53-1005041-01
22 May 2017

Brocade Virtual Traffic Manager: Data Plane Acceleration Configuration Guide

Supporting 17.2

BROCADE

Brocade Communications Systems, Incorporated

Corporate and Latin American Headquarters
Brocade Communications Systems, Inc.
130 Holger Way
San Jose, CA 95134
Tel: 1-408-333-8000
Fax: 1-408-333-8101
E-mail: info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems China HK, Ltd.
No. 1 Guanghua Road
Chao Yang District
Units 2718 and 2818
Beijing 100020, China
Tel: +8610 6588 8888
Fax: +8610 6588 9999
E-mail: china-info@brocade.com

European Headquarters
Brocade Communications Switzerland Sàrl
Centre Swissair
Tour B - 4ème étage
29, Route de l'Aéroport
Case Postale 105
CH-1215 Genève 15
Switzerland
Tel: +41 22 799 5640
Fax: +41 22 799 5641
E-mail: emea-info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems Co., Ltd. (Shenzhen WFOE)
Citic Plaza
No. 233 Tian He Road North
Unit 1308 – 13th Floor
Guangzhou, China
Tel: +8620 3891 2000
Fax: +8620 3891 2111
E-mail: china-info@brocade.com

Contents

Preface **1**

Document Conventions 1
Notes and Warnings 1
Text Formatting Conventions 2
Command Syntax Conventions 2
Brocade Resources 3
Document Feedback 3
Contacting Brocade Technical Support 3
Brocade Customers 3
Brocade OEM Customers 4

Chapter 1 - Getting Started **5**

About This Guide 5
Introducing the Traffic Manager 5
Data Plane Acceleration Mode 6
Data Plane Acceleration in the Traffic Manager 6
Network interfaces in Data Plane Acceleration mode 7
Network Configurations 7
Scenario 1: Simple Network 7
Scenario 2: Public and Private Networks 8
Scenario 3: Multiple Traffic Managers 9

Chapter 2 - Prerequisites and Planning **11**

Prerequisites 11
Additional Prerequisites for Data Plane Acceleration mode 12
Access to the Traffic Manager Administration Interface 13
Additional Clustering Considerations 13

Chapter 3 - Installing the Traffic Manager Virtual Appliance on VMware **15**

System Requirements 15

Cloning and Guest OS Customization 16
Importing the OVF package 16
Checking the Initial IP Address 19
Connecting to the Admin UI 20
Expanding the Log File Partition 20

Chapter 4 - Installing the Traffic Manager Virtual Appliance on QEMU/KVM 23
QEMU/KVM System Requirements 23
Installing the Virtual Appliance 24
Accessing the Virtual Appliance Console 30
Checking the Initial IP Address 31
Connecting to the Admin UI 32
Expanding the Logs Partition 32

Chapter 5 - Installing the Traffic Manager Appliance Image 35
Before you Begin 35
Creating an Installation Disk or USB Flash Drive 36
Installing the Traffic Manager From a Disk or USB Flash Drive 37
Installing Through a PXE Boot Environment 39
IPMI Management 39

Chapter 6 - Configuring your Traffic Manager Instance 41
Administration User Interface Authentication 41
Running the Initial Configuration Wizard 42
Accepting the Terms and Conditions of Sale 42
Configuring Networking 42
DNS Settings 45
Host Name Resolution 46
Time Zone Settings 47
Admin Password 47
IPMI Settings 48
License Key 48
Summary 49
Configuring the Traffic Manager From the Command Line 50
Performing an Unattended Configuration 54
Enabling Data Plane Acceleration 55
Creating a New Traffic Manager Cluster 55
Upgrading and Downgrading 58
Before You Start 58
Caveats for VMware Users 59

Installing Incremental Software Revisions 60
Installing Full Upgrades (Version Number Changes)....61
Downgrading to an Earlier Version 62
Downgrading a Traffic Manager Manually 64

Chapter 7 - Configuring Your L4Accel Services 65

Structure of a Basic L4Accel Service 65
Source Network Address Translation....66
L4Accel Virtual Server Settings 68
L4Accel Protocol Modes 68
L4Accel Protocol Settings 71
Traffic Inspection Restrictions with L4Accel Services 71
Layer 4 Request Logging 72
L4Accel State Synchronization 72
Pools and Load Balancing 75
Node Deletion Behavior for L4Accel Services....76
Session Persistence in L4Accel Services 76
Configuring Source NAT for a Pool....76
Traffic IP Groups and Fault Tolerance 77
Adding Back-end IP Addresses....79
System Settings 80
L4Accel Settings....81
Source NAT Tuneables....81
TCP Settings 82
Troubleshooting 83
Bypassing Data Plane Acceleration in a Layer 7 Virtual Server 83
Troubleshooting Failure to Enable Data Plane Acceleration....83

Preface

Read this preface for an overview of the information provided in this guide. This preface includes the following sections:

- "Document Conventions," next
- "Brocade Resources" on page 3
- "Document Feedback" on page 3
- "Contacting Brocade Technical Support" on page 3

Document Conventions

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

Notes and Warnings

Note, important, and caution statements might 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.

Important: An Important 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.

Text Formatting Conventions

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

Format	Description
bold text	Identifies command names
	Identifies keywords and operands
	Identifies the names of user-manipulated GUI elements
	Identifies text to enter at the GUI
italic text	Identifies emphasis
	Identifies variables
	Identifies document titles
`Courier font`	Identifies CLI output
	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 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, by telephone, or by e-mail. Brocade OEM customers contact their OEM/Solutions 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	E-mail
Preferred method of contact for nonurgent 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	support@brocade.com Please include: • Problem summary • Serial number • Installation details • Environment description

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.

CHAPTER 1 Getting Started

This chapter introduces Brocade Virtual Traffic Manager (the Traffic Manager) and describes how to get started planning your deployment. This chapter contains the following sections:

- "About This Guide," next
- "Introducing the Traffic Manager" on page 5
- "Data Plane Acceleration Mode" on page 6
- "Data Plane Acceleration in the Traffic Manager" on page 6
- "Network Configurations" on page 7

About This Guide

The *Brocade Virtual Traffic Manager: Data Plane Acceleration Configuration Guide* describes how to configure the Traffic Manager to use Data Plane Acceleration mode, including all functionality changes while in this mode.

Introducing the Traffic Manager

The Traffic Manager product family provides comprehensive traffic management and load balancing solutions in a range of software, hardware-ready, virtual appliance, and cloud-compute product variants. The Traffic Manager provides control, intelligence, security, and resilience for all your network traffic.

Data Plane Acceleration Mode

Traffic Manager bare-metal appliance images and virtual appliances for VMware and KVM/QEMU hypervisors can be configured with Data Plane Acceleration mode. This mode leverages a new transport layer network stack, unlike the traditional kernel network stack, to deliver increased performance for applications, as well as linear scaling of performance with the addition of more CPU cores.

Note: For the most up-to-date list of Traffic Manager product variants and versions that support Data Plane Acceleration mode, refer to the release notes supplied with your version.

By default, the Traffic Manager is supplied with Data Plane Acceleration mode disabled. Existing deployments see no change if you upgrade to the latest Traffic Manager version. For full details of how to enable Data Plane Acceleration mode in your Traffic Manager, refer to Chapter 6, "Configuring your Traffic Manager Instance."

For a complete list of hardware and software requirements for running Data Plane Acceleration, refer to "Prerequisites" on page 11.

Data Plane Acceleration in the Traffic Manager

In Data Plane Acceleration mode, traffic is distributed to an application process based on an algorithm that ensures forward and reverse traffic for each feature configured on the Traffic Manager is forwarded to the correct application process. This distribution minimizes flow information sharing or replication across application processes. The new transport layer stack is extremely lightweight and works in a high-performance mode by parsing the transport headers of each incoming packet and instead bypassing higher level headers.

TCP- and UDP-based applications utilize Data Plane Acceleration mode to boost the connection rate and application bandwidth through the Traffic Manager. You configure these services with the protocol type "L4Accel" which supports five modes: L4Accel TCP, L4Accel UDP, L4Accel DNS, L4Accel Generic, and L4Accel Stateless. For further information, refer to Chapter 7, "Configuring Your L4Accel Services."

In a cluster, the Traffic Manager supports synchronization of the Layer 4 connection state for stateful L4Accel services between cluster members. If a Traffic Manager fails, the passive Traffic Manager becomes active and continues to process the connections that were established by the failed Traffic Manager, thus presenting a seamless experience to the end user. For further information, refer to "L4Accel State Synchronization" on page 72.

L4Accel services run in IP Transparency mode by default (Layer 7 services must still explicitly enable IP Transparency). Alternatively, Data Plane Acceleration mode provides the use of Source Network Address Translation (Source NAT) using either the Traffic Manager's network interface IP addresses or by adding a specific Source NAT IP address list. For further information, refer to "Source Network Address Translation" on page 66.

To achieve the improved performance and availability offered by Data Plane Acceleration mode, the Traffic Manager does not inspect connection data beyond the Transport layer headers for L4Accel services. High-level inspection features such as TrafficScript Rules are not available for L4Accel services.

Network interfaces in Data Plane Acceleration mode

In Data Plane Acceleration mode, the new transport layer network stack takes control of the Traffic Manager's network interfaces in order to provide high performance packet input/output, bypassing the Linux stack. The Traffic Manager software provides emulated network interfaces to the Linux stack, transparently bridging packets between an emulated network interface and its corresponding actual network interface.

While in Data Plane Accleration mode, the output of the **ifconfig** command displays emulated Linux interfaces only. The new transport layer network stack processes data packets while the Linux stack processes control packets such as ARP, neighbor discovery, DHCP, HA, and health checks. As a result, the packet counters shown in **ifconfig** show only the number of packets processed by the Linux stack. To see the packet counters on actual network interfaces, use instead the Traffic Manager's networking SNMP counters or the zcli command **stats interface**.

Note: To reconfigure any of your Traffic Manager network settings, use only the Admin UI, REST API, SOAP API, or zcli.

Network Configurations

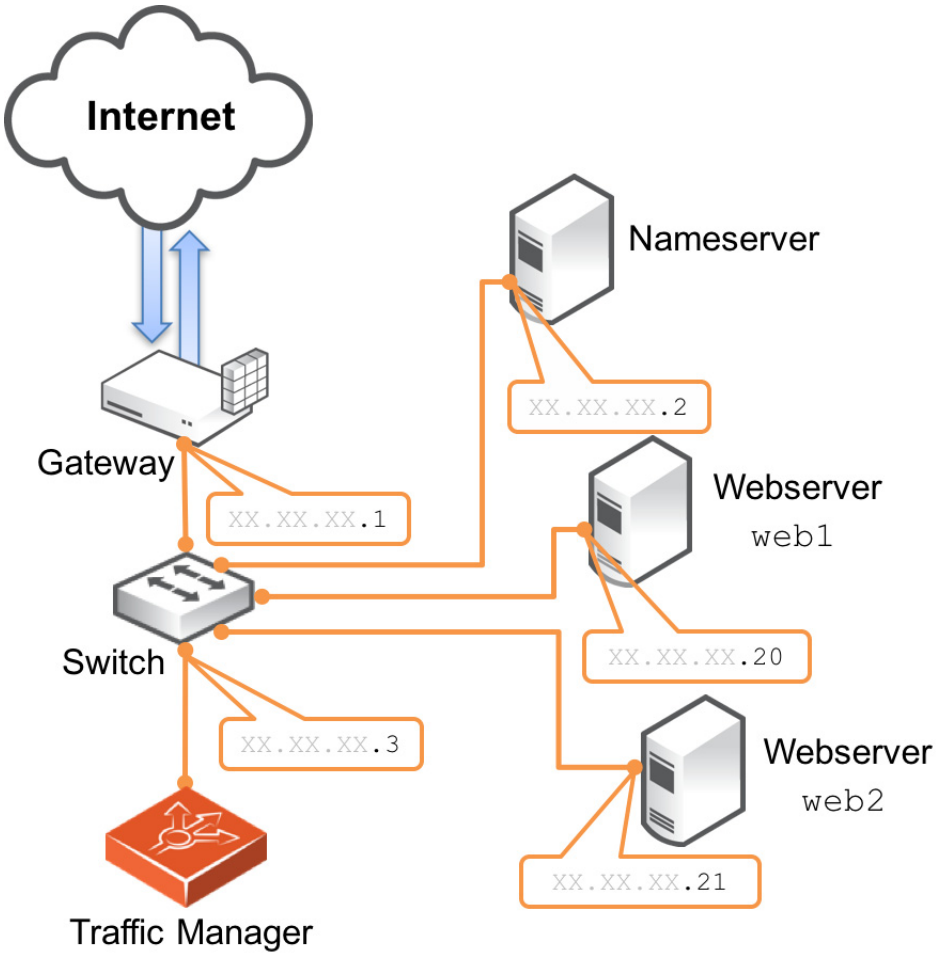
This section provides a number of scenarios showing how you can deploy the Traffic Manager into your network.

Scenario 1: Simple Network

This scenario demonstrates how you can place a single Traffic Manager into an existing network to handle traffic for a website. All IP addresses run on a publicly addressable network (represented by xx.xx.xx in the figure, with a netmask of 255.255.255.0).

Without the Traffic Manager, clients connecting to the website are directed, through the gateway, to one of the web servers hosting the site (for example, “web1” on the IP address xx.xx.xx.20).

