	Hourly	N/A	Hourly backup schedule

Schedule Name: sched-hourly-01

Schedule Info: Hourly backup schedu

Frequency: ● Hourly ○ Daily ○ Weekly ○ Monthly ○ Instant backup

Schedule At: 30 ▼ minutes past the hour

	Schedule Name	Frequency	Backup Time	Details
▸	sched-monthly-01	Monthly	11:30	Monthly (11th) backup schedule
▸	sched-user-01	Every 12 Hours (Instant Backup)	14:16	12-hourly backup schedule
▸	sched-weekly-01	Weekly	10:10	Weekly backup schedule
▸	sched-weekly-02	Weekly	12:16	Weekly backup schedule (Friday)

5. (Optional) Specify a new **Schedule Name** for the backup schedule.
6. (Optional) Enter a new description for the backup schedule as its **Schedule Info**.

NOTE
This will be displayed as **Details** in the table of schedules.

7. (Optional) Select a new **Frequency** for the backup schedule:
   - **Hourly** - this schedule will be performed once every hour. By default, this is on the hour. You can also choose to **Schedule At** 15, 30 and 45 minutes past the hour.
   - **Daily** - this schedule will be performed once per day. By default, this is at midnight. Alternatively, you choose to **Schedule At** a specific time (hh:mm).
   - **Weekly** - this schedule will be performed once per week. By default, this is on Monday at midnight. Alternatively, you choose to **Schedule On** the required day (Monday - Sunday) and **Schedule At** a specific time (hh:mm).
   - **Monthly** - this schedule will be performed once per month. By default, this is on Monday at midnight. Alternatively, you choose to **Schedule On** the required day (typically, 1-28) and **Schedule At** a specific time (hh:mm).
   - **Instant Backup** - this schedule will be performed at a custom frequency. Instead of specifying an exact time, the first backup will be taken immediately when the schedule is applied to a cluster, and then at the defined **Schedule Every** frequency: every 15 minutes, hourly, every 12 hours, every week, every month).

     NOTE
     If your **Schedule Name** and **Schedule Info** include references to the Frequency, remember to update these also.

8. Click **Apply**.
   The schedule is updated in the table of backup schedules.

   NOTE
   Any cluster that uses the backup schedule will automatically make use of the revised updated schedule.

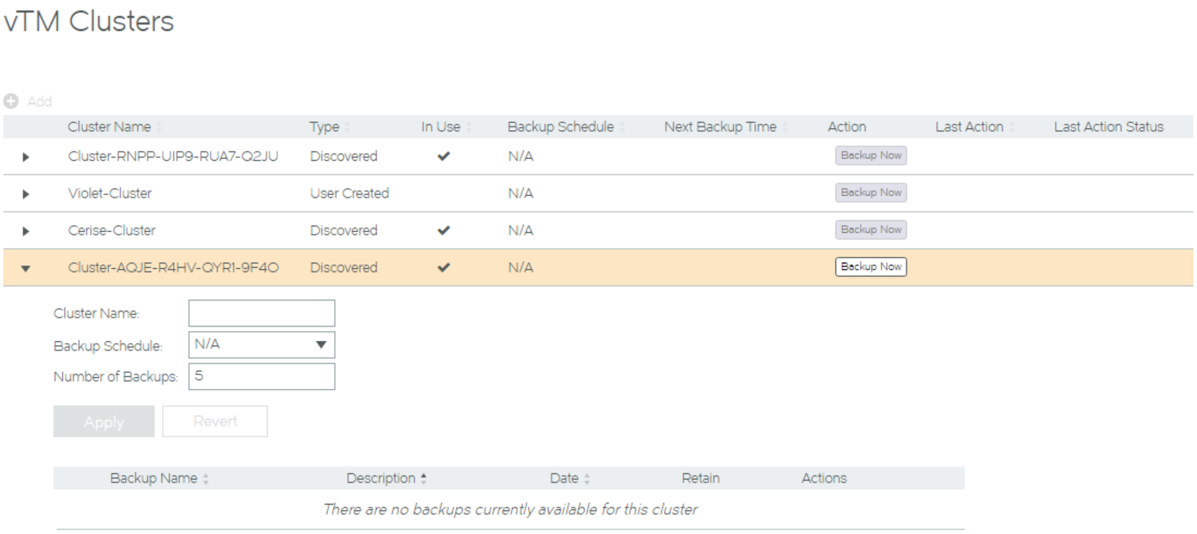
Adding a Backup Schedule to a Cluster

Once you have created a cluster backup schedule (refer to Creating a Cluster Backup Schedule on page 158), it can be applied to one or more clusters. This ensures that the required cluster backup schedule is performed for all of those clusters.

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.
3. Click the **Services** menu, and then click **Services Director: vTM Clusters**. The **vTM Clusters** page appears.

4. Expand the required cluster.

FIGURE 147 Cluster Without Backup Schedule



vTM Clusters

	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status
▸	Cluster-RNPP-UIP9-RUA7-Q2JU	Discovered	✓	N/A		Backup Now		
▸	Violet-Cluster	User Created		N/A		Backup Now		
▸	Cerise-Cluster	Discovered	✓	N/A		Backup Now		
▾	Cluster-AQJE-R4HV-QYRI-9F4O	Discovered	✓	N/A		Backup Now		

Cluster Name:

Backup Schedule: N/A

Number of Backups: 5

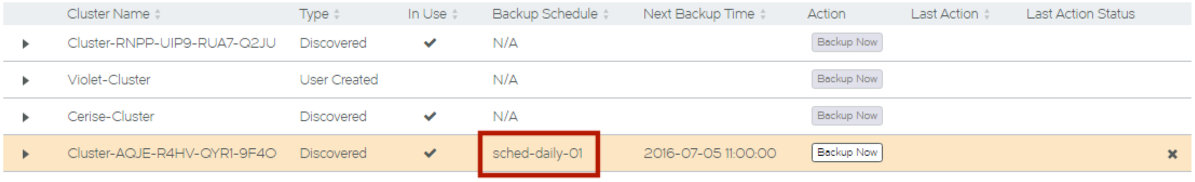
Backup Name	Description	Date	Retain	Actions
There are no backups currently available for this cluster				

5. Select the required **Backup Schedule**.
6. Specify the required **Number of Backups**. The default is 5.

   NOTE
   Retained backups are not included in this number. Refer to Overview: Cluster Backups on page 157.

7. Click **Apply**.
   The required backup schedule is added to the cluster.

FIGURE 148 Cluster With Backup Schedule Added



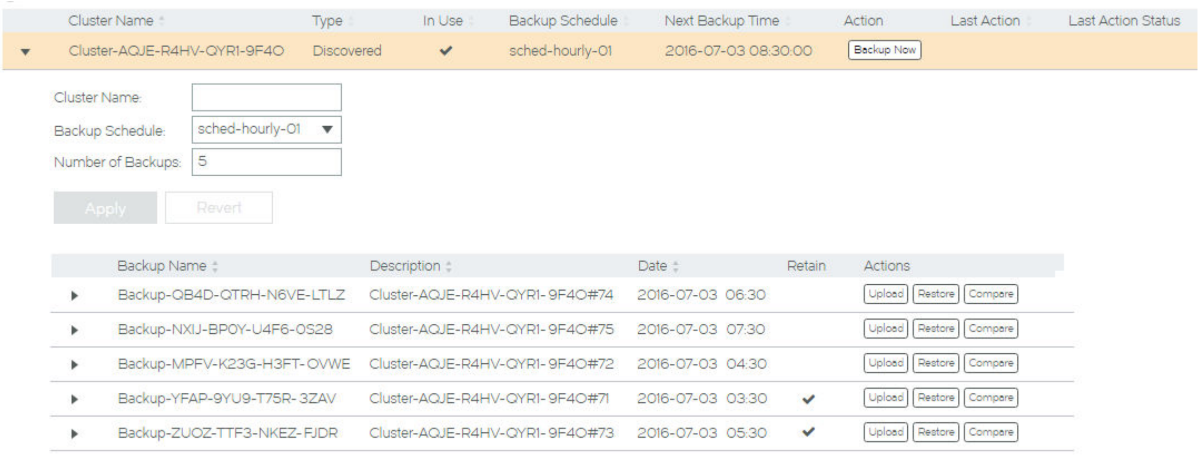
	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status
▸	Cluster-RNPP-UIP9-RUA7-Q2JU	Discovered	✓	N/A		Backup Now		
▸	Violet-Cluster	User Created		N/A		Backup Now		
▸	Cerise-Cluster	Discovered	✓	N/A		Backup Now		
▸	Cluster-AQJE-R4HV-QYRI-9F4O	Discovered	✓	sched-daily-01	2016-07-05 11:00:00	Backup Now		✖

Viewing Backups for a Cluster

Once you have added a backup schedule to a cluster (refer to Adding a Backup Schedule to a Cluster on page 161), backups will begin to accumulate.

Backups are listed in the detailed view of the cluster. For example:

FIGURE 149 Cluster With Backup Schedule and Backups



	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status
▼	Cluster-AQJE-R4HV-QYR1-9F4O	Discovered	✓	sched-hourly-01	2016-07-03 08:30:00	Backup Now		

Cluster Name:

Backup Schedule: sched-hourly-01

Number of Backups: 5

Apply Revert

	Backup Name	Description	Date	Retain	Actions
▶	Backup-QB4D-QTRH-N6VE-LTLZ	Cluster-AQJE-R4HV-QYR1-9F4O#74	2016-07-03 06:30		Upload Restore Compare
▶	Backup-NXIJ-BP0Y-U4F6-0S28	Cluster-AQJE-R4HV-QYR1-9F4O#75	2016-07-03 07:30		Upload Restore Compare
▶	Backup-MPFV-K23G-H3FT-OVWE	Cluster-AQJE-R4HV-QYR1-9F4O#72	2016-07-03 04:30		Upload Restore Compare
▶	Backup-YFAP-9YU9-T75R-3ZAV	Cluster-AQJE-R4HV-QYR1-9F4O#71	2016-07-03 03:30	✓	Upload Restore Compare
▶	Backup-ZUOZ-TTF3-NKEZ-FJDR	Cluster-AQJE-R4HV-QYR1-9F4O#73	2016-07-03 05:30	✓	Upload Restore Compare

In this cluster:

- The cluster **Type** is *Discovered*. Refer to Understanding Traffic Manager Cluster Details on page 150.
- The cluster is **In Use**. That is, the cluster contains one or more Virtual Traffic Managers (vTMs).

  NOTE
  When a cluster is not **In Use**, you can delete it, refer to Deleting an Empty Traffic Manager Cluster on page 177.

- The **Next Backup Time** for the cluster is displayed.
- The **Backup** button in the **Action** column enables you to take an immediate backup without disrupting the schedule. Refer to Performing an Immediate Backup for a Cluster on page 165.
- There is a **Backup Schedule** in use on this cluster: *sched-hourly-01*
- The maximum **Number of Backups** is 5.
- The cluster contains the three most recent backups, plus two backups that have been *retained* for future use. The retained backup will not be replaced by the addition of newer cluster backups. Refer to Overview: Cluster Backups on page 157.

For each listed backup file:

- The default **Description** for a cluster backup is the cluster name plus a sequence number. You can update this if required, along with other details, refer to Updating Details for a Cluster Backup on page 164.
- You can compare any backup to any other backup using the **Compare** button in the **Actions** column. Refer to Comparing Two Cluster Backups on page 167.
- You can restore any of the backups to this (or another) cluster using the **Restore** button in the **Actions** column. Refer to Restoring a Backup to a Cluster on page 169.
- You can upload any of the backups to any vTM. The vTM can be either inside or outside the cluster. You can then compare the cluster backup to either a running cluster configuration, or to another cluster backup on that vTM. Refer to Uploading a Cluster Backup to a Traffic Manager on page 172.

To update details for a cluster backup, refer to Updating Details for a Cluster Backup on page 164.

Updating Details for a Cluster Backup

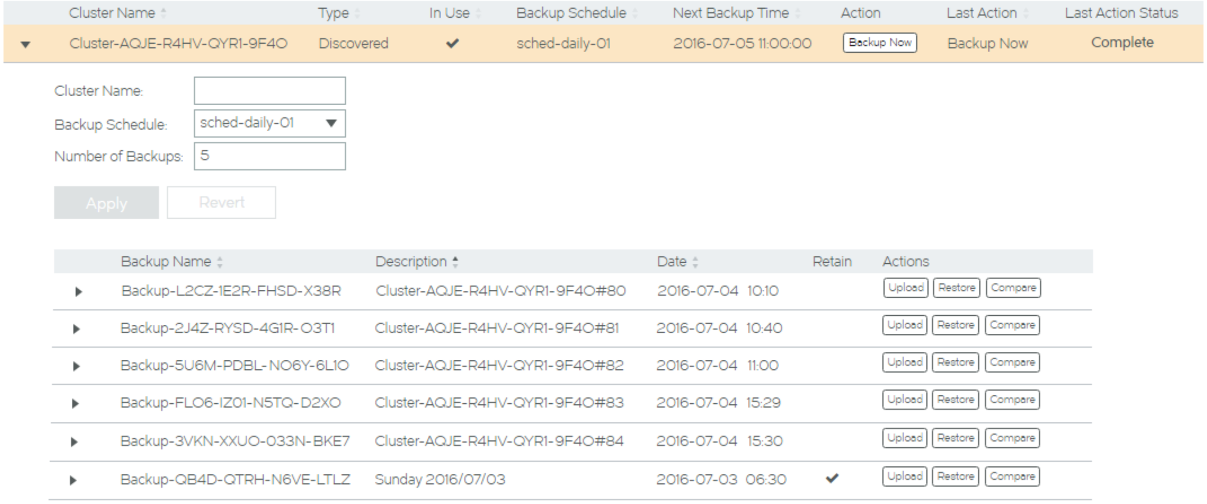
Each cluster that has an assigned backup schedule will accumulate backups over time. These backups are displayed in the detailed view of a cluster on the **vTM Clusters** page.

You cannot change the **Backup Name**, but you can update the **Description** to provide memorable information. This is useful when you choose to **Retain** a backup. Refer to Overview: Cluster Backups on page 157.

You update details for a cluster backup from the **vTM Clusters** page.

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.
3. Click the **Services** menu, and then click **Services Director: vTM Clusters**. The **vTM Clusters** page appears.
4. Expand the required cluster.

FIGURE 150 Viewing Backups for a Cluster



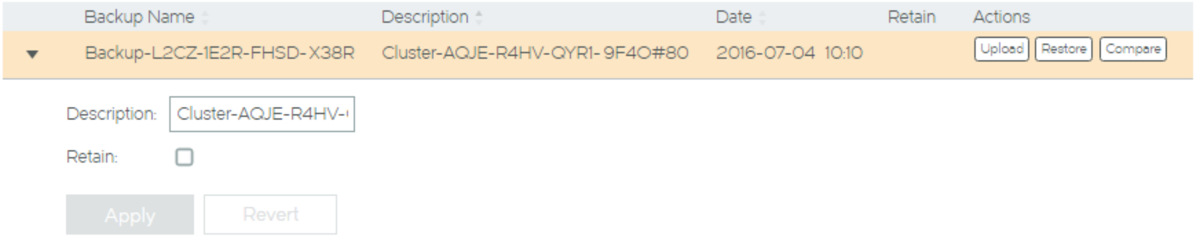
	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status
▼	Cluster-AQJE-R4HV-QYR1-9F4O	Discovered	✓	sched-daily-01	2016-07-05 11:00:00	Backup Now	Backup Now	Complete

Cluster Name:	
Backup Schedule:	sched-daily-01
Number of Backups:	5

	Backup Name	Description	Date	Retain	Actions
▶	Backup-L2CZ-1E2R-FHSD-X38R	Cluster-AQJE-R4HV-QYR1-9F4O#80	2016-07-04 10:10		Upload Restore Compare
▶	Backup-2J4Z-RYSD-4G1R-O3T1	Cluster-AQJE-R4HV-QYR1-9F4O#81	2016-07-04 10:40		Upload Restore Compare
▶	Backup-5U6M-PDBL-NO6Y-6L1O	Cluster-AQJE-R4HV-QYR1-9F4O#82	2016-07-04 11:00		Upload Restore Compare
▶	Backup-FLO6-IZ01-N5TQ-D2XO	Cluster-AQJE-R4HV-QYR1-9F4O#83	2016-07-04 15:29		Upload Restore Compare
▶	Backup-3VKN-XXUO-033N-BKE7	Cluster-AQJE-R4HV-QYR1-9F4O#84	2016-07-04 15:30		Upload Restore Compare
▶	Backup-QB4D-QTRH-N6VE-LTLZ	Sunday 2016/07/03	2016-07-03 06:30	✓	Upload Restore Compare

5. Expand the required backup. For example:

FIGURE 151 Updating Details for a Cluster Backup



	Backup Name	Description	Date	Retain	Actions
▼	Backup-L2CZ-1E2R-FHSD-X38R	Cluster-AQJE-R4HV-QYR1-9F4O#80	2016-07-04 10:10		Upload Restore Compare

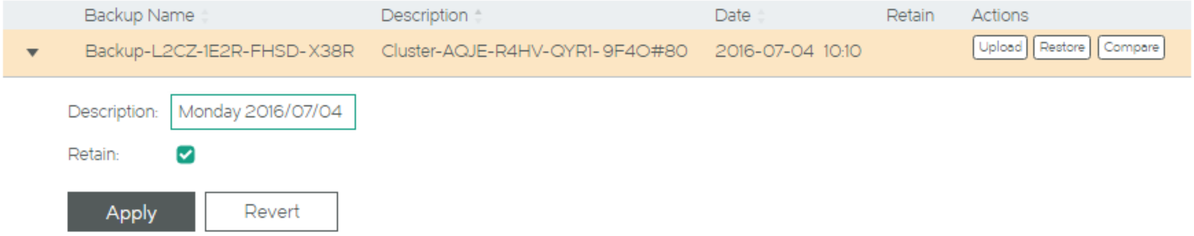
Description:	Cluster-AQJE-R4HV-‹
Retain:	□

6. Update the details for the backup as required:
   - (Optional) Enter a new **Description**.
   - (Optional) Select the **Retain** check box.

     NOTE
     When a backup is *retained*, it is not deleted as newer backups are created, and does not count towards the number of backups stored by the cluster. Refer to the **Number of Backups** in step 4 and also Overview: Cluster Backups on page 157.

   For example:

   FIGURE 152 Example: Updating Details for a Cluster Backup



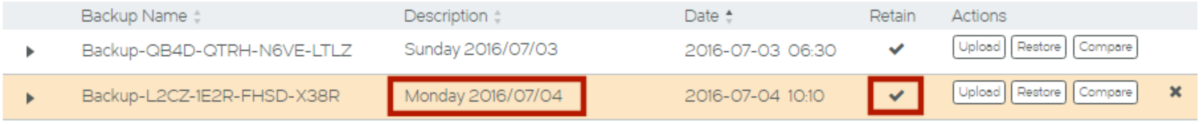
	Backup Name	Description	Date	Retain	Actions
▼	Backup-L2CZ-1E2R-FHSD-X38R	Cluster-AQJE-R4HV-QYR1-9F4O#80	2016-07-04 10:10		Upload Restore Compare

Description: Monday 2016/07/04

Retain: ☑

7. Click **Apply**.
   The table of backups updates to reflect the changes.

   FIGURE 153 Example: Updated Cluster Backup



	Backup Name	Description	Date	Retain	Actions	
▶	Backup-QB4D-QTRH-N6VE-LTLZ	Sunday 2016/07/03	2016-07-03 06:30	✓	Upload Restore Compare	
▶	Backup-L2CZ-1E2R-FHSD-X38R	Monday 2016/07/04	2016-07-04 10:10	✓	Upload Restore Compare	✖

Performing an Immediate Backup for a Cluster

When a cluster has an assigned backup schedule, over time it accumulates backups automatically.

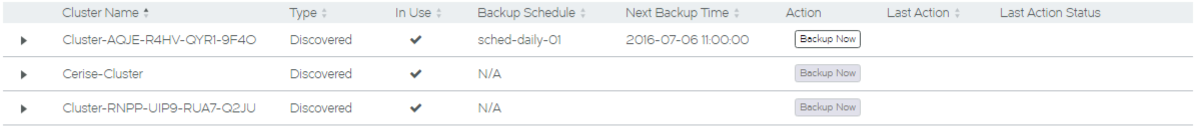
However, you can also create a cluster backup at any time as an immediate manual operation.

Performing an Immediate Backup

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.

3. Click the **Services** menu, and then click **Services Director: vTM Clusters**. The **vTM Clusters** page appears.

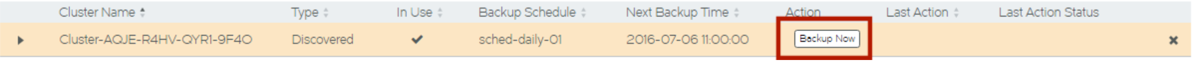
FIGURE 154 Immediate Backup: Table of Clusters



	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status
▸	Cluster-AQJE-R4HV-QYR1-9F4O	Discovered	✓	sched-daily-01	2016-07-06 11:00:00	Backup Now		
▸	Cerise-Cluster	Discovered	✓	N/A		Backup Now		
▸	Cluster-RNPP-UIP9-RUA7-Q2JU	Discovered	✓	N/A		Backup Now		

4. Locate the required cluster and click the **Backup Now** button for its entry.

FIGURE 155 Immediate Backup: Starting the Operation

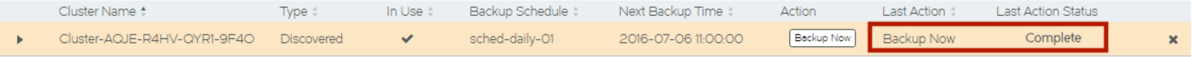


	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status	
▸	Cluster-AQJE-R4HV-QYR1-9F4O	Discovered	✓	sched-daily-01	2016-07-06 11:00:00	Backup Now			×

The Services Director attempts an immediate backup, and indicates this.

If the immediate backup succeeds, the **Last Action** and **Last Action Status** columns are updated as follows:

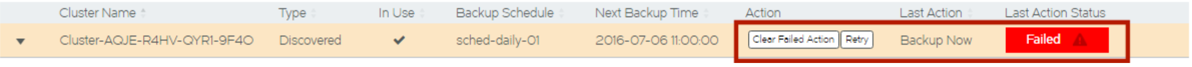
FIGURE 156 Immediate Backup: Success



	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status	
▸	Cluster-AQJE-R4HV-QYR1-9F4O	Discovered	✓	sched-daily-01	2016-07-06 11:00:00	Backup Now	Backup Now	Complete	×

If the immediate backup fails, the **Action**, **Last Action** and **Last Action Status** columns are updated as follows:

FIGURE 157 Immediate Backup: Failure



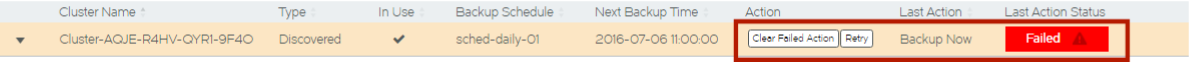
	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status
▾	Cluster-AQJE-R4HV-QYR1-9F4O	Discovered	✓	sched-daily-01	2016-07-06 11:00:00	Clear Failed Action Retry	Backup Now	Failed ⚠

To re-attempt a failed immediate backup, refer to Retrying An Immediate Backup After a Failure on page 166.

Retrying An Immediate Backup After a Failure

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.
3. Click the **Services** menu, and then click **Services Director: vTM Clusters**. The **vTM Clusters** page appears.
4. Locate the required cluster. Any cluster with an immediate backup failure will show the **Action**, **Last Action** and **Last Action Status** columns as follows:

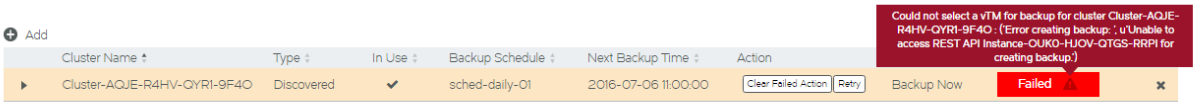
FIGURE 158 Immediate Backup: Failed Immediate Backup



	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status
▾	Cluster-AQJE-R4HV-QYR1-9F4O	Discovered	✓	sched-daily-01	2016-07-06 11:00:00	Clear Failed Action Retry	Backup Now	Failed ⚠

5. Pause the pointer over the Failure warning triangle to view more information about the failure. For example:

   FIGURE 159 Immediate Backup: Failed Immediate Backup Reason



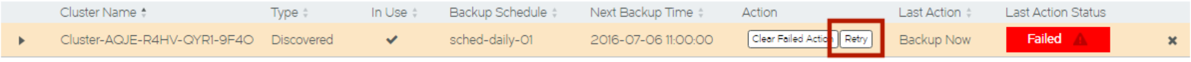
Could not select a vTM for backup for cluster Cluster-AQJE-R4HV-QYR1-9F4O : ('Error creating backup: ', u'Unable to access REST API Instance-OUK0-HJOV-QTGS-RRPI for creating backup.')

⊕ Add

	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action			
▸	Cluster-AQJE-R4HV-QYR1-9F4O	Discovered	✓	sched-daily-01	2016-07-06 11:00:00	Clear Failed Action Retry	Backup Now	Failed ⚠	✖

6. Investigate and resolve the issue. This may require you to log in to one of the vTMs in the cluster. Refer to the Virtual Traffic Manager documentation for details of vTM operations.
7. (Optional) Click the **Clear Failed Action** button for the cluster.
   This action clears the **Last Action** and **Last Action Status** columns before you re-attempt the immediate backup. It is not required.
8. Once the issue is resolved, click the **Retry** button for the cluster:

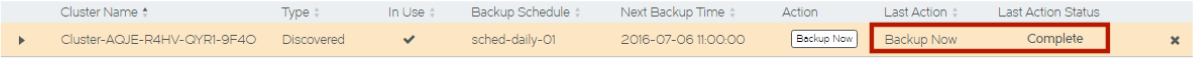
   FIGURE 160 Immediate Backup: Retrying an Immediate Backup



	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status	
▸	Cluster-AQJE-R4HV-QYR1-9F4O	Discovered	✓	sched-daily-01	2016-07-06 11:00:00	Clear Failed Actio Retry	Backup Now	Failed ⚠	✖

   If the immediate backup succeeds, the failure is cleared, and the status becomes Complete:

   FIGURE 161 Immediate Backup: Success



	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status	
▸	Cluster-AQJE-R4HV-QYR1-9F4O	Discovered	✓	sched-daily-01	2016-07-06 11:00:00	Backup Now	Backup Now	Complete	✖

   If the immediate backup fails again, repeat this procedure from step 5.

Comparing Two Cluster Backups

When a cluster has an assigned backup schedule, over time it accumulates backups. Before choosing a cluster backup from which to perform a restore, it may be useful to compare two backups from the same cluster.

The resulting differences are grouped by resource type and individual resource differences.

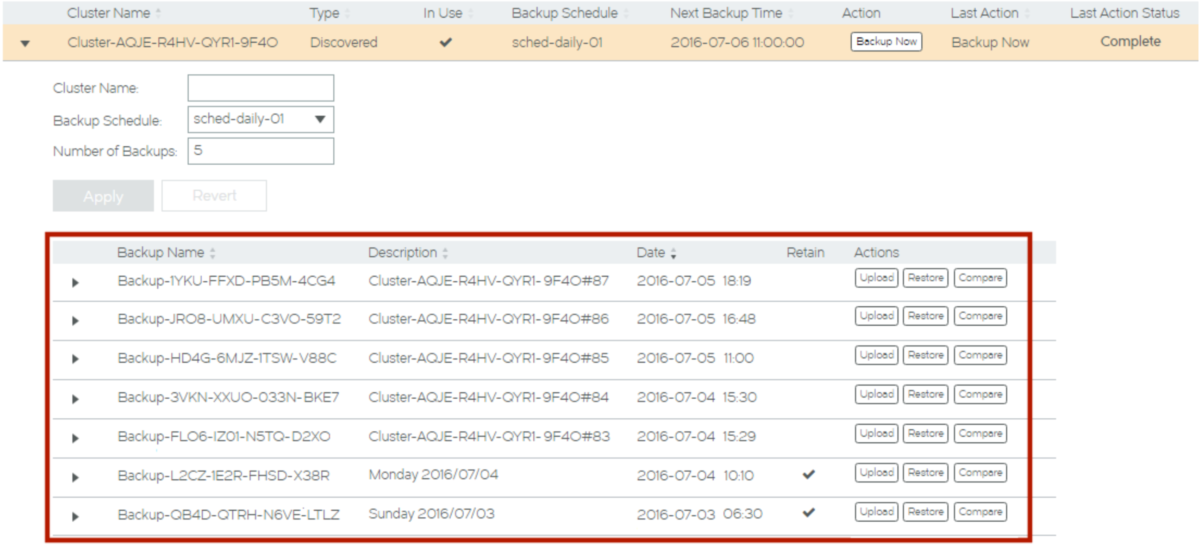
Analysing the differences between cluster backups supports you making an informed decision about which backup is required for a given situation.

NOTE
You are also able to upload a cluster backup file to a vTM, so that you can compare it to either a running cluster configuration, or to another backup on that vTM. Refer to Uploading a Cluster Backup to a Traffic Manager on page 172.

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.
3. Click the **Services** menu, and then click **Services Director: vTM Clusters**. The **vTM Clusters** page appears.

4. Expand the required cluster. The backups taken for the cluster are listed. For example:

FIGURE 162 Comparing Two Cluster Backups



	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status
▾	Cluster-AQJE-R4HV-QYR1-9F4O	Discovered	✓	sched-daily-01	2016-07-06 11:00:00	Backup Now	Backup Now	Complete

Cluster Name:

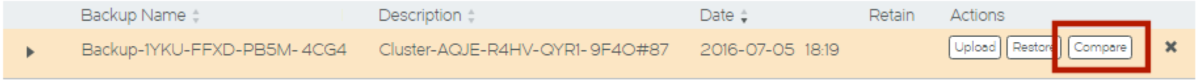
Backup Schedule: sched-daily-01

Number of Backups: 5

	Backup Name	Description	Date	Retain	Actions
▸	Backup-1YKU-FFXD-PB5M-4CG4	Cluster-AQJE-R4HV-QYR1-9F4O#87	2016-07-05 18:19		Upload Restore Compare
▸	Backup-JRO8-UMXU-C3VO-59T2	Cluster-AQJE-R4HV-QYR1-9F4O#86	2016-07-05 16:48		Upload Restore Compare
▸	Backup-HD4G-6MJZ-1TSW-V88C	Cluster-AQJE-R4HV-QYR1-9F4O#85	2016-07-05 11:00		Upload Restore Compare
▸	Backup-3VKN-XXUO-033N-BKE7	Cluster-AQJE-R4HV-QYR1-9F4O#84	2016-07-04 15:30		Upload Restore Compare
▸	Backup-FLO6-IZ01-N5TQ-D2XO	Cluster-AQJE-R4HV-QYR1-9F4O#83	2016-07-04 15:29		Upload Restore Compare
▸	Backup-L2CZ-1E2R-FHSD-X38R	Monday 2016/07/04	2016-07-04 10:10	✓	Upload Restore Compare
▸	Backup-QB4D-QTRH-N6VE-LTLZ	Sunday 2016/07/03	2016-07-03 06:30	✓	Upload Restore Compare

5. Identify the first backup for the comparison and click its **Compare** button.

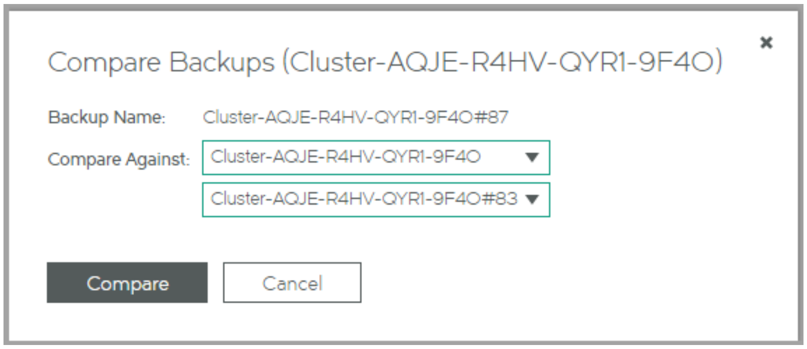
FIGURE 163 Identifying the First Backup



	Backup Name	Description	Date	Retain	Actions
▸	Backup-1YKU-FFXD-PB5M-4CG4	Cluster-AQJE-R4HV-QYR1-9F4O#87	2016-07-05 18:19		Upload Restore Compare ✖

The **Compare Backups (<cluster_id>)** dialog box appears. For example:

FIGURE 164 Selecting the Second Backup



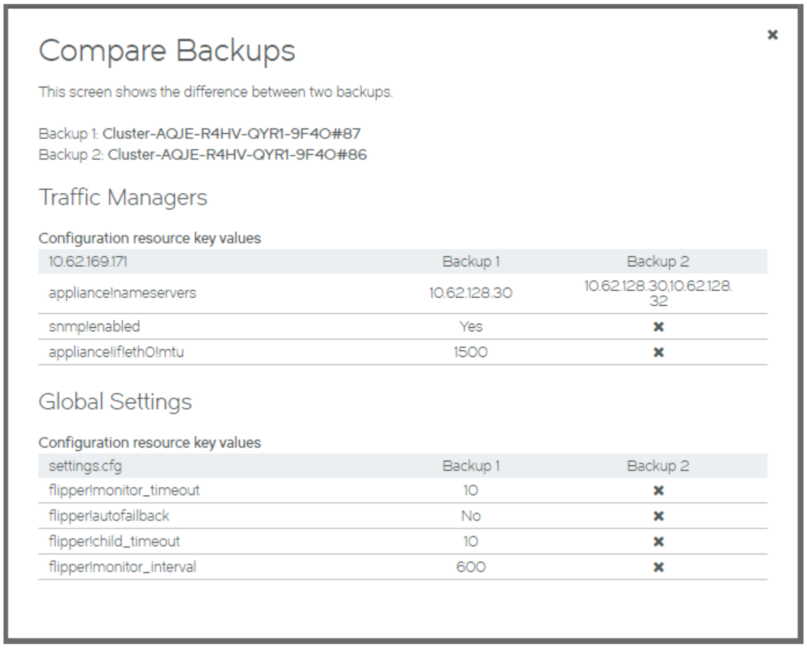
Compare Backups (Cluster-AQJE-R4HV-QYR1-9F4O)

Backup Name: Cluster-AQJE-R4HV-QYR1-9F4O#87

Compare Against: Cluster-AQJE-R4HV-QYR1-9F4O
Cluster-AQJE-R4HV-QYR1-9F4O#83

6. Select the required **Compare Against** values to identify the second backup:
   - The top **Compare Against** field lists all clusters known to the Services Director. Select the current cluster (the default) or a different cluster.
   - The bottom **Compare Against** field lists all backups within the selected cluster. Select the required backup for the comparison.
7. Click **Compare** to perform a comparison of the two backups.
   The **Compare Backups** dialog box displays the results of the comparison. For example:

FIGURE 165 Results of the Backup Comparison



Compare Backups

This screen shows the difference between two backups.

Backup 1: Cluster-AQJE-R4HV-QYR1-9F4O#87
Backup 2: Cluster-AQJE-R4HV-QYR1-9F4O#86

Traffic Managers

Configuration resource key values

10.62.169.171	Backup 1	Backup 2
appliance!nameservers	10.62.128.30	10.62.128.30,10.62.128.32
snmp!enabled	Yes	✖
appliance!if!eth0!mtu	1500	✖

Global Settings

Configuration resource key values

settings.cfg	Backup 1	Backup 2
flipper!monitor_timeout	10	✖
flipper!autofailback	No	✖
flipper!child_timeout	10	✖
flipper!monitor_interval	600	✖

Backup 1 and **Backup 2** identify settings that have changed between the two backups.

Refer to the Virtual Traffic Manager documentation for details of these settings.

Restoring a Backup to a Cluster

At any point, you can restore the configuration of a cluster from a cluster backup.

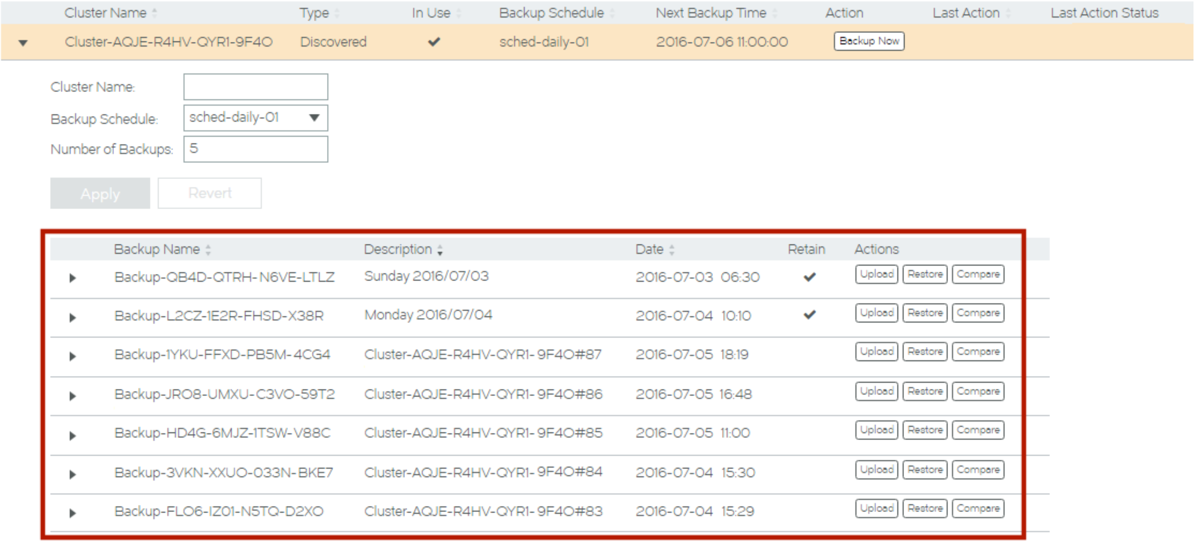
Typically, the backup will be one that was generated for the cluster. However, it is possible to restore a backup from any cluster to any other cluster.

Restoring a Cluster Backup

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.
3. Click the **Services** menu, and then click **Services Director: vTM Clusters**. The **vTM Clusters** page appears.

4. Expand the required cluster to view its accumulated backups. For example:

FIGURE 166 Viewing Accumulated Backups for a Cluster



	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status
▼	Cluster-AQJE-R4HV-QYR1-9F4O	Discovered	✓	sched-daily-01	2016-07-06 11:00:00	Backup Now		

Cluster Name:

Backup Schedule: sched-daily-01

Number of Backups: 5

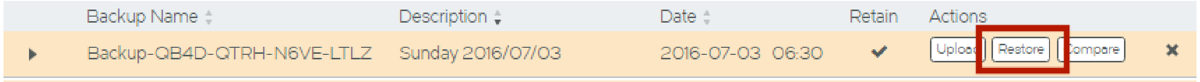
	Backup Name	Description	Date	Retain	Actions
▶	Backup-QB4D-QTRH-N6VE-LTLZ	Sunday 2016/07/03	2016-07-03 06:30	✓	Upload Restore Compare
▶	Backup-L2CZ-1E2R-FHSD-X38R	Monday 2016/07/04	2016-07-04 10:10	✓	Upload Restore Compare
▶	Backup-1YKU-FFXD-PB5M-4CG4	Cluster-AQJE-R4HV-QYR1- 9F4O#87	2016-07-05 18:19		Upload Restore Compare
▶	Backup-JRO8-UMXU-C3VO-59T2	Cluster-AQJE-R4HV-QYR1- 9F4O#86	2016-07-05 16:48		Upload Restore Compare
▶	Backup-HD4G-6MJZ-1TSW-V88C	Cluster-AQJE-R4HV-QYR1- 9F4O#85	2016-07-05 11:00		Upload Restore Compare
▶	Backup-3VKN-XXUO-033N-BKE7	Cluster-AQJE-R4HV-QYR1- 9F4O#84	2016-07-04 15:30		Upload Restore Compare
▶	Backup-FLO6-IZ01-N5TQ-D2XO	Cluster-AQJE-R4HV-QYR1- 9F4O#83	2016-07-04 15:29		Upload Restore Compare

5. Locate the required backup. This can be any of the listed cluster backups: scheduled, immediate or retained.

   NOTE
   If you are unsure which is required, you can compare any two backups to identify the differences, refer to Comparing Two Cluster Backups on page 167.

6. Click the **Restore** button for the required backup.

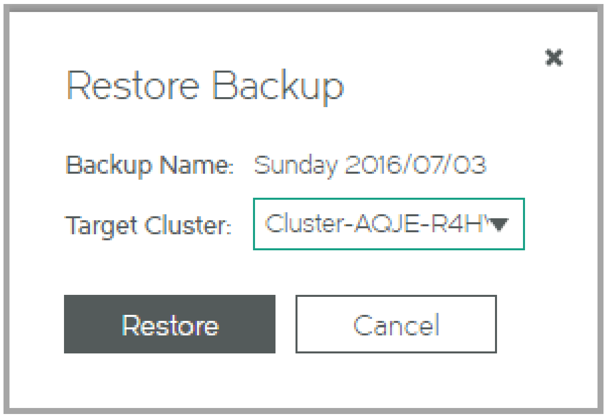
FIGURE 167 Starting a Restore from a Cluster Backup



	Backup Name	Description	Date	Retain	Actions	
▶	Backup-QB4D-QTRH-N6VE-LTLZ	Sunday 2016/07/03	2016-07-03 06:30	✓	Upload Restore Compare	✖

The **Restore Backup** dialog box appears.

FIGURE 168 Selecting a Target Cluster for a Restore



Restore Backup

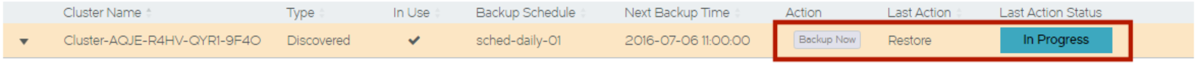
Backup Name: Sunday 2016/07/03

Target Cluster: Cluster-AQJE-R4H

7. Select the **Target Cluster** from the list of clusters known to the Services Director.
8. Click **Restore**.

The Services Director begins the restore process.

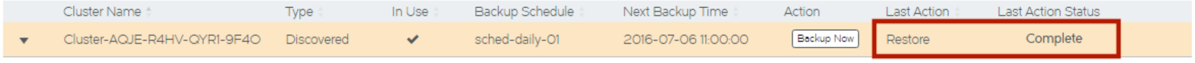
FIGURE 169 Restoring a Cluster Backup: In Progress



	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status
▼	Cluster-AQJE-R4HV-QYRI-9F4O	Discovered	✓	sched-daily-01	2016-07-06 11:00:00	Backup Now	Restore	In Progress

When this completes, the selected backup has been restored to the selected cluster.

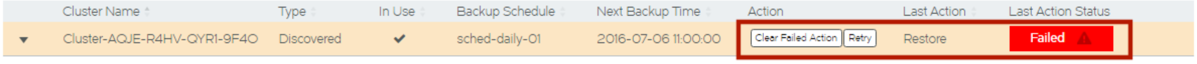
FIGURE 170 Restoring a Cluster Backup: Complete



	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status
▼	Cluster-AQJE-R4HV-QYRI-9F4O	Discovered	✓	sched-daily-01	2016-07-06 11:00:00	Backup Now	Restore	Complete

If the restore fails, the following is displayed:

FIGURE 171 Restoring a Cluster Backup: Failure



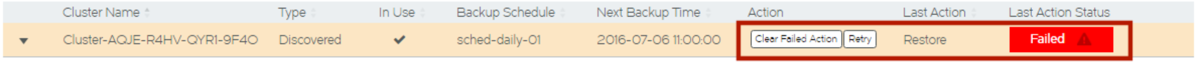
	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status
▼	Cluster-AQJE-R4HV-QYRI-9F4O	Discovered	✓	sched-daily-01	2016-07-06 11:00:00	Clear Failed Action Retry	Restore	Failed ⚠

To resolve a failed restore, refer to Retrying A Cluster Restore After a Failure on page 172.

Retrying A Cluster Restore After a Failure

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.
3. Click the **Services** menu, and then click **Services Director: vTM Clusters**. The **vTM Clusters** page appears.
4. Locate the required cluster. Any cluster with a restore failure will show the **Action**, **Last Action** and **Last Action Status** columns as follows:

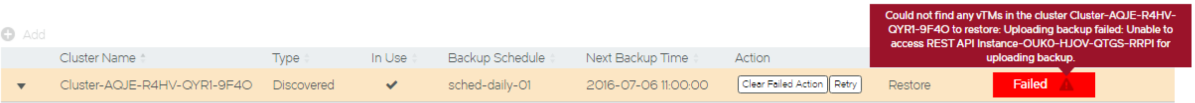
   FIGURE 172 Cluster Restore: Failure



	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status
▼	Cluster-AQJE-R4HV-QYR1-9F4O	Discovered	✓	sched-daily-01	2016-07-06 11:00:00	Clear Failed Action Retry	Restore	Failed ⚠

5. Pause the pointer over the Failure warning triangle to view more information about the failure. For example:

   FIGURE 173 Cluster Restore: Reasons For Failure

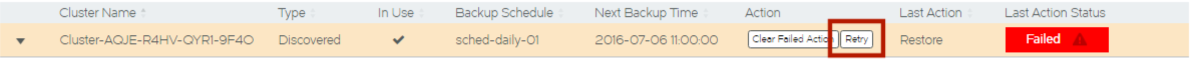


Could not find any vTMs in the cluster Cluster-AQJE-R4HV-QYR1-9F4O to restore: Uploading backup failed: Unable to access REST API Instance-OUK0-HJOV-QTGS-RRPI for uploading backup.