Figure 1-1. Single setup of a Traffic Manager into an existing network



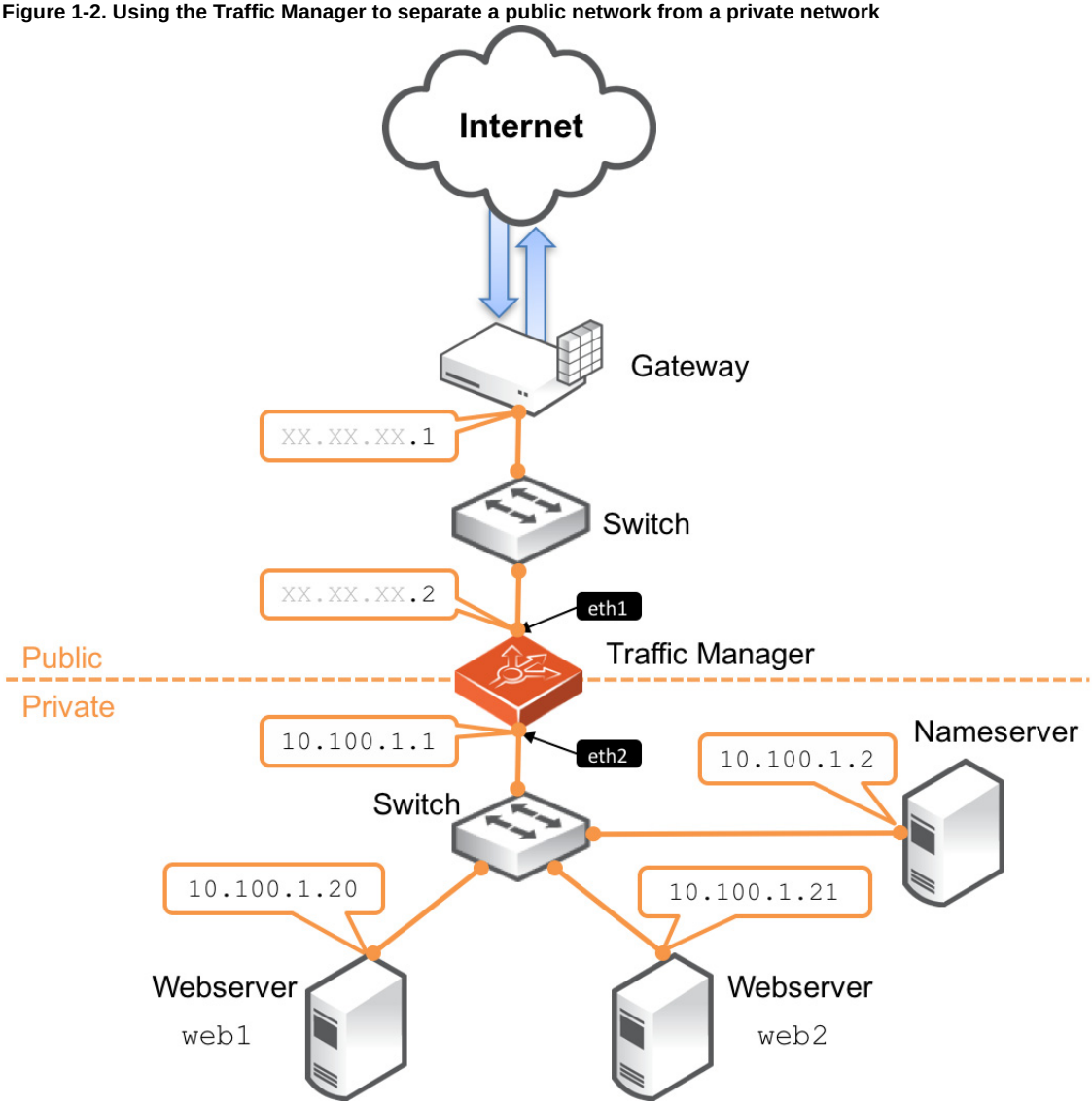
By installing a Traffic Manager configured to receive traffic over a single network port and IP address xx.xx.xx.3, you can alter your DNS record to direct clients to xx.xx.xx.3. In this way, the Traffic Manager receives the web page requests and responds with content from one of the available web servers.

Scenario 2: Public and Private Networks

This scenario splits your network infrastructure into separate public and private networks. This scenario offers greater security as the private network hides the internal back-end services from the outside world. Access is permitted only through the Traffic Manager. Using more network interfaces also gives higher performance because there is greater bandwidth capacity.

The figure shows how you can configure the network gateway and the Traffic Manager front-end interface (eth1) with publicly routable IP addresses (the xx.xx.xx network, netmask 255.255.255.0). You then configure the Traffic Manager's back-end interface (eth2) on the internal network (10.100.xx.xx, netmask 255.255.0.0).

Figure 1-2. Using the Traffic Manager to separate a public network from a private network

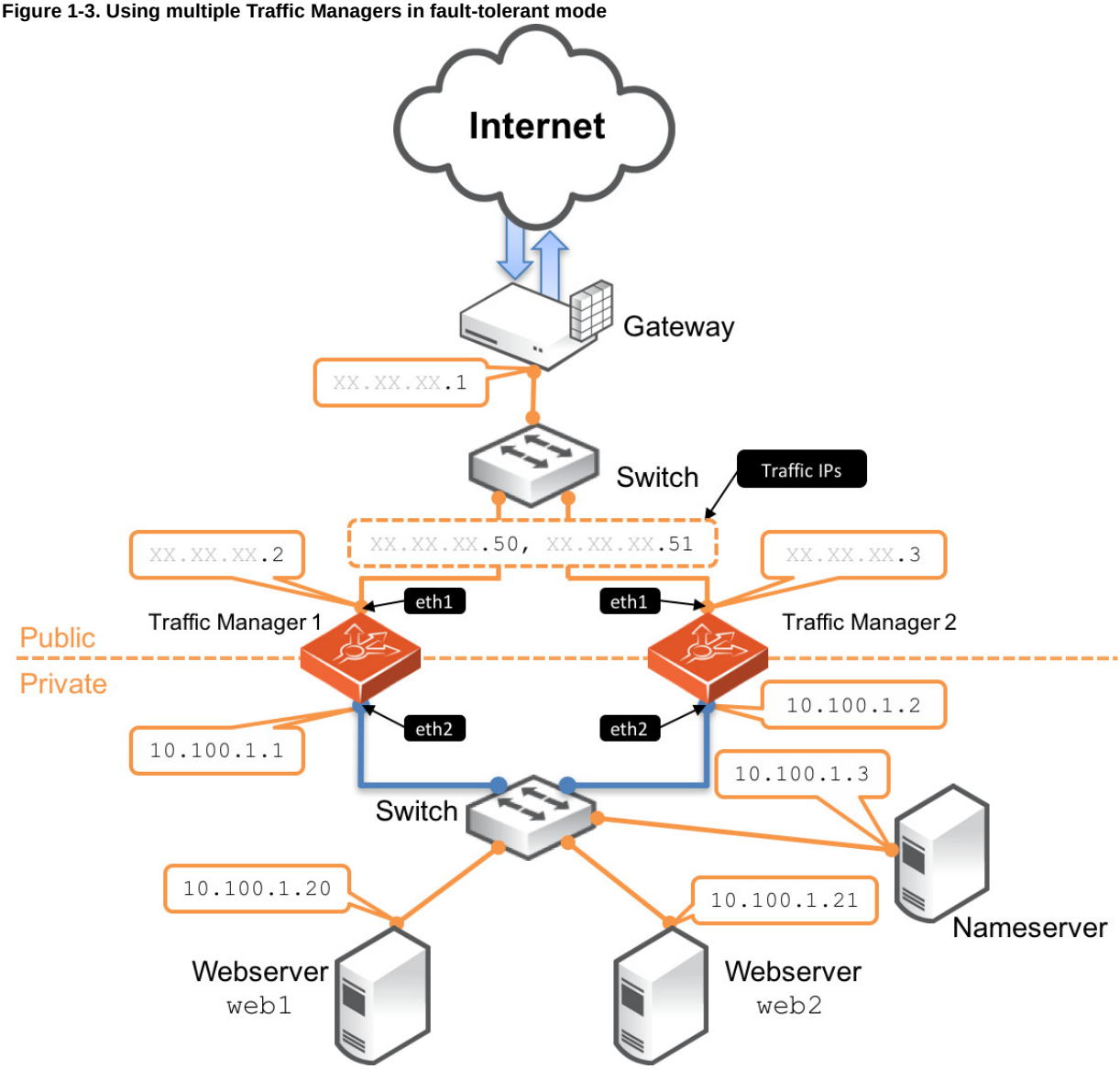


Scenario 3: Multiple Traffic Managers

This scenario deploys two Traffic Managers in a public and private network. The Traffic Managers make use of Traffic IP addresses to provide a fault-tolerant service. Traffic IP addresses are additional IP addresses that are distributed across the front-end network interfaces. If one Traffic Manager becomes uncontactable, the other Traffic Manager is able to adopt the Traffic IP address and continue handling requests.

You define and manage your Traffic IP addresses through the web-based administration user interface (Admin UI) of the Traffic Manager, and you set them up after the initial low-level networking is complete. For more information, refer to the *Brocade Virtual Traffic Manager: User's Guide*.

Figure 1-3. Using multiple Traffic Managers in fault-tolerant mode



CHAPTER 2

Prerequisites and Planning

Before you install the Traffic Manager, read this chapter for a description of the prerequisites and planning considerations. This chapter contains the following sections:

- "Prerequisites," next
- "Additional Clustering Considerations" on page 13

Prerequisites

Brocade supports Data Plane Acceleration mode in the Traffic Manager bare-metal appliance image, and virtual appliance running on the following hypervisors:

- VMware
- KVM/QEMU

To view the current reference hardware specifications for the Traffic Manager appliance image variant, see the Brocade Community website at:

http://community.brocade.com

The following resources are the minimum requirement for running Data Plane Acceleration mode on all Traffic Manager variants:

- Two CPU cores
- Allocated memory (RAM): 3 GB
- Disk allocation: 16 GB

Note: Brocade recommends using a minimum of 3 GB of RAM and two CPU cores. If you add further CPU cores, increase the memory allocation by 1 GB for each additional core.

Before you begin installation of the Traffic Manager, make sure you have the version appropriate to your target platform, and suitable license keys for each Traffic Manager instance you want to create.

For each Traffic Manager you are configuring, make sure that you have the following information:

- A valid host name

- An IP address and corresponding subnet mask for each network interface you want to use
- The IP address for the default network gateway
- An Admin password for the Administration Interface
- (Optional) The domain name to which your Traffic Manager belongs
- (Optional) The IP address for each name server that the Traffic Manager uses to resolve your internal network addresses
- (Optional) The DNS search path (commonly the same as the domain name); the "local part" of your machine host names

---

Caution: The Traffic Manager does not support the use of DHCP for your network configuration while in DPA mode. You must specify static values only.

Brocade recommends using one or more test servers (for example, web servers) to which you can direct traffic.

Note: References to $ZEUSHOME throughout this guide refer to the Traffic Manager software installation directory you specify during the installation process.

Additional Prerequisites for Data Plane Acceleration mode

The following additional requirements must be satisfied to run the Traffic Manager in Data Plane Acceleration mode:

- Your CPU must support the SSSE3 and SSE4.2 instruction sets.
- A minimum of 1 network interface, and up to a maximum of 16 network interfaces.
- Your network interfaces must be configured to auto-negotiate speed and duplex settings. For further information, see “Configuring System Level Settings” in the *Brocade Virtual Traffic Manager: User’s Guide*.
- Your network interfaces are controlled by one of the following compatible drivers:
  - vmxnet3
  - virtio-net
  - e1000
  - e1000e
  - igb
  - ixgbe
  - i40e

Note: For the most up to date list of CPU requirements and network interface driver versions, refer to the release notes provided with your product variant.

Access to the Traffic Manager Administration Interface

You administer all Traffic Manager variants through a web-enabled user interface. The Traffic Manager supports the following browsers for this purpose:

- Internet Explorer: v.7 or later
- Firefox: v.3 or later
- Safari: v.4 or later
- Chrome: v.5 or later

Additional Clustering Considerations

Before joining a new Traffic Manager instance to an existing instance to form a cluster, make sure both instances conform to each of the following conditions first:

- Data Plane Acceleration mode supports a maximum cluster size of two Traffic Managers.
- Cluster members must be Data Plane Acceleration-compatible Traffic Manager instances.
- Cluster members must have the same number of CPU cores.
- Cluster members must have the same amount of RAM.
- Cluster members must have the same number of network interfaces, with each interface controlled by a compatible driver. For the list of compatible drivers, refer to "Additional Prerequisites for Data Plane Acceleration mode" on page 12.
- Multi-Site Management must be disabled across your cluster. For more information, refer to the *Brocade Virtual Traffic Manager: User's Guide*.

Caution: The Traffic Manager software is designed to reject any joining instance in which any of the clustering conditions are not met.

For full instructions on how to create a cluster, refer to "Creating a New Traffic Manager Cluster" on page 55.

For instructions on how to upgrade an existing Traffic Manager cluster, refer to "Upgrading and Downgrading" on page 58.

CHAPTER 3

Installing the Traffic Manager Virtual Appliance on VMware

This chapter describes how to install the Traffic Manager virtual appliance on VMware. This chapter contains the following sections:

- "System Requirements," next
- "Importing the OVF package" on page 16
- "Checking the Initial IP Address" on page 19
- "Connecting to the Admin UI" on page 20
- "Expanding the Log File Partition" on page 20

System Requirements

The Traffic Manager virtual appliance is supported for production use on VMware vSphere.

Brocade provides a virtual machine deployment package conforming to the VMware Open Virtualization Format (OVF) standard in a ZIP archive file.

For a full list of the supported platforms and versions, refer to the release notes included with your Traffic Manager virtual appliance package.

Before you continue, make sure you have satisfied all of the necessary prerequisites shown in Chapter 2, "Prerequisites and Planning."

Caution: If you are upgrading your virtual appliance from a previous Traffic Manager version, you can find information specific to VMware users in "Upgrading and Downgrading" on page 61.

Note: The Traffic Manager supports the VMware hot-plug capability for RAM and CPU allocation. This capability can enable you to dynamically adjust RAM and CPU resources while the virtual machine is powered on. Certain limitations might apply depending on the version you are running. For more information, refer to the release notes, or contact your support provider for assistance.

Cloning and Guest OS Customization

The Traffic Manager supports vSphere Client cloning, which provides a mechanism to create and deploy new instances of a previously installed virtual machine. These new instances are configured with the same virtual hardware, installed software, and other properties that were configured for the original virtual machine.

This capability includes Guest Operating System (OS) Customization, which can help prevent conflicts in cloned virtual machines by allowing you to specify unique settings such as name and network configuration. It also enables the automation of virtual machine provisioning.

To use Guest OS Customization

1. Deploy a Traffic Manager OVF package in vSphere Client to be used as a template.
2. Navigate to the administration user interface (Admin UI) and complete the Initial Configuration wizard. For more information, refer to Chapter 8, "Configuring the Traffic Manager Virtual Appliance."

If you are unable to successfully complete the Initial Configuration Wizard, incorrect network settings might be applied to any cloned virtual machines based on this template.

Caution: The Guest OS Customization process does not support bonded network interfaces within the Traffic Manager virtual machine to be cloned. If you use such a setup, you must manually check and set the network configuration for each cloned virtual machine.

Caution: The Guest OS Customization process causes the Traffic Manager to disable use of the *nameip* feature. In situations where your DNS cannot successfully resolve your Traffic Manager host name, nameip allows you to configure the Traffic Manager to use its IP address instead to identify itself to other cluster members.