	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action		
▼	Cluster-AQJE-R4HV-QYR1-9F4O	Discovered	✓	sched-daily-01	2016-07-06 11:00:00	Clear Failed Action Retry	Restore	Failed ⚠

6. Investigate and resolve the issue. This may require you to log in to one of the vTMs in the cluster. Refer to the Virtual Traffic Manager documentation for details of vTM operations.
7. (Optional) Click the **Clear Failed Action** button for the cluster.
   This action clears the **Last Action** and **Last Action Status** columns before you re-attempt the cluster restore. It is not required.
8. Once the issue is resolved, click the **Retry** button for the cluster:

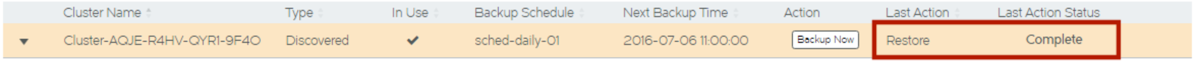
   FIGURE 174 Cluster Restore: Retrying



	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status
▼	Cluster-AQJE-R4HV-QYR1-9F4O	Discovered	✓	sched-daily-01	2016-07-06 11:00:00	Clear Failed Actio Retry	Restore	Failed ⚠

   If the restore succeeds, the failure is cleared, and the status becomes Complete:

   FIGURE 175 Cluster Restore: Success



	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status
▼	Cluster-AQJE-R4HV-QYR1-9F4O	Discovered	✓	sched-daily-01	2016-07-06 11:00:00	Backup Now	Restore	Complete

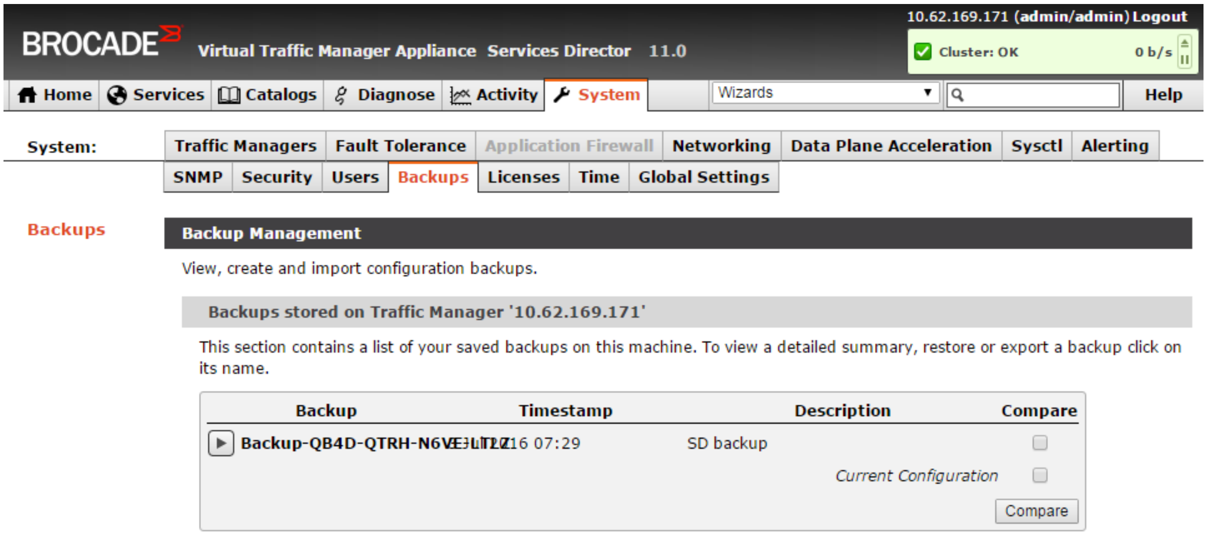
   If the restore fails again, repeat this procedure from step 5.

Uploading a Cluster Backup to a Traffic Manager

In addition to cluster backup comparisons (refer to Comparing Two Cluster Backups on page 167), you can upload a cluster backup file to a vTM. The uploaded cluster backup file is stored by the vTM, but not restored. This enables you to perform a comparison of the cluster backup with a running cluster configuration, or to another backup on the vTM.

After you have uploaded a cluster backup file, it is visible in the Virtual Traffic Manager's graphical user interface:

FIGURE 176 Viewing an Uploaded Cluster Backup in the vTM User Interface



Backup Management

View, create and import configuration backups.

Backups stored on Traffic Manager '10.62.169.171'

This section contains a list of your saved backups on this machine. To view a detailed summary, restore or export a backup click on its name.

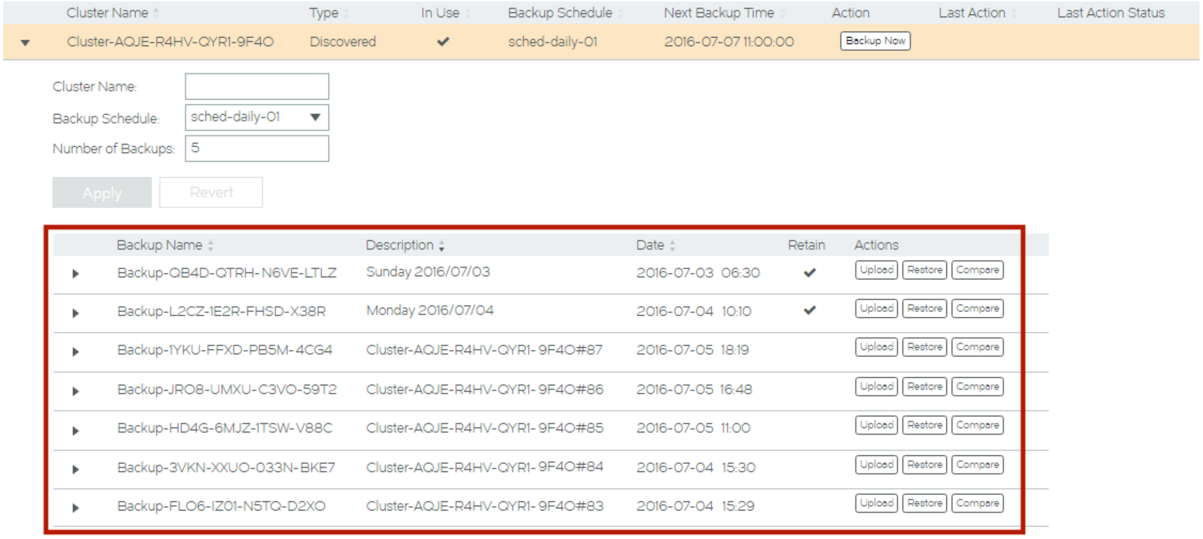
Backup	Timestamp	Description	Compare
Backup-QB4D-QTRH-N6VE-LTLZ	16 07:29	SD backup	□
		Current Configuration	□

Refer to the Virtual Traffic Manager documentation for a description of supported activities with this backup.

Uploading a Cluster Backup

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.
3. Click the **Services** menu, and then click **Services Director: vTM Clusters**. The **vTM Clusters** page appears.
4. Expand the required cluster to view its accumulated backups. For example:

FIGURE 177 Viewing Accumulated Backups for a Cluster



Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status
Cluster-AQJE-R4HV-QYR1-9F4O	Discovered	✓	sched-daily-01	2016-07-07 11:00:00	Backup Now		

Cluster Name:

Backup Schedule: sched-daily-01

Number of Backups: 5

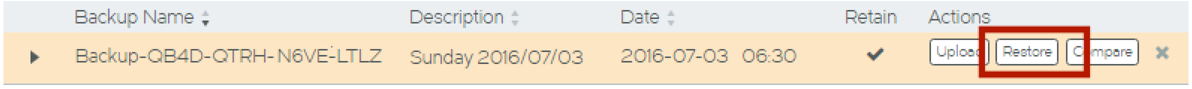
Backup Name	Description	Date	Retain	Actions
Backup-QB4D-QTRH-N6VE-LTLZ	Sunday 2016/07/03	2016-07-03 06:30	✓	Upload Restore Compare
Backup-L2CZ-1E2R-FHSD-X38R	Monday 2016/07/04	2016-07-04 10:10	✓	Upload Restore Compare
Backup-1YKU-FFXD-PB5M-4CG4	Cluster-AQJE-R4HV-QYR1- 9F4O#87	2016-07-05 18:19		Upload Restore Compare
Backup-JRO8-UMXU-C3VO-59T2	Cluster-AQJE-R4HV-QYR1- 9F4O#86	2016-07-05 16:48		Upload Restore Compare
Backup-HD4G-6MJZ-1TSW-V88C	Cluster-AQJE-R4HV-QYR1- 9F4O#85	2016-07-05 11:00		Upload Restore Compare
Backup-3VKN-XXUO-033N-BKE7	Cluster-AQJE-R4HV-QYR1- 9F4O#84	2016-07-04 15:30		Upload Restore Compare
Backup-FLO6-IZ01-N5TQ-D2XO	Cluster-AQJE-R4HV-QYR1- 9F4O#83	2016-07-04 15:29		Upload Restore Compare

5. Locate the required backup. This can be any of the listed cluster backups: scheduled, immediate or retained.

   NOTE
   If you are unsure which is required, you can compare any two backups to identify the differences, refer to Comparing Two Cluster Backups on page 167.

6. Click the **Upload** button for the required backup.

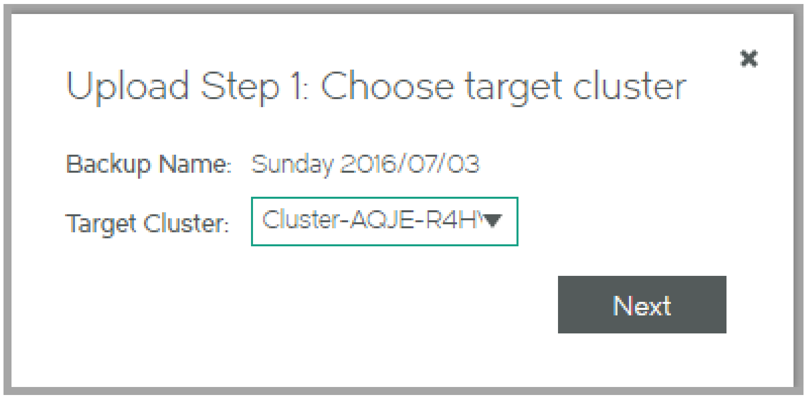
   FIGURE 178 Starting a Cluster Backup Upload

	Backup Name	Description	Date	Retain	Actions
▸	Backup-QB4D-QTRH-N6VE-LTLZ	Sunday 2016/07/03	2016-07-03 06:30	✓	Upload Restore Compare ✖

   The **Upload Step 1** dialog box appears.

   FIGURE 179 Selecting a Cluster for an Upload

   Upload Step 1: Choose target cluster

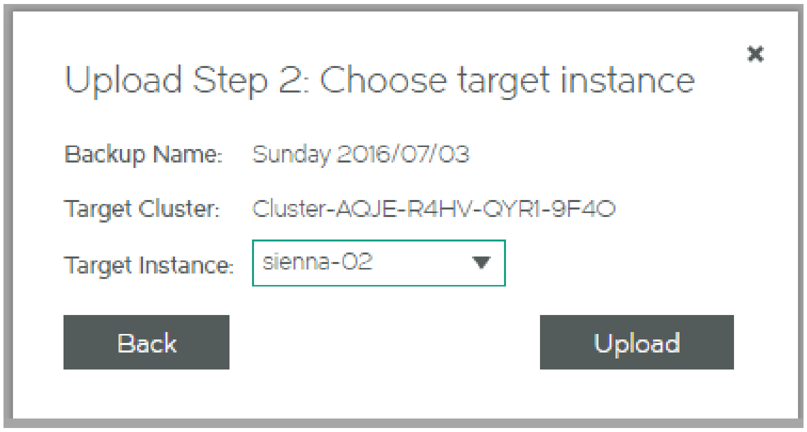
   Backup Name: Sunday 2016/07/03

   Target Cluster: Cluster-AQJE-R4H

7. Select the **Target Cluster** from the list of clusters known to the Services Director.
8. Click **Next**.

   The **Upload Step 2** dialog box appears.

   FIGURE 180 Selecting a vTM for an Upload

   Upload Step 2: Choose target instance

   Backup Name: Sunday 2016/07/03

   Target Cluster: Cluster-AQJE-R4HV-QYR1-9F4O

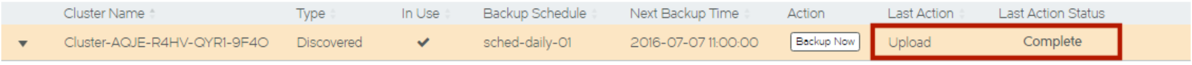
   Target Instance: sienna-02

9. Select the **Target Instance** from the list of vTMs for the cluster.

10. Click **Upload** to start the upload process.

    When this completes, the selected cluster backup has been uploaded to the selected vTM.

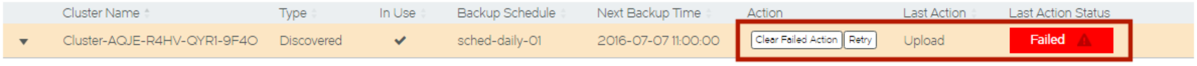
    FIGURE 181 Uploading a Cluster Backup: Complete



	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status
▾	Cluster-AQJE-R4HV-QYR1-9F4O	Discovered	✓	sched-daily-01	2016-07-07 11:00:00	Backup Now	Upload	Complete

If the upload fails, the following is displayed:

FIGURE 182 Uploading a Cluster Backup: Failure



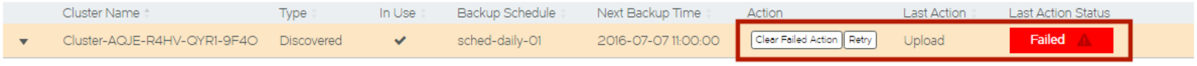
	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status
▾	Cluster-AQJE-R4HV-QYR1-9F4O	Discovered	✓	sched-daily-01	2016-07-07 11:00:00	Clear Failed Action Retry	Upload	Failed ⚠

To resolve a failed upload, refer to Retrying A Cluster Backup Upload After a Failure on page 175.

Retrying A Cluster Backup Upload After a Failure

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.
3. Click the **Services** menu, and then click **Services Director: vTM Clusters**. The **vTM Clusters** page appears.
4. Locate the required cluster. Any cluster with an upload failure will show the **Action**, **Last Action** and **Last Action Status** columns as follows:

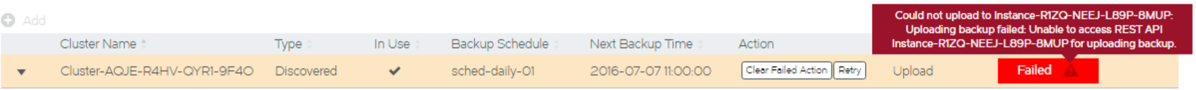
   FIGURE 183 Cluster Upload: Failure



	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status
▾	Cluster-AQJE-R4HV-QYR1-9F4O	Discovered	✓	sched-daily-01	2016-07-07 11:00:00	Clear Failed Action Retry	Upload	Failed ⚠

5. Pause the pointer over the Failure warning triangle to view more information about the failure. For example:

   FIGURE 184 Cluster Upload: Reasons For Failure



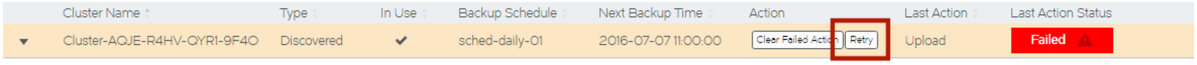
Could not upload to Instance-R1ZQ-NEEJ-L89P-8MUP: Uploading backup failed: Unable to access REST API Instance-R1ZQ-NEEJ-L89P-8MUP for uploading backup.

	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action		
▾	Cluster-AQJE-R4HV-QYR1-9F4O	Discovered	✓	sched-daily-01	2016-07-07 11:00:00	Clear Failed Action Retry	Upload	Failed ⚠

6. Investigate and resolve the issue. This may require you to log in to one of the vTMs in the cluster. Refer to the Virtual Traffic Manager documentation for details of vTM operations.
7. (Optional) Click the **Clear Failed Action** button for the cluster.
   This action clears the **Last Action** and **Last Action Status** columns before you re-attempt the cluster upload. It is not required.

8. Once the issue is resolved, click the **Retry** button for the cluster:

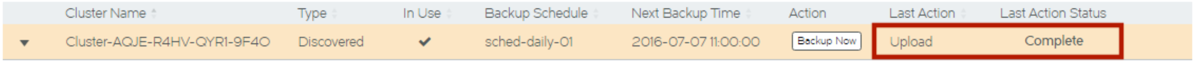
   FIGURE 185 Cluster Upload: Retrying

	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status
▼	Cluster-AQJE-R4HV-QYR1-9F4O	Discovered	✓	sched-daily-01	2016-07-07 11:00:00	Clear Failed Actio Retry	Upload	Failed ⚠

   If the upload succeeds, the failure is cleared, and the status becomes Complete:

   FIGURE 186 Cluster Upload: Success

	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status
▼	Cluster-AQJE-R4HV-QYR1-9F4O	Discovered	✓	sched-daily-01	2016-07-07 11:00:00	Backup Now	Upload	Complete

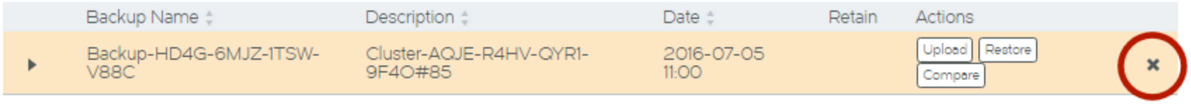
   If the upload fails again, repeat this procedure from step 5.

Deleting a Cluster Backup

The Services Director stores the most recent cluster backups, subject to a maximum number that you can you can define on a per-cluster basis. Older backups beyond this maximum are deleted automatically. You can choose to mark one or more cluster backups as *retained*. *Retained* backups are not deleted automatically, and do not count towards the maximum number of backups for the cluster. Refer to Updating a Traffic Manager Cluster on page 155.

You can delete any cluster backup manually. To do this, expand a cluster on the **vTM Clusters** page, and locate the required cluster backup. Then, click its delete (**X**) button:

FIGURE 187 Deleting a Cluster Backup



	Backup Name	Description	Date	Retain	Actions	
▶	Backup-HD4G-6MJZ-1TSW-V88C	Cluster-AQJE-R4HV-QYR1-9F4O#85	2016-07-05 11:00		Upload Restore Compare	✖

If you attempt to delete a *retained* cluster backup, you must confirm the deletion.

Moving a vTM Between Clusters

You cannot change a vTM's cluster from the Services Director. This is true for both registered vTMs (in *Discovered* clusters) and deployed vTMs (in *User Created* clusters).

However, you can change a VTM's cluster from the user interface of the Virtual Traffic Manager software itself. Refer to the Virtual Traffic Manager docs for information.

After you move a vTM between clusters, the existing administration credentials for the vTM in the Services Director VA will be wrong. As a result, the **Instance Health** for the vTM will change to "N/A", and its software version will show as Unknown.

To fix this:

1. Access the detailed view for the vTM in the **vTM Instances** page.
2. Update the administration credentials for the vTM to those of the new cluster.

After a short time, the **Instance Health** will change to reflect the state of its new cluster, and the displayed software version will return to its usual setting.

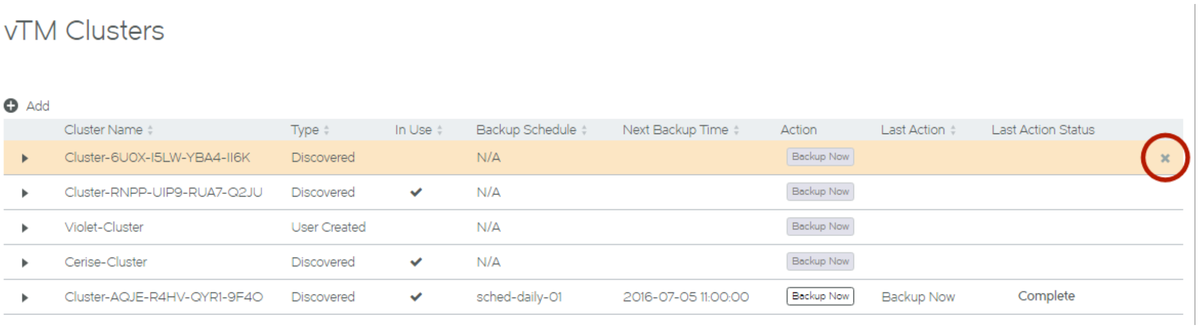
Deleting an Empty Traffic Manager Cluster

The **vTM Clusters** page displays all clusters known to the Services Director. This page can include clusters that are not flagged as **In Use**, such as one that remains after a vTM joins another cluster, leaving its original cluster empty.

You can delete any cluster that is not flagged as **In Use**, and which does not contain cluster backups.

To delete a cluster, pause the pointer over it in the table of clusters, and then click the delete (X) button that appears at the end of the row.

FIGURE 188 Deleting an Empty Cluster



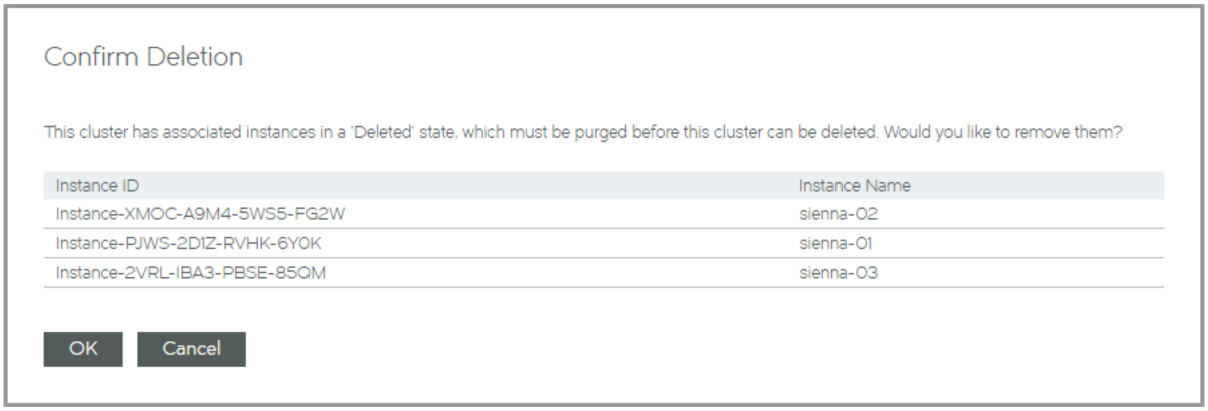
vTM Clusters

	Cluster Name	Type	In Use	Backup Schedule	Next Backup Time	Action	Last Action	Last Action Status	
▸	Cluster-6U0X-I5LW-YBA4-II6K	Discovered		N/A		Backup Now			×
▸	Cluster-RNPP-UIP9-RUA7-Q2JU	Discovered	✓	N/A		Backup Now			
▸	Violet-Cluster	User Created		N/A		Backup Now			
▸	Cerise-Cluster	Discovered	✓	N/A		Backup Now			
▸	Cluster-AQJE-R4HV-QYR1-9F4O	Discovered	✓	sched-daily-01	2016-07-05 11:00:00	Backup Now	Backup Now	Complete	

Select the **Delete** option to remove the empty cluster from the table.

> **NOTE**
> A dialog box appears if the empty cluster had ever contained a vTM that is now Deleted. This indicates that any Deleted vTMs will be purged from the database. For example:

FIGURE 189 Purging Deleted vTMs



Confirm Deletion

This cluster has associated instances in a 'Deleted' state, which must be purged before this cluster can be deleted. Would you like to remove them?

Instance ID	Instance Name
Instance-XMOC-A9M4-5WS5-FG2W	sienna-02
Instance-PJWS-2D1Z-RVHK-6YOK	sienna-01
Instance-2VRL-IBA3-PBSE-85QM	sienna-03

Click **OK** to purge the Deleted vTMs and remove the cluster from the database.

Working with User Authentication

The Services Director VA supports user authentication in two forms.

- vTM user authentication controls access to individual vTM instances. Refer to Overview: vTM User Authentication on page 179.
- Services Director user authentication controls access to the Services Director's graphical user interface (GUI), command line interface (CLI) and REST API. Refer to Overview: Services Director User Authentication on page 180.

Overview: vTM User Authentication

Each Virtual Traffic Manager (vTM) supports *user authentication*. This enables the vTM to verify the identify of any connecting user.

> NOTE
> The use of vTM user authentication is optional.

The vTM verifies a user's credentials (username and password) against two possible user authentication sources:

- Local users - user credentials are authenticated against all locally-defined user accounts (such as admin).
- Remote authenticators - user credentials are authenticated against externally-located servers that are based on RADIUS, LDAP or TACACS+ services.

Successful authentication identifies the user's permission group. This defines the activities that the connected user can perform on the vTM.

The Services Director VA enables you to optionally configure the authenticators and permissions groups that will be used by the vTMs within its estate. Specific combinations of authenticators and permission groups are combined as access profiles on the Services Director.

To configure vTM user authentication, you must create:

- One or more Services Director authenticators, refer to Creating an Authenticator on page 180.
- One or more permission groups. Refer to Creating a Permission Group on page 188.
- One or more access profiles. Refer to Creating an Access Profile (vTM User Authentication Only) on page 192.

The Services Director Administrator chooses when to apply user authentication to a vTM. This is either:

- During the acceptance of a vTM self-registration request. Refer to Accepting a Pending Self-Registration Request on page 119.
- During later configuration of the vTM from the Services Director VA. Refer to Applying User Authentication to a vTM on page 195.

Both processes require the Services Director Administrator to choose an access profile. The access profile identifies the authenticators and permission groups that are applied to the vTM to define its user authentication. These will be applied to the vTM. All cluster members are affected.

NOTE
The vTM Administrator can also configure user authentication directly from the vTM. The Services Director does not track any such activity, and cannot display live user authentication settings for the vTM.

Overview: Services Director User Authentication

Services Director user authentication controls access to the Services Director's graphical user interface (GUI), command line interface (CLI) and REST API.

NOTE
The use of Services Director user authentication is optional.

User credentials (username and password) are evaluated against two possible user authentication sources:

- Local users - user credentials are authenticated against all locally-defined user accounts (such as admin).
- Remote authenticators - user credentials are authenticated against externally-located servers that are based on RADIUS, LDAP or TACACS+ services.

Successful authentication identifies the user's permission group. This defines the activities that the connected user can perform on the vTM.

NOTE
For Services Director user authentication, there is typically a single permission group, which has access to all functionality.

To configure Services Director user authentication, you must create:

- One or more Services Director authenticators, refer to Creating an Authenticator on page 180.
- A permission group. Refer to Creating a Permission Group on page 188.

NOTE
Access profiles (which are required for vTM user authentication) are not required for Services Director user authentication.

Once you have created a Services Director authenticator and a permission group, the configuration of Services Director user authentication is complete.

Creating an Authenticator

Services Director supports user authentication at both the vTM level and the Services Director level.

One or more authenticators are required when establishing user authentication from the Services Director VA. An authenticator defines an external user authentication service. Three proprietary authentication services are supported, each of which has service-specific settings.

- LDAP, refer to Creating an LDAP Authenticator on page 182.
- RADIUS, refer to Creating a RADIUS Authenticator on page 185.
- TACACS+, refer to Creating a TACACS+ Authenticator on page 186.

Authenticators are listed on the **Authenticators** page, refer to Viewing Authenticators on page 181.

NOTE
A vTM administrator can also create and implement an authenticator on the vTM directly. Refer to the Virtual Traffic Manager documentation for details.

Viewing Authenticators

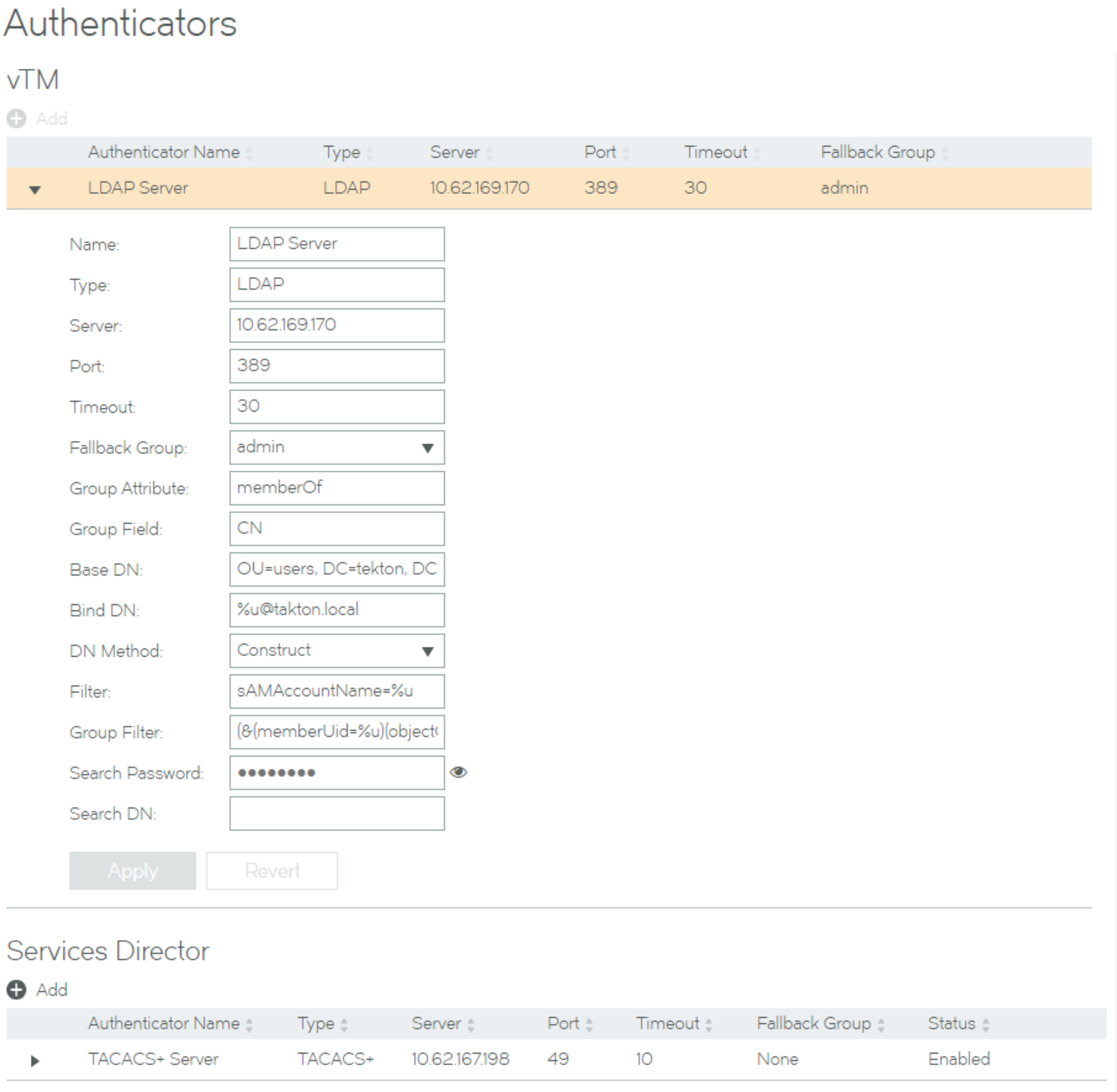
One or more authenticators are required when establishing user authentication from the Services Director VA.

The **Authenticators** page includes a table of vTM authenticators and a table of Services Director authenticators. Each entry in these tables shows the details that are common to all user authentication services (LDAP, Radius, TACACS+).

Name	Description
Authenticator Name	The name of the authenticator.
Type	The user authentication service for the authenticator. That is: LDAP, RADIUS or TACACS+.
Server	The IP address or hostname of the user authentication server.
Port	The port used to connect to the user authentication server.
Timeout	The timeout period (in seconds) for a connection to the user authentication server.
Fallback Group	The permissions group to which a valid user will belong if its group is not identified.
Status	(Services Director authenticators only). Indicates whether the authenticator is the active authenticator.

Expand an entry in either table to see full details for an authenticator. The displayed details will vary, depending on whether the authenticator is LDAP, RADIUS or TACACS+.

FIGURE 190 The Authenticators Page



Authenticators

vTM

	Authenticator Name	Type	Server	Port	Timeout	Fallback Group
▼	LDAP Server	LDAP	10.62.169.170	389	30	admin

Name:	LDAP Server
Type:	LDAP
Server:	10.62.169.170
Port:	389
Timeout:	30
Fallback Group:	admin ▼
Group Attribute:	memberOf
Group Field:	CN
Base DN:	OU=users, DC=tekton, DC
Bind DN:	%u@takton.local
DN Method:	Construct ▼
Filter:	sAMAccountName=%u
Group Filter:	(&(memberUid=%u)(object(
Search Password:	••••••••
Search DN:	

Services Director

	Authenticator Name	Type	Server	Port	Timeout	Fallback Group	Status
▶	TACACS+ Server	TACACS+	10.62.167.198	49	10	None	Enabled

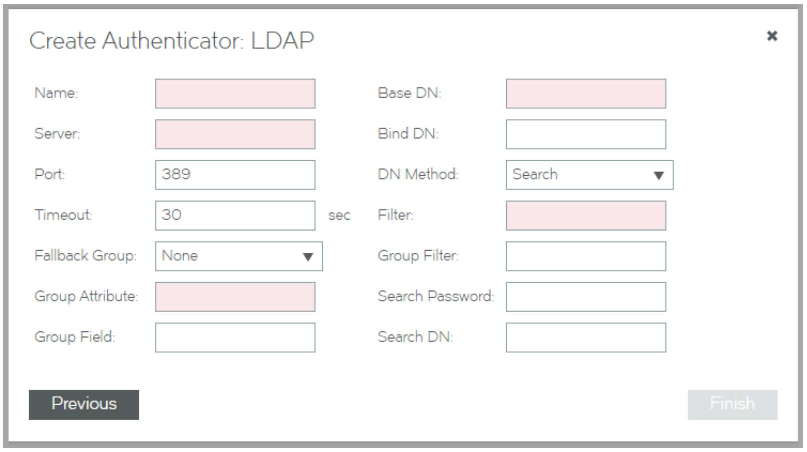
Creating an LDAP Authenticator

This procedure supports both vTM authenticators and Services Director authenticators.

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.
3. Click the **Catalogs** menu, and then click **Authentication: Authenticators**. The **Authenticators** page appears.
4. Click the plus symbol above either the vTM authenticator table or the Services Director authenticator table. The **Create Authenticator** dialog box appears.

5. Select the **LDAP** authenticator type, and click **Next**.
   The **Create Authenticator: LDAP** dialog box appears.

FIGURE 191 Specifying LDAP Authenticator Details



Create Authenticator: LDAP

Name:		Base DN:	
Server:		Bind DN:	
Port:	389	DN Method:	Search ▼
Timeout:	30 sec	Filter:	
Fallback Group:	None ▼	Group Filter:	
Group Attribute:		Search Password:	
Group Field:		Search DN:	

6. Specify the following authenticator properties:
   - **Name**: The name of the LDAP authenticator on the Services Director.
   - **Server**: The IP address or hostname of the LDAP server.
   - **Port**: The port used to connect to the LDAP server.
   - **Timeout**: The timeout period (in seconds) for a connection to the LDAP server.
   - **Group Attribute**: The LDAP attribute that gives a user's group. For example: "memberOf".

     If multiple values are returned by the LDAP server the first valid one will be used.

     This is required if **Fallback Group** is unset.
   - **Group Field** - the sub-field of the **Group Attribute** that gives a user's group.

     For example: if **Group Attribute** is "memberOf" which delivers "CN=mygroup, OU=groups, OU=users, DC=mycompany, DC=local", set **Group Field** to "CN". The first matching field will be used.
   - **Fallback Group**: A permission group, for example: "admin".

     If **Group Attribute** is not defined, or is not set for the user, the permission group named here will be used.
   - **Base DN**: The base DN (Distinguished Name) for directory searches.
   - **DN Method**: This value determines relevance/requirement of **Bind DN** and **Search DN**.

     Use "Construct" when the bind DN for a user can be constructed from a known string. Refer to the **Bind DN** field.

     Use "Search" when the bind DN for a user can be searched for in the directory. This is necessary if you have users under different directory paths. Refer to the **Search DN** and **Search Password** fields.
   - **Bind DN**: A template to construct the bind DN from the username. This is only used when the **DN Method** is "Construct".

     The string "%u" is replaced by the username. For example: "%u@mycompany.local" or "cn=%u, dn=mycompany, dn=local"
   - **Filter**: A filter that uniquely identifies a user located under the Base DN.

     The string "%u" will be substituted with the username. For example: "sAMAccountName=%u" (Active Directory), or "uid=%u" (Unix LDAP).
   - **Group Filter**: If the user record returned by the LDAP **Filter** does not contain the required group information, you can specify an alternative group search filter here. This will typically be required if you have Unix/POSIX-style user records. If multiple records are returned the list of group names will be extracted from all of them.

     The string "%u" will be replaced by the username. For example: "(&(memberUid=%u)(objectClass=posixGroup))"
   - **Search DN / Search Password** - the DN and password to use when searching the directory for a user's bind DN. These are only used when the **DN Method** is "Search". You can leave these blank if it is possible to perform the bind DN search using an anonymous bind.
7. (Optional) Set the **Enabled** check box if this is to be the active Services Director authenticator.
8. (Optional) Test the specified details for a Services Director user authentication by specifying a **Username** and **Password** and clicking **Test**.

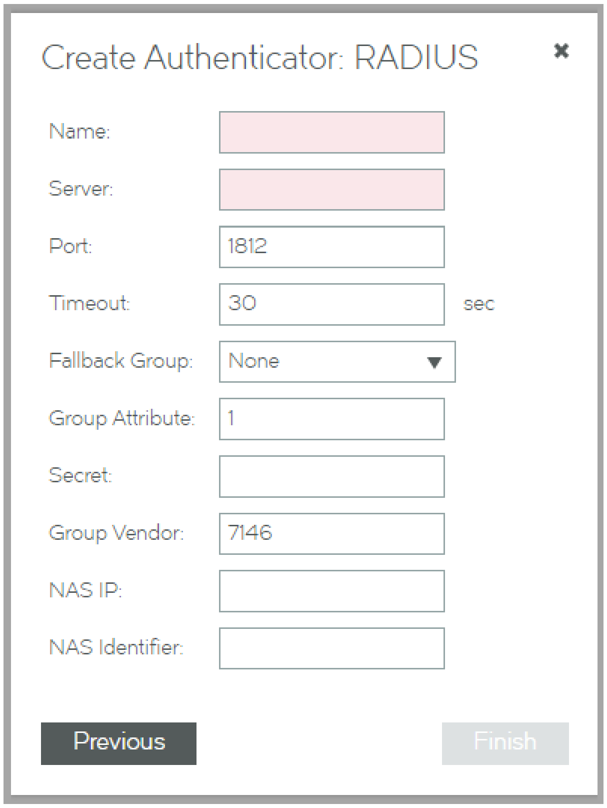
   NOTE
   This function is not available for vTM authenticators.
9. Click **Finish**.
   The LDAP authenticator is added to the Authenticator table.

Creating a RADIUS Authenticator

This procedure supports both vTM authenticators and Services Director authenticators.

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.
3. Click the **Catalogs** menu, and then click **Authentication: Authenticators**. The **Authenticators** page appears.
4. Click the plus symbol above either the vTM authenticator table or the Services Director authenticator table.
   The **Create Authenticator** dialog box appears.
5. Select the **RADIUS** authenticator type, and click **Next**.
   The **Create Authenticator: RADIUS** dialog box appears.

FIGURE 192 Specifying RADIUS Authenticator Details



Create Authenticator: RADIUS

Name:	
Server:	
Port:	1812
Timeout:	30 sec
Fallback Group:	None ▼
Group Attribute:	1
Secret:	
Group Vendor:	7146
NAS IP:	
NAS Identifier:	

6. Specify the following authenticator properties:
   - **Name**: The name of the RADIUS authenticator on the Services Director.
   - **Server**: The IP address or hostname of the RADIUS server.
   - **Port**: The port used to connect to the RADIUS server.
   - **Timeout**: The timeout period (in seconds) for a connection to the RADIUS server.
   - **Fallback Group**: If no group is found using the vendor and group identifiers, or the group found is not valid, the group specified here will be used.
   - **Group Attribute**: The RADIUS identifier for the attribute that specifies an account's group.

     Optional if **Fallback Group** is specified, but required if **Fallback Group** is unset.
   - **Secret**: The secret key shared with the RADIUS server.
   - **Group Vendor**: The RADIUS identifier for the vendor of the RADIUS attribute that specifies an account's group.

     Leave blank if using a standard attribute such as Filter-Id.
   - **NAS IP**: A string identifying the Network Access Server (NAS) which is requesting authentication of the user. This value is sent to the RADIUS server.

     If left blank, the address of the interface used to connect to the server will be used.
   - **NAS Identifier**: The identifying IP Address of the NAS which is requesting authentication of the user. This value is sent to the RADIUS server.
7. (Optional) Set the **Enabled** check box if this is to be the active Services Director authenticator.

   NOTE
   This property is not available for vTM authenticators.

8. Click **Finish**.
   The RADIUS authenticator is added to the Authenticator table.

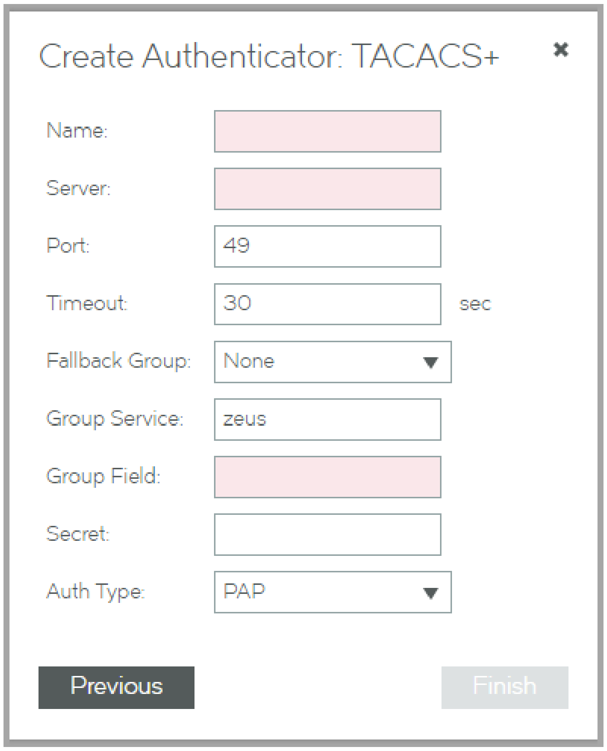
Creating a TACACS+ Authenticator

This procedure supports both vTM authenticators and Services Director authenticators.

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.
3. Click the **Catalogs** menu, and then click **Authentication: Authenticators**. The **Authenticators** page appears.
4. Click the plus symbol above either the vTM authenticator table or the Services Director authenticator table.
   The **Create Authenticator** dialog box appears.

5. Select the **TACACS+** authenticator type, and click **Next**.
   The **Create Authenticator: TACACS+** dialog box appears.

   FIGURE 193 Specifying TACACS+ Authenticator Details



Create Authenticator: TACACS+

Name:	
Server:	
Port:	49
Timeout:	30 sec
Fallback Group:	None
Group Service:	zeus
Group Field:	
Secret:	
Auth Type:	PAP

6. Specify the following authenticator properties:
   - **Name**: The name of the TACACS+ authenticator on the Services Director.
   - **Server**: The IP address or hostname of the TACACS+ server.
   - **Port**: The port used to connect to the TACACS+ server.
   - **Timeout**: The timeout period (in seconds) for a connection to the TACACS+ server.
   - **Fallback Group**: If **Group Service** is not defined, or no group value is provided for the user by the TACACS+ server, the group specified here will be used.
   - **Secret**: The secret key shared with the TACACS+ server.
   - **Auth Type**: The TACACS+ authentication type, either "PAP" or "ASCII".
   - **Group Service**: The TACACS+ "service" that identifies a user's group field. This is required if **Fallback Group** is unset.
   - **Group Field**: The TACACS+ "service" field that provides each user's group.
7. (Optional) Set the **Enabled** check box if this is to be the active Services Director authenticator.

   NOTE
   This property is not available for vTM authenticators.

8. Click **Finish**.
   The TACACS+ authenticator is added to its authenticator table.

Creating a Permission Group

Services Director supports user authentication at both the vTM level and the Services Director level.