Caution: If you are using Guest OS Customization to clone a virtual appliance with a management interface configured, the management interface settings are cleared to ensure that the cloned appliance is accessible.

For further information on cloning and Guest OS Customization, refer to the VMware documentation website: http://www.vmware.com/support/pubs.

Importing the OVF package

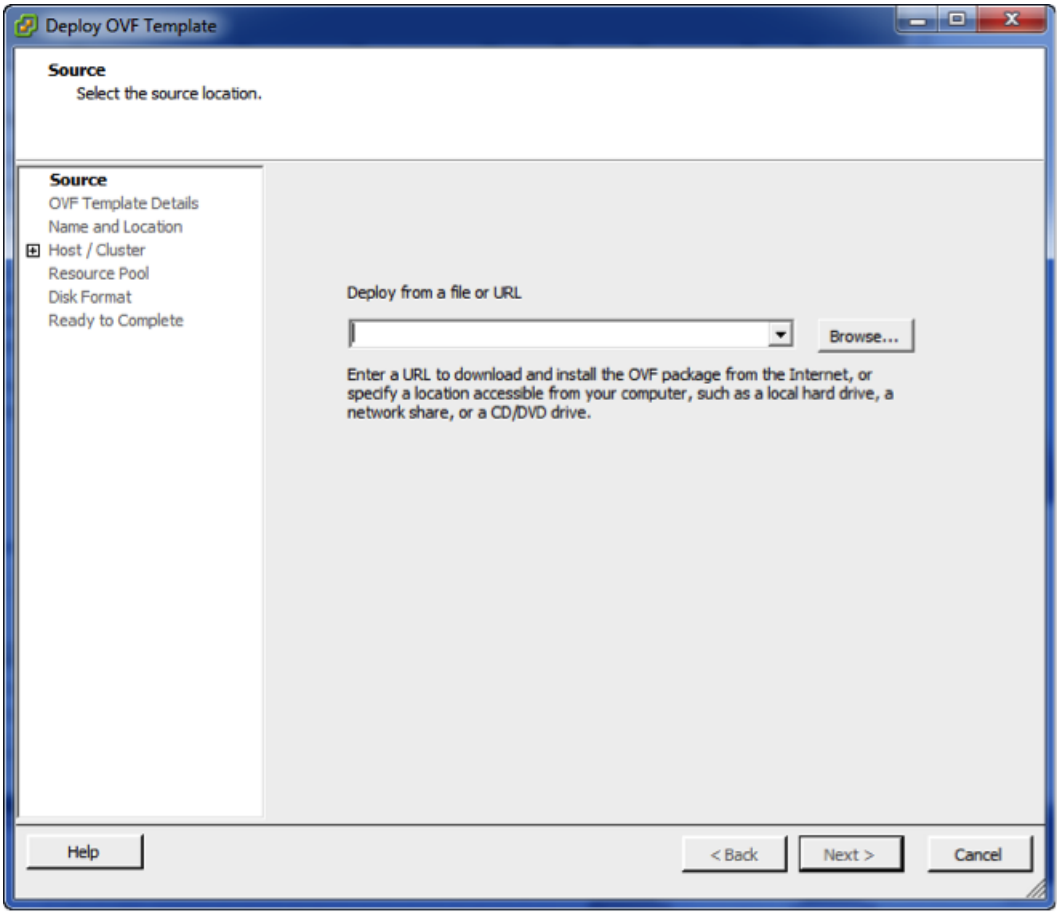
This section describes the process of importing your Traffic Manager OVF package into your VMware infrastructure.

To import the OVF package

1. Run the VMware vSphere Client program.
2. Choose **File > Deploy OVF Template…** to launch the Deploy OVF Template wizard. The individual steps to follow are shown on the left of the wizard window, with the current step displayed in the central

pane. Click **Back** and **Next** to navigate between steps, and **Cancel** to exit the wizard without deploying the OVF template.

Figure 3-1. Deploy OVF Template wizard



3. Specify the location of the Traffic Manager OVF file on your hard disk, or from some other location on the Internet. For OVF packages on your local hard disk, unpack the ZIP archive and locate the .ovf file contained inside. Click **Next** to continue.

4. Verify the details of your successfully validated virtual appliance package and click **Next**.

5. Read and accept the Brocade Terms and Conditions of Sale. To view the agreement, use the URL provided. To confirm your acceptance of the terms in the agreement, click **Accept** and then click **Next** to continue.

6. Enter an identifying name for this virtual appliance. Depending on your infrastructure configuration, you might be prompted to provide a location within the inventory for the virtual appliance. If you are connected directly to the host, the location is not applicable. Click **Next** to continue.

7. Select the appropriate host or cluster on which you intend to install and run the virtual appliance, then click **Next** to continue.

8. If you have multiple resource pools, hosts, or clusters set up within your infrastructure, select the resource within which you want your virtual appliance to reside. Click **Next** to continue.

9. Select either "thin" or "thick" disk provisioning according to your organizational policy or requirements, then click **Next** to continue.

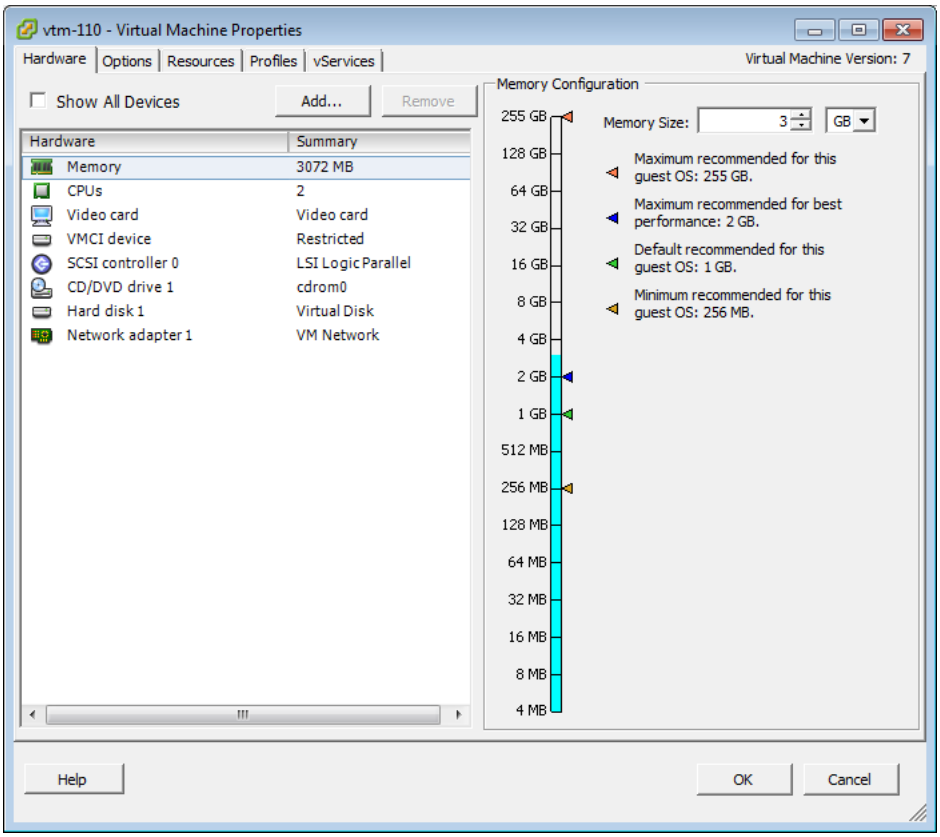
10. Depending on your VMware infrastructure, you might be prompted to specify a network mapping for your virtual appliance to a network in your inventory. Select the inventory network from the drop-down list and click **Next** to continue.

11. Check the configuration summary of your virtual appliance deployment and click **Finish** to begin the import process. To go back and modify any step of the wizard, click **Back** or click the relevant step link in the left pane.

12. After the Traffic Manager has finished importing, right-click the Traffic Manager virtual machine in your vSphere Client program and then choose “Edit Settings...”.

    The Traffic Manager OVF is packaged with the minimum resources necessary to run a standard Traffic Manager virtual appliance. To use Data Plane Acceleration mode in your virtual appliance, you must amend the properties of a newly imported virtual machine before you power it on in accordance with the prerequisites contained in Chapter 2, “Prerequisites and Planning.”

Figure 3-2. Editing the virtual machine settings



Caution: Your virtual machine might need to be powered down before you can make any changes, depending on the hot-plug capabilities of your VMware infrastructure.

13. For each change you need to make, click the appropriate category in the hardware list and update the corresponding values in the right pane.

14. (Optional) The Traffic Manager virtual appliance is supplied preconfigured with one network interface. If you require more than one interface, add new Ethernet adapters here as required.

Note: If different network drivers (for example, e1000, vmxnet3, and so on) are used for different interfaces, the mapping of network interface to MAC address might vary from reboot to reboot. Brocade recommends that you select the same network driver for each defined interface if MAC address preservation is required across your network interfaces.

---

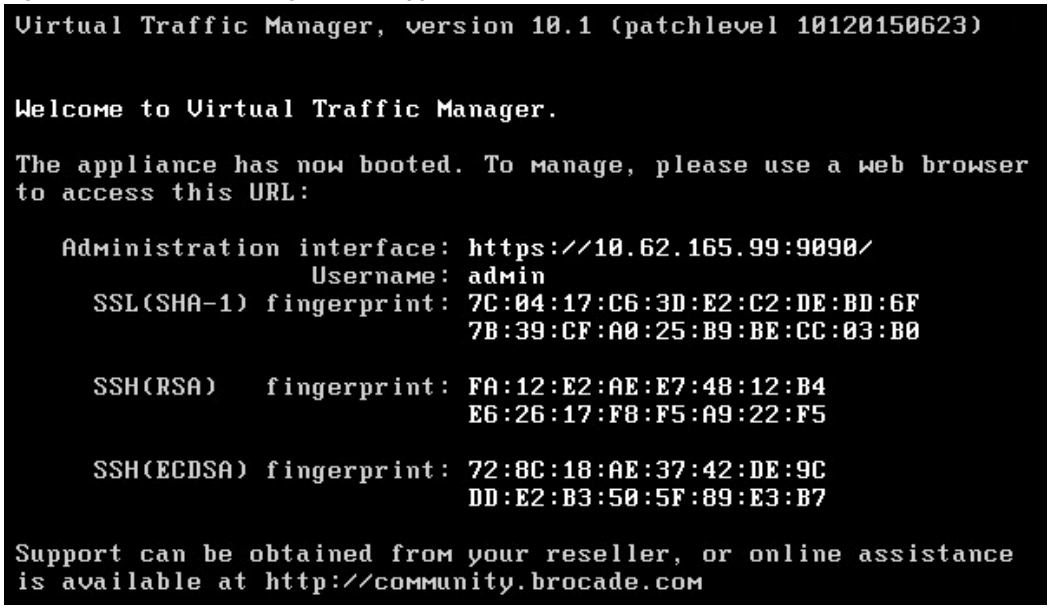
15. Click **OK** to save your virtual machine settings.

16. In the main vSphere Client window, click **Power on the virtual machine** to start the Traffic Manager.

Checking the Initial IP Address

When you first start the Traffic Manager virtual appliance, it attempts to obtain an IPv4 address using DHCP. If it receives no response to its DHCP requests, the virtual appliance configures itself with the static IP address 192.168.1.101 (on the 192.168.1.0/24 network). The configured IP address is displayed on the console.

Figure 3-3. The Traffic Manager virtual appliance console



If the virtual appliance could not obtain an address using DHCP and the default 192.168.1.101 IP address is not appropriate for your network, you can manually set the initial IP address.

To set the initial IP address

1. Access the Traffic Manager virtual appliance console interface.

2. Press Alt+F2 to switch to the alternative console display "tty2".

3. Log in as "admin" with the default password of "admin".

4. Run the following command:

```
z-set-initial-address
```

5. Enter an IP address and netmask at the prompt.

6. Once the command terminates, type **logout** to log out of the console.

7. Press ALT+F1 to switch back to "tty1".

Observe that the IP address in the URL for the Traffic Manager administration user interface (Admin UI) has changed to your new IP address.

Connecting to the Admin UI

To connect to the Traffic Manager administration user interface (Admin UI), enter the URL displayed on the appliance console into your web browser.

By default, this URL is "https://<appliance_IP>:9090/", where <appliance_IP> is one of the following addresses:

- The IP address obtained using DHCP
- The IP address specified with the **z-set-initial-address** command (if used)
- 192.168.1.101

Note: Before you can connect to the Admin UI, your web browser might report problems with the SSL certificate (either that it cannot trust it, or that the host name in the certificate does not match the host name in the URL). These problems can safely be ignored; the certificate is a self-signed certificate, and the host name in the certificate might not match the URL you have used to access it, particularly if you have used the appliance's IP address in the URL.

Expanding the Log File Partition

If you want to allocate more space for your log files, expand the virtual disk, and then resize the file system from the virtual appliance's command line.

Before you start, make sure you have completed the following steps:

1. Performed a backup of your Traffic Manager configuration and log files.

2. Stopped the virtual appliance using either the Admin UI or vSphere Client.

To resize the virtual hard disk

1. On the command line of the ESX Server, change to the directory containing the virtual disk file (.vmdk) for your virtual appliance.

2. Use the **vmkfstools** command to expand the disk:

```
vmkfstools -X 24G <Virtual Appliance Name>.vmdk
```

To expand the log partition

1. Start the virtual appliance using the vSphere Client.
2. Access the virtual appliance console, or connect using SSH.
3. Log in as the “admin” user.
4. Resize the /logs partition by using the following command:

```
z-expand-logs-partition
```

CHAPTER 4

Installing the Traffic Manager Virtual Appliance on QEMU/KVM

This chapter describes how to install the Traffic Manager virtual appliance on the QEMU Kernel Virtual Machine (QEMU/KVM) hypervisor.

This chapter contains the following sections:

- "QEMU/KVM System Requirements," next
- "Installing the Virtual Appliance" on page 24
- "Accessing the Virtual Appliance Console" on page 30
- "Checking the Initial IP Address" on page 31
- "Connecting to the Admin UI" on page 32
- "Expanding the Logs Partition" on page 32

QEMU/KVM System Requirements

The Traffic Manager virtual appliance is supported for production use on the QEMU/KVM hypervisor. The Traffic Manager is available on QEMU/KVM as a 64-bit version only.

For a full list of the supported platforms and versions, refer to the release notes included with your virtual appliance package.

Before you continue, make sure you have satisfied all of the necessary prerequisites shown in Chapter 2, "Prerequisites and Planning."

To run the installation process, use either the Virtual Machine Manager (VMM) Graphical User Interface (GUI) tool or the command line interface (CLI) provided by the libvirt software library. The VMM GUI is provided by the virt-manager software package and the CLI is provided by the virt-install software package.

First obtain the appropriate Traffic Manager virtual appliance package in ZIP archive format. Unpack the archive file to your QEMU/KVM host prior to setting up the virtual machine.

Installing the Virtual Appliance

The installation procedure consists of two separate steps. The virtual appliance disk file must first be added to an appropriate storage pool. You can then install the virtual appliance software through the CLI or VMM GUI, based on the disk file from the storage pool.

In a standard implementation, libvirt manages designated directories, known as storage pools, to store virtual machine disk volume files. Other complex setup scenarios are possible, but are not discussed here. Your system administrator determines which storage pool to use, with the default being /var/lib/libvirt/images.

To add the disk file to an appropriate storage pool:

1. Copy the virtual appliance ZIP archive file to the host machine.
2. Log in to the host machine and uncompress the archive file to the local disk. The uncompressed contents include the following files:
   - **VirtualTrafficManager.qcow2**: The virtual machine disk file
   - **RELEASE_NOTES.txt**: a text file containing the release notes.
3. Copy VirtualTrafficManager.qcow2 to the storage pool directory.
4. Rename VirtualTrafficManager.qcow2 to your virtual machine name (for example, "MyTrafficManager-01.qcow2"). Because each .qcow2 file corresponds to a specific virtual appliance, this step ensures that your disk image files remain unique within the storage pool.
5. Use the following command to ensure the .qcow2 file appears correctly inside a storage pool:

```
virsh <connectionURI> pool-refresh --pool <poolname>
```

To install the virtual appliance software using virt-install in the CLI:

1. Use the **virt-install** command to install the virtual appliance:

```
virt-install --import --cpu=host --vcpus=2 --ram=3072
             --connect <connectionURL>
             --disk <full path to disk file>,format=qcow2,bus=virtio
             --name=<Virtual Appliance name> --os-type=linux
             --os-variant=ubuntuprecise --network bridge=br0,model=virtio
             --graphics=vnc
```

In the **virt-install** command, `br0` is the name of the network bridge interface on the host (if one is used). Interface names in your network infrastructure might vary.

The CPU count (`vcpus=2`) and RAM allocation (`ram=3072`) shown are example values. To ensure Data Plane Acceleration mode is available in your new virtual appliance, set your CPU count and RAM allocation equal to values that correspond to the recommendations in Chapter 2, “Prerequisites and Planning.”

Caution: If the installation process fails with the error: "ERROR OS variant 'ubuntuprecise' does not exist in our dictionary for OS type 'linux'", Brocade recommends changing the OS variant part of the command to an alternative supported Linux variant.

To install the virtual appliance software using the VMM GUI:

1. Start the VMM tool from a client machine, and connect to the host QEMU / KVM machine by using the following command:

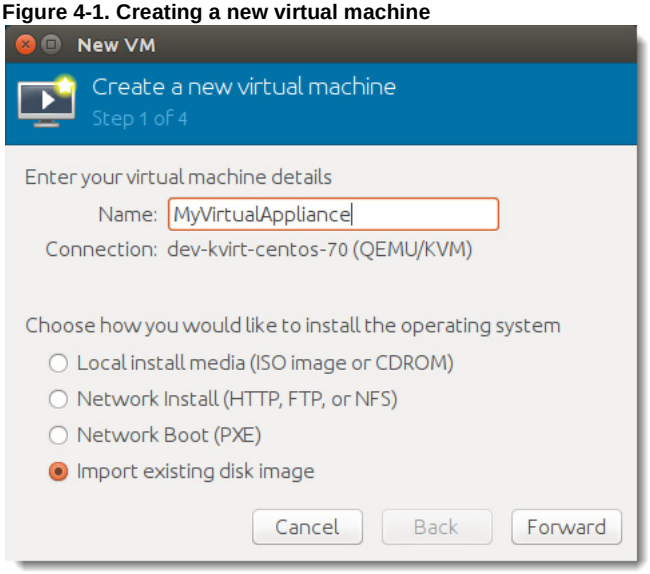
```
virt-manager --connect=qemu+ssh://my-kvm-host.com/system
```

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

   For information on alternative connection methods, refer to the virt-manager documentation.

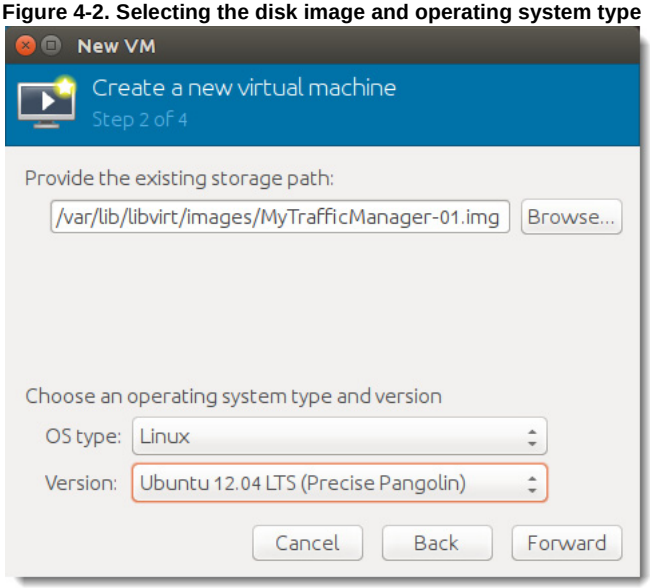
2. Click **New** to start the process of creating a new virtual machine.

Figure 4-1. Creating a new virtual machine



3. Enter a name for your virtual appliance that corresponds with the name used for the virtual machine disk file. From the list of options, click **Import existing image** and then click **Forward** to proceed.

Figure 4-2. Selecting the disk image and operating system type

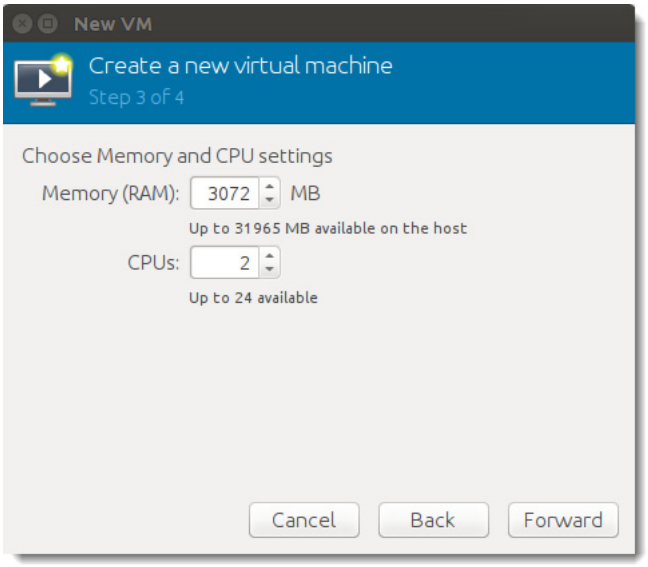


4. Click **Browse** to select the storage pool location and disk file for this virtual machine.

5. In the OS type list, select "Linux", and in the Version list, select a supported Linux variant. Click **Forward** to proceed.

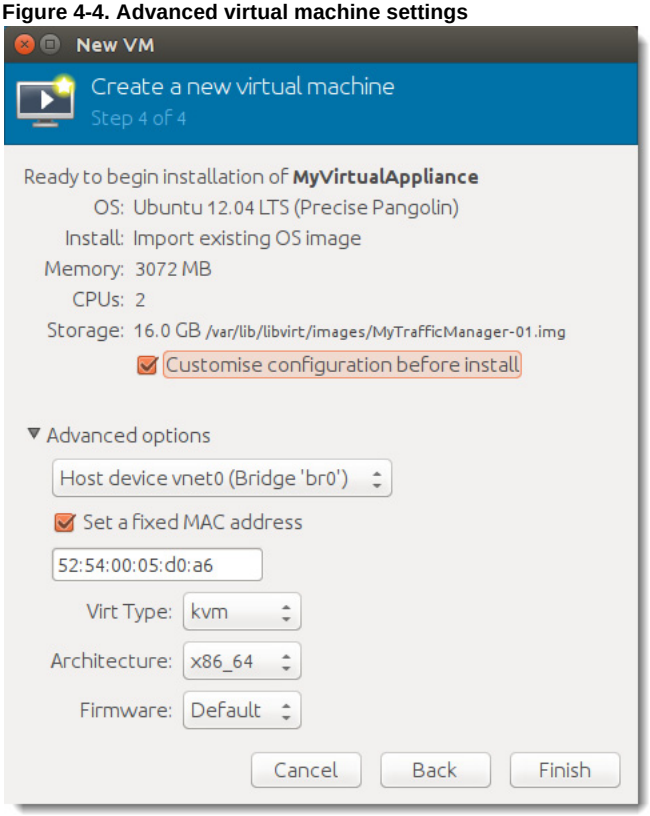
6. Enter the RAM and CPU resource settings required for your virtual machine. For recommended settings, refer to Chapter 2, "Prerequisites and Planning" or the release notes provided with your virtual appliance package. Click **Forward** to proceed.

Figure 4-3. Choosing memory and CPU settings



7. Under **Advanced options**, choose any further settings that you want to apply. Brocade recommends that you select bridged networking using the list provided.

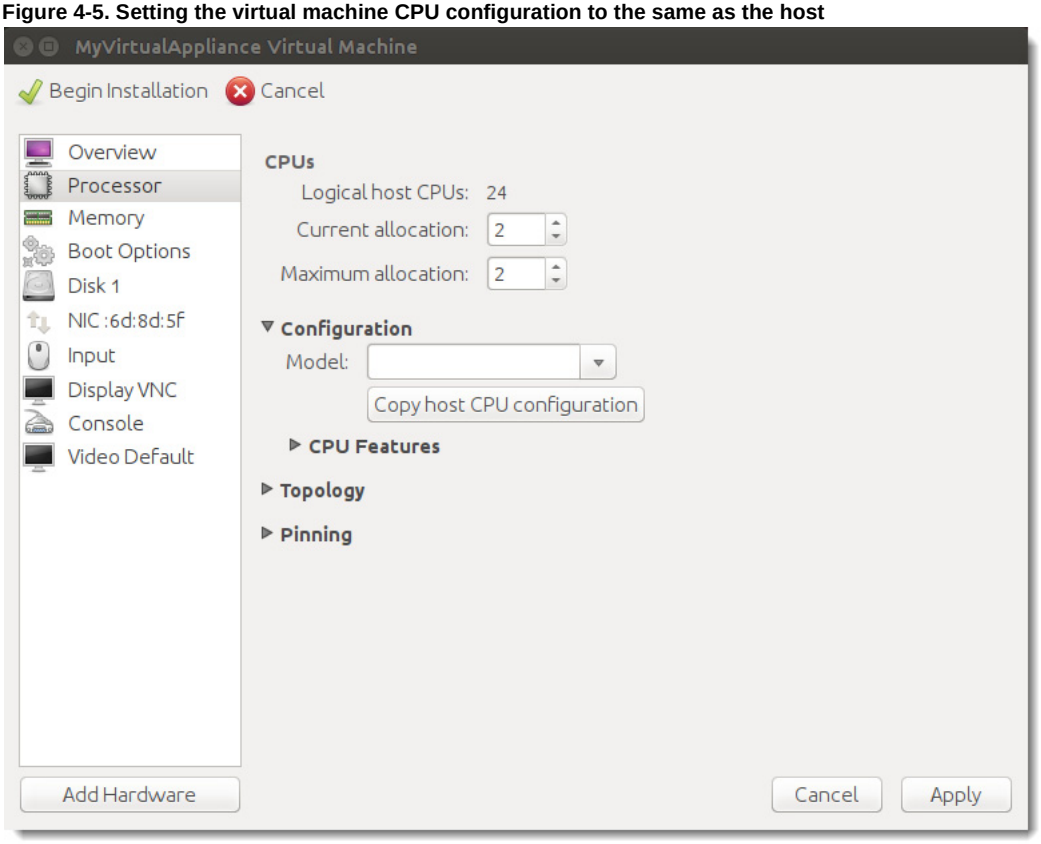
Figure 4-4. Advanced virtual machine settings



8. Click **Customise configuration before install**, and then click **Finish**. Before your Traffic Manager virtual machine is installed, VMM displays the hardware configuration page.

9. Click **Processor** in the category list, then click **Configuration** to display the CPU model selection control, and finally click **Copy host CPU configuration** to set the CPU model to match the host hardware.

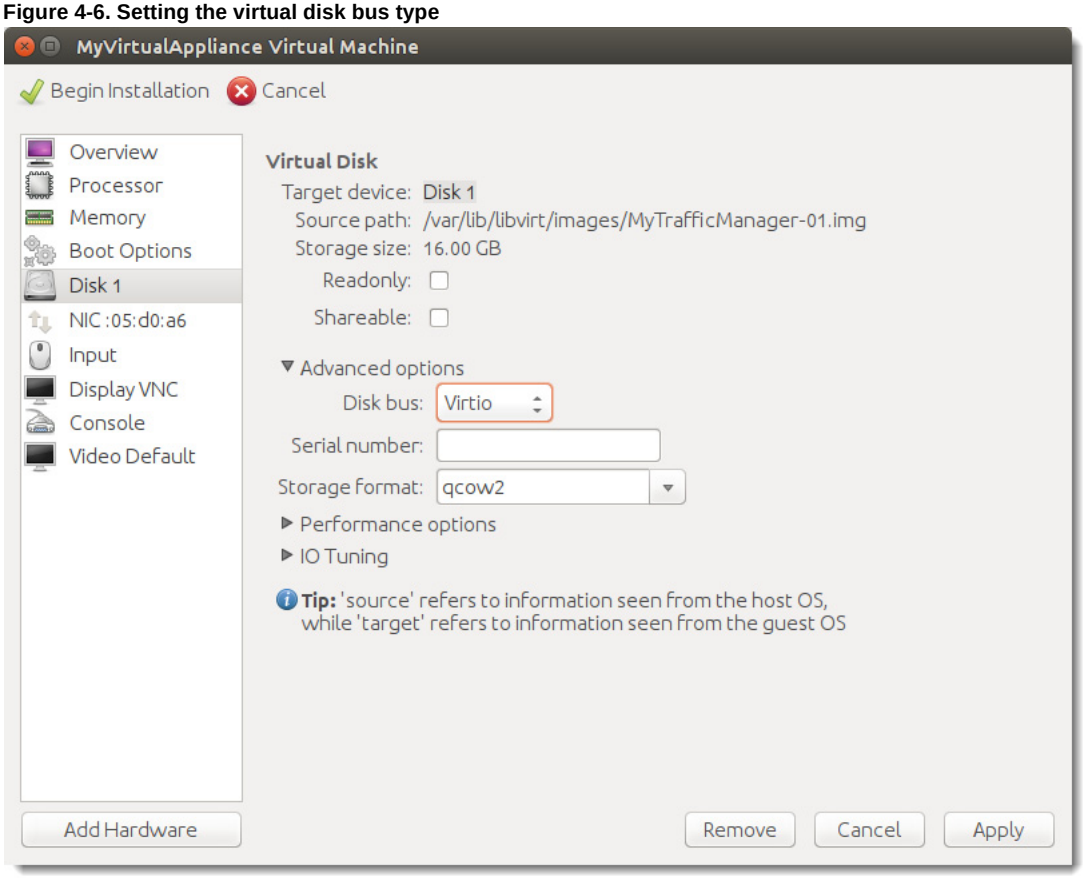
Figure 4-5. Setting the virtual machine CPU configuration to the same as the host



10. Click **Apply** to save your configuration.

11. Click **Disk 1** in the category list and then click the arrow next to **Advanced options**. In the **Disk bus** list, select "Virtio".