- One or more permission groups are required when establishing vTM user authentication. Each permission group defines what a user in the group can do, by combining permission names with access levels. There are four default permission groups:
  - admin - this group has full access to all vTM pages.
  - Demo - this group has full access, except to user management / system.
  - Monitoring - this group has access only to config summary / monitoring pages.
  - Guest - this group has read-only access
- A single permission group is typically required when establishing Services Director user authentication. This permission group has access to all functionality.

Permission groups are listed on the **Permission Groups** page, refer to Viewing Permission Groups on page 188.

You create permission groups from the **Permission Groups** page.

- To create a permission group for vTM user authentication, refer to Creating a Permission Group (vTM User Authentication) on page 190.
- To create a permission group for Services Director authentication, refer to Creating a Permission Group (SD User Authentication) on page 191.

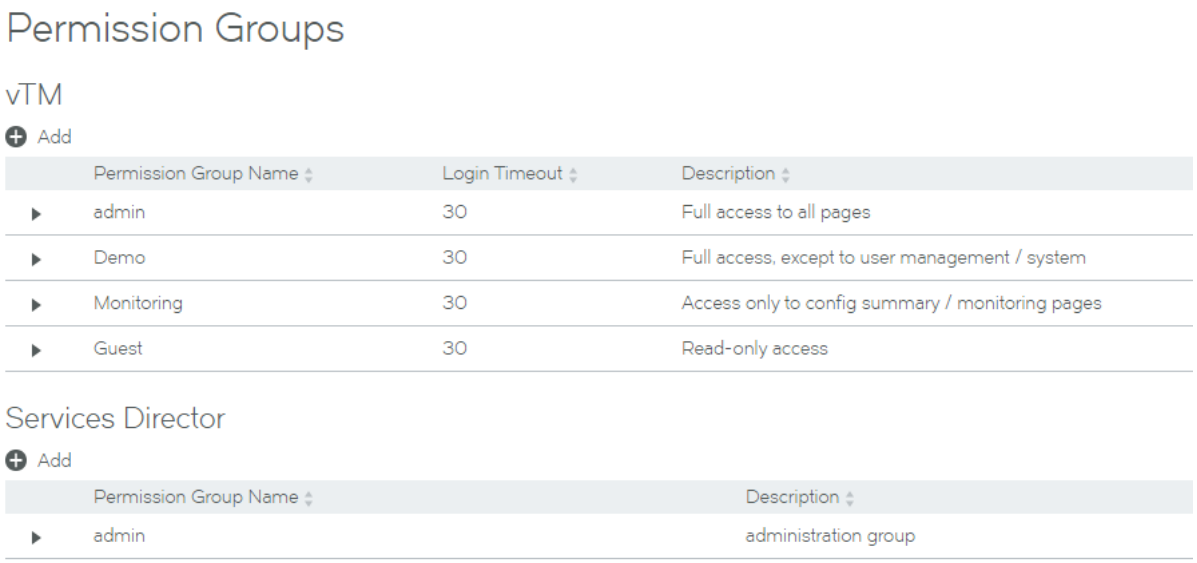
  NOTE
  The vTM administrator can create and implement a permission group on the vTM directly. Refer to the Virtual Traffic Manager documentation for details.

Viewing Permission Groups

One or more authenticators are required when establishing user authentication from the Services Director VA. Each permission group defines what a user in the group can do.

The **Permission Groups** page includes a table of permission groups for vTM user authentication, and a table of permission groups for Services Director user authentication.

FIGURE 194 The Permission Groups Page



Permission Groups

vTM

	Permission Group Name	Login Timeout	Description
▶	admin	30	Full access to all pages
▶	Demo	30	Full access, except to user management / system
▶	Monitoring	30	Access only to config summary / monitoring pages
▶	Guest	30	Read-only access

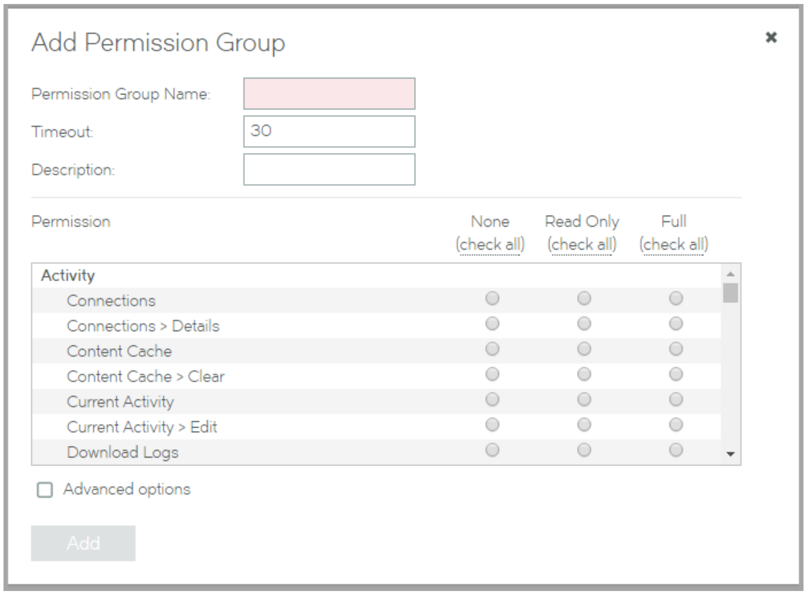
Services Director

	Permission Group Name	Description
▶	admin	administration group

Each entry in the permission groups table displays summary details for the permission group.

To view full details for a vTM user authentication permission group, click the arrow on the left side of the permission group's entry.

FIGURE 195 The Permission Groups Page: vTM Permission Group



Add Permission Group

Permission Group Name:	
Timeout:	30
Description:	

Permission	None (check all)	Read Only (check all)	Full (check all)
Activity			
Connections	○	○	○
Connections > Details	○	○	○
Content Cache	○	○	○
Content Cache > Clear	○	○	○
Current Activity	○	○	○
Current Activity > Edit	○	○	○
Download Logs	○	○	○

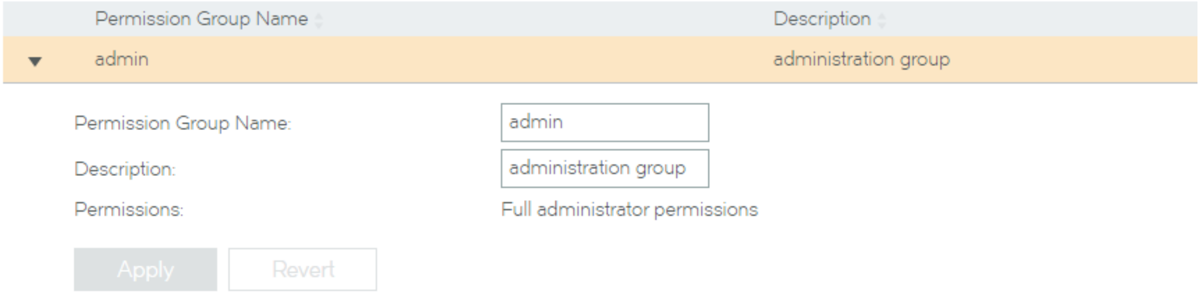
□ Advanced options

Name	Description
Permission Group Name	The name of the permission group.
Timeout (vTM Only)	A timeout setting (in minutes) for a login session for a user in this group. A zero value indicates that sessions should never time out.

Name	Description
Description	A list of permissions known by the Services Director. The access level for each of these can be set to None, Read-Only or Full.
Permission	A list of permissions known by the Services Director. The access level for each of these can be set to None, Read-Only or Full. If you click **Advanced Options**, you can manually specify permissions of which Services Director is not aware. That is, you can reference any permission that is supported by the vTM. To find these permission names, refer to the Virtual Traffic Manager Documentation. NOTE The Services Director VA does not verify permissions entered under **Advanced Options**. The vTM itself verifies all permissions when the permission group is applied to the vTM. Any permission that is not recognised by the vTM is ignored.

To view full details for a Services Director user authentication permission group, click the arrow on the left side of the permission group's entry.

FIGURE 196 The Permission Groups Page: Services Director Permission Group



Permission Group Name	Description
admin	administration group

Permission Group Name: admin

Description: administration group

Permissions: Full administrator permissions

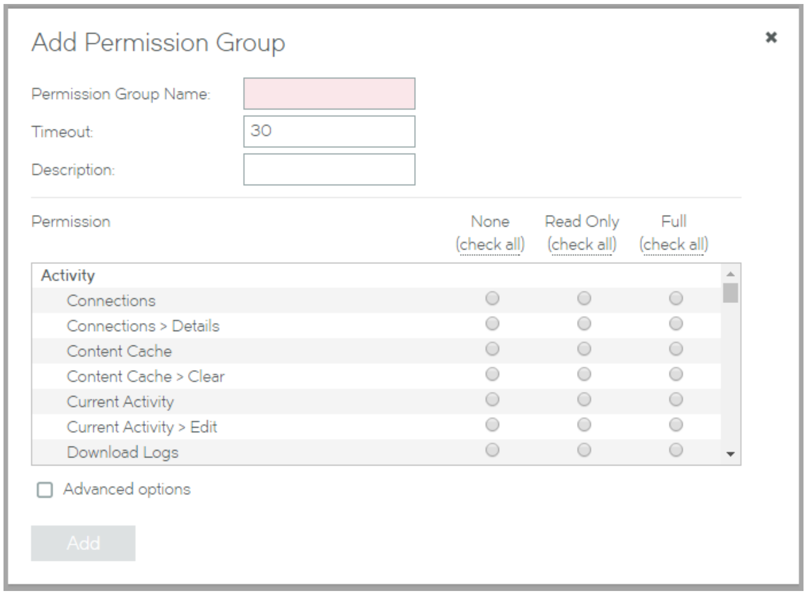
Typically, there is only one Services Director user authentication permission group.

Creating a Permission Group (vTM User Authentication)

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.
3. Click the **Catalogs** menu, and then click **Authentication: Permission Groups**. The **Permission Groups** page appears.

4. Click the plus symbol above the vTM permission group table.
   The **Add Permission Group** dialog box appears.

FIGURE 197 Adding a Permission Group: vTM User Authentication



Add Permission Group

Permission Group Name:

Timeout: 30

Description:

Permission	None (check all)	Read Only (check all)	Full (check all)
Activity			
Connections	○	○	○
Connections > Details	○	○	○
Content Cache	○	○	○
Content Cache > Clear	○	○	○
Current Activity	○	○	○
Current Activity > Edit	○	○	○
Download Logs	○	○	○

□ Advanced options

5. Specify a **Permission Group Name**.
6. Specify a **Timeout** period, in minutes.
7. (Optional) Add a description for the permission group.
8. Specify an access level for each listed **Permission**. That is, None, Read-Only or Full.
   - To select None for all listed permissions, click **None (check all)**.
   - To select Read-Only for all listed permissions, click **Read-Only (check all)**.
   - To select Full for all listed permissions, click **Full (check all)**.
9. To specify a permission for an unlisted **Permission**:
   1. Click **Advanced Options**.
   2. Enter the name of the **Permission**. You can reference any permission that is supported by the vTM. To find these permission names, refer to the Virtual Traffic Manager documentation.
   3. Select the required access level. That is, None, Read-Only or Full.
10. Click **Add** to create the vTM permission group.

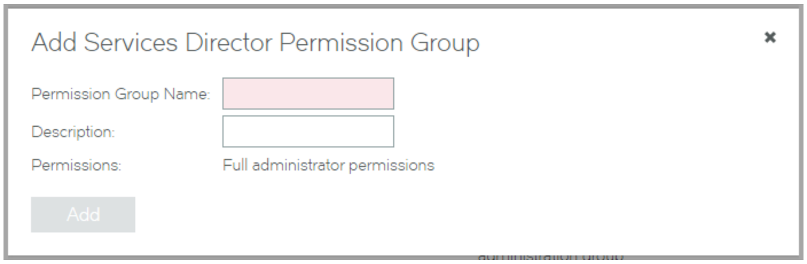
NOTE
The vTM administrator can create and implement a permission group on the vTM. Refer to the Virtual Traffic Manager documentation for details.

Creating a Permission Group (SD User Authentication)

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.

3. Click the **Catalogs** menu, and then click **Authentication: Permission Groups**. The **Permission Groups** page appears.
4. Click the plus symbol above the Services Director permission group table.
   The **Add Permission Group** dialog box appears.

FIGURE 198 Adding a Permission Group: Services Director User Authentication



Add Services Director Permission Group

Permission Group Name:

Description:

Permissions: Full administrator permissions

5. Specify a **Permission Group Name**.
6. (Optional) Add a description for the permission group.
7. Click **Add** to create the Services Director permission group.

Creating an Access Profile (vTM User Authentication Only)

An access profile is required when establishing user authentication for a vTM from the Services Director VA. An access profile combines an authenticator with one or more permission groups. When and access profile is selected, the authenticator and permission groups included in the profile are used by the vTM to define its user authentication.

NOTE
Access profiles are not required when creating Services Director user authentication.

Access profiles are listed on the **Access Profiles** page, refer to Viewing Access Profiles on page 192.

You create access profiles from the **Access Profiles** page, refer to Creating an Access Profile on page 194.

NOTE
The use of access profiles enable the Services Director Administrator to set the user authentication on the vTM from the Services Director VA. However, the vTM Administrator can also configure user authentication directly from the vTM. The Services Director does not track any such activity, and cannot display live user authentication settings for the vTM.

Viewing Access Profiles

An access profile is required when establishing user authentication for a vTM from the Services Director VA. An access profile combines an authenticator with one or more permission groups. When it is selected, the authenticator and permission groups included in the access profile are used by the vTM to define its user authentication.

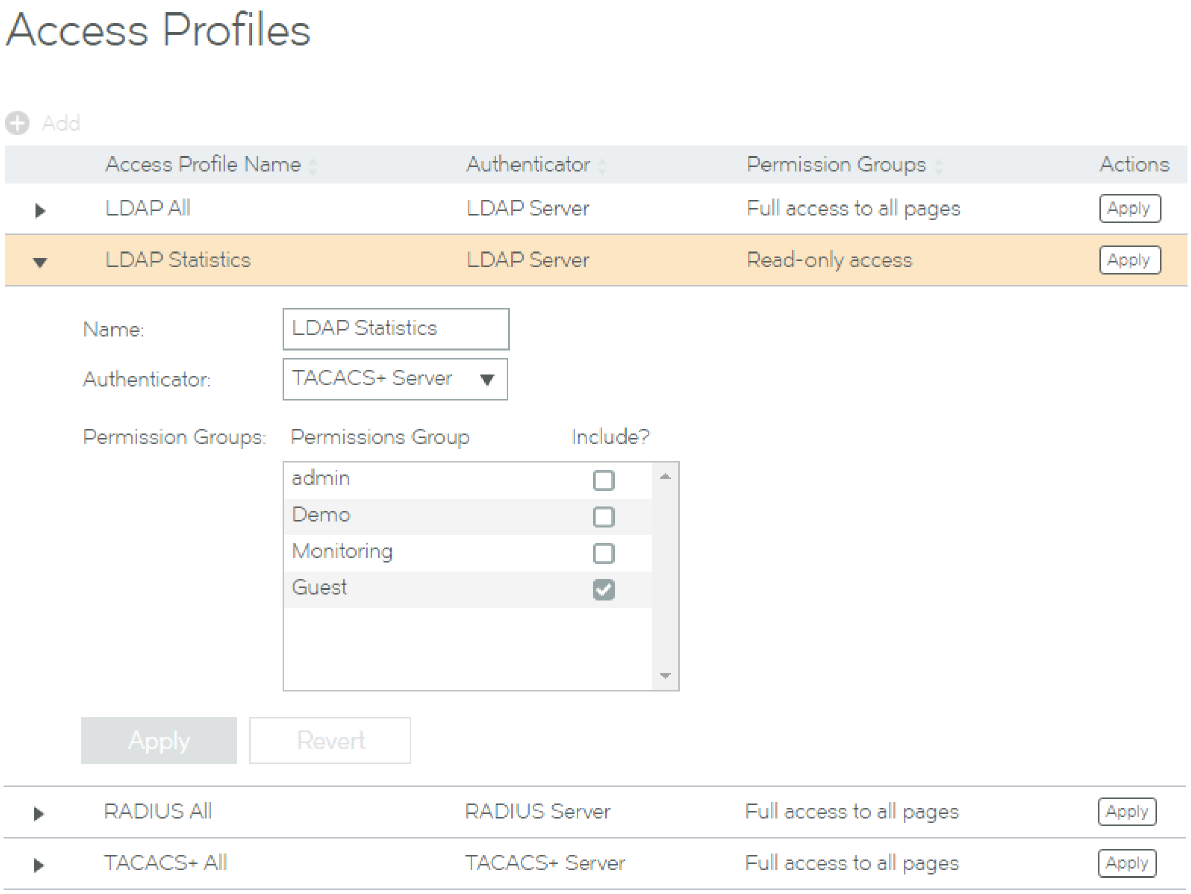
NOTE
Access profiles are not supported for Services Director user authentication.

The **Access Profiles** page shows a table of all access profiles defined on the Services Director. Each entry in the table shows summary details for an access profile.

Name	Description
Access Profile Name	The name of the access profile. This is used when applying an access profile to: • a Pending self-registration request by a vTM. Refer to Accepting a Pending Self-Registration Request on page 119. • one or more registered/deployed vTMs. Refer to Applying User Authentication to a vTM on page 195.
Authenticator	The selected authenticator for the access profile. Refer to Creating an Authenticator on page 180.
Permission Groups	A list of permission groups included in the access profile. There are four default permission groups, but you can define others. Refer to Creating a Permission Group on page 188.
Actions	The **Apply to vTM Instance(s)** control in this column enables you to apply the permissions groups and authenticators associated with this access profile to one or more vTMs. Refer to Applying User Authentication to a vTM on page 195.

To view full details for an access profile, click the arrow on the left side of the access profile's entry.

FIGURE 199 The Access Profiles Page



Access Profiles

	Access Profile Name	Authenticator	Permission Groups	Actions
▸	LDAP All	LDAP Server	Full access to all pages	Apply
▾	LDAP Statistics	LDAP Server	Read-only access	Apply

Name: LDAP Statistics

Authenticator: TACACS+ Server ▼

Permission Groups:

Permissions Group	Include?
admin	□
Demo	□
Monitoring	□
Guest	☑

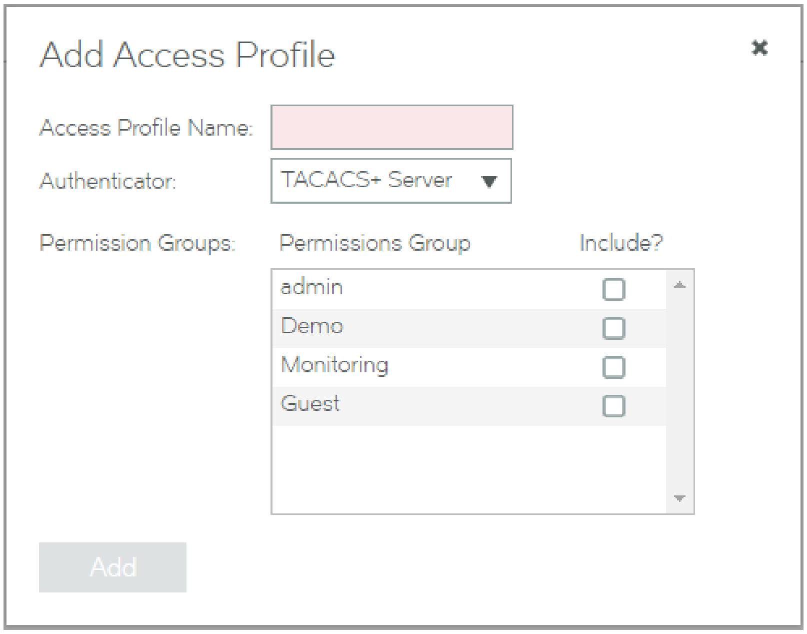
▸	RADIUS All	RADIUS Server	Full access to all pages	Apply
▸	TACACS+ All	TACACS+ Server	Full access to all pages	Apply

Creating an Access Profile

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.
3. Click the **Catalogs** menu, and then click **Authentication: Access Profiles**. The **Access Profiles** page appears.

4. Click the plus symbol above the access profile table.
   The **Add Access Profile** dialog box appears.

FIGURE 200 Adding an Access Profile



Add Access Profile

Access Profile Name:

Authenticator: TACACS+ Server

Permission Groups:

Permissions Group	Include?
admin	□
Demo	□
Monitoring	□
Guest	□

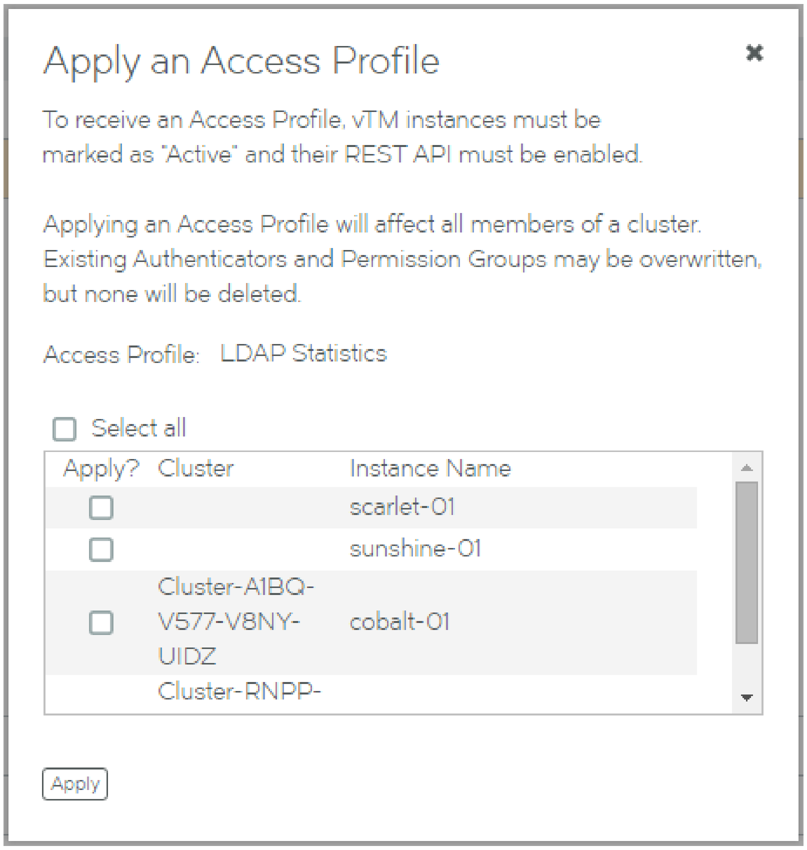
5. Specify an **Access Profile Name**.
6. Select an **Authenticator**.
7. Select one or more permission groups.
8. Click **Add** to create the access profile.

Applying User Authentication to a vTM

1. Access your Services Director VA from a browser, using its Service Endpoint IP Address.
2. Log in as the administration user. The **Home** page appears.
3. Click the **Catalogs** menu, and then click **Authentication: Access Profiles**. The **Access Profiles** page appears.
4. In the table of access profiles, locate the required access profile. Expand the entry to confirm its properties if required.

5. Click the **Apply** button that is next to the required access profile.
   The **Apply an Access Profile** dialog box appears. This dialog box lists all vTMs that are Active and with a REST API enabled.

FIGURE 201 Applying an Access Profile



Apply an Access Profile

To receive an Access Profile, vTM instances must be marked as "Active" and their REST API must be enabled.

Applying an Access Profile will affect all members of a cluster. Existing Authenticators and Permission Groups may be overwritten, but none will be deleted.

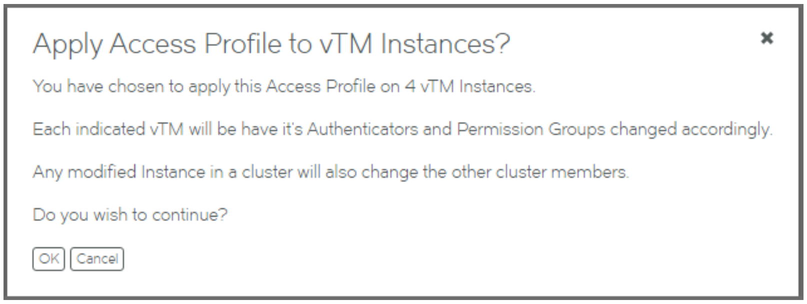
Access Profile: LDAP Statistics

□ Select all

Apply?	Cluster	Instance Name
□		scarlet-01
□		sunshine-01
□	Cluster-A1BQ-V577-V8NY-UIDZ	cobalt-01
	Cluster-RNPP-	

6. Select the check box for each required vTM instance, or click **Select All**.
7. Click **Apply**.
   A summary of selections appears. For example:

FIGURE 202 User Authentication Changes: Summary



Apply Access Profile to vTM Instances?

You have chosen to apply this Access Profile on 4 vTM Instances.

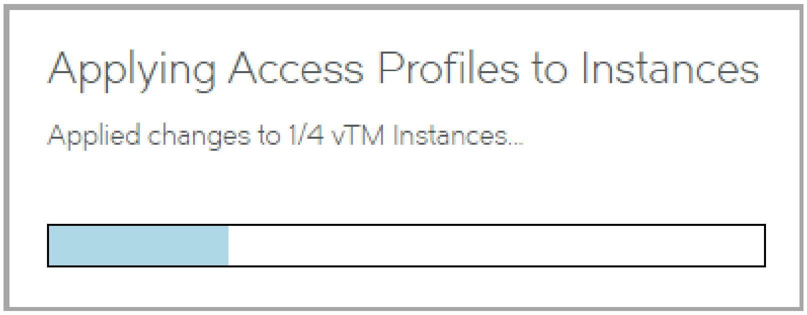
Each indicated vTM will be have it's Authenticators and Permission Groups changed accordingly.

Any modified Instance in a cluster will also change the other cluster members.

Do you wish to continue?

8. Click OK to continue.
   The permissions groups and authenticators associated with the chosen access profile are applied to the selected vTMs. A progress bar tracks this:

   FIGURE 203 User Authentication Changes: Progress

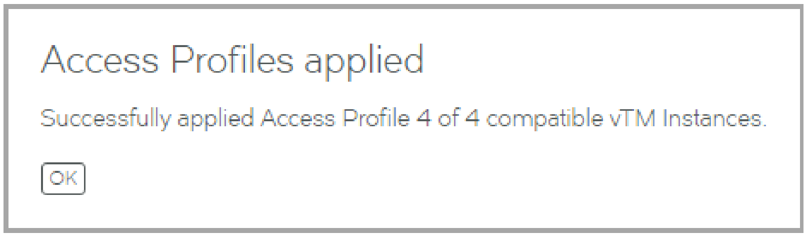
   

   Applying Access Profiles to Instances

   Applied changes to 1/4 vTM Instances...

   Once the changes are complete, a message appears:

   FIGURE 204 User Authentication Changes: Complete

   Access Profiles applied

   Successfully applied Access Profile 4 of 4 compatible vTM Instances.

9. Click **OK**. The process is complete.

Working with vTM Templates

During the process of configuring a vTM for self-registration, you can mark a vTM as a template vTM. This prevents it from self-registering, but ensures that all vTMs made from the template will request self-registration.

The template vTM is visible in the list of virtual machines in VMware, and can be used to create other vTMs. Refer to the Virtual Traffic Manager documentation.

Working with High Availability

Overview: High Availability on Services Director

High Availability (HA) is a Services Director configuration.

An HA configuration enables two Services Director nodes to operate as a synchronized *HA pair*, with an active Services Director being backed up by a standby Services Director.

> NOTE
>
> The Services Director HA pair and its Service Endpoint Address can be in a private network behind a NAT device.

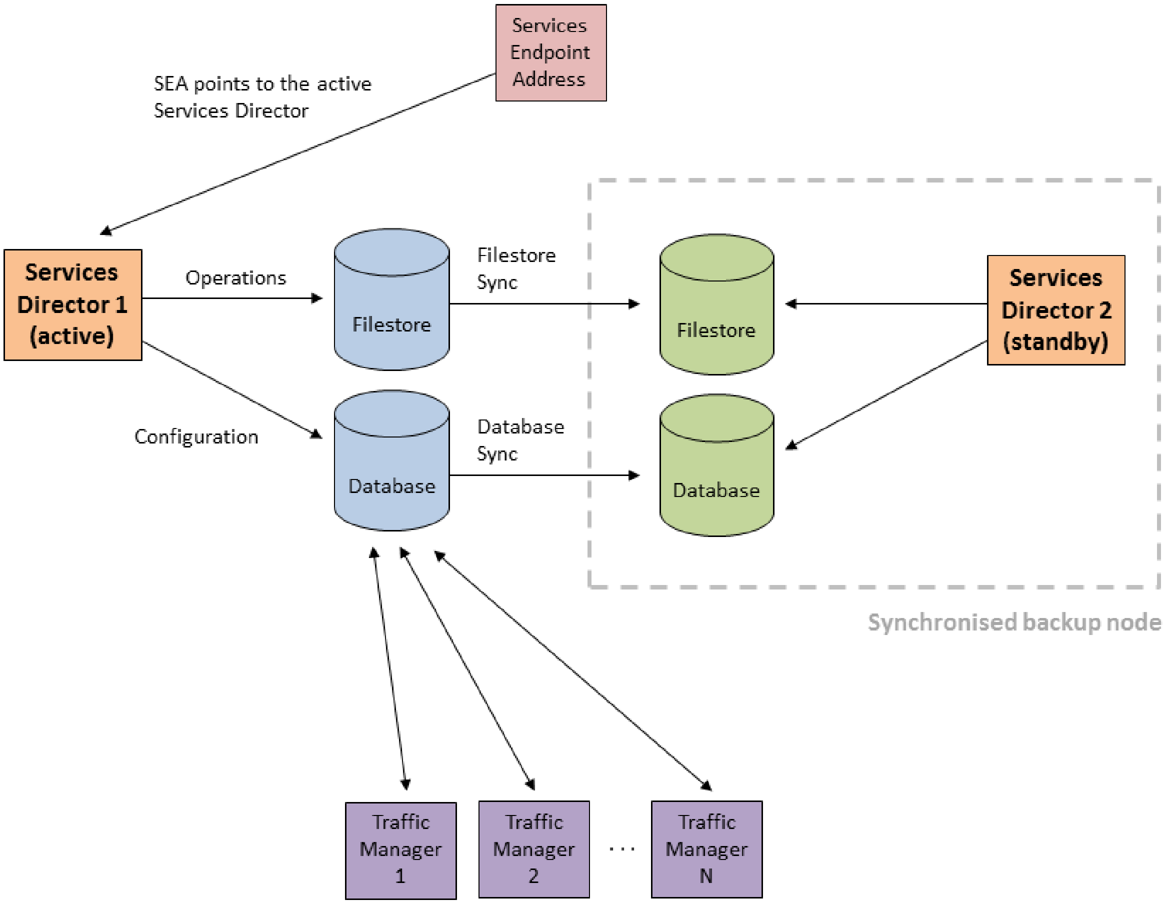
Each node in the HA pair maintains a database and filestore:

- The database stores management metadata for various components, including all registered/deployed Traffic managers in the network.
- The filestore stores essential files for Traffic manager deployment, configuration and operation.

The metadata and files are synchronized from the active node to the standby node.

The HA pair has a Service Endpoint Address (SEA), which points to whichever of the Services Directors is currently the active node. This enables users to always access the Services Director VA using the same hostname/IP address at all times.

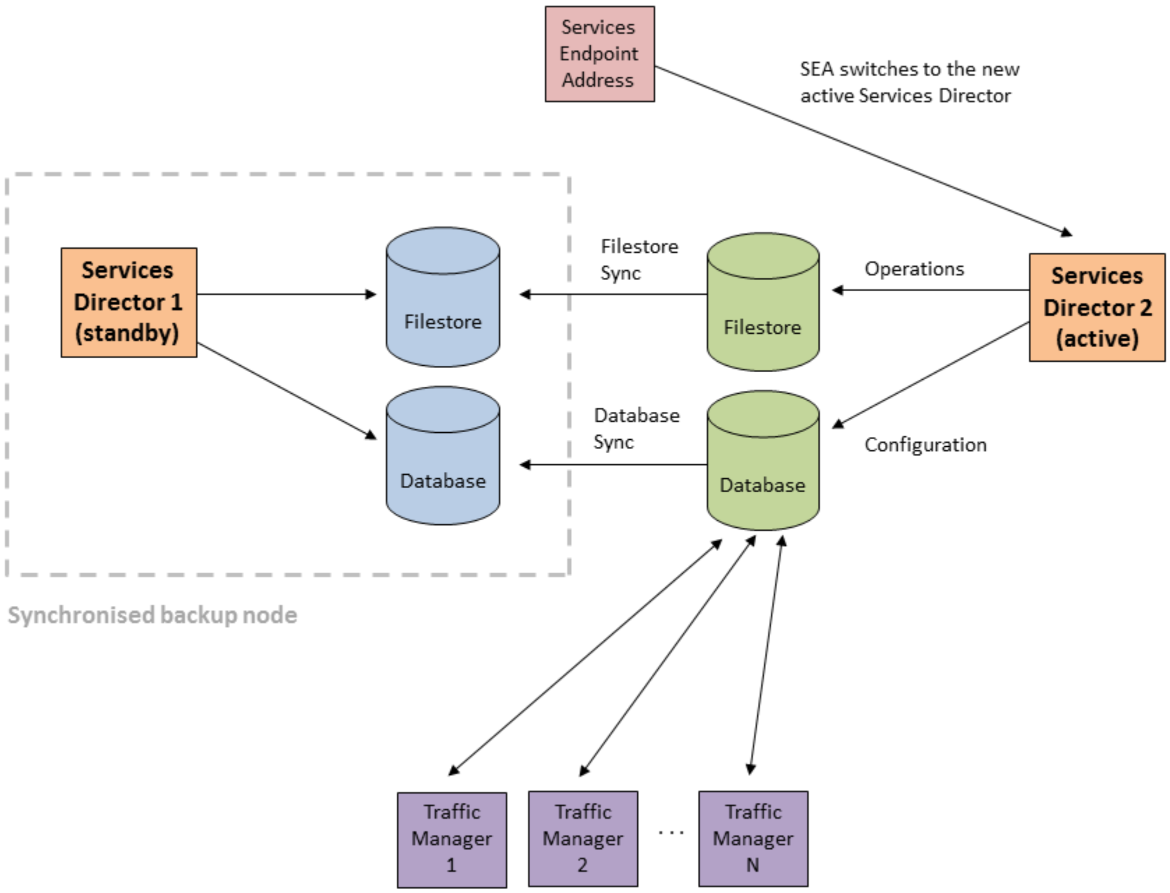
FIGURE 205 High Availability Overview



In the event of failure of the active node, the standby node contains a synchronized copy of the current configuration for the Services Director, and can take over as the active node. The former active node becomes the standby node, and the direction of all synchronization reverses.

The switching process, called *failover*, is triggered manually by the administrator.

FIGURE 206 High Availability Overview: After Failover

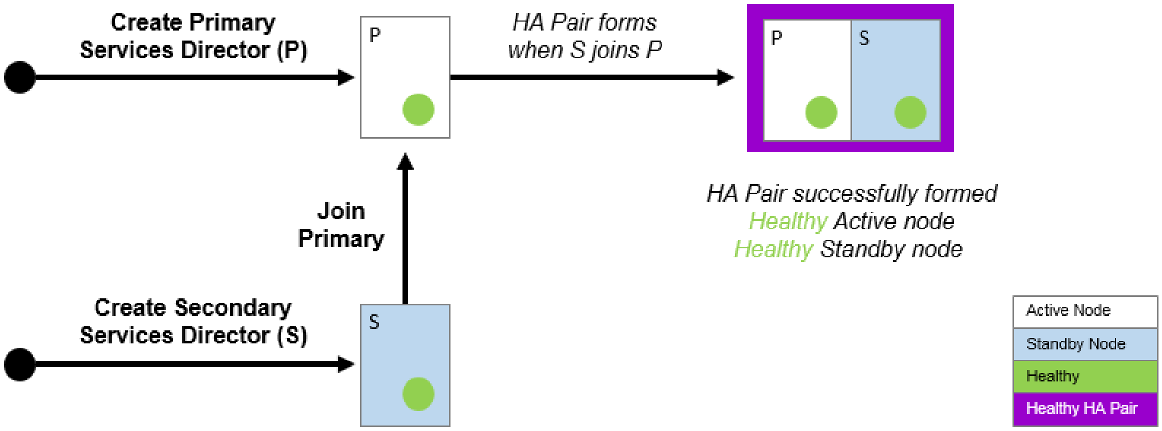


Creating a High Availability Pair in the Services Director VA

In the Services Director VA, an HA pair is formed by joining a Secondary Services Director to an existing Primary Services Director.

This process happens during the Setup Wizard for a Secondary Services Director. Refer to Installing and Configuring a Secondary Services Director on page 53.

FIGURE 207 High Availability: Creating and Joining Services Directors


Create Primary Services Director (P)
P
HA Pair forms when S joins P
P
S
Join Primary
HA Pair successfully formed
Healthy Active node
Healthy Standby node
Create Secondary Services Director (S)
S
Active Node
Standby Node
Healthy
Healthy HA Pair

Once the HA pair is formed, the concepts of Primary and Secondary Services Directors are largely put aside; these represent the *virtual machine* implementations of the Services Directors, each of which can be uniquely identified by an IP address or a DNS hostname.

NOTE
The Services Director HA pair and its Service Endpoint Address can be in a private network behind a NAT device.

The concepts of Primary and Secondary are less important than the *role* that each Services Director performs in the HA pair. The supported roles are:

- The Active role - the Services Director controls the HA pair for:
  - Web Service. That is, it controls use of the REST API and licensing.
  - Database and Database Synchronization. The system configuration is contained in a database on the Active node, and synchronizes to the Standby node.
  - File System and File System Synchronization. The file system of the Active node is synchronized to the Standby node.
- The Standby role - the Services Director receives system information from the Active node:
  - The synchronized database.
  - The synchronized file system.

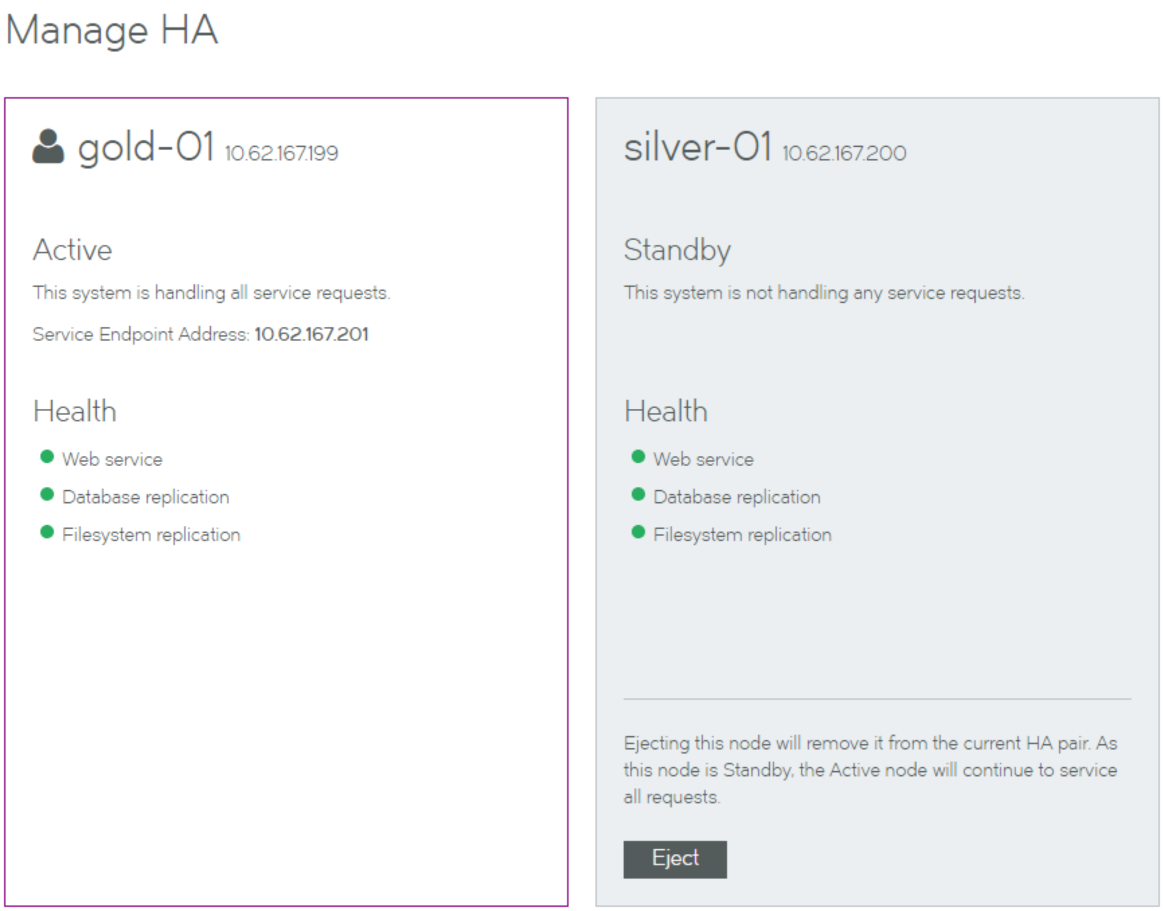
The Active and Standby roles can be changed using software operations, without regard for whether each node is operating on the Primary or Secondary Services Director. Refer to Swapping the Roles of the HA Nodes on page 208.

The Service Endpoint Address is the management address for the Services Director as a whole, and always points to the active Services Director node.

Viewing High Availability Status

The current HA status for the Services Director HA pair is shown on the **Services** > **Manage HA** page of the Services Director VA.

FIGURE 208 Manage HA Page



Manage HA

gold-01 10.62.167.199

Active

This system is handling all service requests.

Service Endpoint Address: **10.62.167.201**

Health

- ● Web service
- ● Database replication
- ● Filesystem replication

silver-01 10.62.167.200

Standby

This system is not handling any service requests.

Health

- ● Web service
- ● Database replication
- ● Filesystem replication

Ejecting this node will remove it from the current HA pair. As this node is Standby, the Active node will continue to service all requests.

The HA pair is represented by a pair of panels on the **Manage HA** page. Each panel shows information for either the Active or the Standby node.

- The node you are logged in to is always presented on the left.

  In this example, you are logged in to the **gold-01** node.
- The Active node is always presented in a white panel.

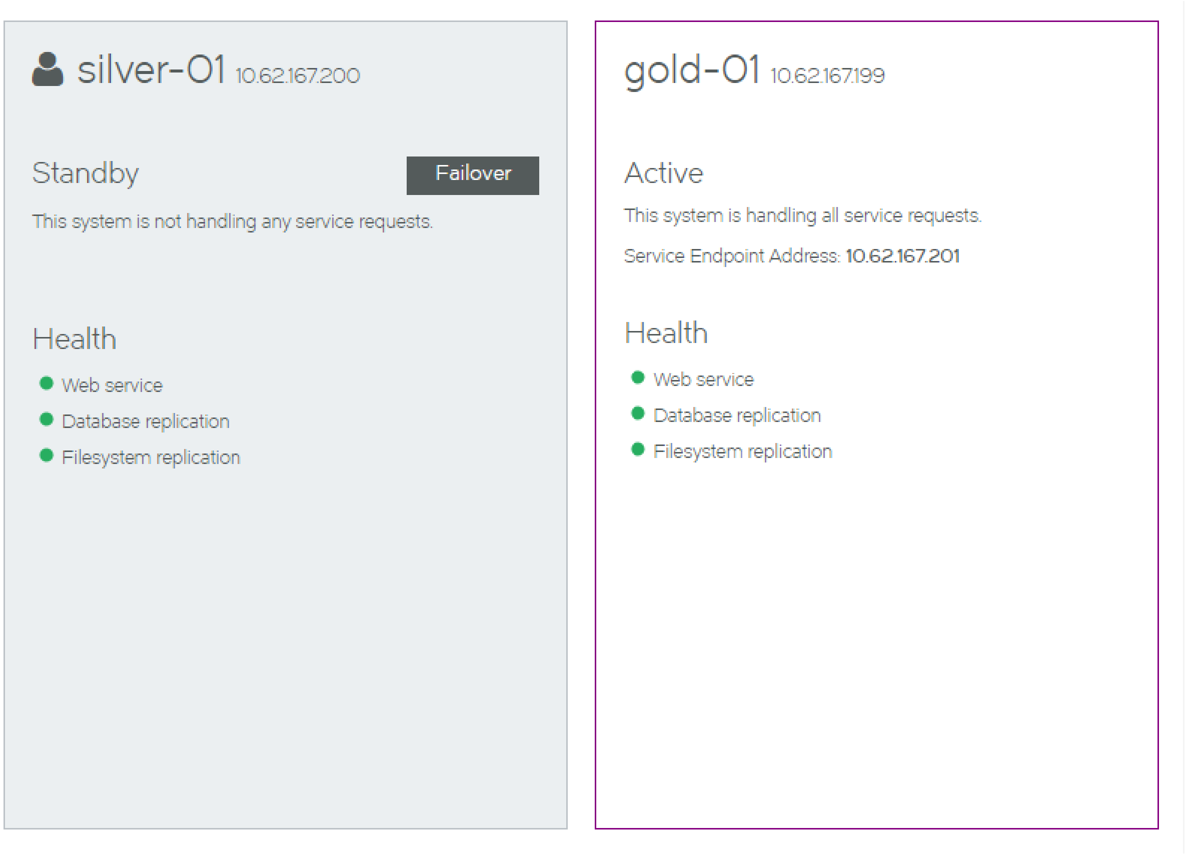
  In this example, **gold-01** is the Active node.
- The Standby node is always presented in a blue/gray panel.