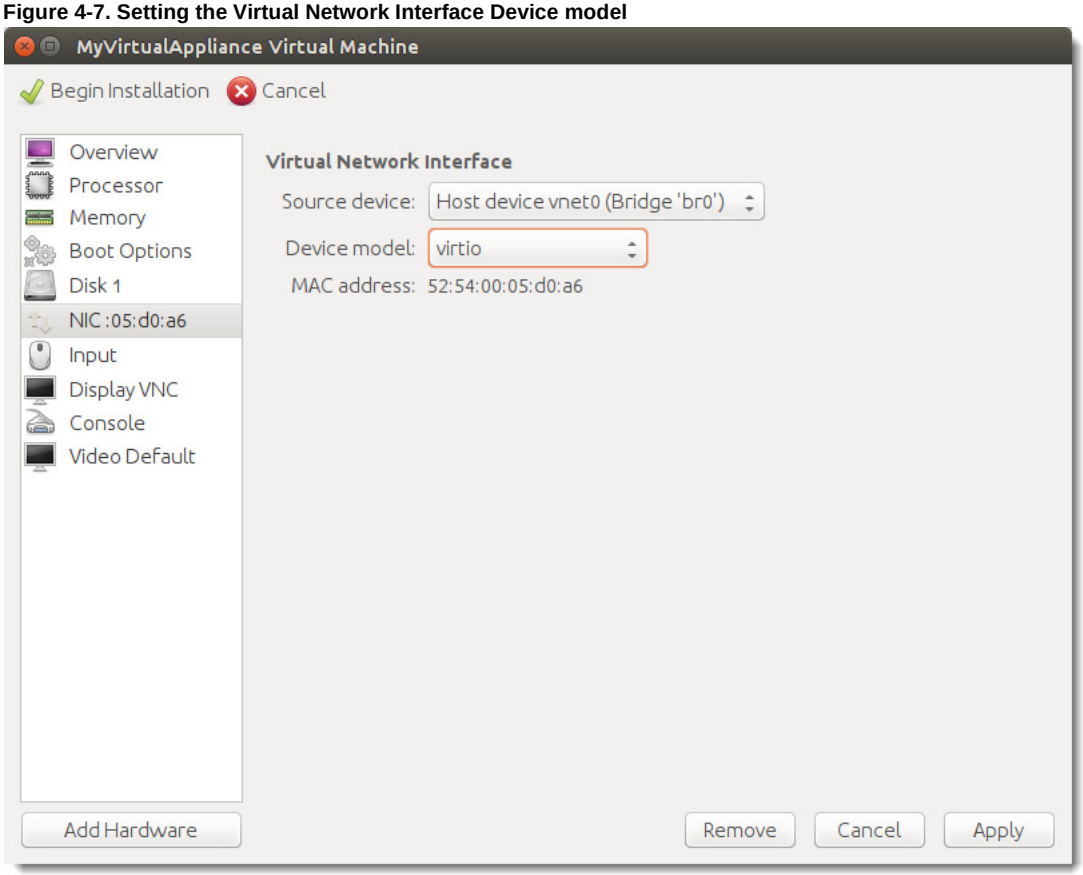
Figure 4-6. Setting the virtual disk bus type



12. Click **Apply** to save your changes.

13. Click **NIC** in the category list and then select a compatible model from the **Device model** list. To view a list of network interface device models compatible with Data Plane Acceleration mode, refer to Chapter 2, "Prerequisites and Planning."

Figure 4-7. Setting the Virtual Network Interface Device model



14. Click **Apply** to save your configuration and then click **Begin Installation** to complete the installation process.

Accessing the Virtual Appliance Console

To connect to your virtual appliance console, use the virt-manager or virt-viewer GUI tools.

You can also connect to the serial console of your virtual appliance using the "virsh" command. SSH to your QEMU/KVM host server and type the following command at the prompt:

```
virsh console <va_name>
```

Replace <va_name> in the above command with the name of your virtual appliance.

These tools are not available on all client platforms. If this is the case, you can enable access to the console for a VNC-compatible client program. Use SSH to connect to your QEMU/KVM host server, and enter the following commands:

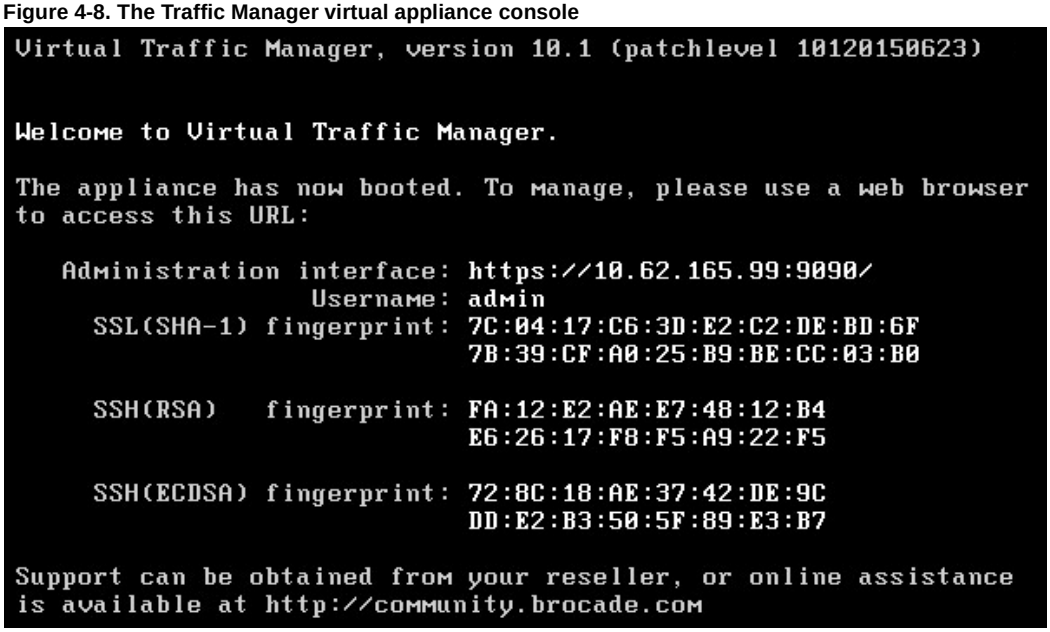
```
virsh vncdisplay <your VM name>
:12
```

The command `:12` means that your virtual machine provides VNC access on this host using the port 5912 (5900 + 12). Connect your VNC client to this host and port to access the console.

Checking the Initial IP Address

When you first start the Traffic Manager virtual appliance, it attempts to obtain an IPv4 address using DHCP. If it receives no response to its DHCP requests, the virtual appliance configures itself with the static IP address 192.168.1.101 (on the 192.168.1.0/24 network). The configured IP address is displayed on the console.

Figure 4-8. The Traffic Manager virtual appliance console



If the virtual appliance could not obtain an address using DHCP and the default 192.168.1.101 IP address is not appropriate for your network, you can manually set the initial IP address.

To set the initial IP address

1. Access the Traffic Manager virtual appliance console interface.
2. Press Alt+F2 to switch to the alternative console display "tty2".
3. Log in as "admin" with the default password of "admin".
4. Run the following command:

```
z-set-initial-address
```

5. Enter an IP address and netmask at the prompt.
6. Once the command terminates, type **logout** to log out of the console.
7. Press ALT+F1 to switch back to “tty1”.

Observe that the IP address in the URL for the Traffic Manager administration user interface (Admin UI) has changed to your new IP address.

Connecting to the Admin UI

To connect to the Traffic Manager administration user interface (Admin UI), enter the URL displayed on the appliance console into your web browser.

By default, this URL is "https://<appliance_IP>:9090/", where <appliance_IP> is one of the following addresses:

- The IP address obtained using DHCP
- The IP address specified with the **z-set-initial-address** command (if used)
- 192.168.1.101

Note: Before you can connect to the Admin UI, your web browser might report problems with the SSL certificate (either that it cannot trust it, or that the host name in the certificate does not match the host name in the URL). These problems can safely be ignored; the certificate is a self-signed certificate, and the host name in the certificate might not match the URL you have used to access it, particularly if you have used the appliance's IP address in the URL.

Expanding the Logs Partition

To increase the disk space for your virtual appliance log files, expand the virtual disk and then resize the file system from the virtual appliance's console interface.

Before you start, make sure you have completed the following steps:

1. Performed a backup of your Traffic Manager configuration and log files.
2. Stopped the virtual appliance.

To resize the virtual disk and expand the /logs partition

1. Log in to the QEMU/KVM host server command line.
2. Type the following command to expand the disk:

```
virsh vol-resize MyTrafficManager-01.qcow2 --pool <pool> --delta 4G
```

   This command expands the disk by 4 GB. To expand the disk by a different amount, use a different value for the `--delta` argument.

3. Start the virtual appliance.
4. Engage the virtual appliance's console interface, or connect using SSH.
5. To resize the /logs partition, enter the following command:

```
z-expand-logs-partition
```

CHAPTER 5

Installing the Traffic Manager Appliance Image

This chapter describes how to install the Traffic Manager appliance image on an approved server hardware platform.

It contains the following sections:

- "Before you Begin," next
- "Creating an Installation Disk or USB Flash Drive" on page 36
- "Installing the Traffic Manager From a Disk or USB Flash Drive" on page 37
- "Installing Through a PXE Boot Environment" on page 39
- "IPMI Management" on page 39

Before you Begin

Brocade provides a Traffic Manager appliance disk image conforming to the ISO standard format, with supporting files supplied in a pair of ZIP archives:

- `ZeusTM_<Version>_Appliance-x86_64.zip`: Contains files for creating boot-able CD-ROMs, DVD-ROMs, and USB flash drives.
- `ZeusTM_<Version>_Appliance-x86_64-PXE.zip`: Contains files for deploying the Traffic Manager through a configured PXE environment.

Note: Throughout this chapter, substitute the string `<Version>` in file names with the release number for the Traffic Manager you are installing. For example, `ZeusTM_17.2_Appliance-x86_64.zip`.

Before you continue, make sure you have satisfied all of the necessary prerequisites shown in Chapter 2, "Prerequisites and Planning."

Creating an Installation Disk or USB Flash Drive

This section describes the process of creating a boot-able Traffic Manager appliance installation CD-ROM, DVD-ROM, or USB flash drive.

To create a boot-able Traffic Manager CD-ROM or DVD-ROM

1. Unpack the Traffic Manager ZIP archive to your workstation.
2. Locate the Traffic Manager .iso disk image file (`ZeusTM_<Version>_Appliance-x86_64.iso`) from within the unpacked file set.
3. Insert a blank CD-ROM or DVD-ROM.
4. Use a suitable CD/DVD writing program to create a boot-able disk from the Traffic Manager .iso disk image file.

To create a boot-able Traffic Manager USB flash drive

1. Before you start, make sure your USB flash drive is compatible with the Traffic Manager appliance files. For preparation advice and instructions covering a variety of flash drive types, search the Brocade Community Web site at http://community.brocade.com.
2. Unpack the Traffic Manager ZIP archive to your Linux or UNIX workstation.
3. Plug your USB drive into the workstation.
4. Locate the USB drive device directory within your filesystem. To list all mounted filesystems and drives, use the `df` command in a console or terminal program. A device directory of "/dev/sdb" is typical.

Caution: Make sure you have identified the correct device directory. The following steps overwrite everything on this device, and your workstation might become unusable if you select the wrong one.

---

5. If your USB drive has auto-mounted, type `umount <device_directory>` to unmount it.
6. Navigate to the directory containing your unpacked Traffic Manager archive.
7. Type `zcat USB-boot.img.amd64.gz > <device_directory>` to perform a raw copy of the boot files to the USB drive.
8. Type `mount <device_directory> /mnt` to re-mount the USB drive using "/mnt" as the mount point.
9. Type `cp ZeusTM_<Version>_Appliance-x86_64.iso /mnt` to copy the Traffic Manager appliance .iso file onto the USB drive.
10. Do not continue until you are satisfied that the file copy process has completed. For example, if your USB drive has a flashing light to indicate when data is being written to it, wait until this indicates completion.
11. Type `umount <device_directory> to` unmount the USB drive.

12. Type `sync` to force completion of any pending disk writes.

13. Remove your USB drive.

Installing the Traffic Manager From a Disk or USB Flash Drive

Note: This section applies only to installation from a physical medium such as a CD-ROM, DVD-ROM, or USB flash drive. To install the Traffic Manager through a PXE boot environment, see instead "Installing Through a PXE Boot Environment" on page 39.

To install the Traffic Manager software on your appliance, insert the CD-ROM, DVD-ROM, or USB flash drive prepared earlier, and then power on the appliance.

Connect to the appliance console, and wait until the Traffic Manager installer screen appears:

Figure 5-1. The installer splash screen

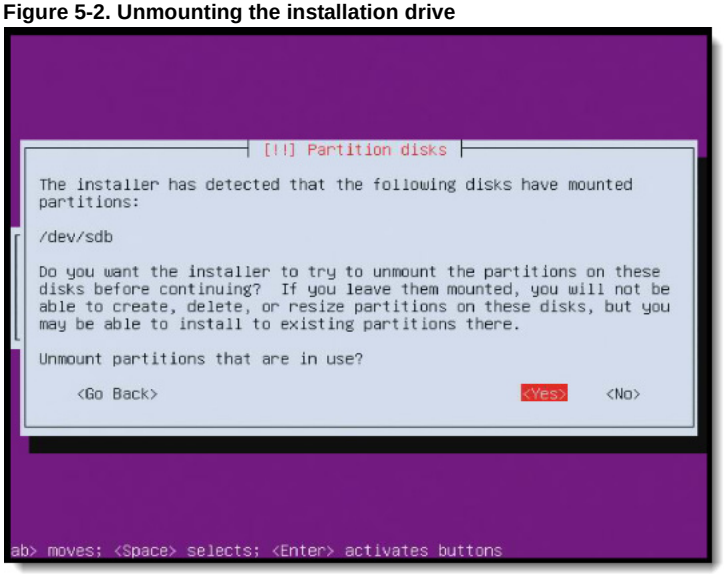
To continue installing the Traffic Manager, type "yes" at the prompt and press Return.

Caution: Be aware that this process completely wipes all data from the hard disk in your appliance.

The installer then proceeds to set up the Traffic Manager software on your appliance.

After a short period of time, the installer requests your confirmation to unmount the source drive before it can complete the installation process:

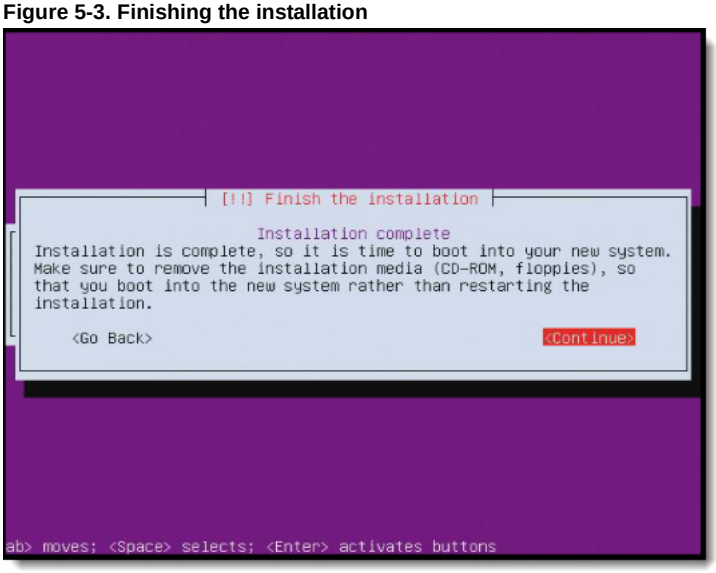
Figure 5-2. Unmounting the installation drive



Select **Yes** and press Return to unmount the installation drive from the system.

Make sure you remove the installation CD-ROM, DVD-ROM, or USB flash drive before continuing.

Figure 5-3. Finishing the installation



To complete the installation and shut down the appliance, select **Continue** and press Return. Your Traffic Manager is now ready for initial configuration.

Installing Through a PXE Boot Environment

Note: This section applies only to installation through PXE. To install the Traffic Manager from a physical medium such as CD-ROM, DVD-ROM, or USB flash drive, see instead "Installing the Traffic Manager From a Disk or USB Flash Drive" on page 37.

This section describes a typical process for setting up a PXE environment with the Traffic Manager installation files.

The minimum required Traffic Manager files for a PXE installation are the following:

- `vmlinuz`: The kernel file
- `initrd.gz`: Contains the Traffic Manager ISO image file
- `pxelinux.cfg`: A PXE configuration file

To configure a PXE environment with the Traffic Manager installation files

1. Ensure you have a properly configured PXE environment, with DHCP records pointing to a working TFTP server.
2. Copy `vmlinuz` and `initrd.gz` into `<TFTP_path>` on the TFTP server.
3. Copy `pxelinux.cfg` into the directory `<TFTP_path>/pxelinux.cfg/` on the TFTP server.
4. Identify the MAC address of the network interface on the appliance you want PXE to use for installing the Traffic Manager. This interface must be contactable from the TFTP server.
5. Using the format "01-<appliance_mac_address>", create a symbolic link in the directory `<TFTP_path>/pxelinux.cfg/` pointing to `<TFTP_path>/pxelinux.cfg/pxelinux.cfg`. For example, the link name might be "01-b6-39-b9-f6-91-2b".
6. Reboot your appliance and check its console output to make sure it is able to load `vmlinuz` and `initrd.gz` through PXE.
7. The appliance shuts down after the installer has finished.

Caution: To avoid PXE attempting to re-install the Traffic Manager appliance software after the initial installation, you must remove the symbolic link containing the identifying appliance MAC address. Failure to remove this link results in the installer being run multiple times.

IPMI Management

Your hardware appliance might contain an Intelligent Platform Management Interface (IPMI) card. IPMI is a remote monitoring and power management interface installed into the appliance that enables remote management, console access, and hardware monitoring functions separate to the Traffic Manager's own administration interfaces.

IPMI is vendor dependent and as such the layout, style, and access mechanism can vary. IPMI is typically accessed through a dedicated Ethernet port in the appliance which, once connected to your network, serves a Web enabled user interface. To gain access to this user interface, type the DHCP-provided IP address into your Web browser (typically over port 80). Use the default credentials provided by your appliance vendor to login to the IPMI user interface.

By default, IPMI is enabled. Use the Traffic Manager initial configuration wizard to disable access to the IPMI Web interface, or to set the IPMI credentials to match the Traffic Manager admin user.

CHAPTER 6

Configuring your Traffic Manager Instance

This chapter describes how to configure a new Traffic Manager instance for the first time, how to enable Data Plane Acceleration, and how to join this instance to an existing cluster of Traffic Managers. It assumes you have already performed the installation procedure described in the preceding chapter applicable to your chosen platform.

This chapter also documents further configuration tasks such as reconfiguring, upgrading, and downgrading.

This chapter contains the following sections:

- "Administration User Interface Authentication," next
- "Running the Initial Configuration Wizard" on page 42
- "Configuring the Traffic Manager From the Command Line" on page 50
- "Enabling Data Plane Acceleration" on page 55
- "Creating a New Traffic Manager Cluster" on page 55
- "Upgrading and Downgrading" on page 58

Administration User Interface Authentication

Access to the administration user interface (also known as the Admin UI) is authenticated with a dedicated SSL certificate. The SHA-1 fingerprint of the SSL certificate is displayed on the instance console. The SHA-1 fingerprint is useful for the following purposes:

- To verify the SSL certificate when connecting with a web browser for the first time.
- To verify the authenticity of Traffic Manager identities when joining a cluster.

Note: When you set up a new Traffic Manager, Brocade recommends noting the SHA-1 fingerprint. You can also display the fingerprint from the host command line using the following command:

```
$ZEUSHOME/admin/bin/cert -f fingerprint -in $ZEUSHOME/admin/etc/admin.public
```

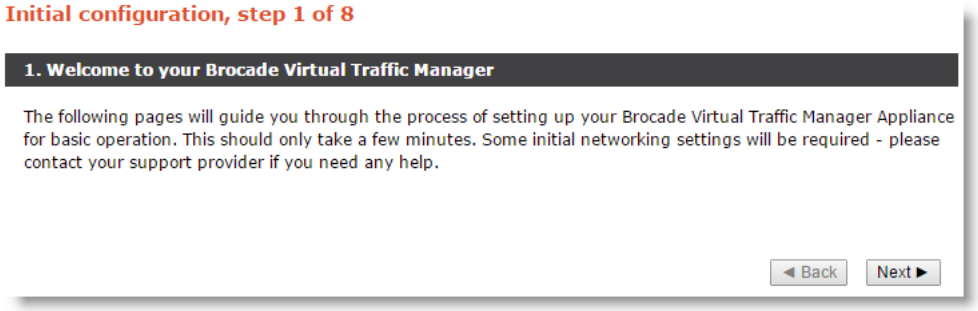
Running the Initial Configuration Wizard

Before you begin, make sure you have met all the requirements listed in Chapter 2, "Prerequisites and Planning."

A newly installed Traffic Manager instance requires some basic information in order to function. The Traffic Manager gathers this information over a series of steps that form the Initial Configuration wizard. To access the wizard, use your web browser. The wizard URL is displayed on the instance console.

Type the URL into your browser to view the first step of the wizard.

Figure 6-1. Accessing the initial configuration wizard

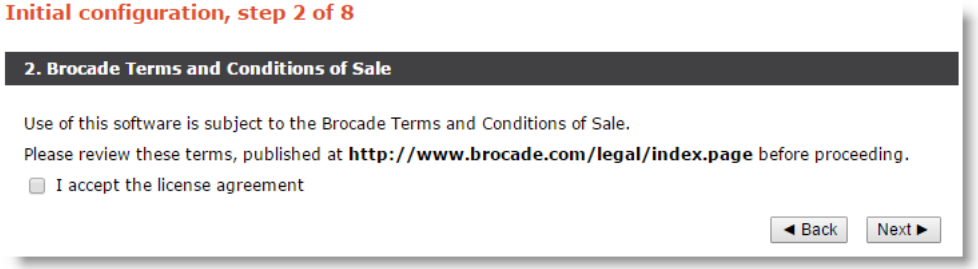


Click **Next** to begin the initial configuration of your Traffic Manager instance.

Accepting the Terms and Conditions of Sale

Read and accept the Brocade Terms and Conditions of Sale, available from the URL shown.

Figure 6-2. Accepting the terms and conditions of sale



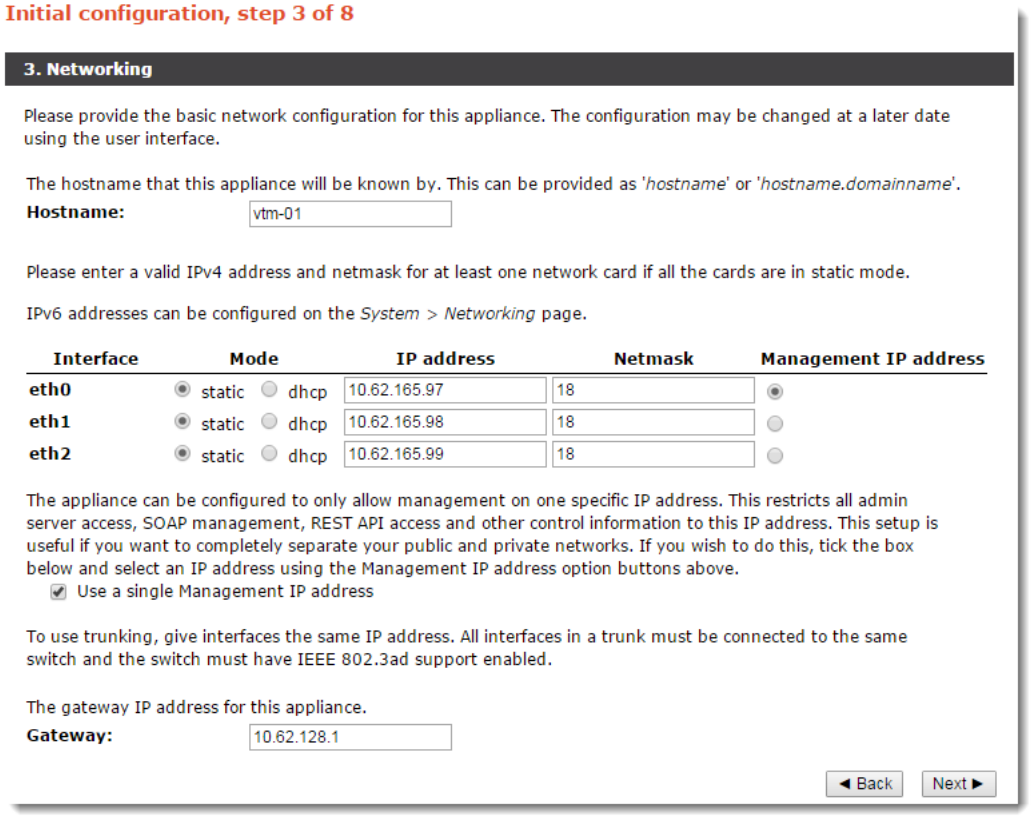
Read the agreement fully. If you agree to its terms, click **I accept the license agreement** and then click **Next** to continue. If you do not accept the license agreement, you cannot proceed with the wizard or use the software.

Configuring Networking

Use the Networking page to set your Traffic Manager basic network configuration. These settings replace the temporary addresses obtained by DHCP at installation.

A summary of the network settings to be applied to your Traffic Manager is given at the end of the wizard.

Figure 6-3. Key networking settings when configuring the Traffic Manager



Configure the following settings:

Setting	Description
Hostname	The host name of the instance, in either the simple form or fully qualified form (for example, "vtm1" or "vtm1.mgmt.site.com"). If you intend to create a cluster of Traffic Managers and you are using DNS servers for name resolution, it is important that the name you choose is resolvable from your name servers. Name resolution issues are handled later in the wizard.
Mode	The mode of the network interface. Choose one of the following options: • **static**: manually configure the IP address and netmask for the interface. • **dhcp**: use DHCP to automatically obtain network settings for the interface. **Note:** The use of DHCP in your networking configuration is not supported in Data Plane Accleration (DPA) mode. If you intend to use DPA mode, configure your network settings with static values only.
IP address	The IP address in dotted quad notation (for example, 192.168.1.101) for each interface.
Netmask	The netmask for the associated IP address (for example, 255.255.0.0) for each interface.

Setting	Description
Use a single Management IP	Click to restrict management traffic to a single interface. Then click the **Management IP Address** radio button next to the interface you want to use. Management traffic includes access to the Traffic Manager Admin UI, external API access, and internal communications within a Traffic Manager cluster. The management IP address normally resides on a private or dedicated management network. **Note:** If you are cloning a VMware-based instance using Guest OS Customization, the Management IP Address feature is disabled on the cloned instances to ensure they remain accessible. For further information, refer to "Cloning and Guest OS Customization" on page 16. **Caution:** Brocade recommends only using a management IP address if you have a dedicated, reliable management network. Each management address is a single point of failure for an entire Traffic Manager cluster. All of your management addresses must always be available. To later modify the management IP address, use the System > Traffic Managers page of the Admin UI. Note that a software restart is required if you change the management IP address.
Gateway	The IP address of the default gateway. This IP address is also used for network connectivity tests by your Traffic Manager, and the gateway machine should respond to "ping" requests for this purpose. If it does not, you must configure your Traffic Manager with an additional machine to ping instead. To set a different address to ping, use the Admin UI after your Traffic Manager has been configured.