  In this example, **silver-01** is the Standby node.
- Where additional actions are supported, a button is shown.

  In this example, the **Eject** button is present on the Standby node.

If you are logged in to the Standby node, your view will be similar to the following:

FIGURE 209 Manage HA Page: Logged in to Standby Node



silver-01 10.62.167.200

Standby

This system is not handling any service requests.

Health

- ● Web service
- ● Database replication
- ● Filesystem replication

gold-01 10.62.167.199

Active

This system is handling all service requests.

Service Endpoint Address: **10.62.167.201**

Health

- ● Web service
- ● Database replication
- ● Filesystem replication

Each panel includes health indicators for the node. These indicate the health of:

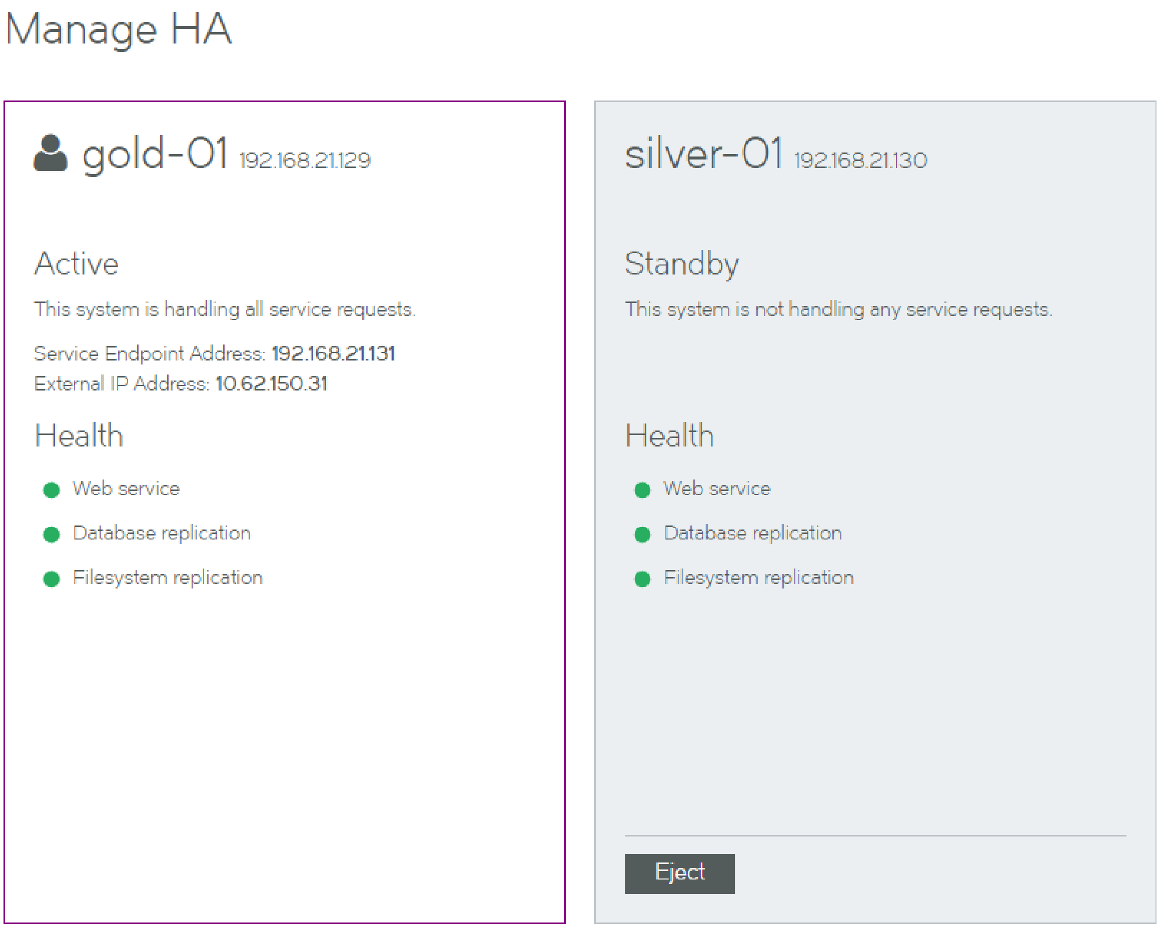
- Web Services. That is, the REST API services and Traffic Manager licensing.
- Database synchronization.
- Filestore synchronization.

While an indicator is green, it is healthy.

When one or more of these operations is unhealthy, it is orange. Refer to Responding to Reported Health Issues on page 205.

If the Services Director HA pair is in a private network behind a NAT device, the internal Service Endpoint Address and the external IP Address for the HA pair are displayed. For example:

FIGURE 210 Manage HA Page: HA Pair in a Private Network Behind a NAT Device



Manage HA

gold-01 192.168.21.129

Active

This system is handling all service requests.

Service Endpoint Address: **192.168.21.131**
External IP Address: **10.62.150.31**

Health

- ● Web service
- ● Database replication
- ● Filesystem replication

silver-01 192.168.21.130

Standby

This system is not handling any service requests.

Health

- ● Web service
- ● Database replication
- ● Filesystem replication

Taking a Backup of Your Services Director

When your Services Director system is fully configured, you can preserve its configuration by taking regular scheduled backups. This serves two purposes:

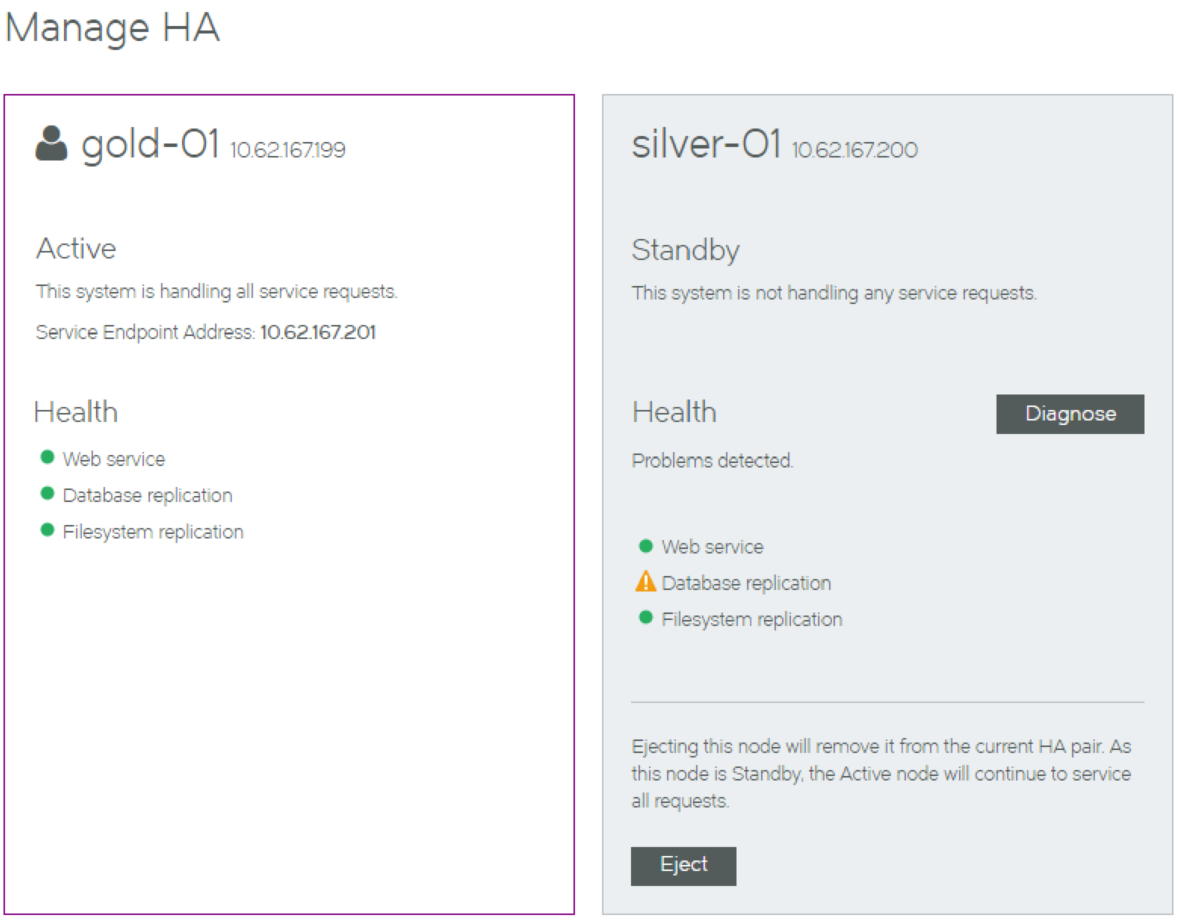
- In the event of a failure of a node's configuration, you can use a backup to recover the configuration.
- In the event of a failure of a Services Director node, you can use a backup to create a new Services Director. This is achieved by using a backup configuration during the Setup Wizard.

Refer to Recovering from a Services Director Failure on page 237 for full details of both scenarios.

Responding to Reported Health Issues

When a node is in an unhealthy state, an orange health indicator is used. For example:

FIGURE 211 Manage HA Page: Unhealthy State



Manage HA

gold-01 10.62.167.199

Active

This system is handling all service requests.

Service Endpoint Address: 10.62.167.201

Health

- ● Web service
- ● Database replication
- ● Filesystem replication

silver-01 10.62.167.200

Standby

This system is not handling any service requests.

Health

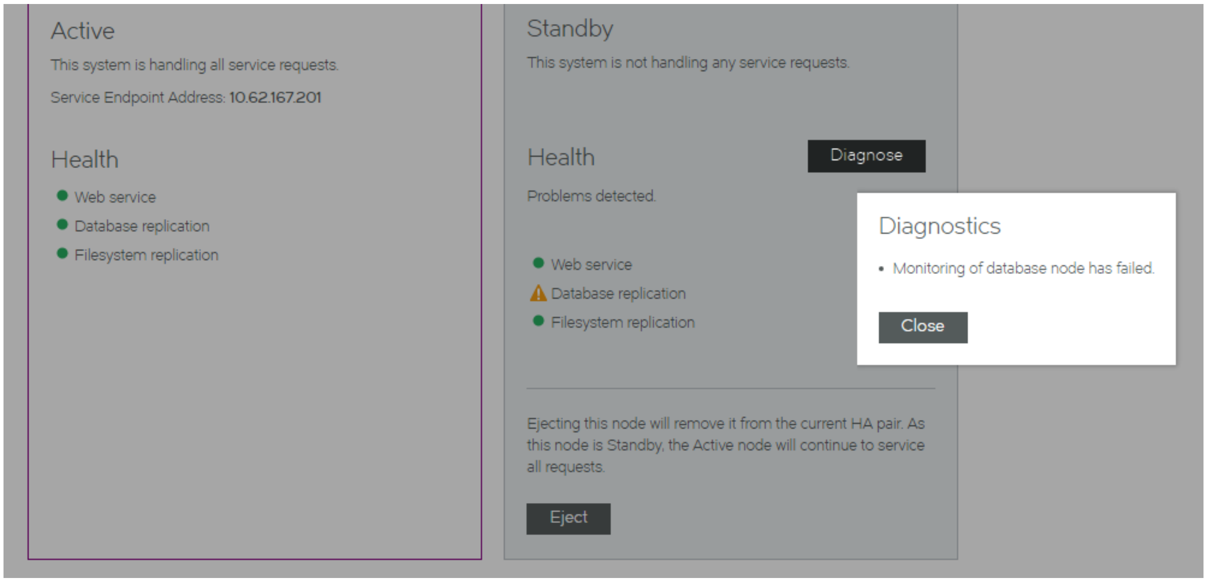
Problems detected.

- ● Web service
- ⚠ Database replication
- ● Filesystem replication

Ejecting this node will remove it from the current HA pair. As this node is Standby, the Active node will continue to service all requests.

Click the **Diagnose** button to understand more about the problem. For example:

FIGURE 212 Manage HA Page: Diagnosing Unhealthy State



Active

This system is handling all service requests.

Service Endpoint Address: 10.62.167.201

Health

- ● Web service
- ● Database replication
- ● Filesystem replication

Standby

This system is not handling any service requests.

Health

Diagnose

Problems detected.

- ● Web service
- ⚠ Database replication
- ● Filesystem replication

Ejecting this node will remove it from the current HA pair. As this node is Standby, the Active node will continue to service all requests.

Eject

Diagnostics

- Monitoring of database node has failed.

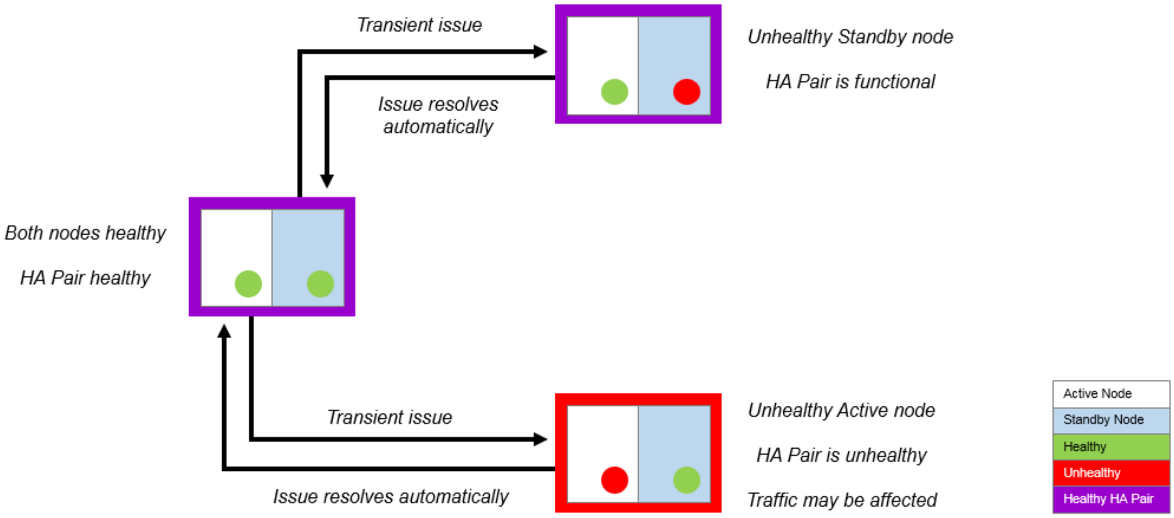
Close

Several kinds of errors can be reported:

- Some errors are caused by transient issues in your network, and will clear once the network recovers.

  If an error does not clear in a few minutes, further investigation may be required.

  FIGURE 213 High Availability: Transient Network Issues

- Some errors may require an Administrator to log in to the affected node directly to analyze and fix a reported issue using a reboot, the REST API or the Command-Line User Interface (CLI). Refer to the *Brocade Services Director Advanced User Guide* and the *Brocade Services Director Command Reference* for details.

- Some errors are caused by the failure of one of the nodes. To respond to this, you can change the Active and Standby roles using software operations:
  - The Standby node can perform a *failover*. This operation swaps the roles performed by the paired Services Director. Both nodes must be healthy to do this, you must repair the unhealthy node first. Failover is commonly used before performing maintenance on an Active node. (refer to Swapping the Roles of the HA Nodes on page 208).
  - The Active node can *eject* an unhealthy Standby node in the event of failure. This creates an Active standalone Services Director and an unpaired Standby Services Director. Refer to Ejecting a Node from an HA Pair on page 212.
  - The Standby node can perform a *forced failover*. This operation attempts to swap the roles performed by the paired Services Director while the Active node is unhealthy. (refer to Recovering from a Failed Active Node on page 218).
  - An Active node can perform a *forced standby* on itself. This operation is used to recover from an exceptional circumstance where both nodes in an HA pair believes itself to be the Active node. Refer to Recovering from a Split Brain Scenario on page 223.

Swapping the Roles of the HA Nodes

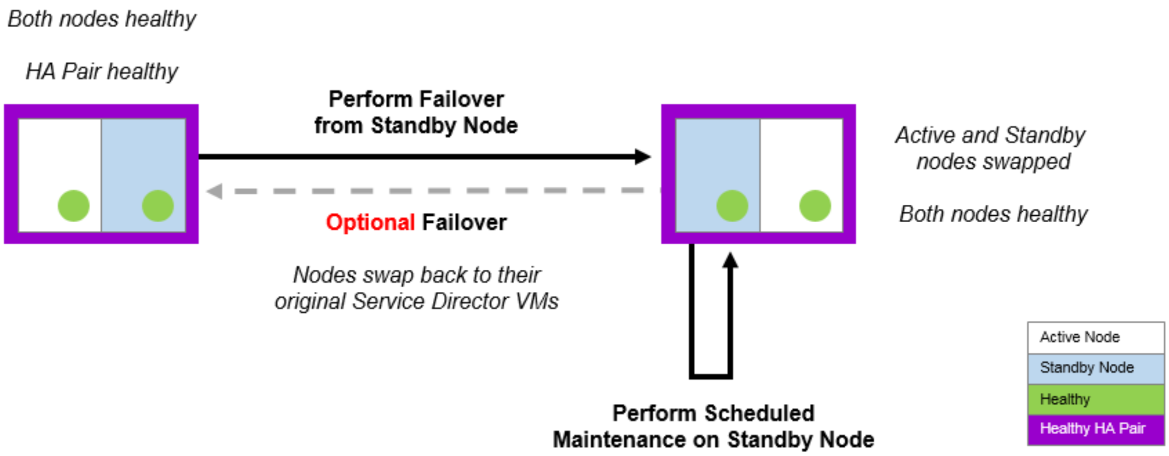
When you swap the roles of the Active and Standby nodes, the process is called *failover*.

Both nodes must be healthy to perform a failover.

Failover is useful in a number of scenarios:

- Before performing scheduled maintenance on the Active node.
- Before performing additional repairs to a recently-repaired Active node.
- To enable the current Active node to be subsequently ejected.

FIGURE 214 High Availability: Failover


Both nodes healthy
HA Pair healthy
Perform Failover from Standby Node
Optional Failover
Nodes swap back to their original Service Director VMs
Active and Standby nodes swapped
Both nodes healthy
Perform Scheduled Maintenance on Standby Node
Active Node
Standby Node
Healthy
Healthy HA Pair

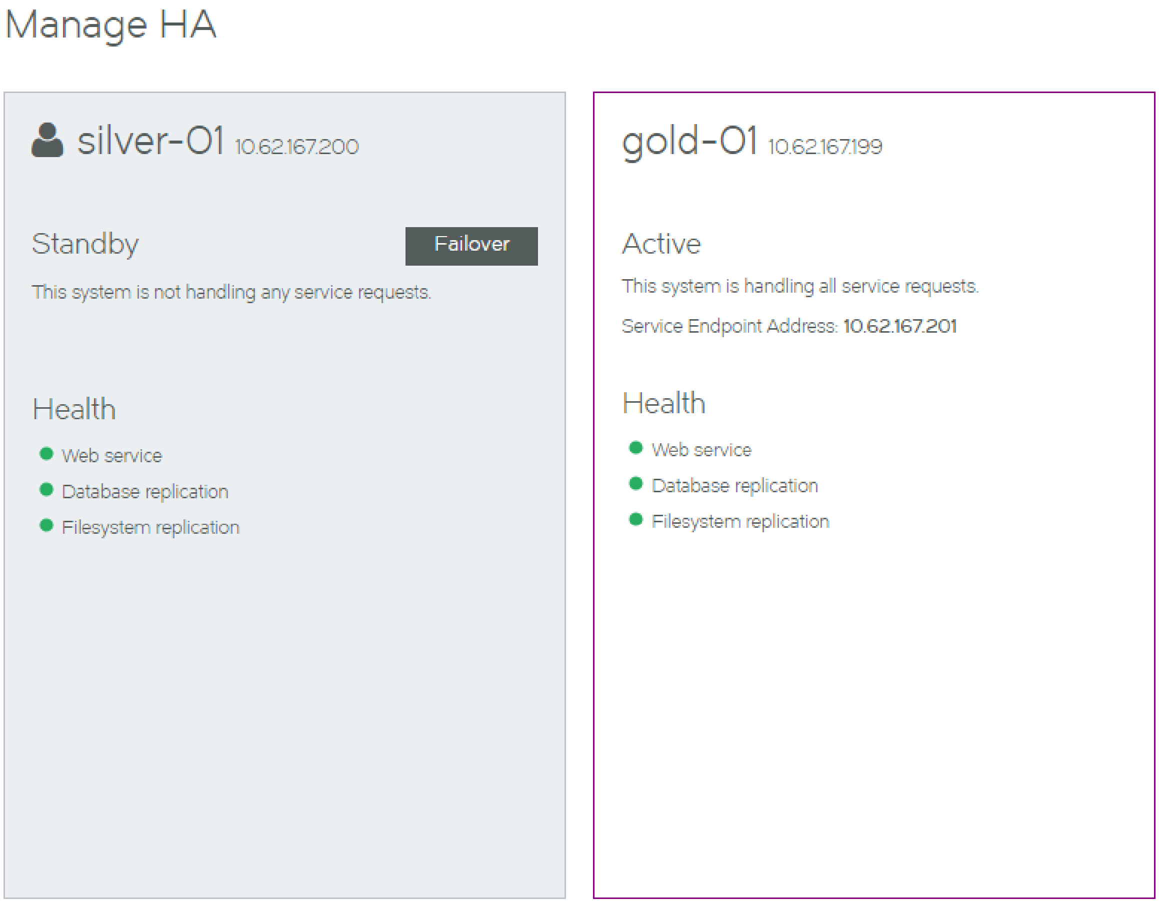
After a failover completes, the Services Endpoint Address points to the new Active node.

If either of the nodes is unhealthy, you must repair the unhealthy node first, or use a different operation such as an ejection (refer to Ejecting a Node from an HA Pair on page 212) or a forced failover (refer to Recovering from a Failed Active Node on page 218).

Performing a Failover from the Standby Node

1. Access your Standby Services Director VA from a browser, using either the IP address or hostname of your Standby node.
2. Log in as the administration user. The **Home** page appears.
3. Click the **Services** menu, and then click **High Availability: Manage HA**. The **Manage HA** page appears.

FIGURE 215 Manage HA Page: Before Failover



Manage HA

silver-01 10.62.167.200

Standby

This system is not handling any service requests.

Health

- Web service
- Database replication
- Filesystem replication

gold-01 10.62.167.199

Active

This system is handling all service requests.

Service Endpoint Address: 10.62.167.201

Health

- Web service
- Database replication
- Filesystem replication

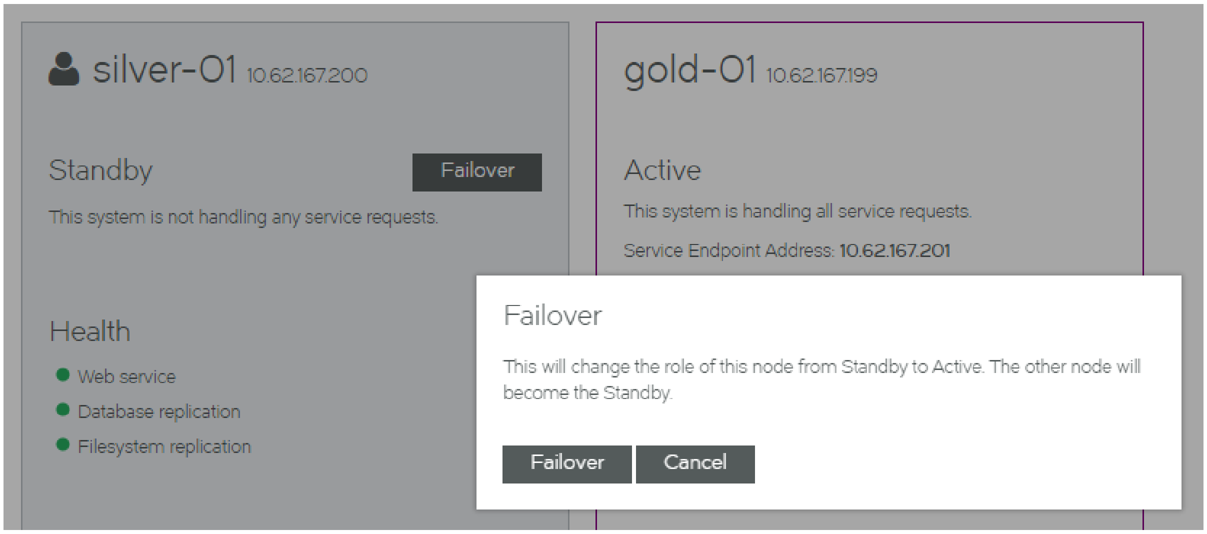
In this example:

- The Standby node (**silver-01**) is displayed on the left in a blue/gray panel.
- The Active node (**gold-01**) is displayed on the right in a white panel.
- A **Failover** button is available for the Standby node.

4. Ensure that all healthy indicators are green.

5. In the Standby panel, click **Failover**. An information panel appears.

FIGURE 216 Manage HA Page: Confirming a Failover



silver-01 10.62.167.200

Standby

This system is not handling any service requests.

Health

● Web service

● Database replication

● Filesystem replication

gold-01 10.62.167.199

Active

This system is handling all service requests.

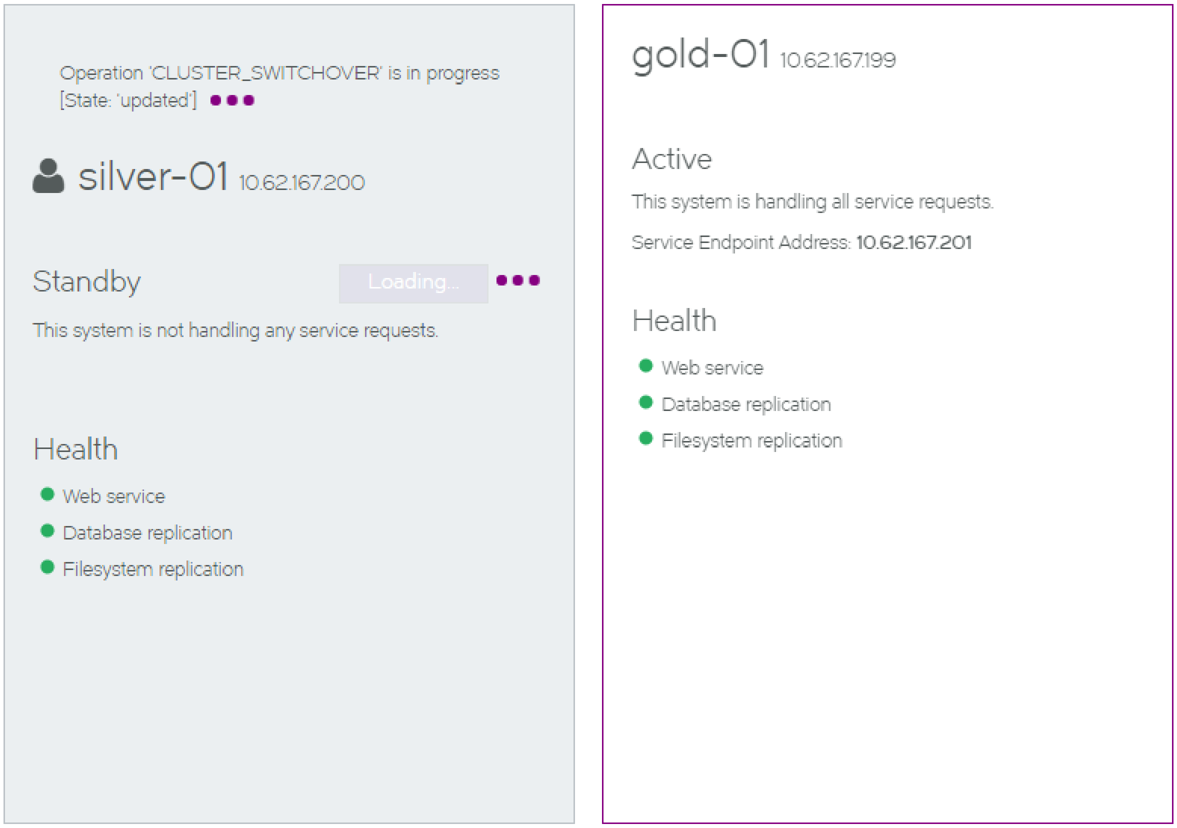
Service Endpoint Address: **10.62.167.201**

Failover

This will change the role of this node from Standby to Active. The other node will become the Standby.

6. Click **Failover**. The failover starts.

FIGURE 217 Manage HA Page: Failover In Progress



Operation 'CLUSTER_SWITCHOVER' is in progress [State: 'updated'] ●●●

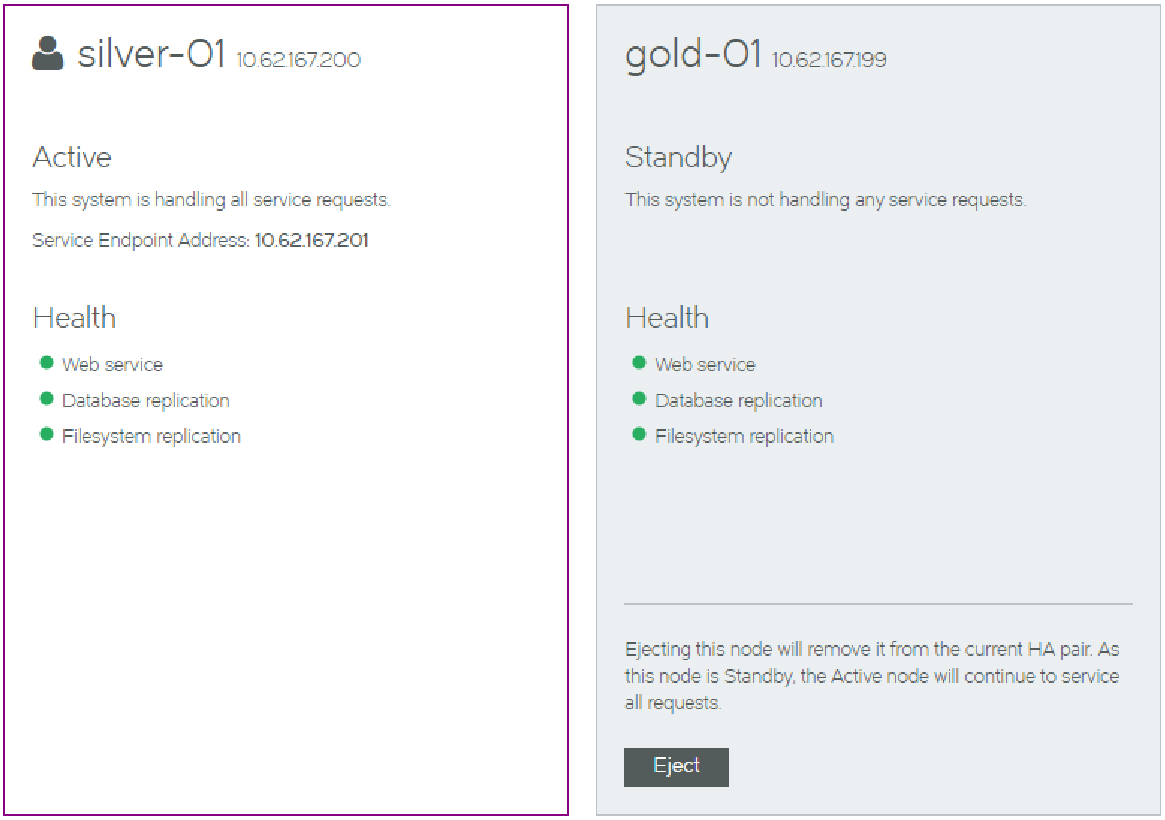
NOTE
The failover process reports an error and stops if the Active node goes down as the failover is started. A retry of the failover will become a forced failover. Refer to Recovering from a Failed Active Node on page 218.

7. Wait for the process to complete. The health indicators may become orange during the transition, but these will clear.

   After the failover completes, the **Manage HA** page updates:

   - the original Standby node (**silver-01**) is now the Active node.
   - the original Active node (**gold-01**) is now the Standby node.
   - All health indicators are green.

   FIGURE 218 Manage HA Page: Failover Complete



silver-01 10.62.167.200

Active

This system is handling all service requests.

Service Endpoint Address: 10.62.167.201

Health

● Web service

● Database replication

● Filesystem replication

gold-01 10.62.167.199

Standby

This system is not handling any service requests.

Health

● Web service

● Database replication

● Filesystem replication

Ejecting this node will remove it from the current HA pair. As this node is Standby, the Active node will continue to service all requests.

8. (Optional) Perform the following actions

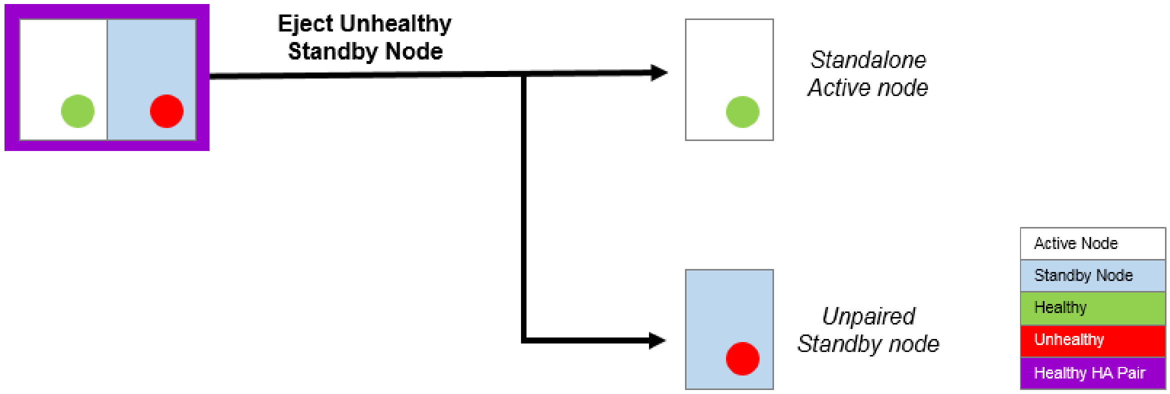
   - Perform maintenance on the new Standby node.
   - Perform another failover to return the Primary Services Director and Secondary Services Director to their original roles.
   - Eject the Standby node. Refer to Ejecting a Node from an HA Pair on page 212.

Ejecting a Node from an HA Pair

A healthy Active node can *eject* the other member of an HA pair. This is useful in a number of scenarios:

- Ejecting an unhealthy Standby node in the event of failure. This creates a standalone Active node and an unpaired unhealthy Standby node.

FIGURE 219 High Availability: Ejecting Unhealthy Standby Node

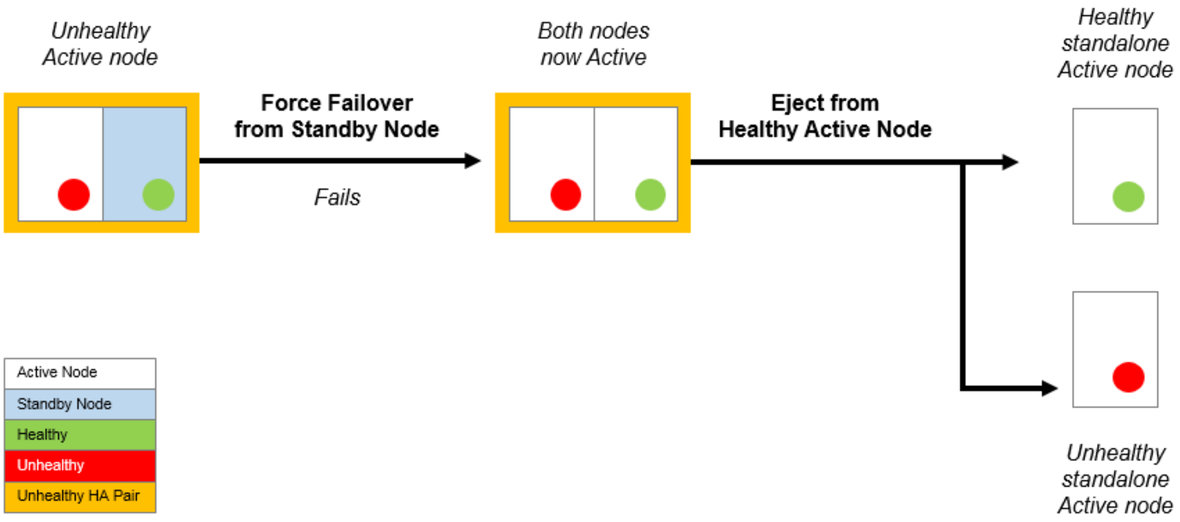


Once the Standby node is repaired, it can be joined to any standalone node to form an HA pair.

- Ejecting an unhealthy node after a forced failover operation fails.

  In this instance, both nodes are Active, but one is unhealthy. The unhealthy Active node can be ejected from the healthy Active node.

  FIGURE 220 High Availability: Ejecting After Forced Failover Fails



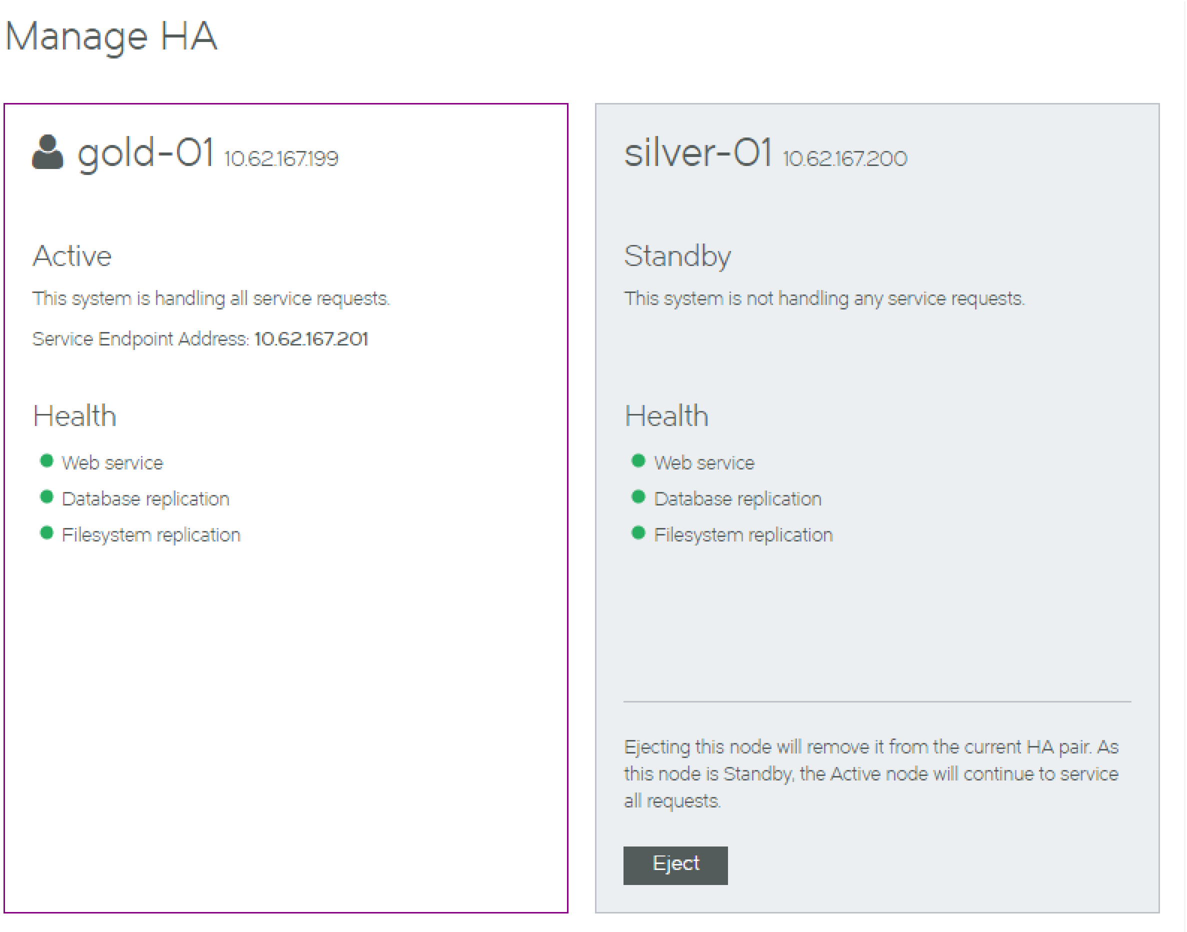
- You can also eject a healthy Standby node if required. This results in a healthy standalone node and a healthy unpaired node.

Ejecting a Standby Node from the Active Node

1. Access your Active Services Director VA from a browser, using the Service Endpoint Address of your Services Director.
2. Log in as the administration user. The **Home** page appears.

3. Click the **Services** menu, and then click **High Availability: Manage HA**. The **Manage HA** page appears.

FIGURE 221 Manage HA Page: Before Ejection



Manage HA

gold-01 10.62.167.199

Active

This system is handling all service requests.

Service Endpoint Address: 10.62.167.201

Health

- ● Web service
- ● Database replication
- ● Filesystem replication

silver-01 10.62.167.200

Standby

This system is not handling any service requests.

Health

- ● Web service
- ● Database replication
- ● Filesystem replication

Ejecting this node will remove it from the current HA pair. As this node is Standby, the Active node will continue to service all requests.

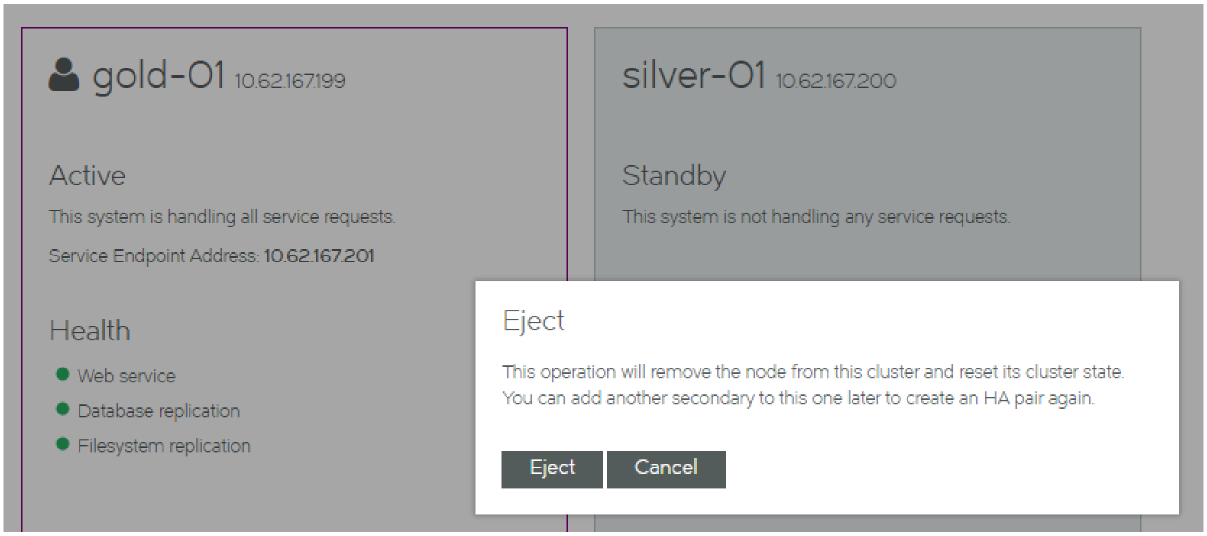
In this example:

- The Active node (**gold-01**) is displayed on the left in a white panel.
- The Standby node (**silver-01**) is displayed on the right in a blue/gray panel.
- An **Eject** button is available for the Standby node.

4. Ensure that all healthy indicators are green.

5. In the Standby panel, click **Eject**. An information panel appears.

FIGURE 222 Manage HA Page: Confirming an Ejection



gold-01 10.62.167.199

Active

This system is handling all service requests.