To modify the network settings of a fully configured Traffic Manager, use the System > Networking page in the Admin UI. For further details, see the "Configuring System Level Settings" chapter of the *Brocade Virtual Traffic Manager: User's Guide*.

Caution: Configuring IP addresses on unplugged interfaces is not recommended. Routing problems might occur if the IP address is located on the same subnet as an IP address on a connected interface. If the IP address is on the same subnet as the management port, your Traffic Manager might become unreachable.

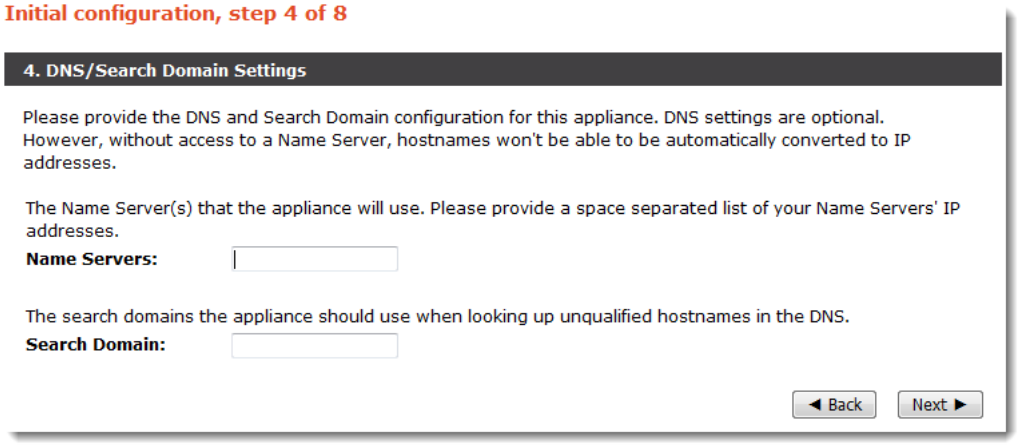
For optimum performance, Brocade recommends that you use separate interfaces for front- and back-end traffic. In other words, use separate interfaces for traffic between remote clients and the Traffic Manager, and for traffic between the Traffic Manager and the servers that it is load balancing.

You might find the "Network Layouts" chapter of the *Brocade Virtual Traffic Manager: User's Guide* helpful in planning your network. Additionally, the Brocade Community website (http://community.brocade.com) contains several articles about configuring your Traffic Manager.

DNS Settings

Use the DNS/Search Domain Settings page to configure the IP addresses of the name servers to use for DNS resolution and the DNS search domains. In each case, enter a single value or space-separated list of values. These settings are optional, but if you configure one or more name servers, you can use your servers' host names rather than IP addresses, which can make subsequent configuration tasks easier.

Figure 6-4. Entering Name Servers and the default Search Domains

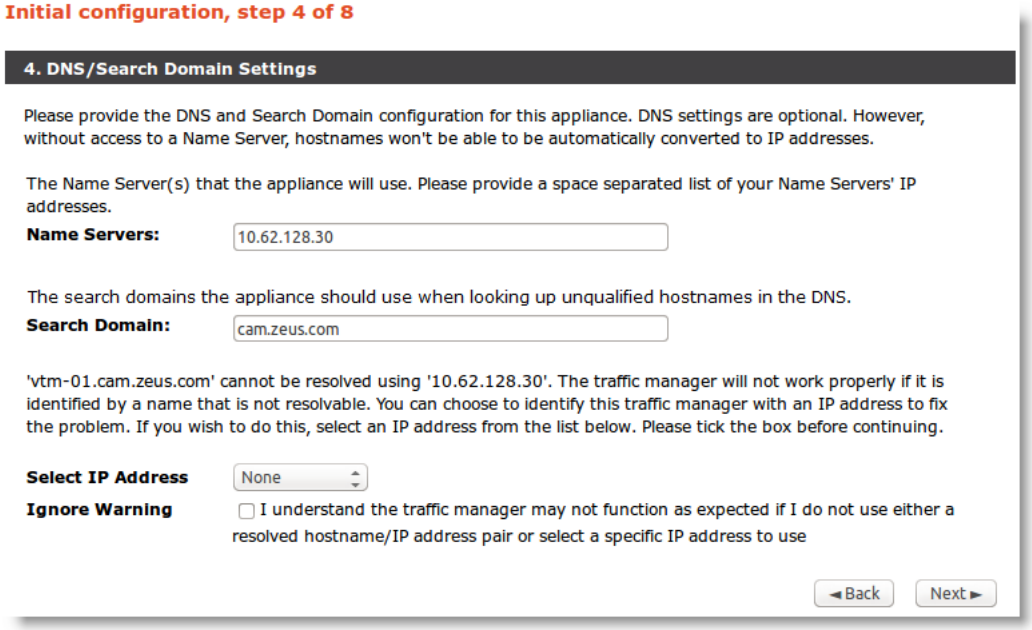


The Traffic Manager works correctly without access to external name servers. However, you then must use IP addresses instead of host names when setting up pools of servers, or manually enter the host name to IP mappings, which can be done from the Admin UI (in the "DNS" section of the System > Networking page) once you have completed the Initial Configuration wizard.

Host Name Resolution

The Traffic Manager attempts to resolve your chosen host name to an IP address using the name servers specified. Where the host name cannot be resolved, the wizard suggests using one of the IP addresses assigned to your network interfaces instead to identify this Traffic Manager to other cluster members.

Figure 6-5. Configuring the resolvable name



Select the desired IP address from the list, or select "None" to force the wizard to set the Traffic Manager name to be the unresolvable host name. You might experience connectivity issues until the host name successfully resolves to an IP address within your DNS. Read and confirm your acknowledgment of the **Ignore Warning** message by clicking the check box provided.

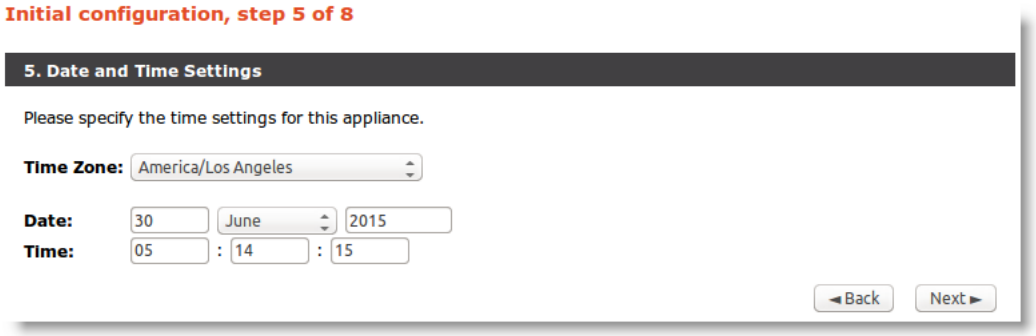
To change the identifying IP address after the wizard has completed, use the “Replace Traffic Manager Name” section on the **System > Traffic Managers** page of the Admin UI.

Note: If you are cloning a VMware based instance using Guest OS Customization, the IP address selection feature is disabled on the cloned instances. For further information, refer to “Cloning and Guest OS Customization” on page 16.

Time Zone Settings

Use the Date and Time Settings page to set the time zone for the Traffic Manager. Setting the time zone ensures that any logs and diagnostic messages generated by the Traffic Manager have the correct timestamps.

Figure 6-6. Configuring the date and time



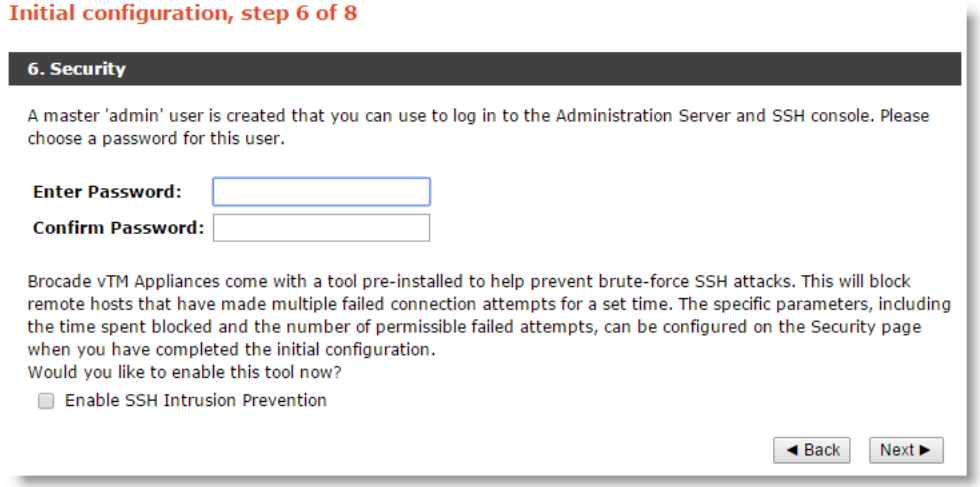
Note: Some Traffic Manager variants manage the date and time through the host environment. In these circumstances, the Date and Time Settings page contains only the time zone setting.

After initial configuration is complete, you can configure some Traffic Manager variants to synchronize with a collection of Network Time Protocol (NTP) servers. For further details, refer to the *Brocade Virtual Traffic Manager: User's Guide*.

Admin Password

Use the Admin Password page to set the password for the admin user. This master password is used when configuring the Traffic Manager through a web browser. If you enable password authentication for SSH, you can also use the this password when you log in to an instance using SSH (with the username "admin").

Figure 6-7. Entering the Admin password



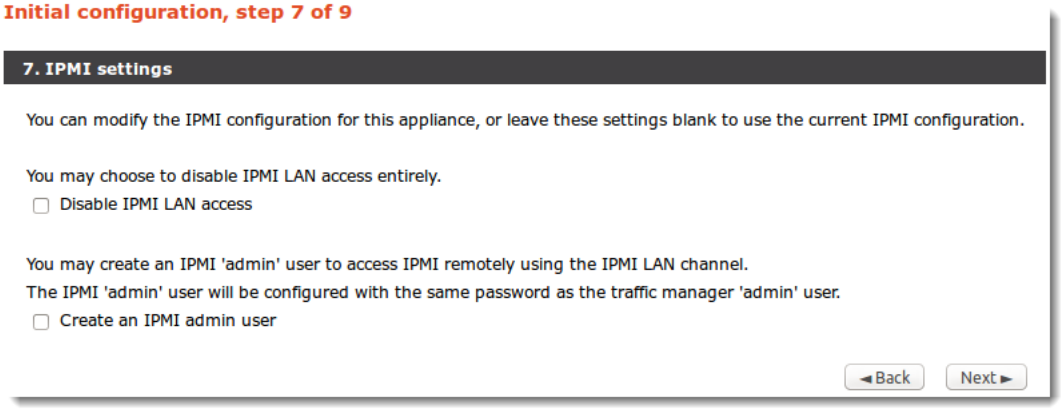
The Traffic Manager also contains the option to enable SSH Intrusion Detection to help prevent brute-force SSH attacks on your Traffic Manager. Brocade strongly recommends you enable this option.

IPMI Settings

Note: This step applies only to Traffic Manager hardware appliances.

Use this page to optionally configure the IPMI settings for this Traffic Manager appliance. Choose whether to disable LAN access to the IPMI module, or whether to set the IPMI user account to the Traffic Manager admin username and password defined in this wizard.

Figure 6-8. Configuring IPMI settings



Note that if you disable IPMI LAN access, you cannot then set the IPMI user.

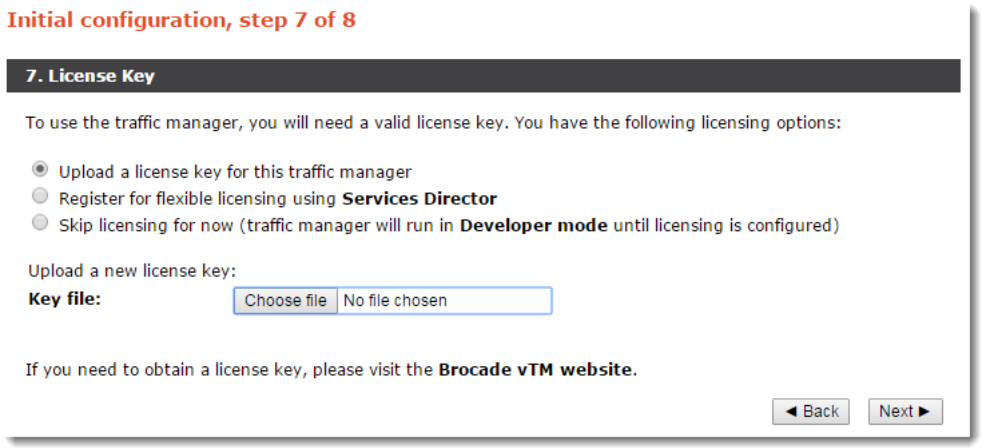
License Key

The Traffic Manager requires a license key to operate in full production mode. The feature set and bandwidth limits are determined by the license applied, the details of which can be viewed on the **System > Licenses** page of the Admin UI after the Initial Configuration wizard has completed.

Choose either to upload the license key now, or to upload it later once you have completed the wizard.

Where no key is provided, the system operates in a default state known as Developer mode. Developer mode is suitable for evaluation and development purposes only and should not be used in a production environment. The maximum available bandwidth is limited to 1Mbps, and SSL transactions are limited to 100 TPS.