Service Endpoint Address: 10.62.167.201

Health

- Web service
- Database replication
- Filesystem replication

silver-01 10.62.167.200

Standby

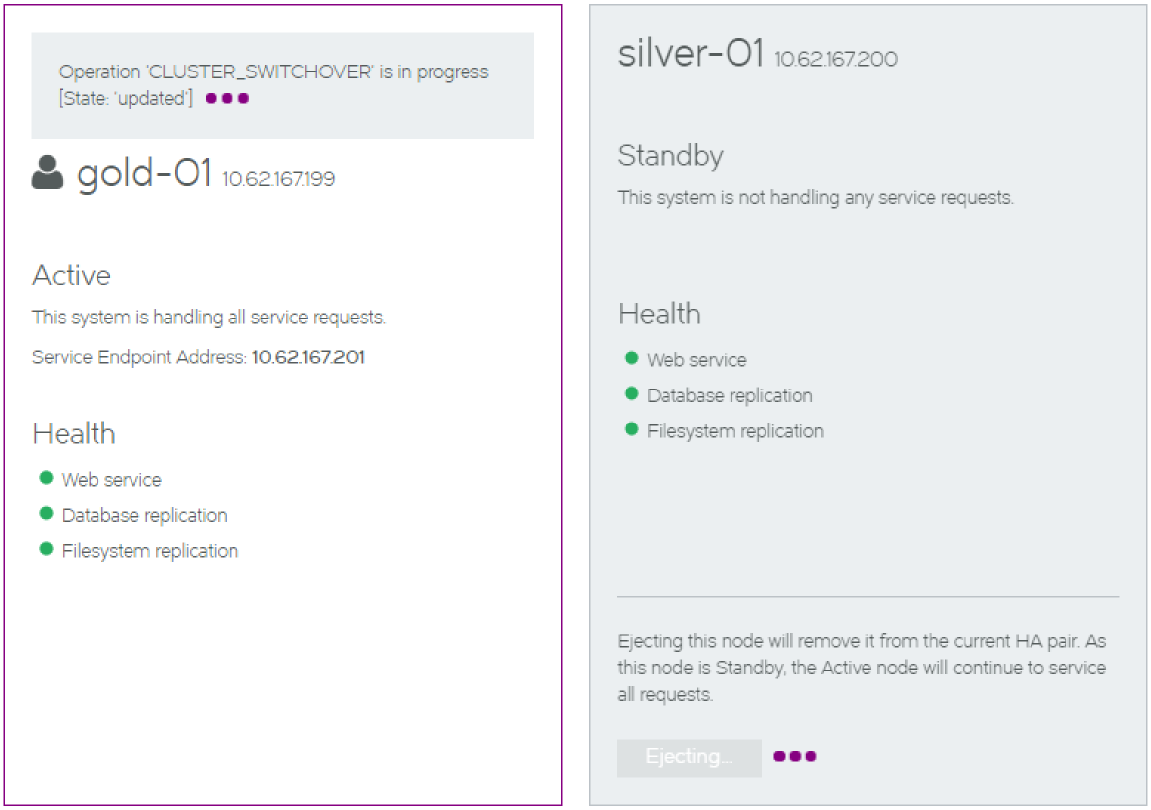
This system is not handling any service requests.

Eject

This operation will remove the node from this cluster and reset its cluster state. You can add another secondary to this one later to create an HA pair again.

6. Click **Eject**. The ejection starts, and reports progress.

FIGURE 223 Manage HA Page: Ejection In Progress



Operation 'CLUSTER_SWITCHOVER' is in progress [State: 'updated'] ●●●

gold-01 10.62.167.199

Active

This system is handling all service requests.

Service Endpoint Address: 10.62.167.201

Health

- ● Web service
- ● Database replication
- ● Filesystem replication

silver-01 10.62.167.200

Standby

This system is not handling any service requests.

Health

- ● Web service
- ● Database replication
- ● Filesystem replication

Ejecting this node will remove it from the current HA pair. As this node is Standby, the Active node will continue to service all requests.

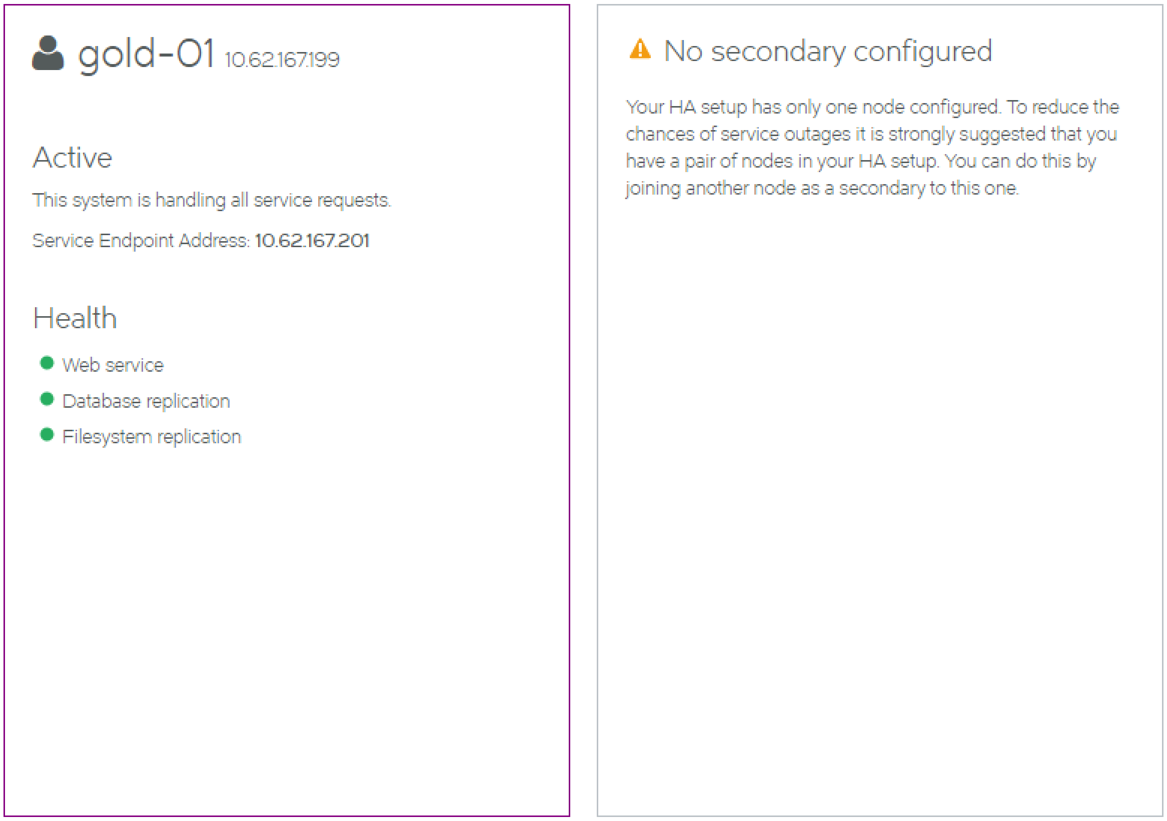
7. Wait for the process to complete. The health indicators may become orange during the transition, but these will clear.

   After the ejection completes, the **Manage HA** page updates:

   - The original Active node (**gold-01**) remains in place as a standalone node.
   - No Standby node is configured.

     The original Standby node still exists, but it is now an unpaired Services Director node.
   - All health indicators are green.

   FIGURE 224 Manage HA Page: Ejection Complete



gold-01 10.62.167.199

Active

This system is handling all service requests.

Service Endpoint Address: 10.62.167.201

Health

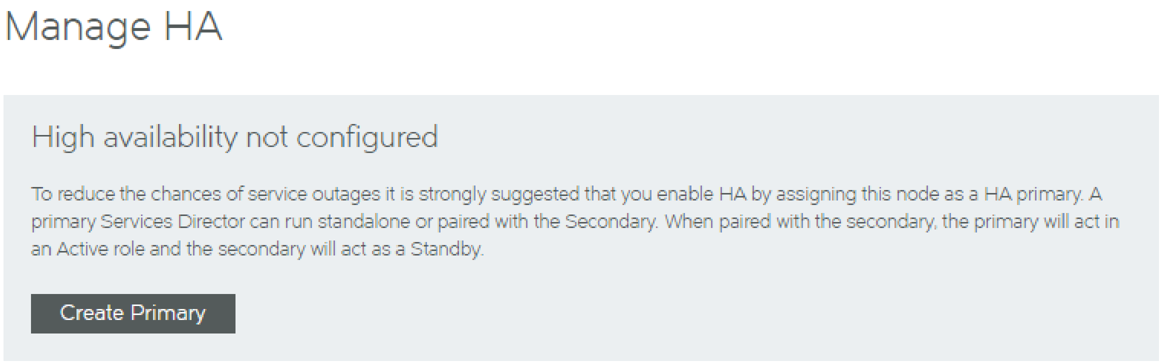
● Web service
● Database replication
● Filesystem replication

⚠ No secondary configured

Your HA setup has only one node configured. To reduce the chances of service outages it is strongly suggested that you have a pair of nodes in your HA setup. You can do this by joining another node as a secondary to this one.

8. (Optional) Confirm the state of the original Standby node. To do this, start its Services Director VA using its IP address or hostname and access its **Manage HA** page.

FIGURE 225 Manage HA Page: Post-Ejection State of Original Standby Node



Manage HA

High availability not configured

To reduce the chances of service outages it is strongly suggested that you enable HA by assigning this node as a HA primary. A primary Services Director can run standalone or paired with the Secondary. When paired with the secondary, the primary will act in an Active role and the secondary will act as a Standby.

From this screen, you can convert this ejected Standby node into a standalone Active node. See Converting an Ejected Node into a Standalone Active Node on page 230.

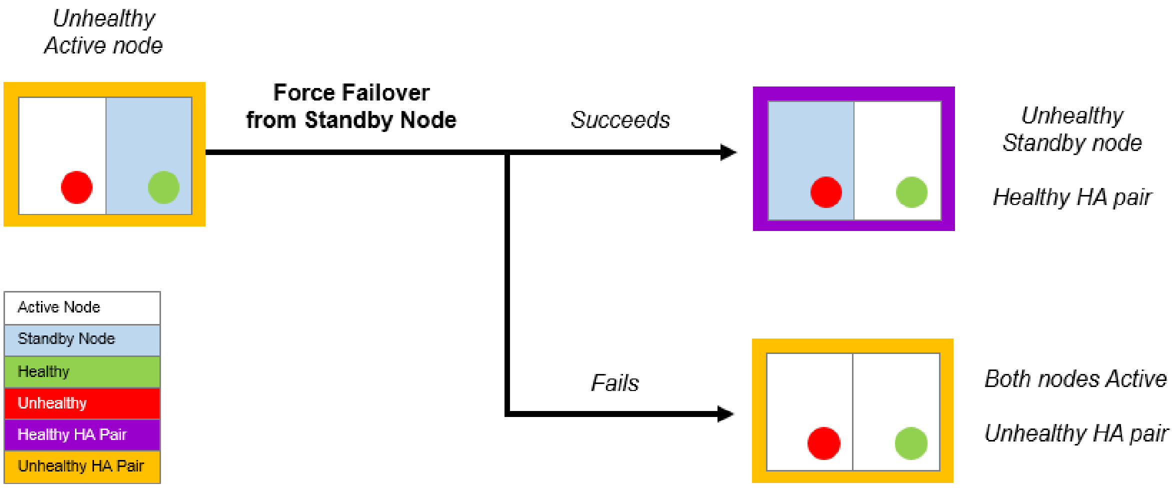
Recovering from a Failed Active Node

If your Active node becomes unhealthy, it must be repaired.

Maintenance is typically performed on a Standby node. However, you cannot perform a failover to swap the Active and Standby nodes, because a failover requires both nodes to be healthy.

To resolve a failed Active node, you must attempt a *forced failover* from the healthy Standby node.

FIGURE 226 High Availability: Attempting a Forced Failover



If the forced failover succeeds:

- The healthy Standby node becomes the healthy Active node.
- The unhealthy Active node becomes a Standby node.
- You can then perform maintenance on the Standby node. Alternatively, you can eject the unhealthy Standby node if required (refer to Ejecting a Node from an HA Pair on page 212).
- The Services Endpoint Address points to the new Active node.

If the forced failover fails:

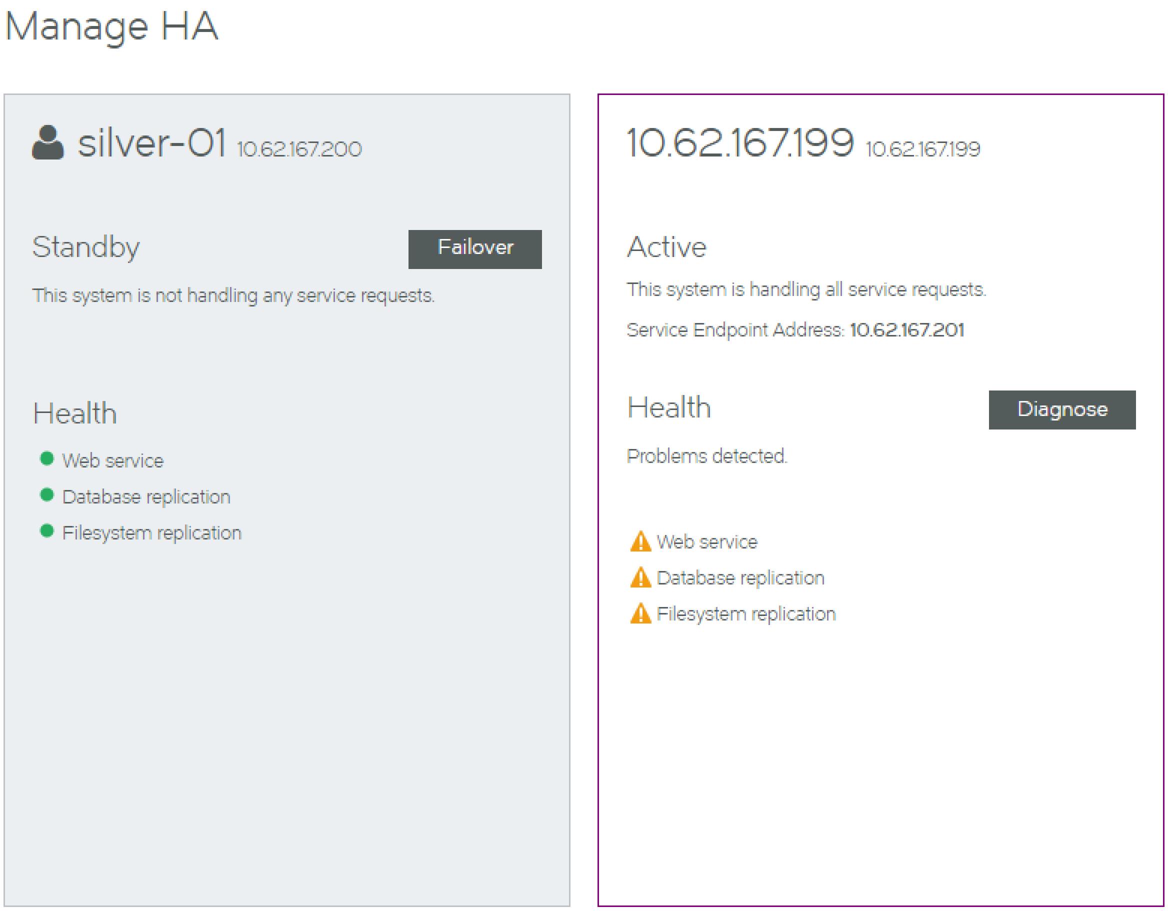
- The healthy Standby node becomes a healthy Active node.
- The unhealthy Active node may remain as an Active node. To resolve this you can:
  - Eject the unhealthy Active node from the healthy Active node (refer to Ejecting a Node from an HA Pair on page 212).
  - Repair the unhealthy Active node. In this case, a "split brain" scenario develops (refer to Recovering from a Split Brain Scenario on page 223).

To Perform a Forced Failover from the Standby Node

1. Access your Active Services Director VA from a browser, using either the IP address or hostname of the healthy Active node.
2. Log in as the administration user. The **Home** page appears.

3. Click the **Services** menu, and then click **High Availability: Manage HA**. The **Manage HA** page appears.

FIGURE 227 Manage HA Page: Before Forced Failover



Manage HA

silver-01 10.62.167.200

Standby

This system is not handling any service requests.

Health

● Web service
● Database replication
● Filesystem replication

10.62.167.199 10.62.167.199

Active

This system is handling all service requests.

Service Endpoint Address: **10.62.167.201**

Health

Problems detected.

⚠ Web service
⚠ Database replication
⚠ Filesystem replication

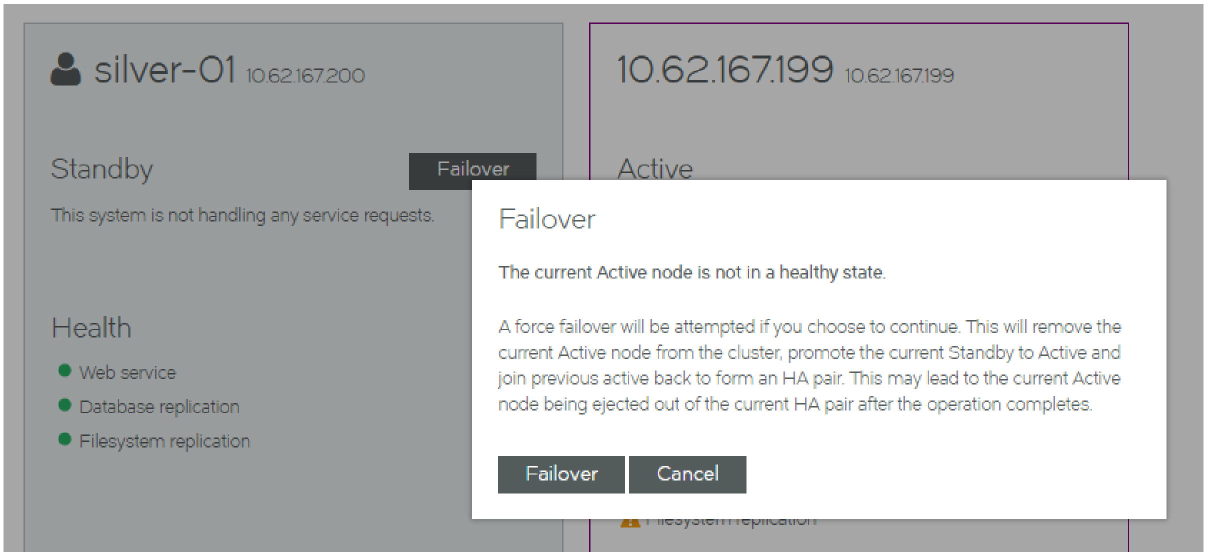
In this example:

- The Standby node (**silver-01**) is healthy.
- The Active node (**gold-01**, identified as 10.62.167.199) is unhealthy.
- The **Failover** button is available for the Standby node.

4. Click the **Failover** button.

   A warning is displayed. This indicates that a forced failover is required, as the Active node is not in a healthy state.

FIGURE 228 Manage HA Page: Confirming Forced Failover



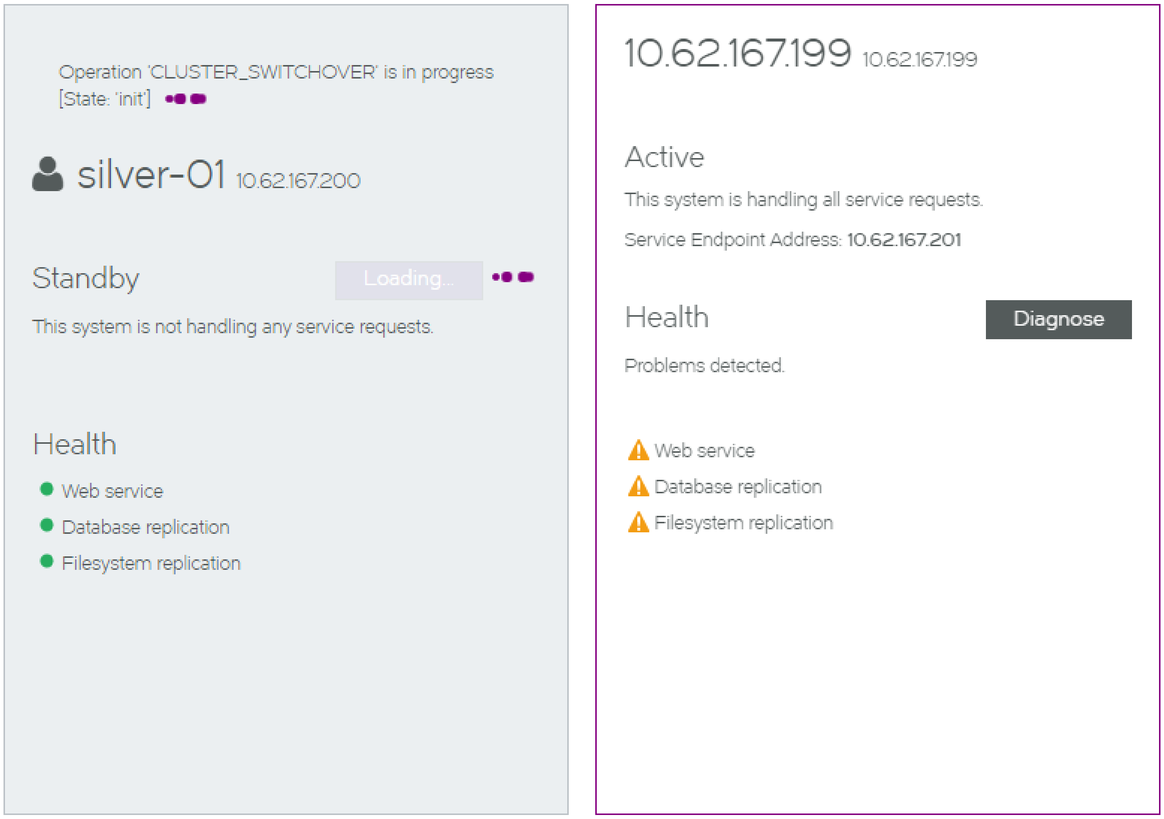
Failover

The current Active node is not in a healthy state.

A force failover will be attempted if you choose to continue. This will remove the current Active node from the cluster, promote the current Standby to Active and join previous active back to form an HA pair. This may lead to the current Active node being ejected out of the current HA pair after the operation completes.

5. Click **Failover** to confirm the forced failover. The process starts, and displays progress.

FIGURE 229 Manage HA Page: Forced Failover In Progress



Operation 'CLUSTER_SWITCHOVER' is in progress [State: 'init']

silver-01 10.62.167.200

Standby

This system is not handling any service requests.

Health

- ● Web service
- ● Database replication
- ● Filesystem replication

10.62.167.199 10.62.167.199

Active

This system is handling all service requests.

Service Endpoint Address: 10.62.167.201

Health

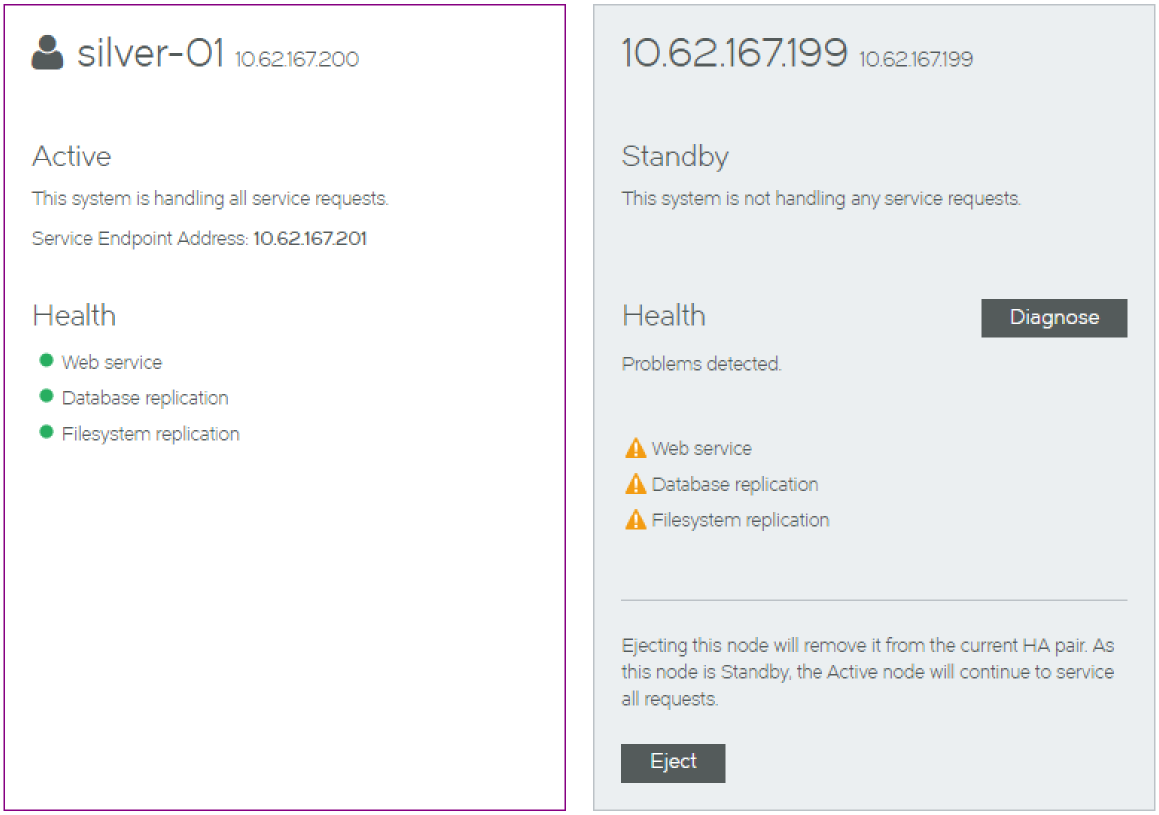
Problems detected.

- ⚠ Web service
- ⚠ Database replication
- ⚠ Filesystem replication

6. Wait for the process to complete.

   After the ejection completes, the **Manage HA** page updates.

   FIGURE 230 Manage HA Page: Forced Failover Complete



silver-01 10.62.167.200

Active

This system is handling all service requests.

Service Endpoint Address: **10.62.167.201**

Health

- ● Web service
- ● Database replication
- ● Filesystem replication

10.62.167.199 10.62.167.199

Standby

This system is not handling any service requests.

Health

Problems detected.

- ⚠ Web service
- ⚠ Database replication
- ⚠ Filesystem replication

Ejecting this node will remove it from the current HA pair. As this node is Standby, the Active node will continue to service all requests.

   It may be difficult to assess the success of this operation from the new Active node.

7. To assess the success/failure of the forced failover, start the Services Director VA for the unhealthy Standby node and access its **Manage HA** page.

   If the process has completed successfully:

   - The unhealthy Standby node is shown on the left
   - The healthy Active node is shown on the right.

   If the process has completed unsuccessfully:

   - The unhealthy Standby node is shown on the left
   - A "split brain" scenario is reported. See Recovering from a Split Brain Scenario on page 223 for details.

Recovering from a Split Brain Scenario

The *"split brain"* scenario is an exceptional circumstance where two healthy nodes in an HA pair both believe themselves to be the Active node, and that the other node is the Standby.

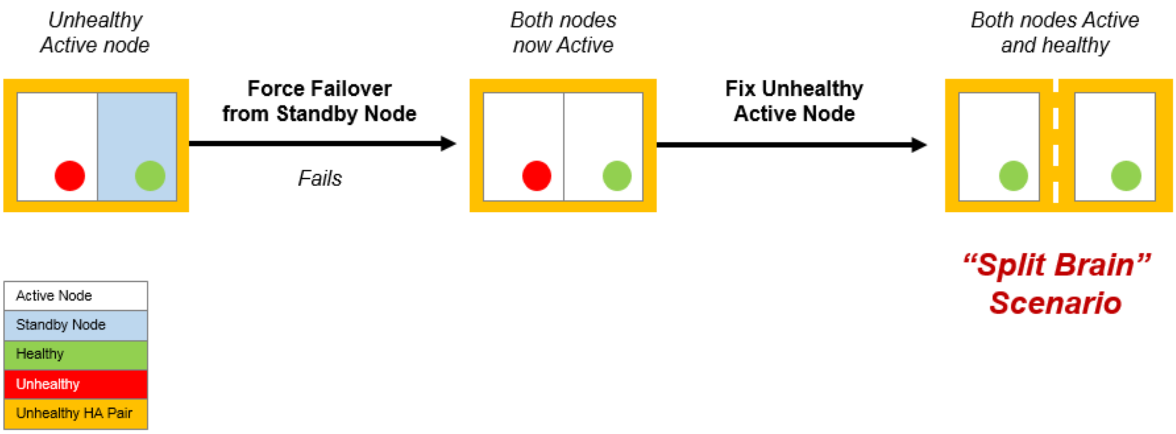
This scenario represents an unhealthy HA pair, and must be resolved.

Understanding How the Split Brain Scenario Arises

The "split brain" scenario can occur after a failed *forced failover* operation. Specifically:

1. The healthy Standby node becomes an Active node.
2. The unhealthy Active node fails to become the Standby node.
3. The unhealthy Active node is repaired. Both nodes are now healthy and Active, and each also believes the other node in the HA pair to be the Standby node. This is the "split brain" scenario.

FIGURE 231 High Availability: How "Split Brain" Scenario Occurs

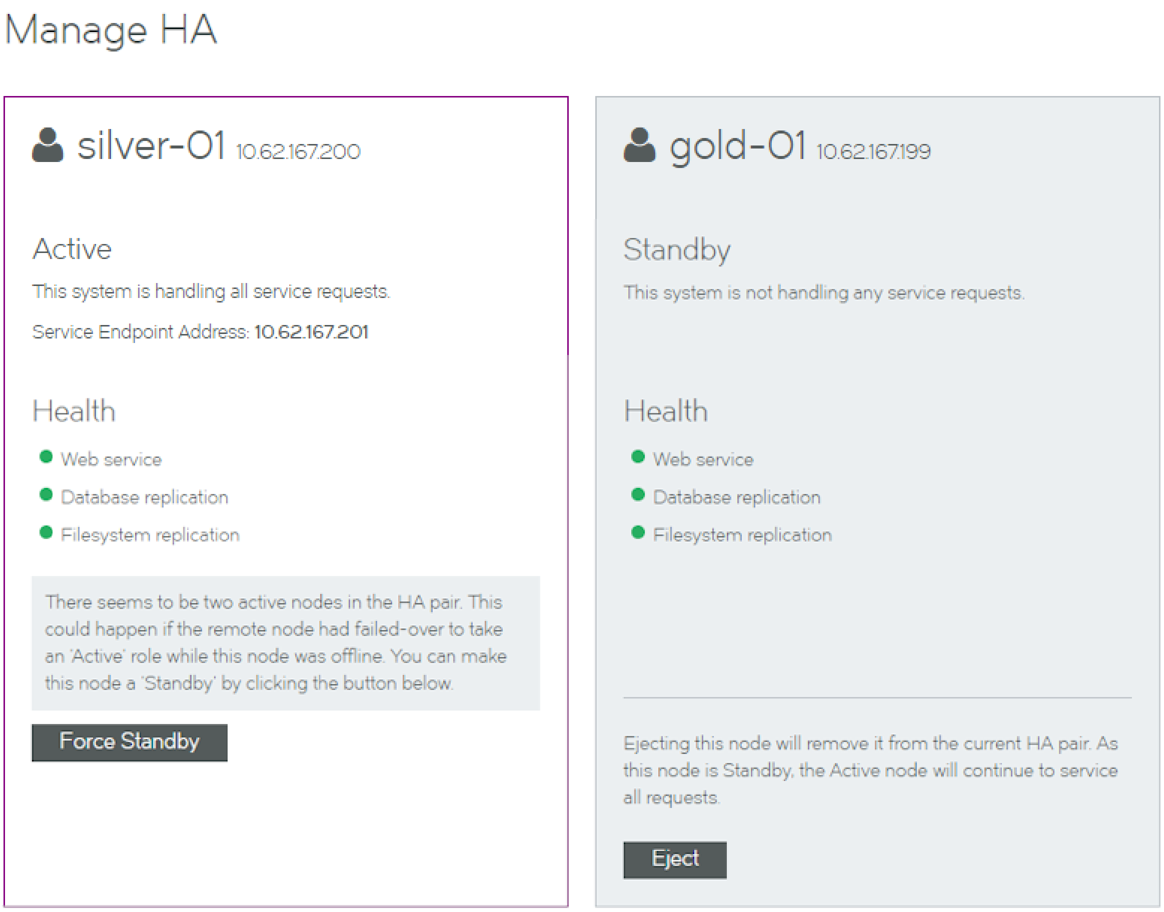


Refer to Recovering from a Failed Active Node on page 218 for details of the Forced Failover operation.

Viewing the Split Brain Scenario

A notification of a "split brain" scenario is included in the **Manage HA** page. It is shown in the panel for the Active node, along with a **Force Standby** button.

FIGURE 232 High Availability: Notification of "Split Brain" Scenario



Manage HA

silver-01 10.62.167.200

Active

This system is handling all service requests.

Service Endpoint Address: **10.62.167.201**

Health

- ● Web service
- ● Database replication
- ● Filesystem replication

There seems to be two active nodes in the HA pair. This could happen if the remote node had failed-over to take an 'Active' role while this node was offline. You can make this node a 'Standby' by clicking the button below.

gold-01 10.62.167.199

Standby

This system is not handling any service requests.

Health

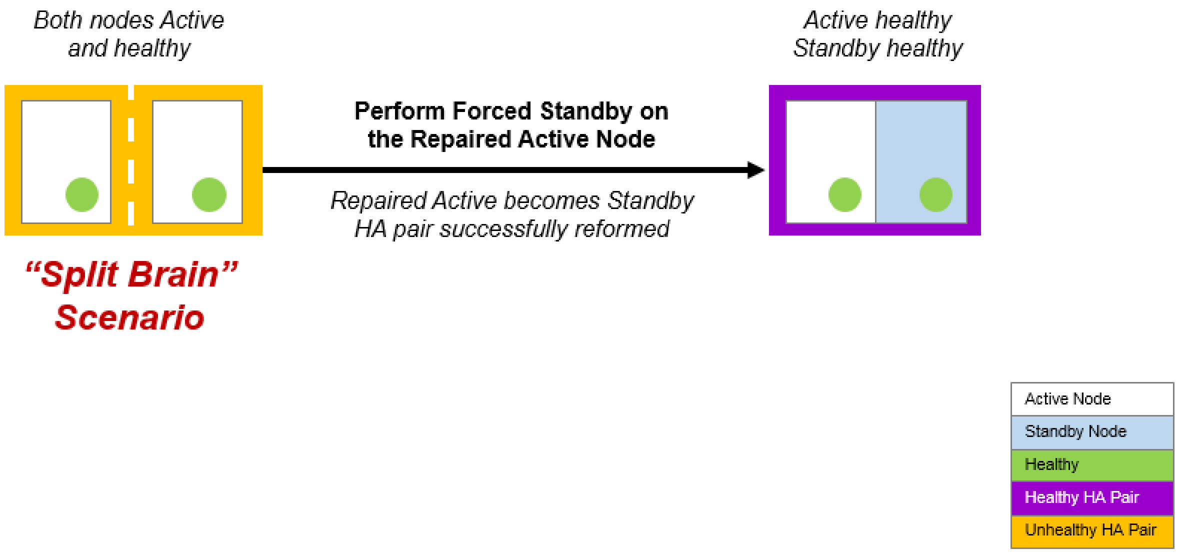
- ● Web service
- ● Database replication
- ● Filesystem replication

Ejecting this node will remove it from the current HA pair. As this node is Standby, the Active node will continue to service all requests.

Resolving a Split Brain Scenario

To resolve the "split brain" scenario, perform a Forced Standby operation from the repaired Active node. This forces the repaired Active node to become the Standby node in the HA pair.

FIGURE 233 High Availability: Resolving a "Split Brain" Scenario


Both nodes Active and healthy
"Split Brain" Scenario
Perform Forced Standby on the Repaired Active Node
Repaired Active becomes Standby
HA pair successfully reformed
Active healthy
Standby healthy
Active Node
Standby Node
Healthy
Healthy HA Pair
Unhealthy HA Pair

1. Access the Services Director VA for the repaired Active node from a browser, using either the IP address or hostname of your repaired Active node.

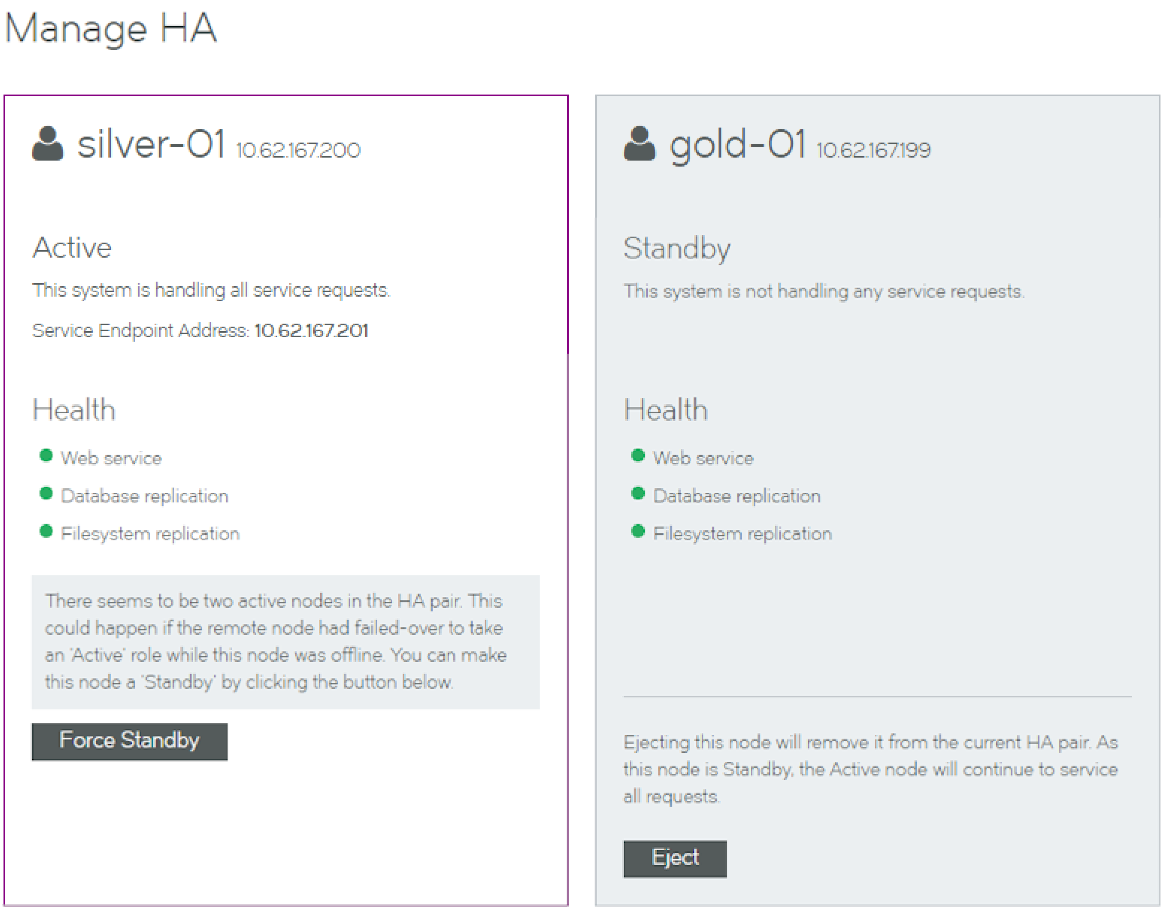
   Do not access the Services Director VA using the Service Endpoint Address.

2. Log in as the administration user. The **Home** page appears.

3. Click the **Services** menu, and then click **High Availability: Manage HA**. The **Manage HA** page appears.

   A notification of a split brain is included in the panel for the Active node, along with a **Force Standby** button.

FIGURE 234 Manage HA Page: Before Forced Standby



Manage HA

silver-01 10.62.167.200

Active

This system is handling all service requests.

Service Endpoint Address: 10.62.167.201

Health

● Web service

● Database replication

● Filesystem replication

There seems to be two active nodes in the HA pair. This could happen if the remote node had failed-over to take an 'Active' role while this node was offline. You can make this node a 'Standby' by clicking the button below.

gold-01 10.62.167.199

Standby

This system is not handling any service requests.

Health

● Web service

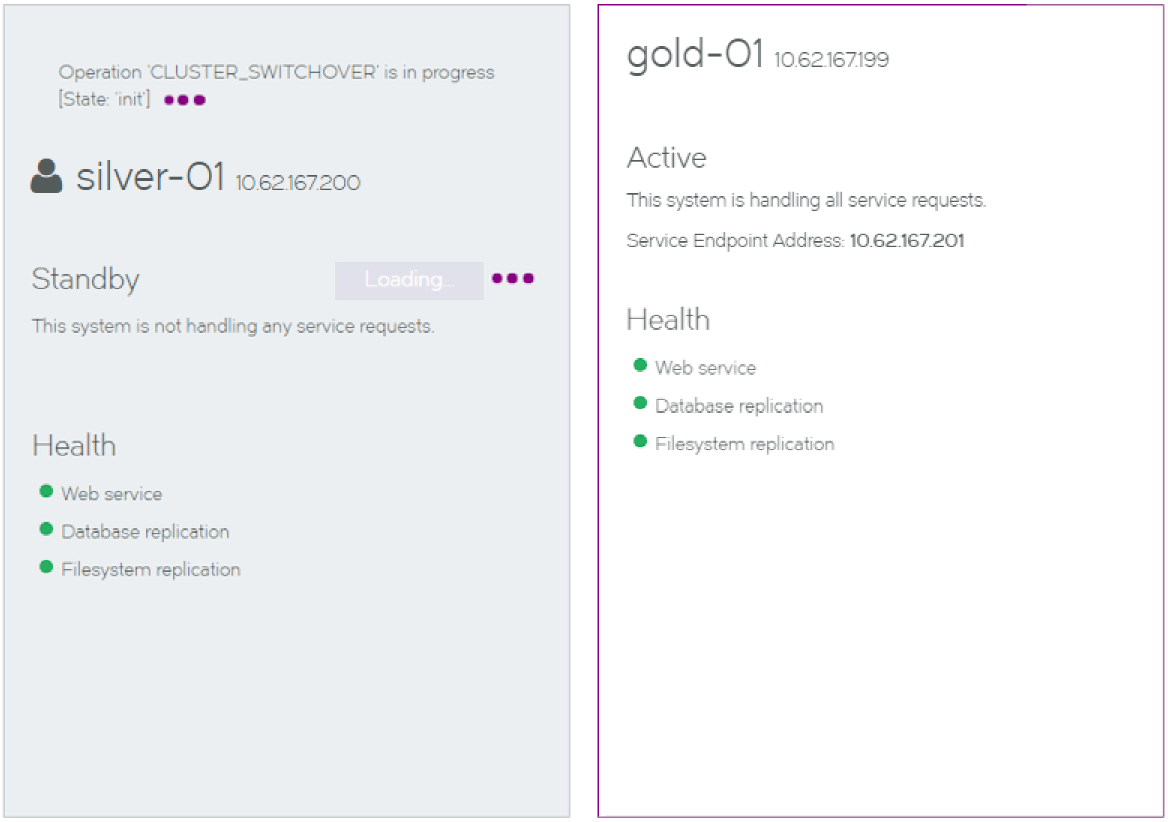
● Database replication

● Filesystem replication

Ejecting this node will remove it from the current HA pair. As this node is Standby, the Active node will continue to service all requests.

4. Click **Force Standby**. The forced standby starts, and progress is reported. During this process:
   - The repaired Active (in this case, **silver-01**) becomes the Standby node.
   - The other Active node becomes correctly identified and colored.

FIGURE 235 Manage HA Page: Forced Standby In Progress



Operation 'CLUSTER_SWITCHOVER' is in progress [State: 'init']

silver-01 10.62.167.200

Standby

This system is not handling any service requests.

Health

- ● Web service
- ● Database replication
- ● Filesystem replication

gold-01 10.62.167.199

Active

This system is handling all service requests.

Service Endpoint Address: **10.62.167.201**

Health

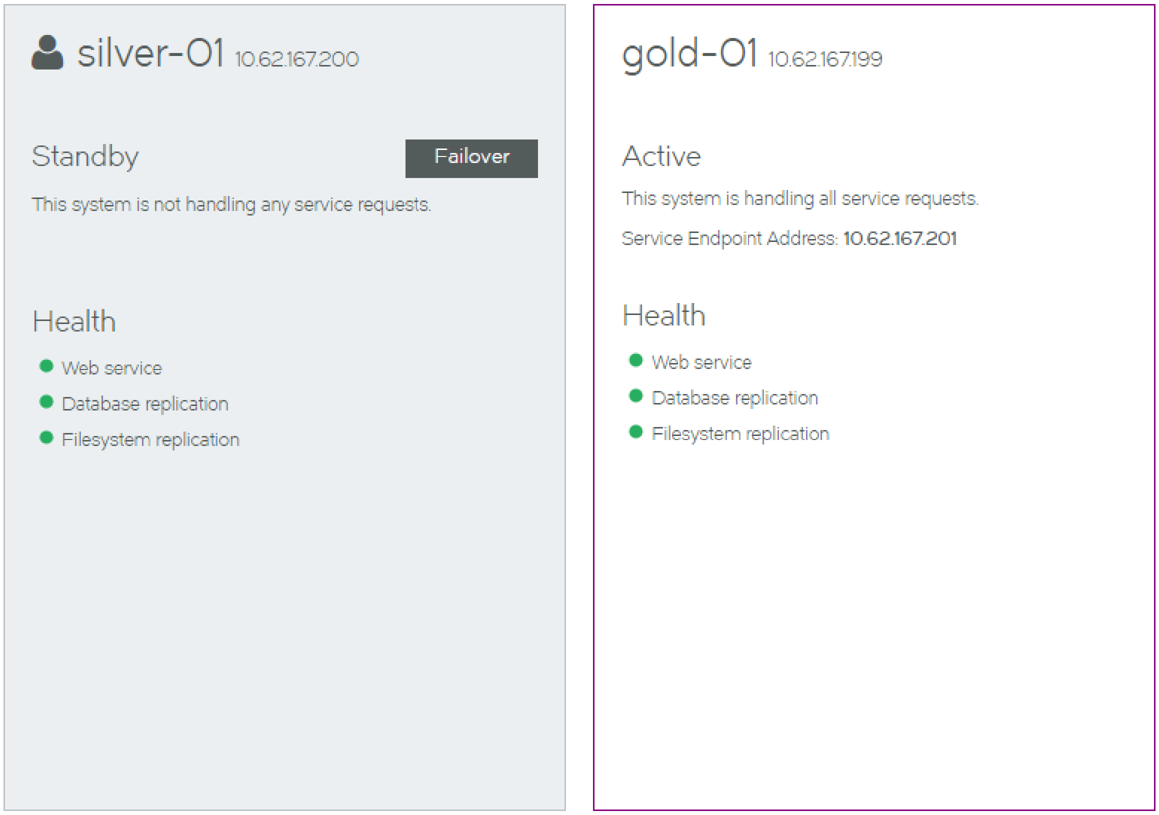
- ● Web service
- ● Database replication
- ● Filesystem replication

5. Wait for the process to complete. The health indicators may become orange during the transition, but these will clear.

   After the forced standby completes, the **Manage HA** page updates:

   - The new Standby node (**silver-01**) is on the left.
   - The Active node (**gold-01**) is on the right.
   - All health indicators are green.

   FIGURE 236 Manage HA Page: Force Standby Complete (Standby Node)



silver-01 10.62.167.200

Standby

This system is not handling any service requests.

Health

● Web service
● Database replication
● Filesystem replication

gold-01 10.62.167.199

Active

This system is handling all service requests.

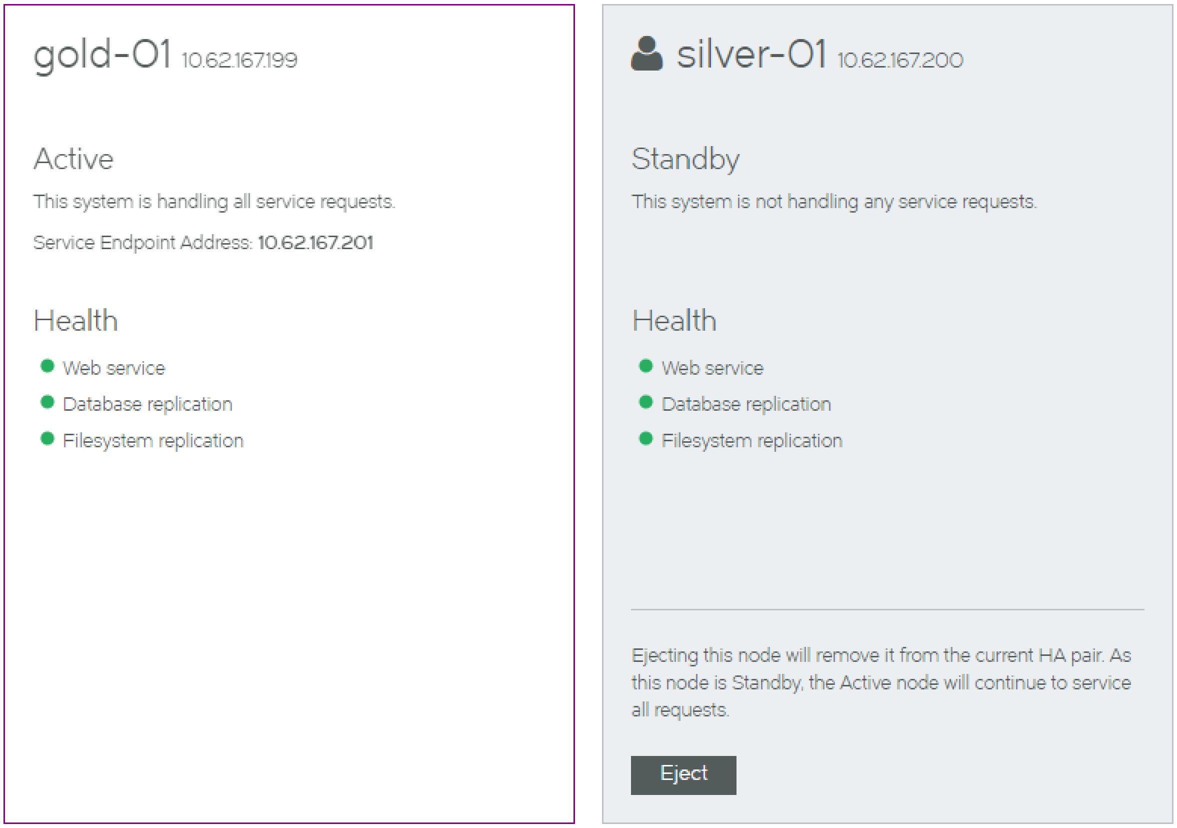
Service Endpoint Address: 10.62.167.201

Health

● Web service
● Database replication
● Filesystem replication

6. (Optional) Log out of the Standby node and start the Services Director VA for the Active node. The **Manage HA** page for this node confirms the correct configuration of nodes following this operation.

FIGURE 237 Manage HA Page: Force Standby Complete (Active Node)



gold-01 10.62.167.199

Active

This system is handling all service requests.

Service Endpoint Address: **10.62.167.201**

Health

● Web service

● Database replication

● Filesystem replication

silver-01 10.62.167.200

Standby

This system is not handling any service requests.

Health

● Web service

● Database replication

● Filesystem replication

Ejecting this node will remove it from the current HA pair. As this node is Standby, the Active node will continue to service all requests.

Converting an Ejected Node into a Standalone Active Node

After you have ejected a node, it becomes an unpaired Services Director node. This node contains no configuration or licenses.

You can convert this unpaired node to be a Primary Services Director node if required.

To do this, you must choose how you want the IP address of the node to be used:

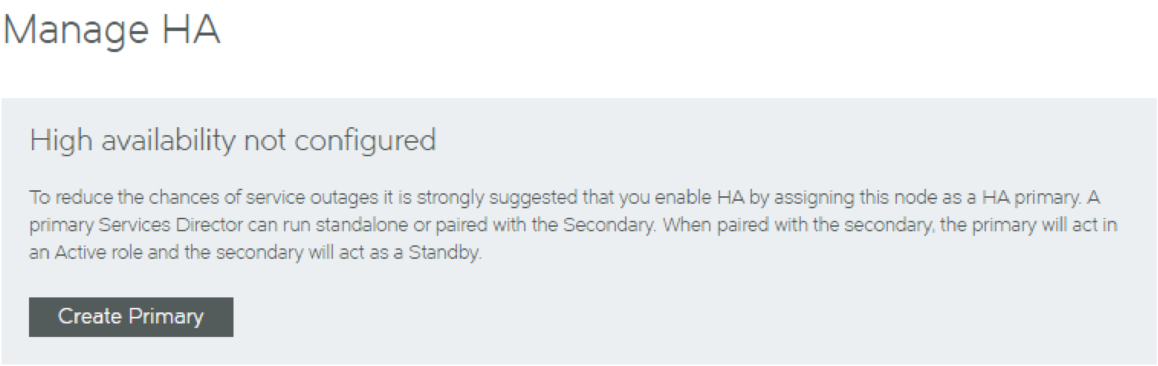
- The current management IP address of the node can be used as its new Service Endpoint Address. This requires you to enter a new management IP address for the node.
- The current management IP address of the node will be retained. This requires you to enter a new Service Endpoint Address for the node.

If the Service Endpoint Address is in a private network behind a NAT device, you must also specify the external IP address for the Service Endpoint Address.

1. Access the Services Director VA for the Standby node from a browser, using either the IP address or hostname of the Standby node.
2. Log in as the administration user. The **Home** page appears.
3. Click the **Services** menu, and then click **High Availability: Manage HA**. The **Manage HA** page appears.

   This page confirms the unpaired state of this Services Director node.

   FIGURE 238 Manage HA Page: Creating a Standalone Node



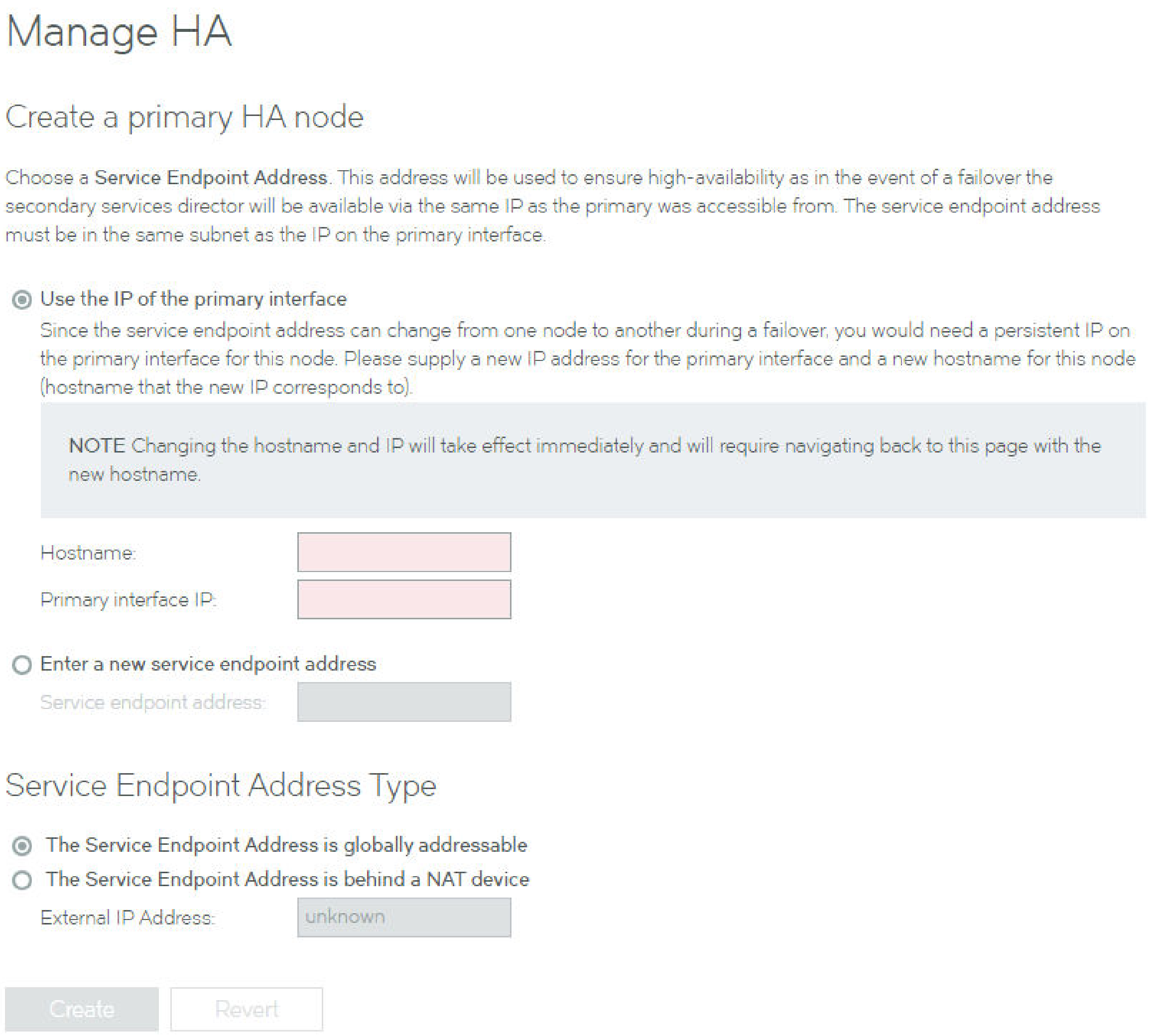
Manage HA

High availability not configured

To reduce the chances of service outages it is strongly suggested that you enable HA by assigning this node as a HA primary. A primary Services Director can run standalone or paired with the Secondary. When paired with the secondary, the primary will act in an Active role and the secondary will act as a Standby.

4. Click **Create Primary**.
   The **Manage HA** page updates to collect the required information.

   FIGURE 239 Manage HA Page: Establishing a New Service Point Address



Manage HA

Create a primary HA node

Choose a **Service Endpoint Address**. This address will be used to ensure high-availability as in the event of a failover the secondary services director will be available via the same IP as the primary was accessible from. The service endpoint address must be in the same subnet as the IP on the primary interface.

● Use the IP of the primary interface
Since the service endpoint address can change from one node to another during a failover, you would need a persistent IP on the primary interface for this node. Please supply a new IP address for the primary interface and a new hostname for this node (hostname that the new IP corresponds to).

NOTE Changing the hostname and IP will take effect immediately and will require navigating back to this page with the new hostname.

Hostname:

Primary interface IP:

○ Enter a new service endpoint address

Service endpoint address:

Service Endpoint Address Type

● The Service Endpoint Address is globally addressable

○ The Service Endpoint Address is behind a NAT device

External IP Address: unknown

5. If you want the current management IP address of the node to be used as its new Service Endpoint Address:
   - Select **Use the IP of the Primary Interface**.
   - Enter a **Hostname** for the new Primary management IP address.
   - Enter the new **Primary interface IP** of the node.

     This will replace the current management IP address of the node.
6. If you want the current management IP address of the node to be retained:
   - Select **Enter a new service endpoint address**.
   - Enter a new **Service endpoint address** for the node.

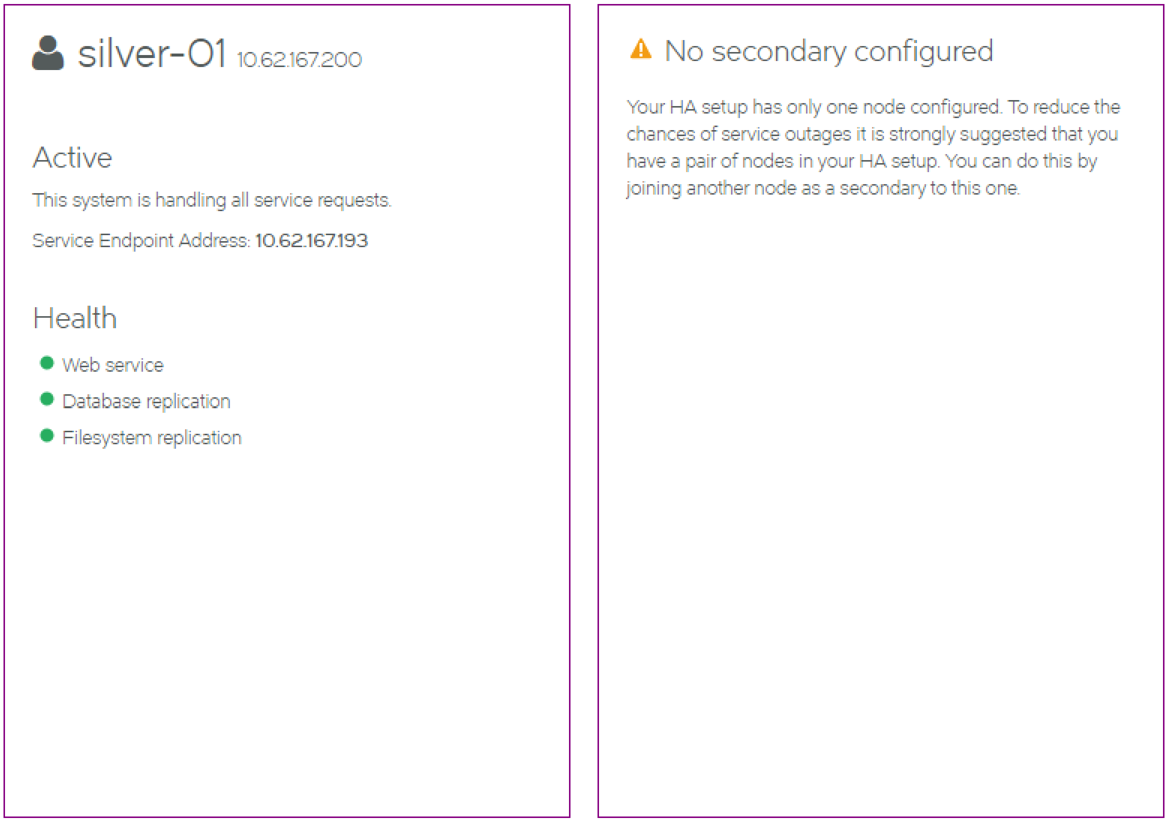
     The current management IP address for the node is retained.

7. If the specified Service Endpoint Address for the Services Director HA pair is globally addressable, select **The Service Endpoint Address is globally addressable**.
8. If the specified Service Endpoint Address for the Services Director HA pair is in a private network behind a NAT device:
   - Select **The Service Endpoint Address is behind a NAT device**.

     The available properties update to include an **External IP Address** property.
   - Enter the external NAT address for your Services Director HA pair as the **External IP Address**.
9. Click **Create**. The process starts and reports progress.

   When the process completes, the original node is now a standalone Primary Services Director.

FIGURE 240 Manage HA Page: Standalone Node Created



silver-01 10.62.167.200

Active

This system is handling all service requests.

Service Endpoint Address: **10.62.167.193**

Health

● Web service

● Database replication

● Filesystem replication

⚠ No secondary configured

Your HA setup has only one node configured. To reduce the chances of service outages it is strongly suggested that you have a pair of nodes in your HA setup. You can do this by joining another node as a secondary to this one.

In this example:

- **silver-01** retains its originally IP address (10.62.167.200)
- **silver-01** has a new Service Endpoint Address defined (10.62.167.193).
- **silver-01** is now a standalone Primary Services Director.
- **silver-01** is not behind a NAT device.

Converting an Upgraded Node into a Standalone Active Node

After you have upgraded your Services Director from an earlier release, it exists as an unpaired Services Director node. This node contains the configuration from the upgraded system.

You can convert this unpaired node to be an Primary Services Director node if required. This enables you to subsequently establish your upgraded node as part of an HA pair.

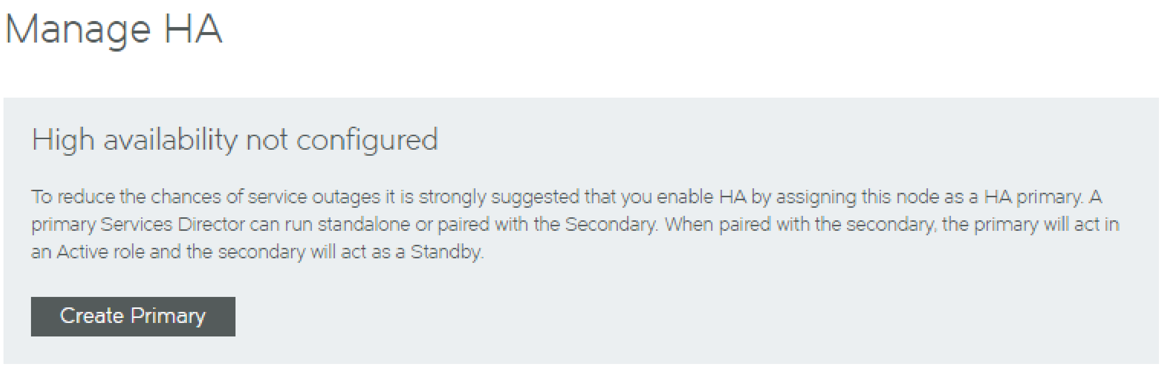
To do this, you will provide the following IP addresses:

- The IP address of your upgraded node becomes the Service Endpoint Address for a standalone Primary Services Director. This ensures that the Legacy FLA licenses that are in use (which must now point to the Service Endpoint Address) will not become invalid during the process.
- Your upgraded node will then require a new IP address for its management interface.
- If the Service Endpoint Address is in a private network behind a NAT device, you must also specify the external IP address for the Service Endpoint Address.

1. Access your Services Director VA for the upgraded node from a browser, using either the IP address or hostname of your Standby node.
2. Log in as the administration user. The **Home** page appears.
3. Click the **Services** menu, and then click **High Availability: Manage HA**. The **Manage HA** page appears.

   This page confirms the unpaired state of this Services Director node.

   FIGURE 241 Manage HA Page: Creating a Standalone Node



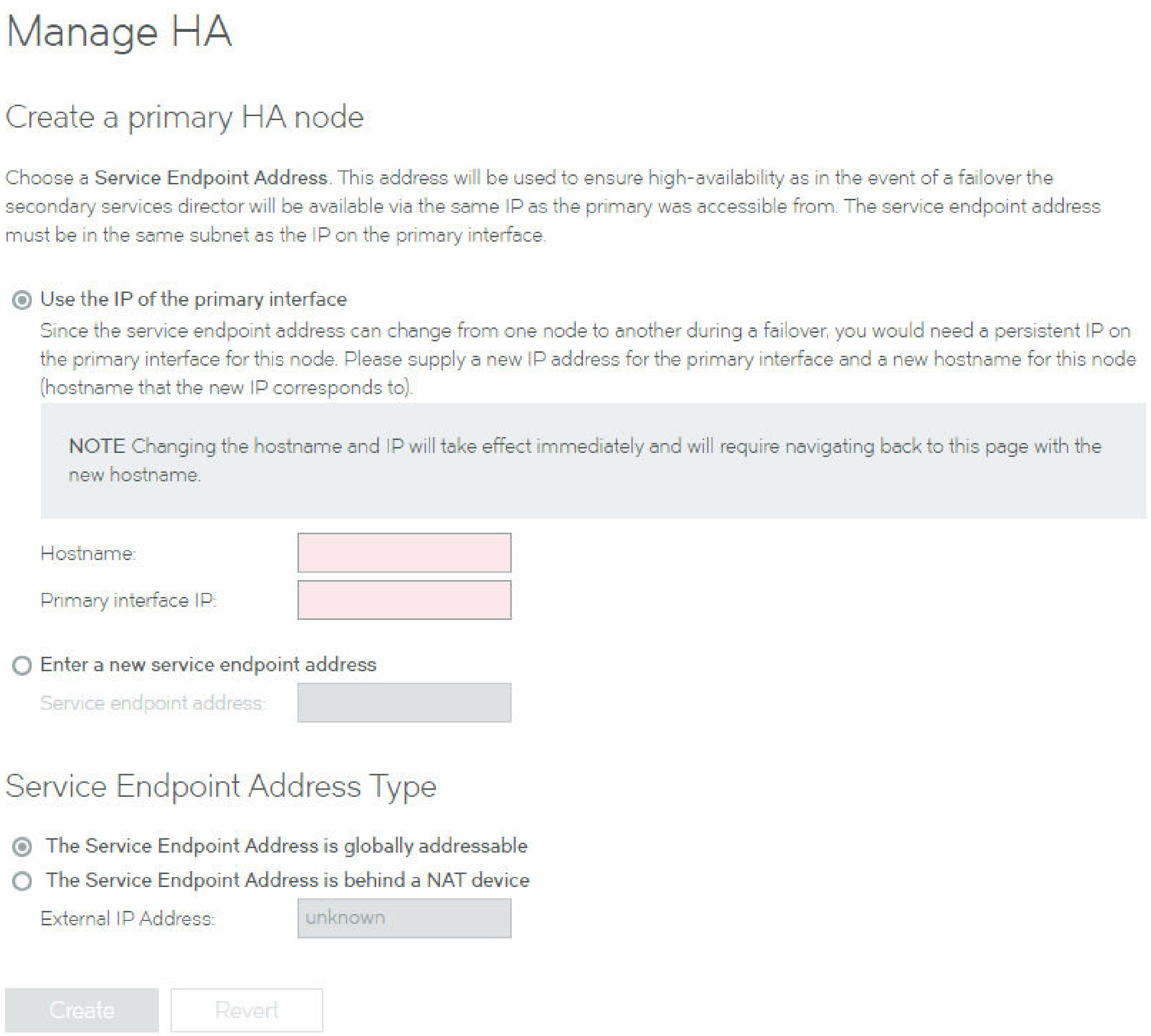
Manage HA

High availability not configured

To reduce the chances of service outages it is strongly suggested that you enable HA by assigning this node as a HA primary. A primary Services Director can run standalone or paired with the Secondary. When paired with the secondary, the primary will act in an Active role and the secondary will act as a Standby.

4. Click **Create Primary**.
   The **Manage HA** page updates to collect the required information.

   FIGURE 242 Manage HA Page: Establishing a New Service Point Address



Manage HA

Create a primary HA node

Choose a **Service Endpoint Address**. This address will be used to ensure high-availability as in the event of a failover the secondary services director will be available via the same IP as the primary was accessible from. The service endpoint address must be in the same subnet as the IP on the primary interface.

● **Use the IP of the primary interface**
Since the service endpoint address can change from one node to another during a failover, you would need a persistent IP on the primary interface for this node. Please supply a new IP address for the primary interface and a new hostname for this node (hostname that the new IP corresponds to).

NOTE Changing the hostname and IP will take effect immediately and will require navigating back to this page with the new hostname.

Hostname:

Primary interface IP:

○ **Enter a new service endpoint address**

Service endpoint address:

Service Endpoint Address Type

● **The Service Endpoint Address is globally addressable**

○ **The Service Endpoint Address is behind a NAT device**

External IP Address: unknown

5. Select **Use the IP of the Primary Interface**.
6. Enter a **Hostname** for the new Primary management IP address.

   This ensures that the current management IP address of your upgraded node becomes its Service Endpoint Address.
7. Enter the new **Primary interface IP** for your upgraded node.

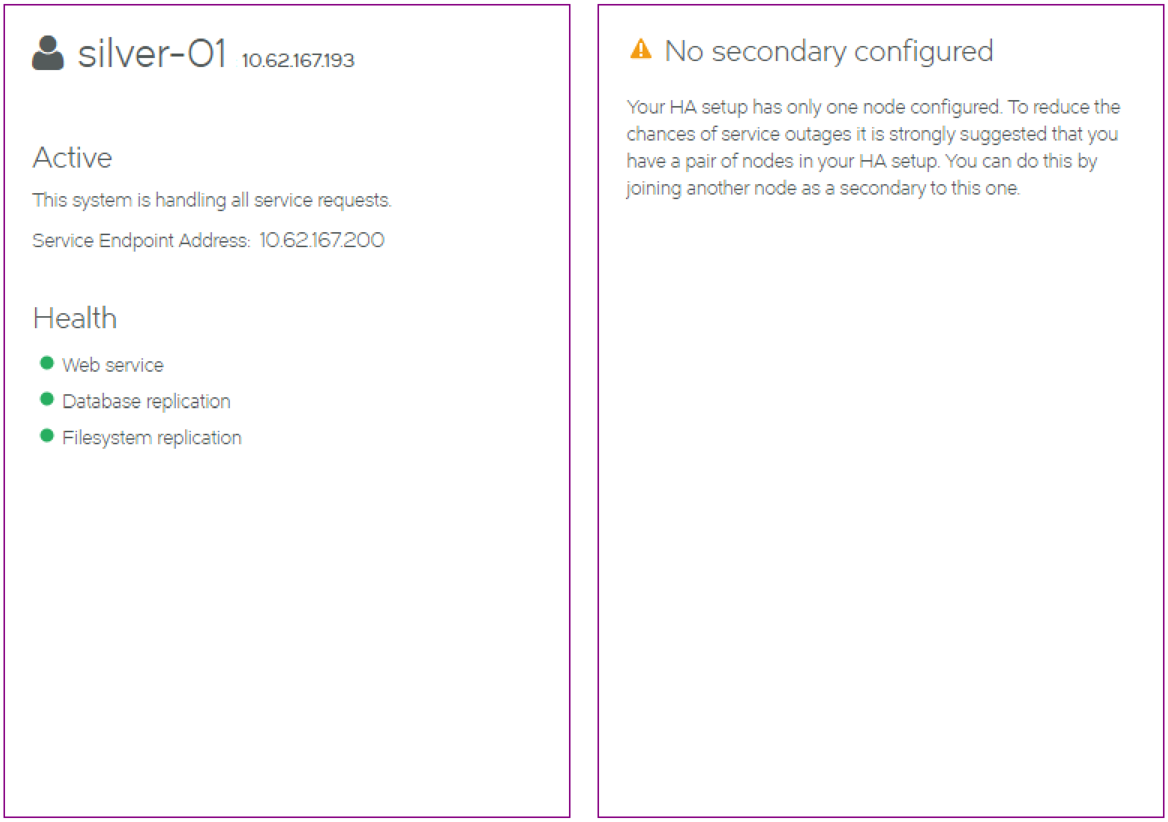
   This will replace the current management IP address of your upgraded node.
8. If the Service Endpoint Address for the Services Director HA pair is globally addressable, select **The Service Endpoint Address is globally addressable**.

9. If the Service Endpoint Address for the Services Director HA pair is in a private network behind a NAT device:
   - Select **The Service Endpoint Address is behind a NAT device**.

     The available properties update to include an **External IP Address**.
   - Enter the external NAT address for your Services Director HA pair as the **External IP Address**.
10. Click **Create**. The process starts and reports progress.

    When the process completes, the original node is now a standalone Primary Services Director.

FIGURE 243 Manage HA Page: Upgraded Node Becomes Standalone Node



silver-01 10.62.167.193

Active

This system is handling all service requests.

Service Endpoint Address: 10.62.167.200

Health

● Web service

● Database replication

● Filesystem replication

No secondary configured

Your HA setup has only one node configured. To reduce the chances of service outages it is strongly suggested that you have a pair of nodes in your HA setup. You can do this by joining another node as a secondary to this one.

In this example:

- **silver-01** changes its IP address from 10.62.167.200 to 10.62.167.193.
- **silver-01** now has a Service Endpoint Address. This is its original IP address (10.62.167.200).
- **silver-01** is now a standalone Primary Services Director. It retains its configuration.
- **silver-01** is not behind a NAT device.

When a new Secondary Services Director is created subsequently, it can be joined to **silver-01** to form an HA pair. This completes the upgrade process.

Recovering from a Services Director Failure

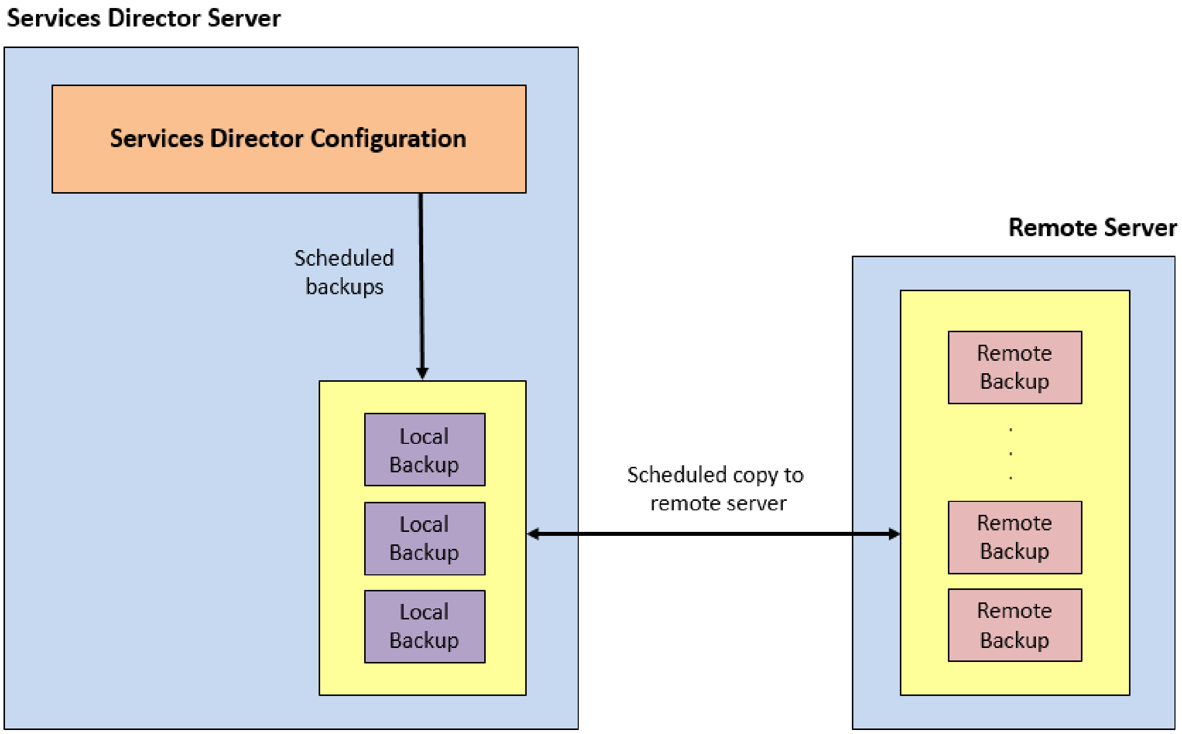
Overview: Recovering from a Services Director Failure

A backup is an encapsulated Services Director configuration. The contents of the backup can be used by the Services Director VA to restore a Services Director configuration.

Backups are made locally according to a backup schedule.

Local backups are copied to a remote server according to a separate schedule.

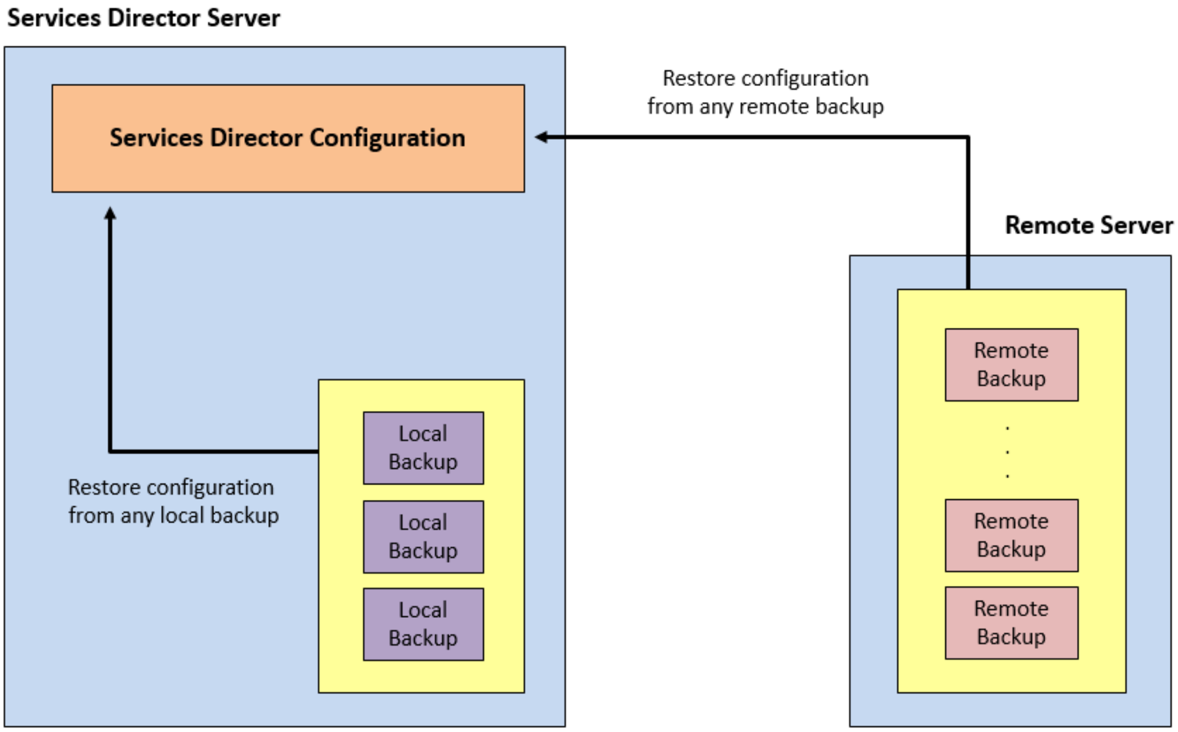
FIGURE 244 Scheduled Backups



NOTE
Where an HA pair is in use, the backup configuration is created on the Active node only. Backups are always restored to an Active (or new Primary) node. Standby nodes always take their configuration from the Active node.

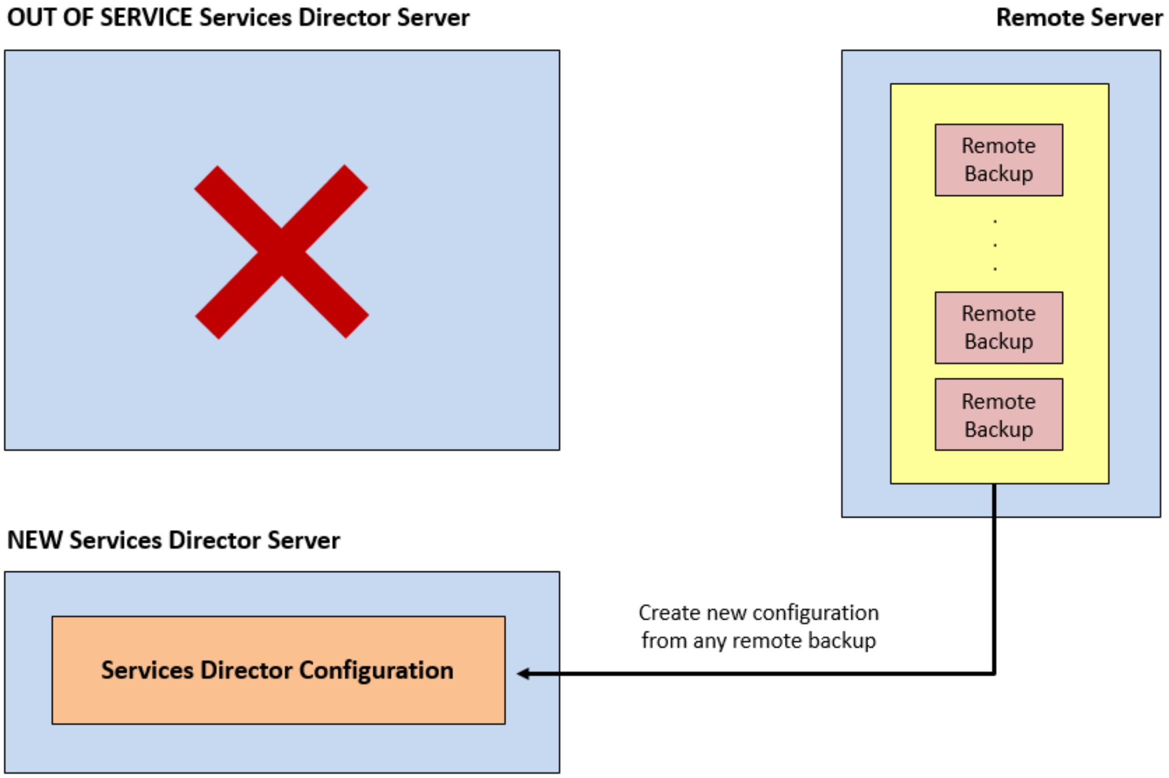
A Services Director VA's configuration can be restored from any backup (either local or remote). You may wish to do this to recover a specific configuration, or to reverse recent changes.

FIGURE 245 Restoring From a Backup


Services Director Server
Services Director Configuration
Restore configuration from any remote backup
Remote Server
Remote Backup
Remote Backup
Remote Backup
Local Backup
Local Backup
Local Backup
Restore configuration from any local backup

After the failure of a Services Director, a new Services Director VA can be created from the configuration stored in a remote backup.

FIGURE 246 Creating a New Services Director VA From a Backup


OUT OF SERVICE Services Director Server
Remote Server
Remote Backup
Remote Backup
Remote Backup
NEW Services Director Server
Services Director Configuration
Create new configuration from any remote backup

Understanding a Backup File

A backup file is a zipped collection of Services Director configuration files. This includes:

- The usernames/passwords for the Services Director.
- The usernames/passwords for all instance hosts.
- The usernames/passwords for all Traffic Managers with REST API access.
- The Services Director controller license.
- The Services Director version information.
- All FLA licenses (both Universal and Legacy).
- A dump of the MySQL database. This database includes Traffic Manager passwords that have been encrypted with a key derived from the master password.
- Additional Services Director configuration settings.
- A list of Traffic Manager images imported by the user. The backup file does not include the actual Traffic Manager image files.

The backup file does *not* include:

- The master password.
- The Traffic Manager image files.
- A record of the backup schedule and remote server details.

- SSH keys required for passwordless SSH access.
- Knowledge of HA pairs, hostnames or IP addresses.

Configuring a Scheduled Backup Schedule

The Services Director VA uses a defined backup schedule for a standalone Services Director node or the Active node in an HA pair.

> NOTE
> Do *not* create a backup schedule from the Standby node in an HA pair. A Standby node always takes its configuration from the Active node.

The backup schedule defines:

- The frequency of local backups, and the maximum number of backup files to retain.
- The identity and credentials of a remote file server.

You must set up this remote server before starting the backup configuration process. The server must accept either SCP or FTP connections (or both), and have the required directory structure.

- The frequency of the copy process of local backups to the remote server.

> NOTE
> Services Director VA has no influence over the number of backup files stored on the remote server, or the management of these files. This is a user activity outside Services Director VA.

Configuring the Backup Schedule

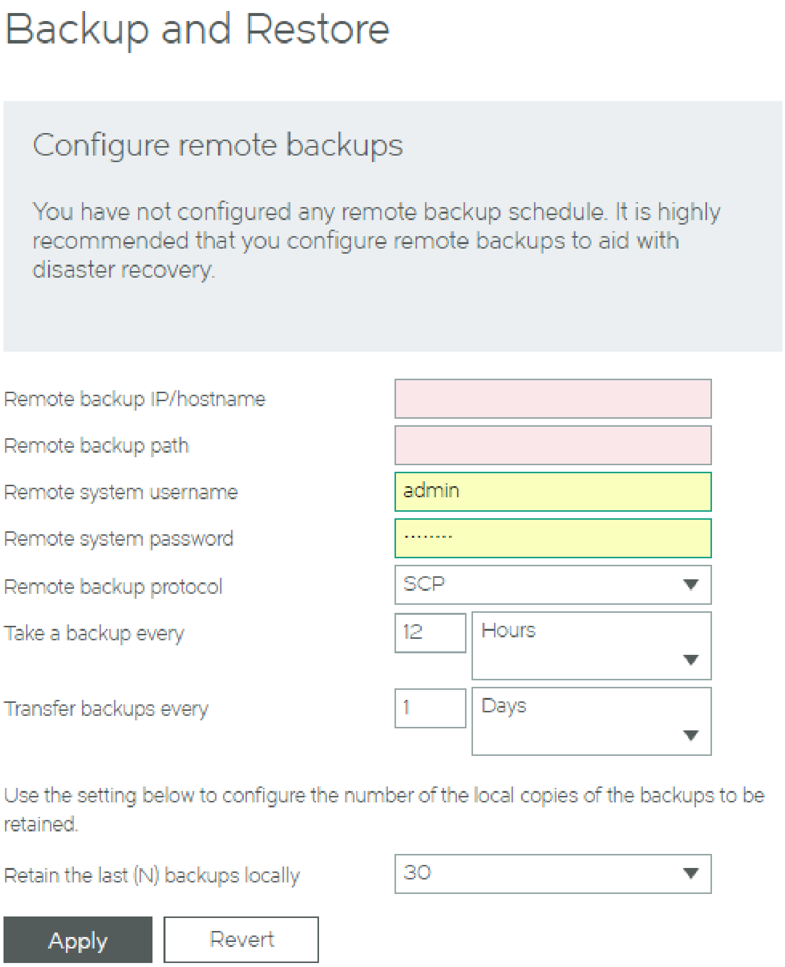
1. Access your Active Services Director VA from a browser, using the Service Endpoint Address of your Services Director.

   > NOTE
   > Do not create a backup schedule from the Standby node in an HA pair. Backups are always created from the Active node.

2. Log in as the administration user. The **Home** page appears.

3. Click the **System** menu, and then click **Disaster Recover: Backup and Restore**. The **Backup and Restore** page appears.

FIGURE 247 Backup and Restore Page



Backup and Restore

Configure remote backups

You have not configured any remote backup schedule. It is highly recommended that you configure remote backups to aid with disaster recovery.

Remote backup IP/hostname		
Remote backup path		
Remote system username	admin	
Remote system password	········	
Remote backup protocol	SCP ▼	
Take a backup every	12	Hours ▼
Transfer backups every	1	Days ▼

Use the setting below to configure the number of the local copies of the backups to be retained.

Retain the last (N) backups locally	30 ▼

This example indicates that no backup configuration currently exists.

4. Enter the details for the remote server:

-
- **Remote backup IP/hostname** : This is the IP address or FQDN of the remote server.
- **Remote backup path**: This identifies a directory on the remote server for the backups.

  NOTE
  This requires a "full path" directory structure. Relative paths cannot be used.

- **Remote system username**: The user name for the remote server.
- **Remote system password**: The password for the user.
- **Remote backup protocol**: The file transfer protocol for the remote backup server. This is either FTP or SCP. Use SCP for secure encrypted transfers.

5. Define the frequency for the local backup. Under **Take a backup every** :
   - Select the units for the backup. This can be *Minutes*, *Hours* (default) or *Days*.
   - Enter the number of the selected units.

   Minutes can range from 1-59, *Hours* from 1-23 and *Days* from 1-31. The default is 12.

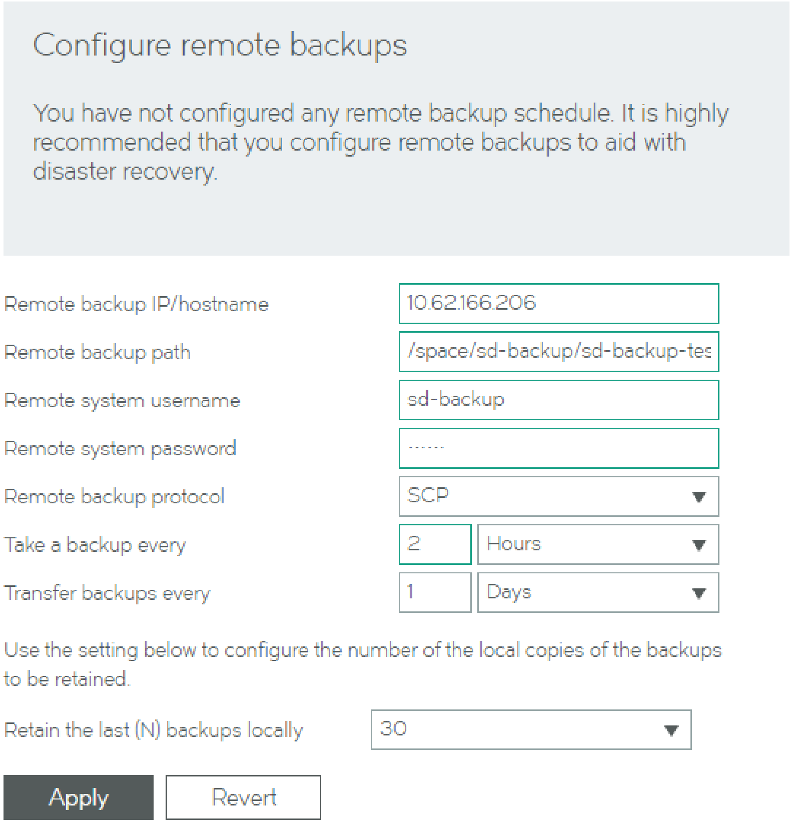
   For example: 30 Minutes.
6. Define the frequency for copying local backups to the remote server. This will typically be a longer frequency than the one used for local backups. Under **Transfer backups every** :
   - Select the units for the backup. This can be *Minutes*, *Hours* or *Days* (default).
   - Enter the number of the selected units.

   Minutes can range from 1-59, *Hours* from 1-23 and *Days* from 1-31. The default is 1.

   For example: 1 Days.
7. Select the maximum number of local backups as **Retain the last (N) backups locally**. The default is 30. This value must be at least equal to the number of backups between remote copies, else backup files will be lost.

   The most recent backup files are retained. Any older files are deleted if this limit is exceeded.

FIGURE 248 Backup and Restore Page: Completed



Configure remote backups

You have not configured any remote backup schedule. It is highly recommended that you configure remote backups to aid with disaster recovery.

Remote backup IP/hostname	10.62.166.206	
Remote backup path	/space/sd-backup/sd-backup-tes	
Remote system username	sd-backup	
Remote system password	······	
Remote backup protocol	SCP ▼	
Take a backup every	2	Hours ▼
Transfer backups every	1	Days ▼

Use the setting below to configure the number of the local copies of the backups to be retained.

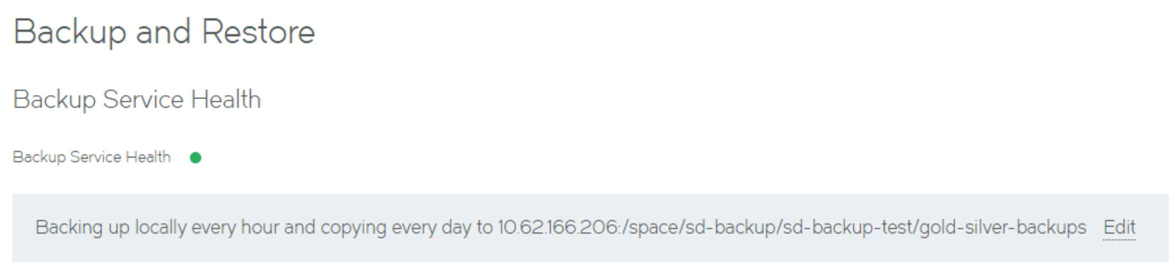
Retain the last (N) backups locally	30 ▼

8. Click **Apply** to confirm the backup schedule.

   An empty test file is sent immediately to the remote server.

   The backup configuration, including a status indicator, is included on the **Backup and Restore** page.

   FIGURE 249 Backup and Restore Page: Healthy Configuration

   Backup and Restore

   Backup Service Health

   Backup Service Health ●

   Backing up locally every hour and copying every day to 10.62.166.206:/space/sd-backup/sd-backup-test/gold-silver-backups

9. Log in to the remote server and ensure that the backup test file is present. If this is not present, check the details for your remote server on the **Backup and Restore** page. An error message will explain the issue.

   The first local backup will be created after the full duration of the local backup frequency. For example, after 2 Hours. The file name has the following general form:

   ```
   backup_<IP_address>_<datestamp>_<timestamp>.zip
   ```

   For example:

   ```
   backup_10.62.167.199_2015-09-09_05-52-02.zip
   ```

   The first copy of local files to the remote server will occur after the full duration of the remote copy frequency. For example, after 1 Days. Any local backup files that are not present on the remote server are copied over.

Updating the Backup Schedule

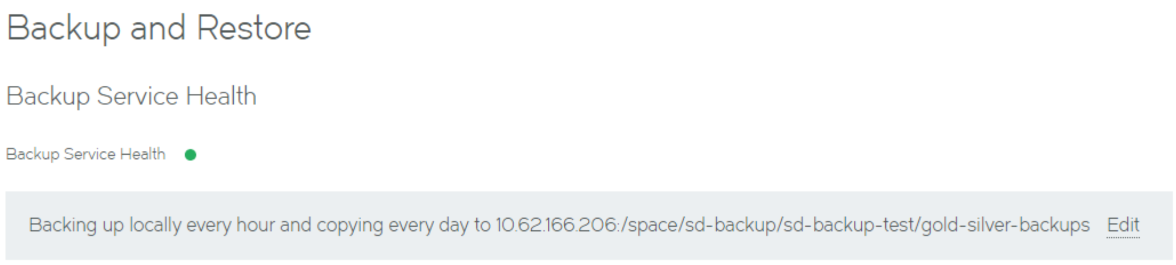
1. Access your Active Services Director VA from a browser, using the Service Endpoint Address of your Services Director.

   NOTE
   Do not update a backup schedule from the Standby node in an HA pair. Backups are always updated from the Active node.

2. Log in as the administration user. The **Home** page appears.

3. Click the **System** menu, and then click **Disaster Recover: Backup and Restore**. The **Backup and Restore** page appears. This displays a summary of your current backup schedule, and includes a status indicator.

   FIGURE 250 Backup and Restore Page: Schedule Summary

   Backup and Restore

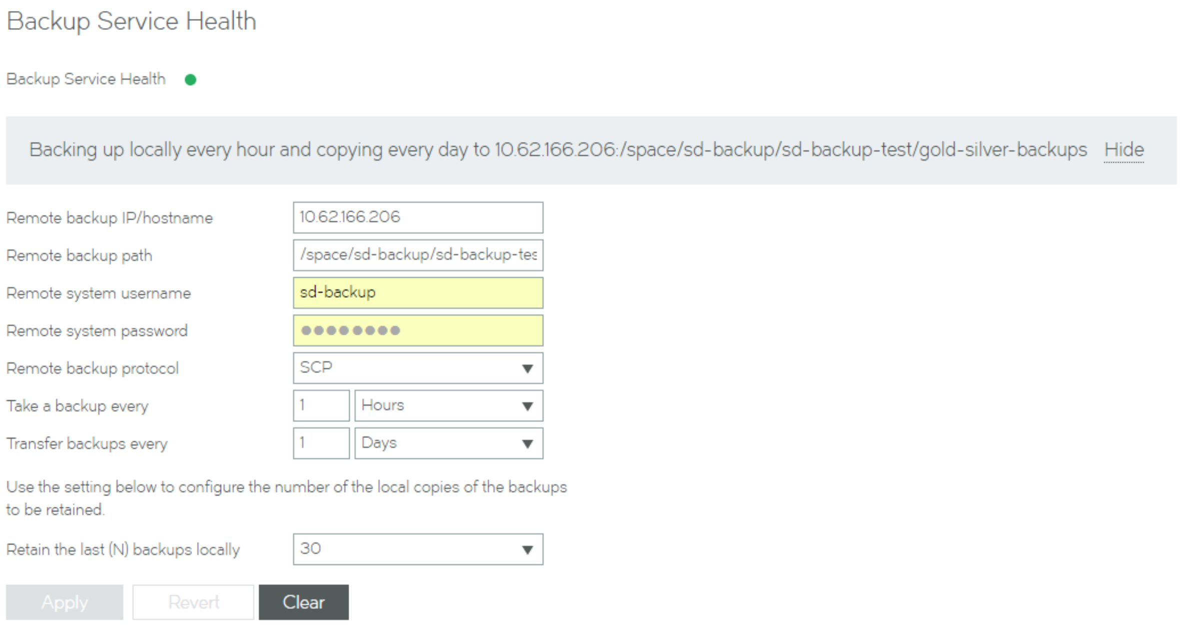
   Backup Service Health

   Backup Service Health ●

   Backing up locally every hour and copying every day to 10.62.166.206:/space/sd-backup/sd-backup-test/gold-silver-backups Edit

4. Click **Edit** to display the full details.

   FIGURE 251 Backup and Restore Page: Editing the Schedule

   Backup Service Health

   Backup Service Health ●

   Backing up locally every hour and copying every day to 10.62.166.206:/space/sd-backup/sd-backup-test/gold-silver-backups Hide

Remote backup IP/hostname	10.62.166.206
Remote backup path	/space/sd-backup/sd-backup-tes
Remote system username	sd-backup
Remote system password	●●●●●●●●
Remote backup protocol	SCP
Take a backup every	1 Hours
Transfer backups every	1 Days

   Use the setting below to configure the number of the local copies of the backups to be retained.

   Retain the last (N) backups locally 30

5. Make the required changes to your schedule.

   NOTE
   Remote backup path requires a "full path" directory structure. Relative paths cannot be used.

6. Click **Apply** to confirm the changes.

   The first local backup will be created after the full duration of the local backup frequency. For example, after 20 minutes.

   The first copy of local files to the remote server will occur after the full duration of the remote copy frequency. For example, after 1 day.

Restoring a Services Director from a Local Backup

A Services Director VA's configuration can be restored from a local backup. You may wish to do this to recover a specific configuration, or to reverse recent changes.

> NOTE
> The backup file does not include any Traffic Manager image files that you have imported. However, a list of these images is included in the backup, and this list is displayed the end of the process.

1. Access your Active Services Director VA graphical interface from a browser, using the Service Endpoint Address of your Services Director.

   Do this from a browser, using the Service Endpoint Address of your Services Director.

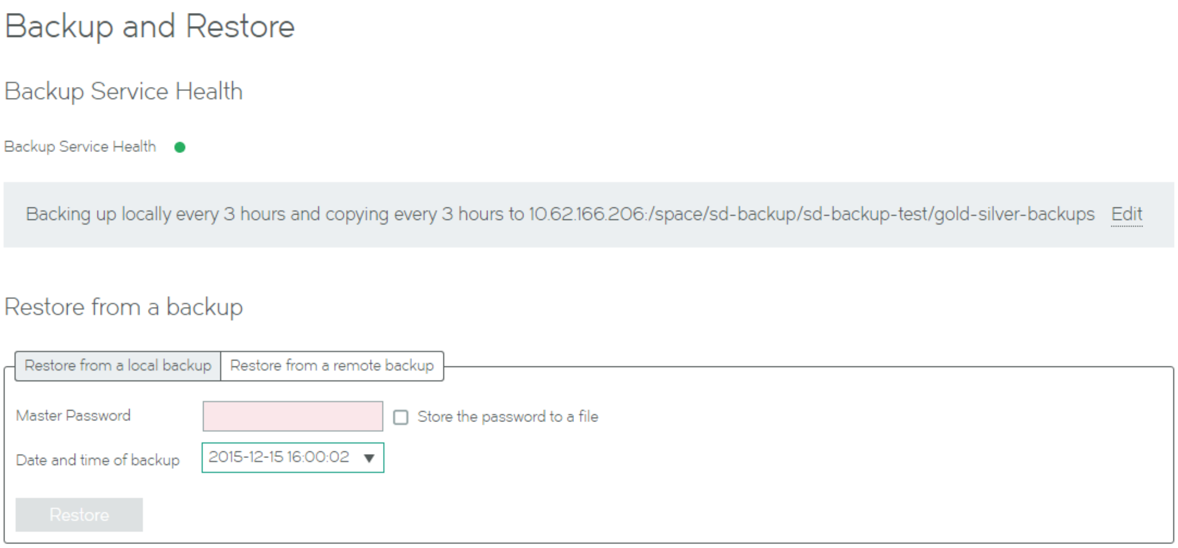
   > NOTE
   > Do not restore a configuration from the Standby node in an HA pair. Backups are always restored on the Active node.

2. Log in as the administration user. The **Home** page appears.
3. Click the **System** menu, and then click **Disaster Recover: Backup and Restore**. The **Backup and Restore** page appears.

   This page contains a summary of the current backup schedule, a backup service health indicator, and provides access to the restore functions.

4. Click the **Restore from a local backup** tab.

FIGURE 252 Backup and Restore Page: Restore from a Local Backup



Backup and Restore

Backup Service Health

Backup Service Health ●

Backing up locally every 3 hours and copying every 3 hours to 10.62.166.206:/space/sd-backup/sd-backup-test/gold-silver-backups Edit

Restore from a backup

Restore from a local backup | Restore from a remote backup

Master Password □ Store the password to a file

Date and time of backup 2015-12-15 16:00:02 ▼

Restore

5. Enter the **Master Password** that was in place when the backup was taken.
6. Select the required local backup from the pull-down list.

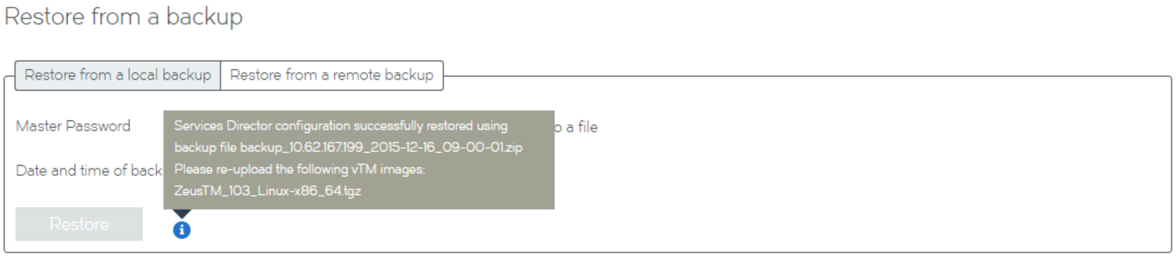
   The file names have the following general form:

```
backup_<IP_address>_<datestamp>_<timestamp>.zip
```

7. Select the **Store the password to a file** check box if you want to store the master password internally for future use.
8. Click **Restore** to start the restore process.

   When the restore completes, any additional information is displayed in an information box.

   FIGURE 253 Backup and Restore Page: Completing a Local Backup

   Services Director configuration successfully restored using backup file backup_10.62.167.199_2015-12-16_09-00-01.zip
   Please re-upload the following vTM images:
   ZeusTM_103_Linux-x86_64.tgz

   In this instance, the following information is displayed:

   ```
   Services Director configuration successfully restored using backup file
   backup_10.62.167.199_2015-12-16_09-00-01.zip Please re-upload the following vTM images:
   ZeusTM_103_Linux-x86_64.tgz
   ```

   This is an example of a Traffic Manager image file that is referenced in the backup, but which is not included in the backup itself. If you have deleted this file, you should reload it. Refer to the *Brocade Services Director Advanced User Guide* for full details.

Restoring a Services Director from a Remote Backup

A Services Director VA's configuration can be restored from a remote backup. You may wish to do this to recover a specific configuration, or to reverse recent changes.

The Services Director VA is not able to list available backup files on the remote server. You must know the name of the file you wish to restore from before beginning this process.

NOTE
The backup file does not include any Traffic Manager image files that you have imported. However, a list of these images is included in the backup, and this list is displayed at the end of the process.

1. Access your Active Services Director VA from a browser, using the Service Endpoint Address of your Services Director.

   Do this from a browser, using the Service Endpoint Address of your Services Director.

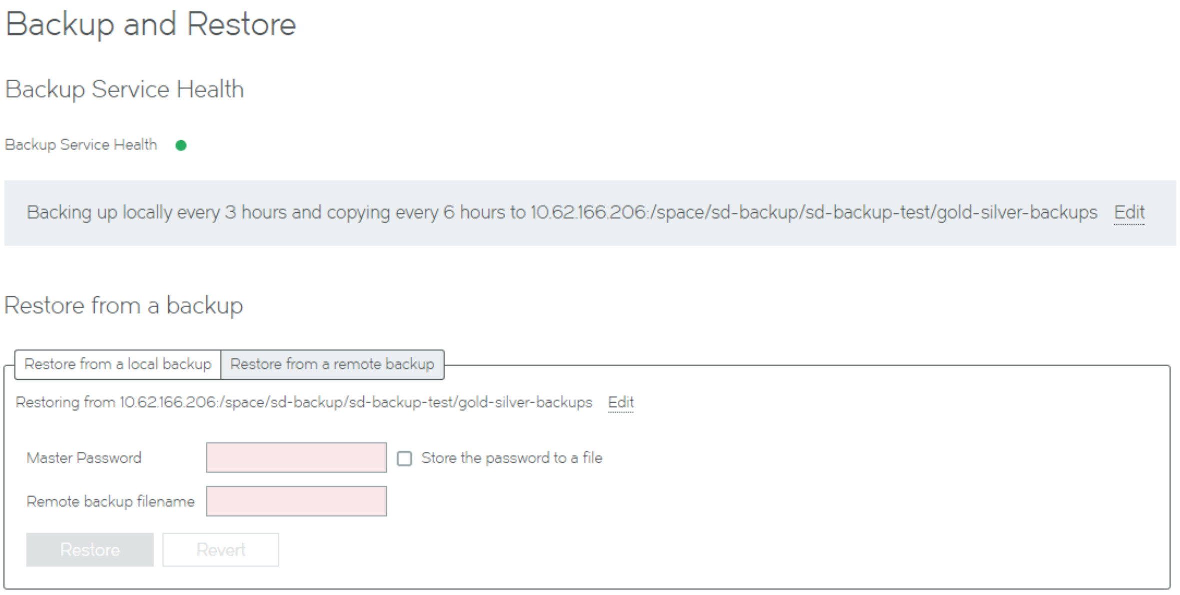
   NOTE
   Do not restore a configuration from the Standby node in an HA pair. Backups are always restored on the Active node.

2. Log in as the administration user. The **Home** page appears.
3. Click the **System** menu, and then click **Disaster Recover: Backup and Restore**. The **Backup and Restore** page appears.

   This page contains a summary of the current backup schedule, a backup service health indicator, and provides access to the restore functions.

4. Click the **Restore from a remote backup** tab.

FIGURE 254 Backup and Restore Page: Restore from a Remote Backup



Backup and Restore

Backup Service Health

Backup Service Health ●

Backing up locally every 3 hours and copying every 6 hours to 10.62.166.206:/space/sd-backup/sd-backup-test/gold-silver-backups Edit

Restore from a backup

Restoring from 10.62.166.206:/space/sd-backup/sd-backup-test/gold-silver-backups Edit

Master Password □ Store the password to a file

Remote backup filename

5. Enter the name of the remote backup file. The file names have the following general form:

```
backup_<IP_address>_<datestamp>_<timestamp>.zip
```

For example:

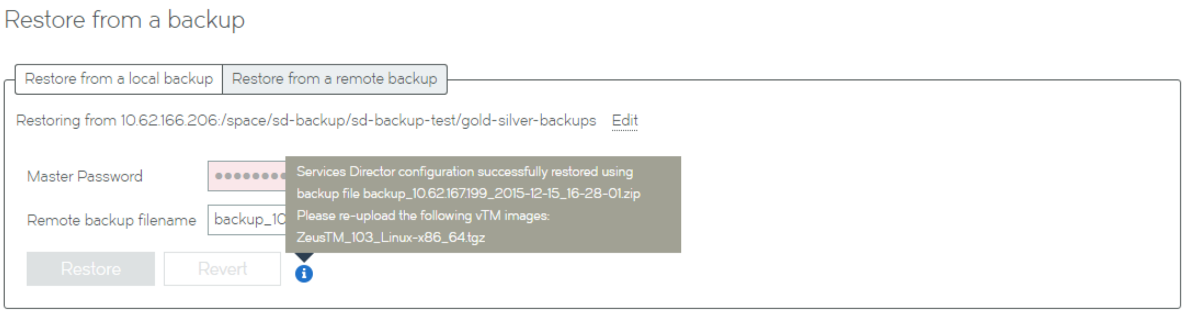
```
backup_10.62.167.199_2015-09-09_05-52-02.zip
```

6. If you want to change the source of the remote backup:
   a) Click **Edit**. The dialog expands to show additional fields.
   b) Enter new details for the remote server:
      - **Remote backup IP/hostname** - this is the IP address or FQDN of the remote server.
      - **Remote backup path** - this identifies a directory on the remote server for the backups. This requires a "full path" directory structure. Relative paths cannot be used.
      - **Remote system username** - the user name for the remote server.
      - **Remote system password** - the password for the user.
      - **Remote backup protocol** - the file transfer protocol for the remote backup server. This is either FTP or SCP. Use SCP for secure encrypted transfers.
   c) Click **Apply** to confirm the changes.
7. Select the **Store the password to a file** check box if you want to store the master password internally for future use.

8. Click **Restore** to start the restore process.

   When the restore completes, any additional information is displayed in an information box.

   FIGURE 255 Backup and Restore Page: Completing a Remote Backup



Restore from a backup

Restoring from 10.62.166.206:/space/sd-backup/sd-backup-test/gold-silver-backups Edit

Master Password ••••••••

Remote backup filename backup_1C

Services Director configuration successfully restored using backup file backup_10.62.167.199_2015-12-15_16-28-01.zip Please re-upload the following vTM images: ZeusTM_103_Linux-x86_64.tgz

   In this instance, the following information is displayed:

```
Services Director configuration successfully restored using backup file
backup_10.62.167.199_2015-12-15_16-28-01.zip Please re-upload the following vTM images:
ZeusTM_103_Linux-x86_64.tgz
```

   This is an example of a Traffic Manager image file that is referenced in the backup, but which is not included in the backup itself. If you have deleted this file, you should reload it. See the *Brocade Services Director Advanced User Guide* for full details.

Restoring a Services Director Using the Setup Wizard

After the failure of a Services Director, you can create a new Primary Services Director VA from a remote backup file. This process uses the Setup Wizard. You can then create a new Secondary Services Director VA and pair it with the recovered Primary Services Director VA.

NOTE
A new Secondary Services Director VA will receive its configuration from the Primary. You do not need to use a restore process when you create the Secondary.

Note that:

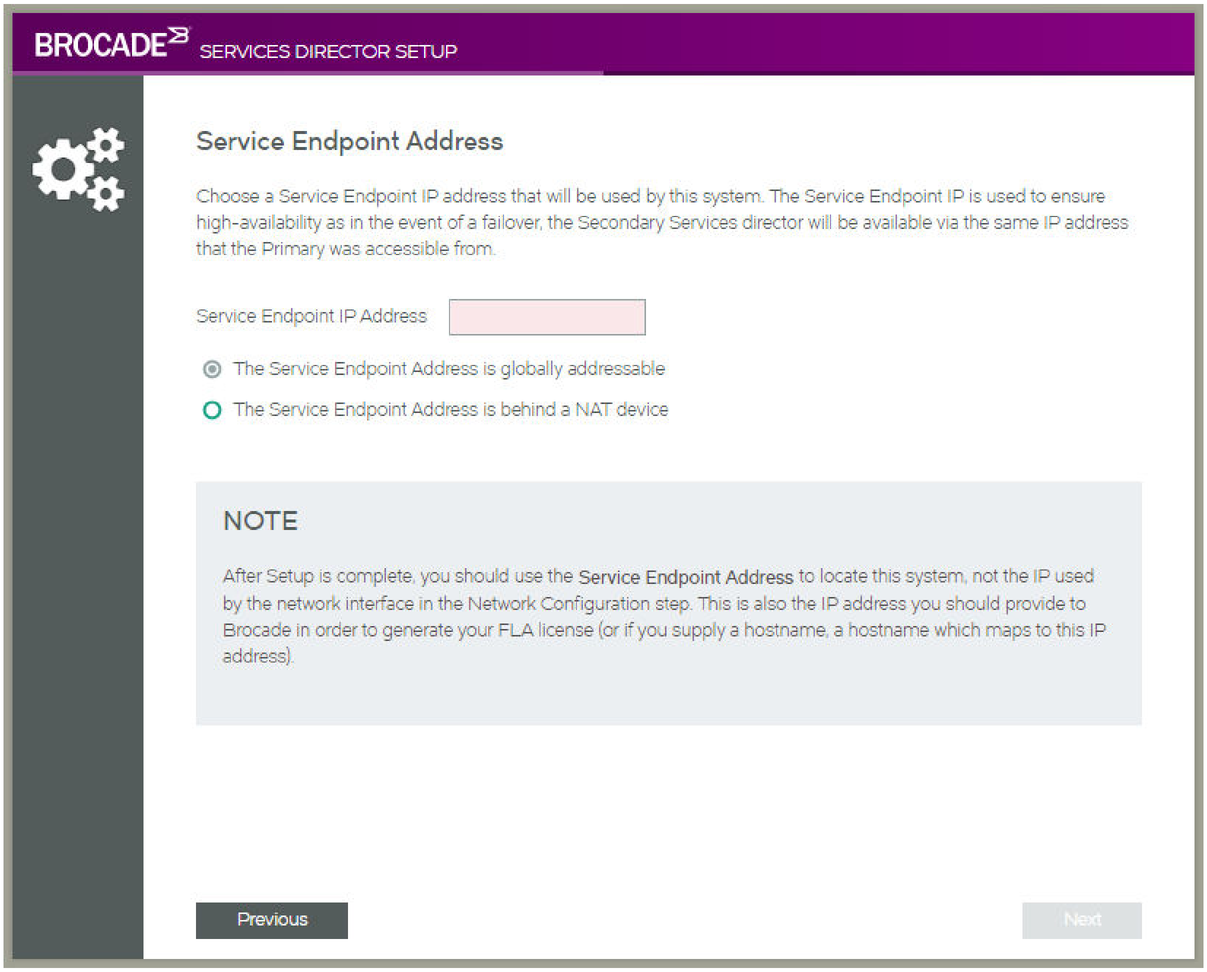
- If your new Services Director VA uses a different Service Endpoint Address than the one used for the original Services Director VA, the FLA Licensing of Traffic Manager instances will be disrupted.
- A Service Endpoint Address is still required a standalone Primary Services Director. It must be different from the IP address of the Primary Services Director.
- The Services Director VA is unconfigured at this point, and has no record of the remote server. The required backup file must be downloaded from the remote server to the local machine before beginning the backup.
- The backup file does not include any Traffic Manager image files that you have imported. However, a list of these images is included in the backup, and this list is displayed at the end of the process.
- You require the master password for the original Services Director VA.

1. Create a new virtual machine for the Services Director VA. Refer to Creating a VM in vSphere on page 17.
2. Start the VM and make a note of its assigned IP address.
3. Access the Services Director VA in a browser window using its IP address.

   The Setup Wizard starts.

4. Work through the Setup Wizard until you reach the **Service Endpoint Address** page.

FIGURE 256 Setup Wizard: Service Endpoint Address Page



Service Endpoint Address

Choose a Service Endpoint IP address that will be used by this system. The Service Endpoint IP is used to ensure high-availability as in the event of a failover, the Secondary Services director will be available via the same IP address that the Primary was accessible from.

Service Endpoint IP Address

● The Service Endpoint Address is globally addressable

○ The Service Endpoint Address is behind a NAT device

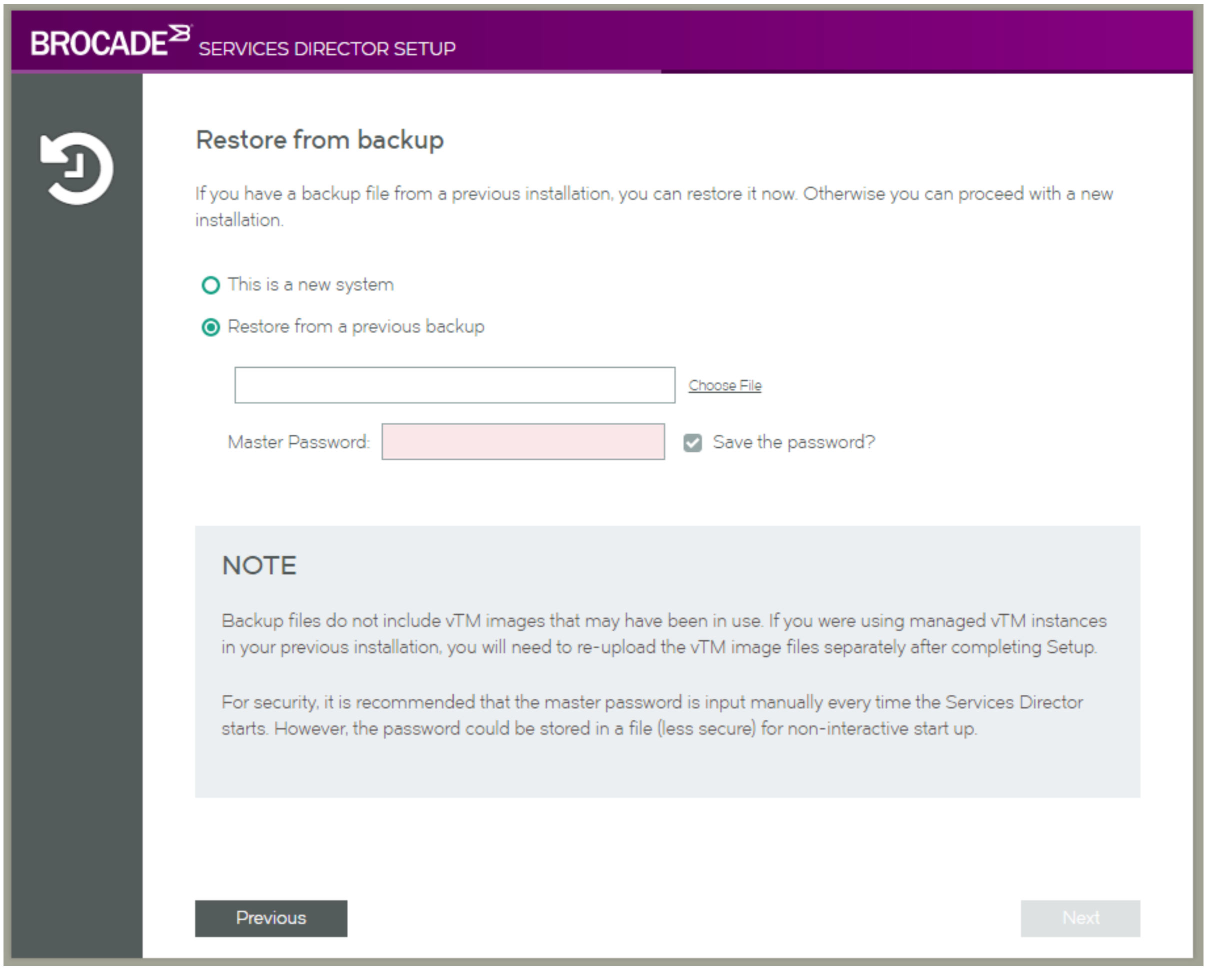
NOTE

After Setup is complete, you should use the **Service Endpoint Address** to locate this system, not the IP used by the network interface in the Network Configuration step. This is also the IP address you should provide to Brocade in order to generate your FLA license (or if you supply a hostname, a hostname which maps to this IP address).

5. If the Service Endpoint Address for the Services Director HA pair is globally addressable:
   - Select **The Service Endpoint Address is globally addressable**.
   - Enter the **Service Endpoint IP Address** for the Services Director HA pair.
6. If Service Endpoint Address for the Services Director HA pair is in a private network behind a NAT device:
   - Select **The Service Endpoint Address is behind a NAT device**. The available properties update to include an **External IP Address**.
   - Enter the internal NAT Service Endpoint Address for your Services Director HA pair as the **Service Endpoint IP Address**.
   - Enter the external NAT address for your Services Director HA pair as the **External IP Address**.

7. Click **Next**. The **Restore from Backup** page appears.

FIGURE 257 Setup Wizard: Restore from Backup Page



Restore from backup

If you have a backup file from a previous installation, you can restore it now. Otherwise you can proceed with a new installation.

○ This is a new system

● Restore from a previous backup

Master Password:

☑ Save the password?

NOTE

Backup files do not include vTM images that may have been in use. If you were using managed vTM instances in your previous installation, you will need to re-upload the vTM image files separately after completing Setup.

For security, it is recommended that the master password is input manually every time the Services Director starts. However, the password could be stored in a file (less secure) for non-interactive start up.

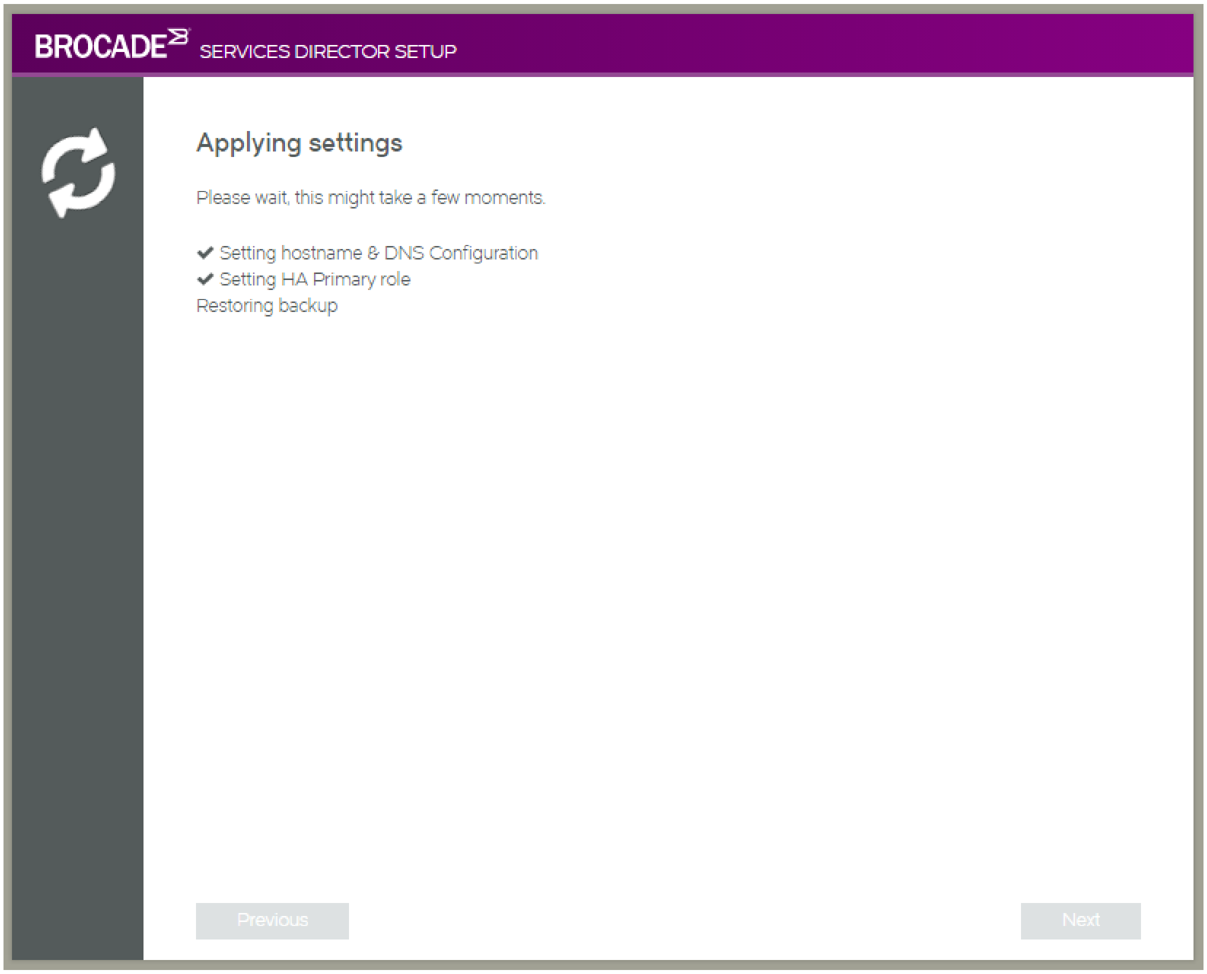
8. Click **Restore from a previous backup**.
9. Click **Choose file** and locate the backup file. This file must already be downloaded from the remote server to a local machine. The file names have the following general form:

   backup_<IP_address>_<datestamp>_<timestamp>.zip
10. Enter the Master Password for the Services Director VA that created the backup.

11. Click **Next**. The **Applying Settings** page appears.

    This page configures the system based on retrieved configuration information.

    FIGURE 258 Setup Wizard: Applying Settings Page



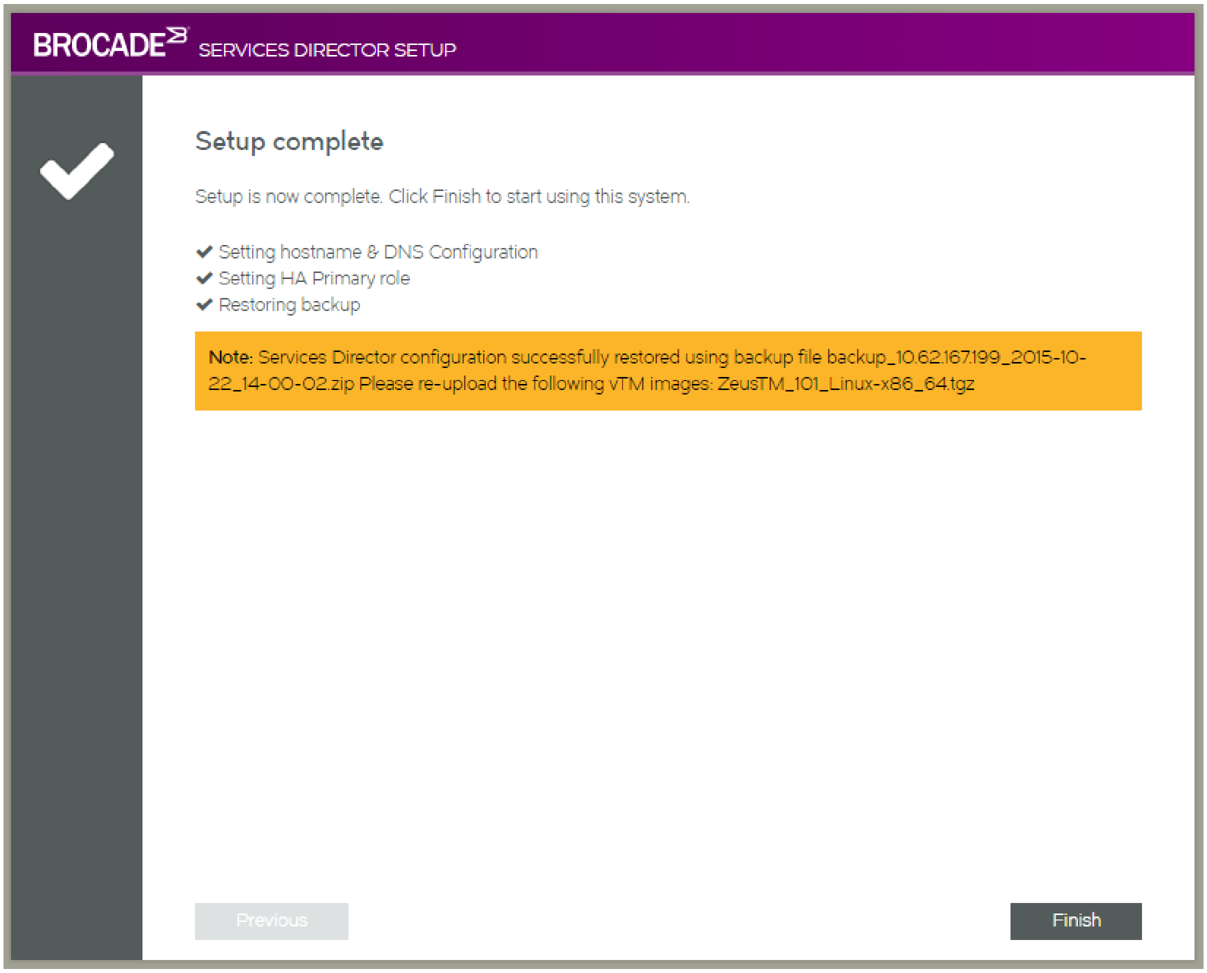
Applying settings

Please wait, this might take a few moments.

✓ Setting hostname & DNS Configuration
✓ Setting HA Primary role
Restoring backup

When this is complete, the **Setup Complete** page appears.

FIGURE 259 Setup Wizard: Setup Complete Page



Setup complete

Setup is now complete. Click Finish to start using this system.

✓ Setting hostname & DNS Configuration
✓ Setting HA Primary role
✓ Restoring backup

Note: Services Director configuration successfully restored using backup file backup_10.62.167.199_2015-10-22_14-00-02.zip Please re-upload the following vTM images: ZeusTM_101_Linux-x86_64.tgz

In this instance, the following information is displayed:

```
Note: Services Director configuration successfully restored using backup file
backup_10.62.167.199_2015-10-22_14-00-02.zip Please re-upload the following vTM images:
ZeusTM_101_Linux-x86_64.tgz
```

This is an example of a Traffic Manager image file that is referenced in the backup, but which is not included in the backup itself. To complete your restore, you must reload this file. Refer to the *Brocade Services Director Advanced User Guide* for full details.

12. Click **Finish**. The **Home** page is displayed.

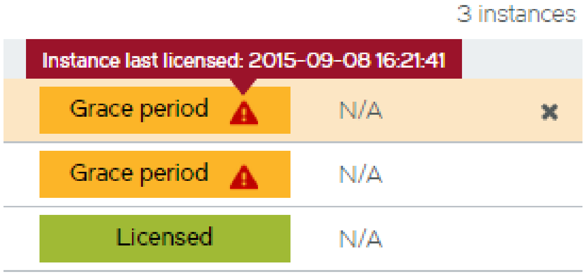
13. Click the **Services** menu, and then click **Services Director: vTM Instances**. The **vTM Instances** page appears.

    This page indicates the licensing state of each Traffic Manager.

    All Traffic Managers that were present in the original configuration should now be present.

    If you are using a different Service Endpoint Address to the one used by the FLA Licensing in the backup, the licensing of the Traffic Managers will be disrupted. Each affected Traffic Manager will enter a grace period. For example:

    FIGURE 260 Grace Periods



3 instances

Instance last licensed: 2015-09-08 16:21:41

Grace period ⚠	N/A	✖
Grace period ⚠	N/A	
Licensed	N/A	

    In this case, generate a FLA license that is keyed to the new Service Endpoint Address. Then, relicense your Traffic Manager instances. Refer to "Relicensing Traffic Managers".

14. Click the **System** menu, and then click **Disaster Recovery: Backup and Restore**. The **Backup and Restore** page appears.

    No backup schedule will be present. This information is not saved in the backup.

15. (Optional) Create a new backup schedule. Refer to Configuring a Scheduled Backup Schedule on page 240.

    The restore process is then complete.

    After the restore process is complete for the Primary Services Director VA, you can then create a new Secondary Services Director VA, and join it to the Primary. Refer to Installing the Brocade Services Director VA on page 13.

    NOTE
    A new Secondary Services Director VA will receive its configuration from the Primary. You do not need to use a restore process when you create the Secondary.

Starting and Stopping the Services Director Service

You can perform a number of master password tasks from the **System** menu.

Restarting the Services Director VA

You can stop, start and restart your Services Director service at any time from the **System** > **Service Status** page.

- When the system is running, click **Stop** to stop the service.
- When the system is running, click **Restart** to stop and restart the service.
- When the system is not running, click **Start** to start the service.

All changes are immediate.

You are *not* required to enter the master password during this operation. The master password is only required when restarting the Virtual Machine for a Services Director VA. Refer to Entering the Master Password After a Virtual Machine Restart on page 254.

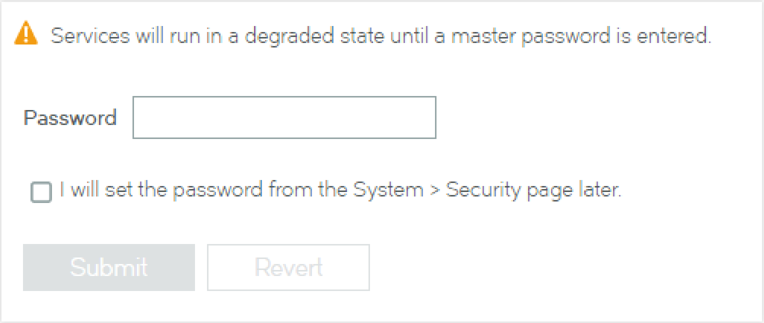
Entering the Master Password After a Virtual Machine Restart

You can restart the Virtual Machine (VM) for a Services Director VA at any time.

- If you chose to store the master password internally when you configured the Services Director VA node, you do not need to enter the master password after a VM restart.
- If you did not store the master password internally, you must enter the master password to unlock access to Traffic Managers.

When the Services Director VA is accessed for the first time after a VM restart, the following dialog box appears:

FIGURE 261 Master Password Entry



⚠ Services will run in a degraded state until a master password is entered.

Password

□ I will set the password from the System > Security page later.

There are two scenarios:

- If you know the master password, you will typically enter it immediately. Refer to Entering the Master Password Immediately After a Restart on page 254.
- If you do not know the master password, but are an administration user, you may want to access the Services Director VA to access functionality that is unrelated to Traffic Managers. For example, to access system logs. You will enter the password at some point afterwards, and regain access to Traffic Manager instances. Refer to Entering the Master Password Later on page 255.

Entering the Master Password Immediately After a Restart

If you know the master password, you will typically enter it immediately.

> NOTE
> You may receive an e-mail notification of a raised **master_password_fail** alarm before you enter the new master password on the Services Director VA.

1. On the master password dialog box, enter the master **Password**.
2. Click **Submit**. This unlocks access to the Services Director VA.
3. To confirm access to Traffic Managers, click the **Services** menu, and then click **Services Director: vTM Instances**. The **vTM Instances** page appears. This page will include all of your Traffic Managers.

Entering the Master Password Later

If you do not know the master password, but are an administration user, you may want to access the Services Director VA to access functionality that is unrelated to Traffic Manager instances. Under these circumstances, you can choose to enter the master password at a later point.

NOTE
If the VM is restarted again, this choice remains in place.

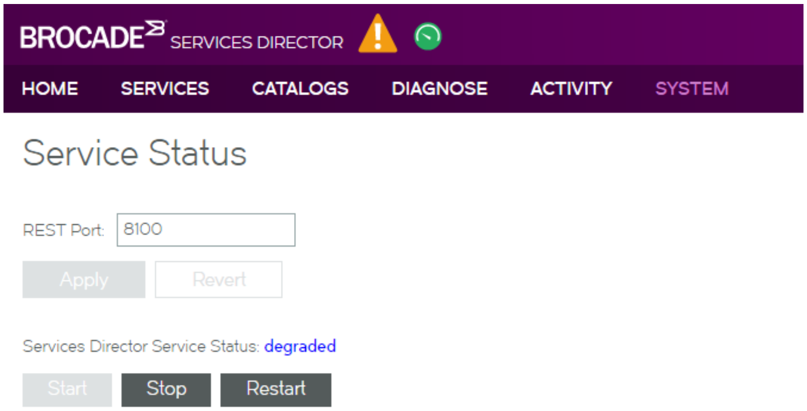
NOTE
You may receive an e-mail notification of a raised **master_password_fail** alarm before you enter the new master password on the Services Director VA.

Choosing to Enter the Master Password Later

1. On the master password dialog box, click the **I will set the password from the System Security page later** check box.
2. Click **Submit**.

   This unlocks access to the Services Director VA. However, until you enter the master password, the Services Director service status is Degraded. This is indicated on the **System** > **Service Status** page.

FIGURE 262 Service Status: Degraded Service



REST Port: 8100

Services Director Service Status: degraded

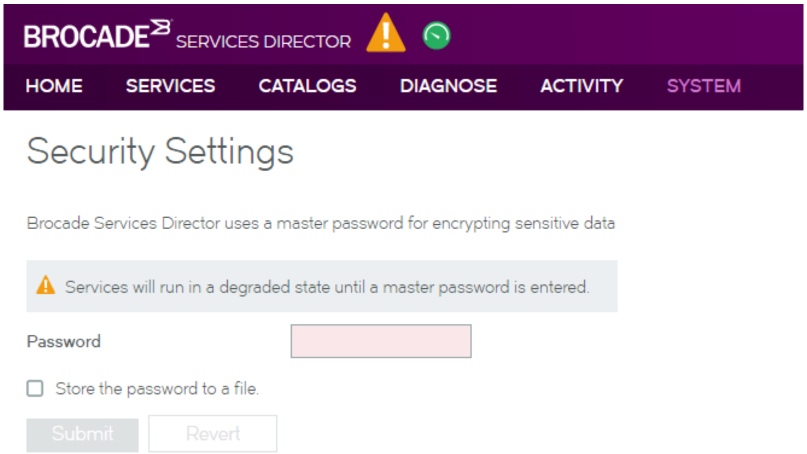
You will have no access to Traffic Managers while in this state.

When you are ready to recover from this Degraded state, you must enter the master password.

Entering the Master Password

1. Click the **System** Menu, then click **Security**. The **Security Settings** page appears.

FIGURE 263 Security Settings Page



Security Settings

Brocade Services Director uses a master password for encrypting sensitive data

Services will run in a degraded state until a master password is entered.

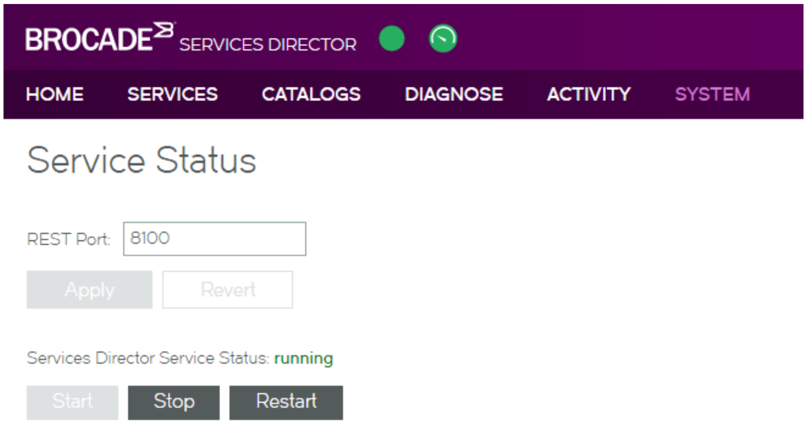
Password

□ Store the password to a file.

2. Enter the master password.
3. Select the **Store the password to a file** check box if you want to store the master password internally for future use.
4. Click **Submit**.

   The **Security Settings** page updates, but no further action is required on this page.
5. Click the **System** menu, then click **Service Status**. The **Service Status** page appears, which enables you to confirm that the Degraded state has changed to Running.

FIGURE 264 Service Status: Running Service



Service Status

REST Port: 8100

Services Director Service Status: running

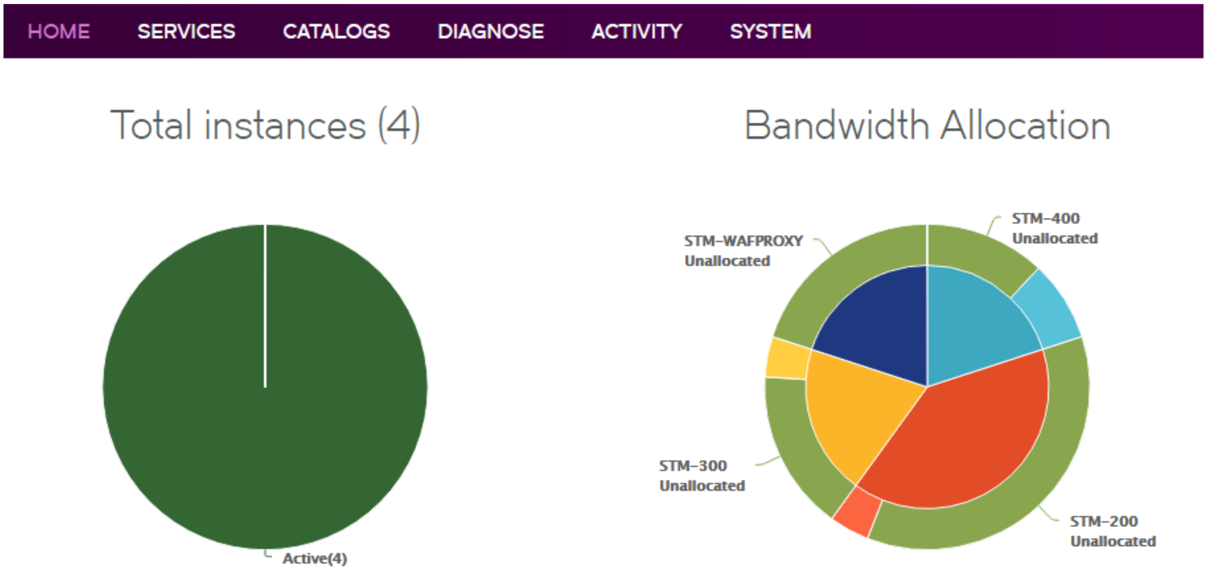
6. To confirm access to Traffic Managers, click the **Services** menu, and then click **Services Director: vTM Instances**. The **vTM Instances** page appears. This page will include all of your Traffic Managers.

Creating and Delivering Services Director Reports

Viewing Reports and Diagnostics

The **Home** page of the Services Director VA shows summary graphs for total instances and of bandwidth allocation.

FIGURE 265 Home Page Summary Graphs



The **Activity** menu in the Services Director VA enables you to generate detailed reports about your current Traffic Manager instances, bandwidth allocation, CPU utilization, and throughput. You can view how your resources are utilized so that you can adjust and reallocate resources as needed.

You can view the following reports:

- **vTM Instance Allocation** - The number of Traffic Manager instances by instance host or feature pack, and the current status of each: Active, Idle, or Failed. For details, refer to The vTM Instance Allocation Report on page 258.
- **Bandwidth Allocation** - The current bandwidth allocation by SKU or feature pack. For details, refer to The Bandwidth Allocation Report on page 260.
- **CPU Utilization** - The current CPU utilization by Traffic Manager instance or instance host. For details, refer to The CPU Utilization Report on page 262.
- **Throughput Utilization** - The current data throughput by Traffic Manager instance or instance host. For details, refer to The Throughput Utilization Report on page 263.

NOTE
Historical reports are not available in this release.

The vTM Instance Allocation Report

The **vTM Instance Allocation** report summarizes the status of all instances as a series of pie charts. The main page is a two-layer pie chart. The inner layer is divided by feature pack by default, while the outer layer is divided by instance status.

The **vTM Instance Allocation** report answers these questions:

- What is the current status of my instance hosts?
- What is the current status of a particular instance host?
- What is the current status of my feature packs?
- What is the current status of a particular feature pack?

The report displays the number of instances and the status with that feature pack. You can drill down into each individual feature pack and another pie chart is presented that gives you a report on that feature pack. You also have the option to divide the inner layer of pie chart in the main page by instance host. Similarly, you can drill down into each instance host.

The **vTM Instance Allocation** report displays the current status of instances in a color coded format.

Instance Status	Color	Description
Active	Green	An instance that is currently running.
Failed	Red	An instance has failed to start.
Idle	Blue	An instance that has been deployed but is not currently running.

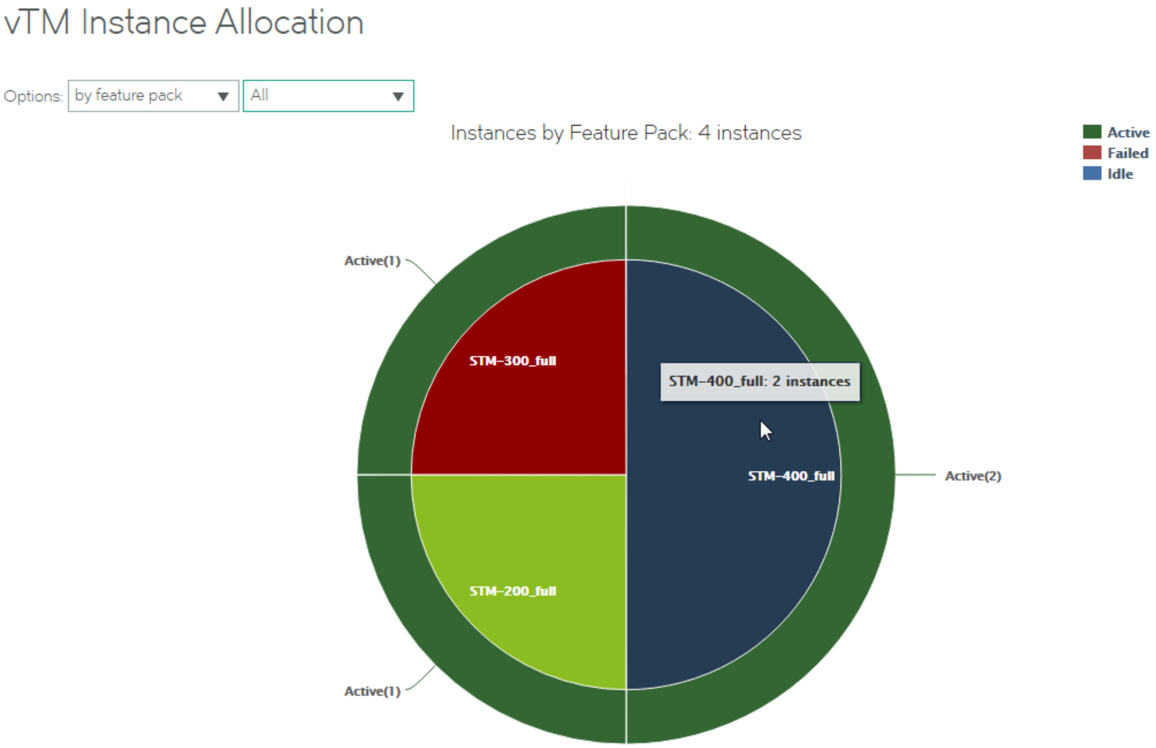
Pause the pointer over a specific area of the pie chart to view the feature pack or instance name (depending on the option chosen) and the number of instances.

Drill down into data by clicking an inner section of the graph.

Viewing the vTM Instance Allocation Report

1. Click **Activity** > **vTM Instance Allocation** to display the **vTM Instance Allocation** report page.

FIGURE 266 vTM Instance Allocation Report

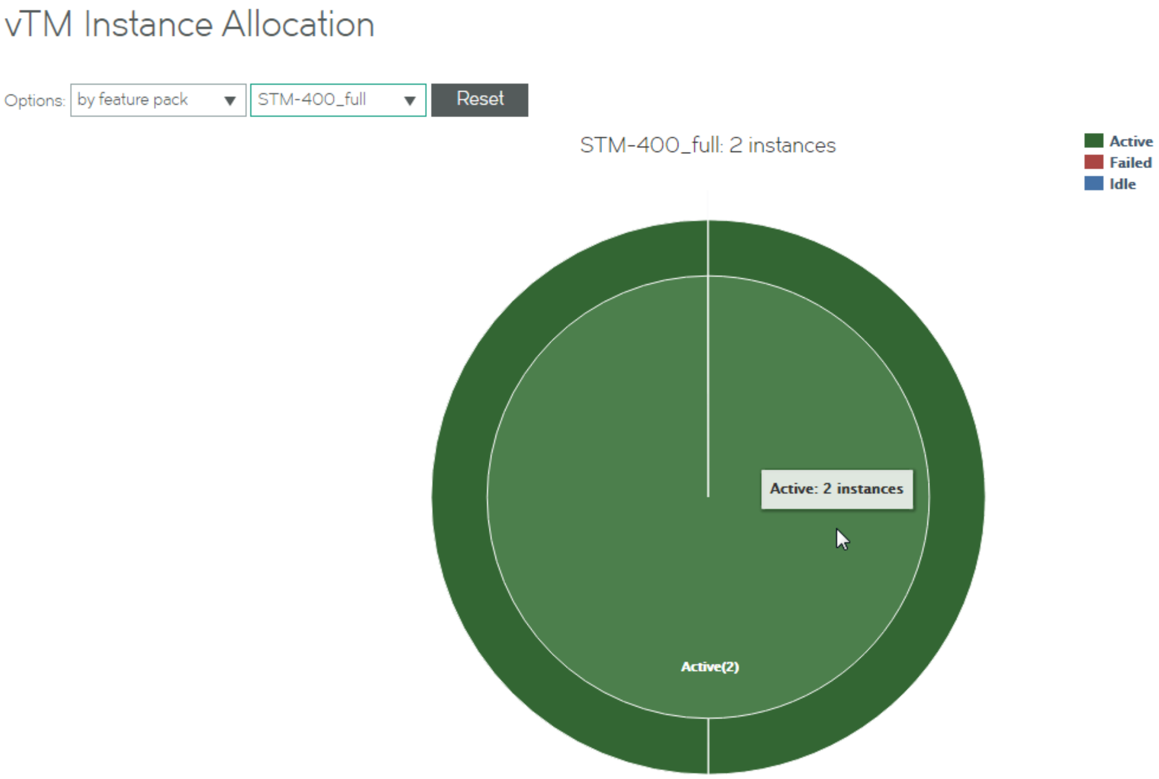


2. Use the Options to change the report type:
   - **Instance host**. Then, select a specific instance host for the report, or select **All**.
   - **Feature pack**. Then, select a specific feature pack for the report, or select **All**.

   When you select All, you can double-click an instance or feature pack in the pie chart to view details for the selected instance or feature pack.

3. Drill down into data by clicking one of the inner sections. For example:

FIGURE 267 vTM Instance Allocation: STM-400_full Feature Pack



The Bandwidth Allocation Report

The **Bandwidth Allocation** report displays allocated bandwidth for your Traffic Manager instances by SKU or feature pack. When you create an instance, you must specify which feature pack you want to use; you do not specify the SKU.

The **Bandwidth Allocation** report answers these questions:

- How much bandwidth is allocated to a SKU or instance?
- How much bandwidth is unallocated for a SKU or instance?

The **Bandwidth Allocation** report is a set of pie charts. The main page is a two-layer pie chart. The inner layer is divided by licensed tied SKUs. The outer layer shows the bandwidth allocated to each of instances and total size of available bandwidth of each SKU.

NOTE
You cannot specify how much bandwidth you want to reserve for a given feature pack.

You can use the **Bandwidth Allocation** report to evaluate whether or not you need to reallocate bandwidth or purchase additional bandwidth licenses.

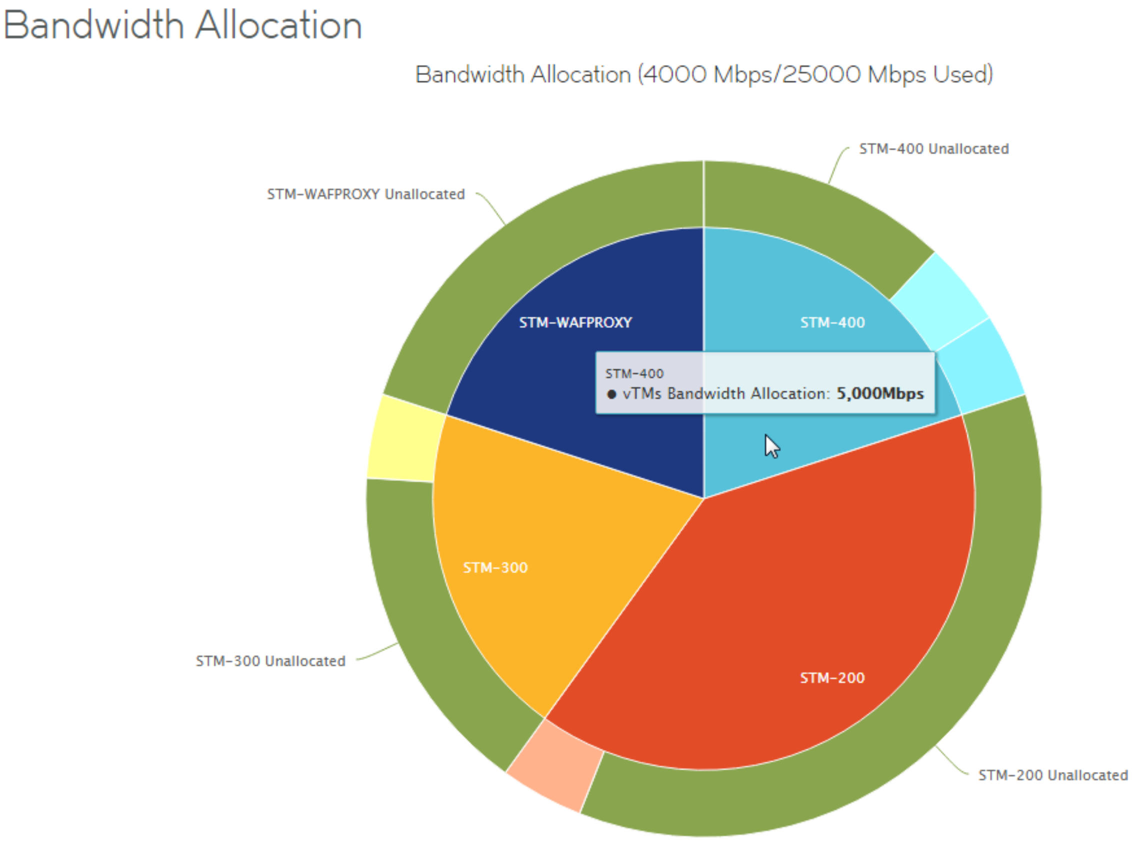
Pause the pointer over a specific area of the pie chart to view the allocated and unallocated bandwidth for a Brocade Virtual Traffic Manager SKU or instance.

Drill down into data by clicking an inner section of the graph.

Viewing the Bandwidth Allocation Report

1. Click **Activity** > **Bandwidth Allocation** to display the **Bandwidth Allocation** report page.

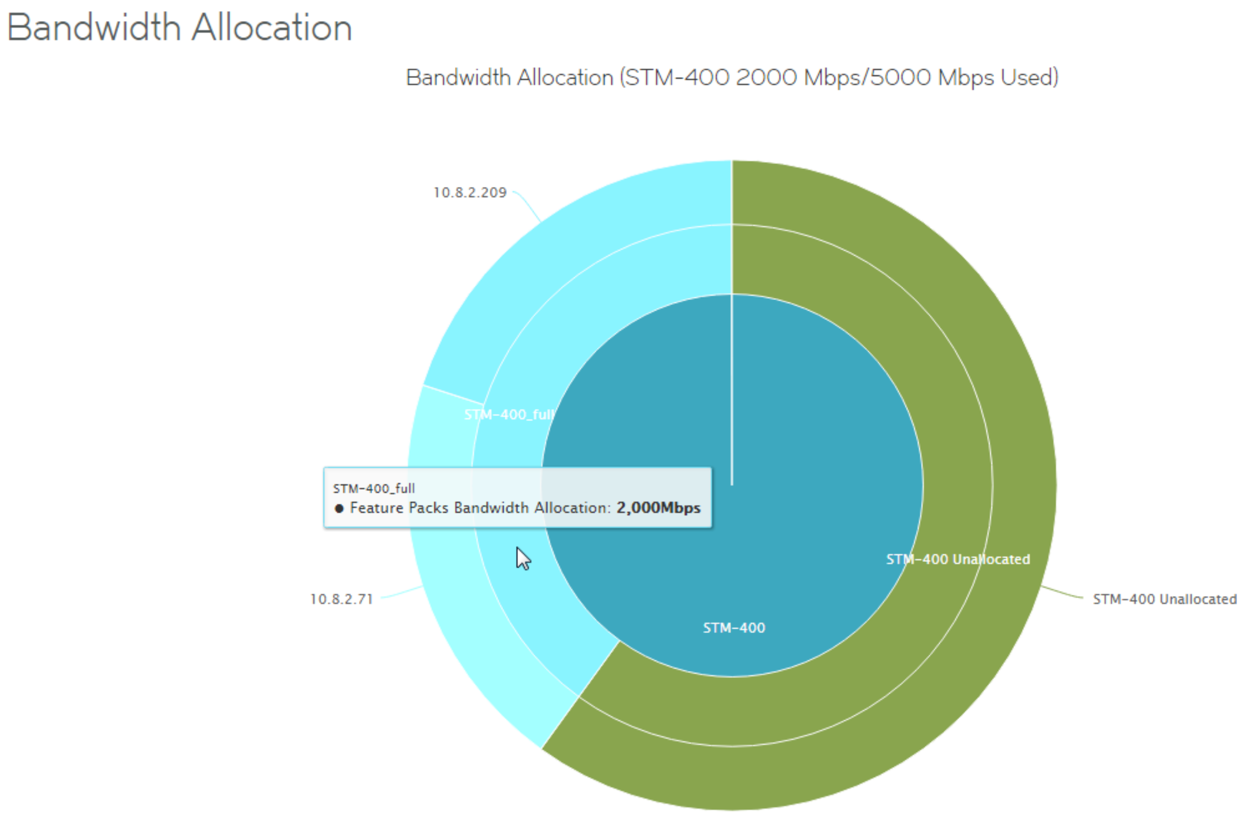
   FIGURE 268 Bandwidth Allocation Report



2. Pause over a graph section with the pointer to view a summary.

3. To drill down into a particular SKU, double-click the area you want to view. A three-layer pie chart appears:
   - The inner layer displays the particular SKU.
   - The middle layer is divided by feature pack created for that SKU.
   - The outer layer represents the bandwidth allocated for each of instance.

   FIGURE 269 Detailed Bandwidth Allocation Report



The CPU Utilization Report

The **CPU Utilization** report displays real-time CPU usage by percentage over time of each instance in an active state and the aggregated CPU usage of all active instances on each host.

The **CPU Utilization** report answers these questions:

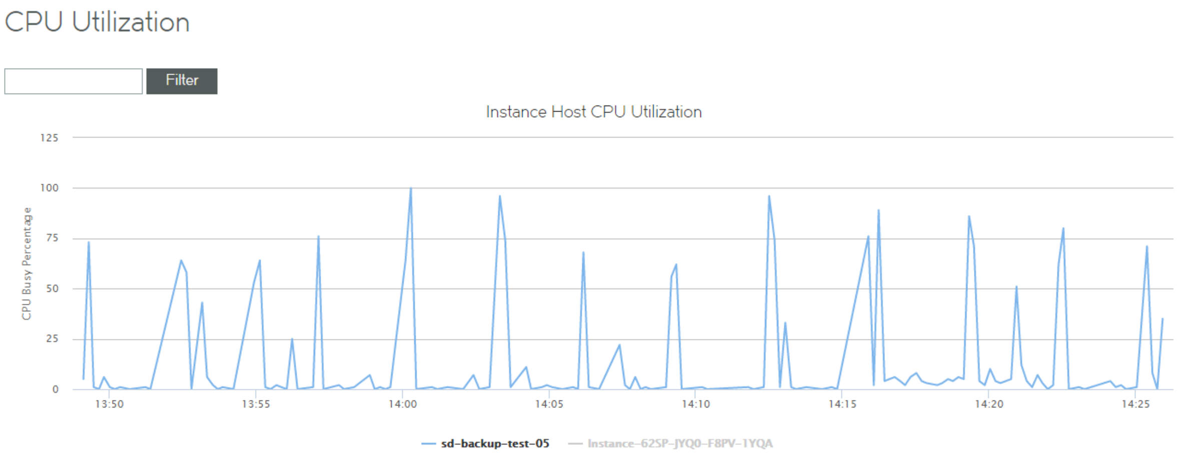
- How much of the CPU is being used?
- What is the average and peak percentage of the CPU being used?

The **CPU Utilization** report is a streaming line chart. The hosts and active instances are listed at the bottom of line charts. You can choose which host or instance CPU usage to displayed in the chart. If you have too many active instances, there is a **Filter** box from which you can filter the report by instance name. Brocade recommends you use the *regular expression* name.

Viewing the CPU Utilization Report

1. Click **Activity** > **CPU Utilization** to display the **CPU Utilization** report page.

FIGURE 270 CPU Utilization Report



2. To view a graph of data points over time, keep the page open. Data points are graphed every ten seconds.
3. To toggle on and off the graph for an instance host, click the instance hostname at the bottom of the page.
4. To view the CPU utilization for a particular instance, enter the Traffic Manager instance name and click **Filter**.
5. To clear the data, refresh the page.

The Throughput Utilization Report

The **Throughput Utilization** report displays the real-time throughput utilization (in B/s) of each instance in an active state and aggregated throughput utilization on each host.

The **Throughput Utilization** report answers these questions:

- What was the average throughput?
- What was the peak throughput?

The **Throughput Utilization** report is a streaming line chart. The real-time throughput per second and peak throughput in last hour is displayed in the chart.

The displayed throughput includes both incoming and outgoing throughput.

Review the **Throughput Utilization** report to find out which instances use the most throughput, and then compare the results to the results you expected. For example, you might expect a lot of throughput for an instance that hosts a popular site. However, if an instance is using more throughput than expected, you can try to discover why so that you can make the appropriate adjustments.

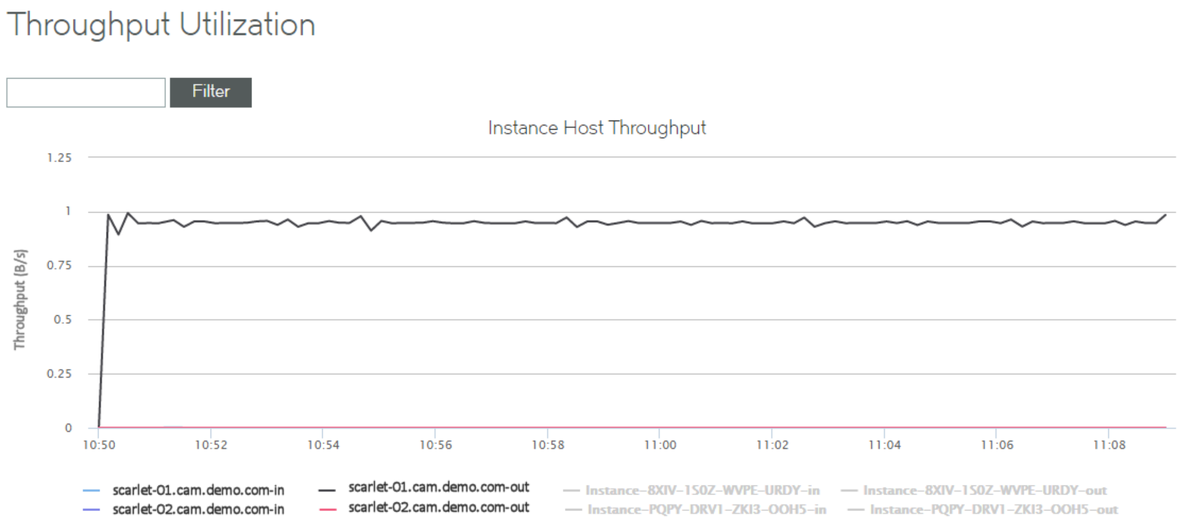
You can also use the **Throughput Utilization** report to monitor how close you are to reaching your license limitations, so that you can evaluate whether or not you should purchase additional licenses.

Pause the pointer over a specific data point to see what its value and exact time stamp were in relation to peaks.

Viewing the Throughput Utilization Report

1. Click **Activity** > **Throughput Utilization** to display the **Throughput Utilization** report page.

FIGURE 271 Throughput Utilization Report


Throughput Utilization
Filter
Instance Host Throughput
Throughput (B/s)
1.25
1
0.75
0.5
0.25
0
10:50
10:52
10:54
10:56
10:58
11:00
11:02
11:04
11:06
11:08
scarlet-01.cam.demo.com-in
scarlet-02.cam.demo.com-in
scarlet-01.cam.demo.com-out
scarlet-02.cam.demo.com-out
Instance-8XIV-1S0Z-WVPE-URDY-in
Instance-PQPY-DRV1-ZKI3-OOH5-in
Instance-8XIV-1S0Z-WVPE-URDY-out
Instance-PQPY-DRV1-ZKI3-OOH5-out

2. To view the throughput for a particular instance, enter the Traffic Manager instance name and click **Filter**.

Viewing Logs and Generating System Dumps

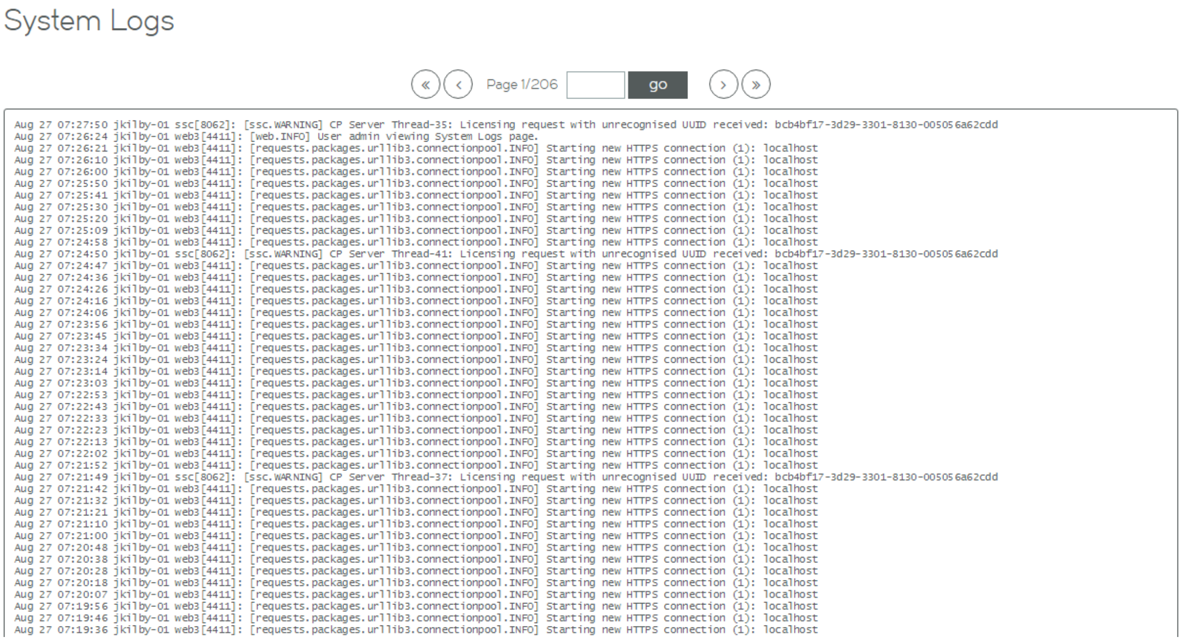
You can view system logs and generate system dumps from the **Diagnose** tab.

Viewing System Logs

You can view current logs for the Services Director in the **System Logs** page.

1. Click **Diagnose** > **System Logs** to display the **System Logs** page.

   FIGURE 272 System Logs Page



```
Aug 27 07:27:50 jkilby-01 ssc[8062]: [ssc.WARNING] CP Server Thread-35: Licensing request with unrecognised UUID received: bcb4bf17-3d29-3301-8130-00505 6a62cdd
Aug 27 07:26:24 jkilby-01 web3[4411]: [web.INFO] User admin viewing System Logs page.
Aug 27 07:26:21 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:26:10 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:26:00 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:25:50 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:25:41 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:25:30 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:25:20 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:25:09 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:24:58 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:24:50 jkilby-01 ssc[8062]: [ssc.WARNING] CP Server Thread-41: Licensing request with unrecognised UUID received: bcb4bf17-3d29-3301-8130-00505 6a62cdd
Aug 27 07:24:47 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:24:36 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:24:26 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:24:16 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:24:06 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:23:56 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:23:45 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:23:34 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:23:24 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:23:14 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:23:03 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:22:53 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:22:43 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:22:33 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:22:23 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:22:13 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:22:02 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:21:52 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:21:49 jkilby-01 ssc[8062]: [ssc.WARNING] CP Server Thread-37: Licensing request with unrecognised UUID received: bcb4bf17-3d29-3301-8130-00505 6a62cdd
Aug 27 07:21:42 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:21:32 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:21:21 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:21:10 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:21:00 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:20:48 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:20:38 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:20:28 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:20:18 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:20:07 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:19:56 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:19:46 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
Aug 27 07:19:36 jkilby-01 web3[4411]: [requests.packages.urllib3.connectionpool.INFO] Starting new HTTPS connection (1): localhost
```

2. Click **<<** (first), **<** (previous), **>** (next) or **>>** (last) to navigate through the log pages.

   Alternatively, type a number in the **Page** text box and click **Go** to navigate to a specific page.

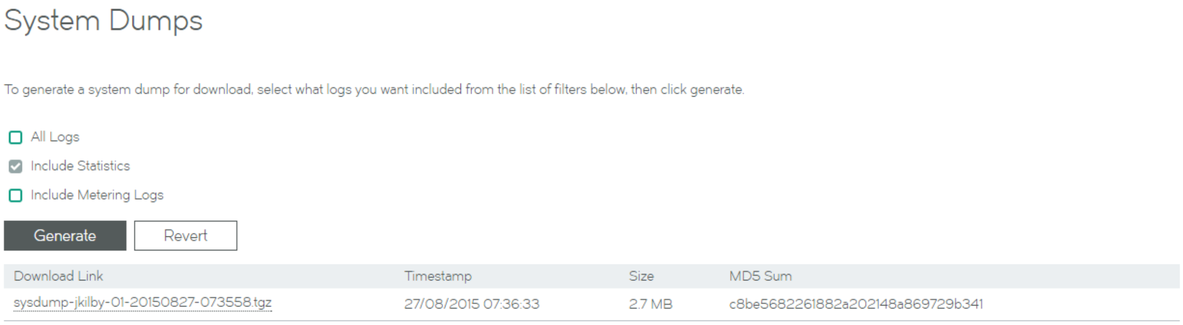
Generating System Dumps

You can generate system dumps for the Services Director from the **Diagnose** menu.

You can tailor the contents of the system dumps to include statistics if required.

1. Click **Diagnose** > **System Dumps** to display the **System Dumps** page.

   FIGURE 273 System Dumps Page



System Dumps

To generate a system dump for download, select what logs you want included from the list of filters below, then click generate.

☐ All Logs
☑ Include Statistics
☐ Include Metering Logs

Download Link	Timestamp	Size	MD5 Sum
sysdump-jkilby-01-20150827-073558.tgz	27/08/2015 07:36:33	2.7 MB	c8be5682261882a202148a869729b341

2. Complete the configuration according to this table.

Control	Description
All Logs	Select to generate all current system logs.
Include Statistics	Select to include all statistics in system dump files.
Include Metering	Select to include all metering logs in system dump files.

3. Click **Generate** to create the system dump.

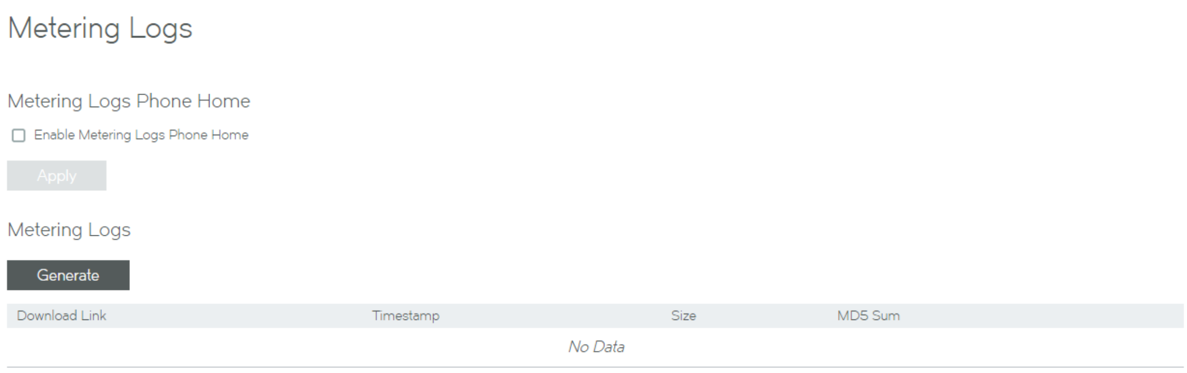
   Generated logs are listed in a table of download hyperlinks.

Working with Metering Logs

You can generate metering logs from the **Metering Logs** page. The files are created as .ZIP files and listed in a table. A maximum of ten metering logs can be generated by this process.

NOTE
Cloud Service Provider customers must ensure that SNMP is enabled on all externally-deployed Traffic Managers to support metering.

FIGURE 274 Metering Logs Page



Metering Logs

Metering Logs Phone Home

□ Enable Metering Logs Phone Home

Metering Logs

Download Link	Timestamp	Size	MD5 Sum
	No Data		

You can download any listed log files directly from the table.

You can also enable/disable the phone home feature from this page. For details of the phone home feature, refer to the *Brocade Services Director Advanced User Guide*.

Generating Metering Logs

1. Click **Diagnose > Metering Logs** to display the **Metering Logs** page.
2. Clear the **Enable Metering Logs Phone Home** check box.
3. Click **Generate** to create the metering logs.

Downloading Metering Logs

1. Click **Diagnose** > **Metering Logs** to display the **Metering Logs** page.
2. Click the name of the required log file (.ZIP) in the metering log table.
3. Select a save location and click **Save**.

Configuring the Phone Home Function

1. Click **Diagnose** > **Metering Logs** to display the **Metering Logs** page.
2. Select the **Enable Metering Logs Phone Home** check box.
3. Click **Apply** to confirm your setting.

> NOTE
> A warning e-mail will be sent every 24 hours if the phone home feature is enabled and Services Director is unable to connect to the phone home server.

Understanding Metering Logs

The Services Director automatically meters usage on a regular basis, and it optionally sends this information to Brocade for billing purposes. By default, it records this information once per hour.

If a Traffic Manager instance is active, the Services Director polls it to obtain total throughput and peak activity metrics. The Services Director creates a metrics log file with one line of metrics data for each Traffic Manager instance. Each line of metrics data records the name of the instance, the time elapsed since the resource was created, and the polled metrics. If an instance is not active, only the elapsed time is recorded.

If you want to generate usage or billing information, typically you process all metering log files and aggregate the results. You should use caution when aggregating data results for billing since metering records include failed deployments.

NOTE
Generating log files has a cumulative impact on disk
space.

The Services Director collects metering data from Traffic Manager instances as follows:

- Instances that are at version 9.4 or earlier (or have no REST API enabled) have their metering collected through SNMP.
- Instances that are at version 9.5 or later with the REST API enabled have their metering collected through their REST API. If REST-based metering fails (or is not possible), the Services Director falls back to collecting using SNMP. Any metering issues will be included in the warning logs, as before.

The Services Director records the most recent metrics information for each instance in the inventory database. You can obtain this data using the REST API. The REST API does not supply bulk metrics data.

The Metering Log file is structured as follows:

- The first row contains version data for the metering log format. This first line can be ignored by customers. Ignore this line when you aggregate data for billing.
- Each subsequent row records one set of metrics for a Traffic Manager instance, in comma-separated value (CSV) format.
- The final line contains an MD5 hash of the previous lines. Ignore this line when you aggregate data for billing.

Each line of metrics contains the following fields:

Field	Description
Timestamp	The date and time, in UTC format, that the line was written.
Instance ID	The unique instance ID for the Traffic Manager instance.
Instance Tag	This information may be empty but it is included, even if empty.
Owner	(Optional) T he owner of the Traffic Manager instance.
Cluster ID	The cluster for the Traffic Manager instance.
Management IP	The management IP address of the Traffic Manager instance.
Instance SKU	The SKU (or SKU combination) assigned to the Traffic Manager instance (at the time of writing to the log). The SKU might vary between readings, and variations are not recorded in the metrics log file. This property includes a hash of features applicable to the SKU. Ignore these features for billing purposes.
Feature Pack	The feature pack assigned to the Traffic Manager instance (at the time of writing to the log).
Deploy Time	The length of time (in days, hours and minutes) since the instance was deployed.
Throughput	The number of bytes sent by the Traffic Manager instance, as recorded in the SNMP counter.

Field	Description
	This number is cumulative and is reset whenever the Traffic Manager instance is restarted. It is not the throughput since the latest metering action. To generate usage or billing information based on throughput, you should set your aggregating script to detect a drop in throughput and designate this as a restart. This property is applicable to active Traffic Manager instances only. • For Idle or Inactive instances, it contains a value of 0 (zero) in the log. • For uncontactable instances, it contains a value of -1 in the log.
Peak Throughput	The highest number of bytes sent by the Traffic Manager instance in any second of the previous hour. This property is applicable to active Traffic Manager instances only. • For Idle or Inactive instances, it contains a value of 0 (zero) in the log. • For uncontactable instances, it contains a value of -1 in the log.
Peak Requests	The highest number of requests received by the Traffic Manager instance in any second of the previous hour. This property is applicable to active Traffic Manager instances only. • For Idle or Inactive instances, it contains a value of 0 (zero) in the log. • For uncontactable instances, it contains a value of -1 in the log.
Peak SSL Requests	The highest number of Secure Socket Layer (SSL) requests received by the Traffic Manager instance in any second of the previous hour. This property is applicable to active Traffic Manager instances only. • For Idle or Inactive instances, it contains a value of 0 (zero) in the log. • For uncontactable instances, it contains a value of -1 in the log.
Instance Bandwidth	The bandwidth (in Mbps) allocated to the Traffic Manager instance.
Record Hash	An MD5 or similar hash of the record from the Services Director license file for tamper detection. Ignore this for billing purposes.

If metrics are not collected for a period of time, peaks for the missing time are not recorded. If you reduce the metering interval, the peak values are still relative to the previous hour rather than the time since metrics were last collected.