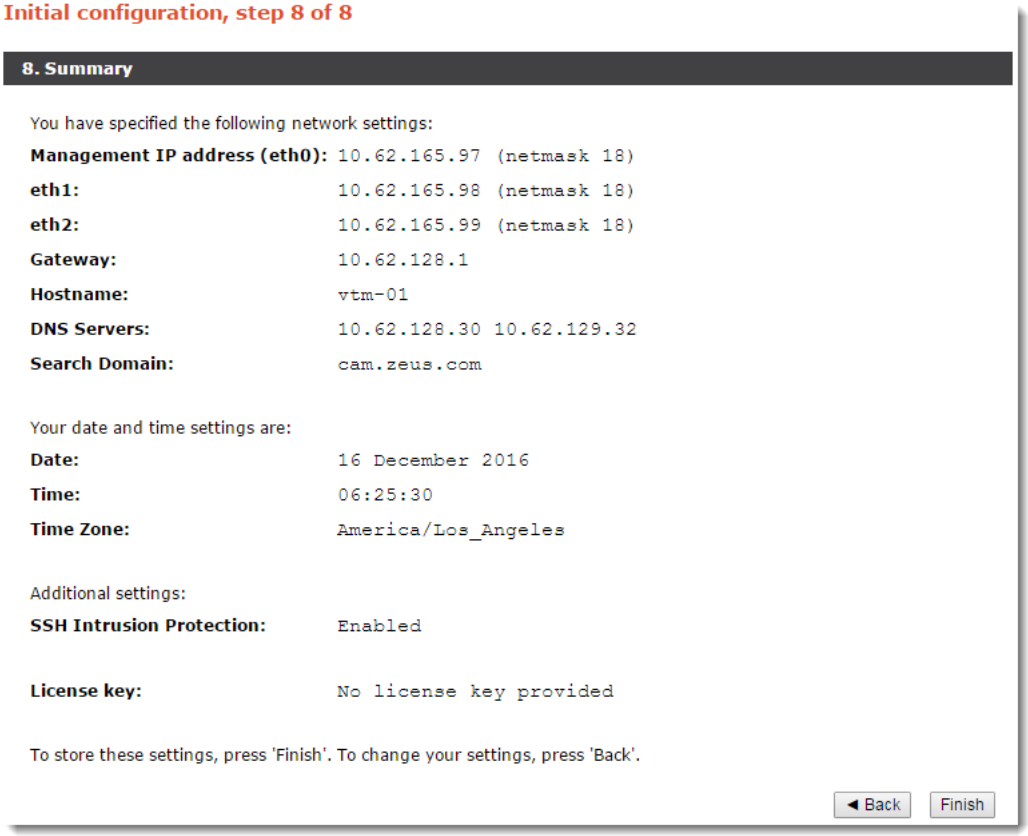
Figure 6-9. Uploading a license key file to the Traffic Manager



Summary

Before your settings are applied to the Traffic Manager instance, the Initial Configuration wizard displays a summary of the settings you have configured.

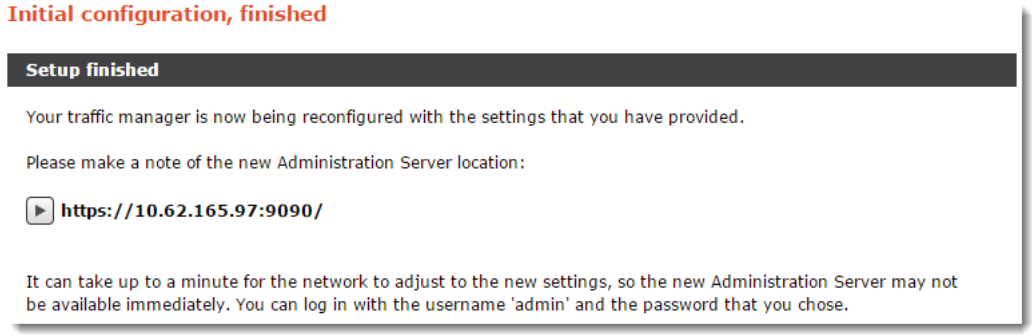
Figure 6-10. Configuration summary



Review these settings, and in particular the specified network settings, because your Traffic Manager might become uncontactable if any of the settings are incorrect. Use the **Back** button to go back through the wizard to make any changes.

To apply your settings, click **Finish**.

Figure 6-11. Configuration is complete



The Traffic Manager presents the Setup Finished page with a link to the new URL of the Admin UI. Brocade recommends waiting a short period (typically 10 to 30 seconds) before clicking the link to allow the Traffic Manager time to reconfigure its network interfaces. You might also need to reconfigure your computer's network settings to be able to send packets to the IP address of the Traffic Manager management interface.

Click the link to view the login page of the Admin UI. Log in using the username "admin" and the password you configured in the wizard.

Configuring the Traffic Manager From the Command Line

The Traffic Manager supports performing initial configuration through the command line, as an alternative to using the Web-based Initial Configuration Wizard.

To use the Initial Configuration Wizard, see "Running the Initial Configuration Wizard" on page 42.

To start the configuration program, login to the appliance console and type the following command at the prompt:

```
z-initial-config
```

Follow the on-screen instructions to proceed.

```
Brocade Virtual Traffic Manager Installation Program
Copyright (C) 2017, Brocade Communications. All rights reserved.


Welcome to your Brocade Virtual Traffic Manager Appliance

This application will guide you through the process of setting up
your Brocade Virtual Traffic Manager Appliance for basic operation.
This should only take a few minutes. Some initial networking settings
will be required - please contact your support provider if you need any help.

Press return to continue.
```

Press RETURN to start configuring the appliance.

```
------------------------------------------------------------------------
Use of this software is subject to the Brocade Terms and Conditions
```

```
of Sale.

Please review these terms, published at
http://www.brocade.com/legal/index.page before proceeding.
------------------------------------------------------------------------


Enter 'accept' to accept this license, or press return to abort:
```

Read and accept the Brocade Terms and Conditions of Sale, available from the URL indicated. If you agree to its terms, type “accept” at the prompt to continue. You cannot proceed with the configuration program, and thus use the software, if you do not accept the terms of the agreement.

```
Would you like to register this traffic manager with a Services Director,
for remote licensing purposes? If not, a license file can be specified.

Note that registering will enforce that the REST API is enabled.

Register with a Services Director? [Y/N] [N]:
```

To register this Traffic Manager to use remote licensing as part of a Brocade Services Director deployment, type “Y” and follow the instructions contained in your Services Director documentation.

Note: To use remote licensing, make sure you are using Brocade Services Director version 2.4 or later.

Type “N” to license this Traffic Manager directly.

```
Enter the license key file name, or leave blank for developer mode.
Enter 'help' for more information.

License key file:
```

The Traffic Manager requires a license key to operate in full production mode. The feature set and bandwidth limits are determined by the license applied, the details of which can be seen on the System > Licenses page of the Admin UI after you have finished configuring the appliance.

Choose either to install the license key now, or to upload it later from the Admin UI. If you choose to leave this entry blank, the system operates in a default state known as *Developer* mode. This mode is suitable for evaluation and development purposes only and should not be used in a production environment. The maximum available bandwidth is limited to 1Mb/sec, and SSL transactions are limited to 100 TPS.

```
Please provide the basic network configuration for this appliance.
The configuration may be changed at a later date
using the administration server.


Please provide the hostname that this appliance will be known by.
This can be provided as 'hostname' or 'hostname.domainname'.

Hostname:
```

Type the desired hostname for the appliance, in either the simple form or fully qualified form (for example, "vtm1" or "vtm1.mgmt.site.com"). If you intend to create a cluster of Traffic Manager appliances and you are using DNS servers for name resolution, it is important that the name you choose here is resolvable from your name servers. If you are unable to specify a resolvable hostname, type a suitable text name here and use the IP address identification option offered later in the configuration program.

```
To use trunking, give interfaces the same IP address.
All interfaces in a trunk must be connected to the same switch and
the switch must have IEEE 802.3ad support enabled.
```

```
Enter space separated list of interfaces you would like to configure.
Available options: eth0 eth1 eth2. At least one
network interface must be selected.

Interfaces:
```

Type the interface names you want to configure from the list given. For example, “eth0 eth1 eth2”.

```
Would you like to enable DHCP on eth0? Y/N [N]: n
Would you like to enable DHCP on eth1? Y/N [N]: n
Would you like to enable DHCP on eth2? Y/N [N]: n
```

For each interface, type “N” to specify an IP address and netmask manually. The use of DHCP in your networking configuration is not supported in Data Plane Acceleration (DPA) mode.

```
Enter eth0 IPv4 address or 'use_current' to use currently configured IP which is none.
IP:
```

For the interface shown, type the required IP address in dotted quad notation. For example, “192.168.1.101”.

```
Enter eth0 netmask:
```

Type the netmask for the associated IP address. For example, “16” or “255.255.0.0”.

Repeat the previous two steps for each interface you want to configure.

```
The gateway IP address for this appliance:
```

Type the IP address of the default gateway. This IP address is also used for network connectivity tests by your Traffic Manager, and the gateway machine should respond to "ping" requests for this purpose. If it does not, you must configure your Traffic Manager with an additional machine to ping instead. To set a different address to ping, use the Admin UI after your Traffic Manager has been configured.

```
Optional: choose management IP, or press return to skip.
Available options: 192.168.1.101
Enter 'help' for more information.

Management IP [none]:
```

Type the IP address of the interface you want to use as the management IP address, based on the list of IP addresses you configured earlier. Management traffic includes access to the Traffic Manager Admin UI, external API access, and internal communications within a Traffic Manager cluster. This address normally resides on a private or dedicated management network.

Caution: Brocade recommends only choosing to use a management address if you have a dedicated, reliable management network. Each management address is a single point of failure for an entire Traffic Manager cluster. All of your management addresses must always be available.

```
Please provide the DNS and Search Domain configuration for this appliance.
DNS settings are optional. However, without access to a Name Server, hostnames
won't be able to be automatically converted to IP addresses.


Optional: the Name Server(s) that the appliance will use.
Please provide a space separated list of your Name Servers' IP addresses or
'use_current' to use system settings.
Currently system is configured to use: '192.168.1.127 192.168.1.128'.

Nameservers:
```

Type the IP addresses of the external name servers the appliance should use for DNS resolution.

The Traffic Manager works correctly without access to external name servers, however you then have to use IP addresses instead of hostnames when setting up pools of servers. Alternatively, you can manually enter hostname-to-IP address mappings in the Admin UI (in the "DNS" section of the System > Networking page) after you have completed the configuration program.

```
Optional: the default domain name used when looking up unqualified
hostnames in the DNS. Please provide a space separated list of search domains.

Search domains:
```

Type the default search domains the appliance should use when looking up unqualified hostnames.

```
Optional: do you want to replace the traffic manager name with an IP address?
You might want to identify this traffic manager instance using its IP address
if its hostname is not resolvable.
Available options: 192.168.1.101.
Enter the value of nameip parameter, or press return to skip,

nameip [none]:
```

If your designated appliance hostname is not resolvable, you must use the IP address of a configured network interface as the appliance identifier. Type the desired IP address from list of available addresses, or type "None" (the default value) to force the wizard to set the Traffic Manager name to be the unresolvable hostname. Be aware that you might experience connectivity issues until the hostname successfully resolves to an IP address within your DNS.

To change the identifying IP address after you have completed the configuration program, use the “Replace Traffic Manager Name” section on the System > Traffic Managers page of the Admin UI.

```
Please specify the time zone of this appliance, or enter 'help'
for the list of available time zones.

Timezone:
```

Type the time zone you want this appliance to use, or type “help” to first display a list of available time zones.

```
A master 'admin' user is created that you can use to log in to the
Administration Server and SSH console.
Please choose a password for this user:
Re-enter:
```

Type (and confirm) a password for the Traffic Manager “admin” user. This is the master password that is used when configuring the appliance through a Web browser, or when you log in to the Traffic Manager command line using SSH (with the username "admin").

```
Do you want to enable SSH intrusion detection?
Enter 'help' for more information:

Enable SSH intrusion detection? Y/N [N]:
```

The Traffic Manager also contains the option to enable SSH Intrusion Detection to help prevent brute-force SSH attacks on your appliance. Brocade strongly recommends you enable this option.

```
Do you want to enable REST API access to the appliance?

Enable REST API? Y/N [N]:
```

The Traffic Manager provides an industry-standard REST API. Type "Y" to enable or "N" to disable the REST API. For further information, see the *Brocade Virtual Traffic Manager: REST API Guide*.

Note: The following settings for IPMI are applicable only to Traffic Manager hardware appliances.

```
Do you want to disable IPMI LAN access? Y/N [N]:
```

Your appliance hardware might come supplied with an Intelligent Platform Management Interface (IPMI) card. Type "Y" if you want to disable LAN access to the IPMI module for increased security.

```
You may create an IPMI admin user to access IPMI remotely
using IPMI LAN channel.

Do you want to create an IPMI admin user? Y/N [N]:
```

If you choose to retain IPMI LAN access, type "Y" here to set the IPMI administration user credentials to match the Traffic Manager admin user configured earlier.

```
You have specified the following settings:

No license file:              the traffic manager will run in developer mode
Hostname:                     vtm-01
eth0 IP address:              192.168.1.101
eth0 netmask:                 16
eth1 IP address:              192.168.1.102
eth1 netmask:                 16
eth2 IP address:              192.168.1.103
eth2 netmask:                 16
Gateway:                      192.168.1.1
Management IP:                192.168.1.101
Nameservers:                  192.168.1.30
DNS search domains :          cam.zeus.com
Traffic Manager Name IP:      (none)
Timezone:                     Europe/London
SSH protection enabled:       Yes
REST enabled:                 No

You may be logged out when the network configuration changes.

Proceed with configuration? Y/N:
```

Before you finish, check through the summary to confirm your intended settings. To configure your appliance with these settings, type "Y" at the prompt.

If your configuration is successful, the following message is displayed:

```
Initial configuration completed successfully.
```

Performing an Unattended Configuration

The Traffic Manager provides the ability to automate `z-initial-config` using a *replay file* containing pre-determined responses to the questions asked during the configuration process. To perform an unattended configuration, type the following command at the prompt:

```
z-initial-config --replay-from=<replay filename>
```

To create a suitable replay file, capture your responses using the following command:

```
z-initial-config --record-to=<replay filename>
```

Enabling Data Plane Acceleration

To enable (or disable) Data Plane Acceleration in your Traffic Manager system, click **Global Settings > Data Plane Acceleration** in the Admin UI. Set **data_plane_acceleration_mode** to "Yes" and click **Update**. You must reboot your Traffic Manager instance for the change to take effect.

For further information on this and other system-level settings, refer to "System Settings" on page 80.

Note: With Data Plane Acceleration mode enabled, but before you reboot the Traffic Manager, it is possible to create L4Accel services and make other related configuration changes. Be aware that such services are not enabled until after you reboot the system.

Creating a New Traffic Manager Cluster

To create a new cluster, first perform the initial configuration process for each Traffic Manager instance you want to use.

With Data Plane Acceleration mode enabled, you are limited to a maximum of two Traffic Manager instances in a single cluster. Both instances must be configured in the same mode before you start, with no pending reboots outstanding, and must adhere to the clustering considerations shown in "Additional Clustering Considerations" on page 13.

Caution: The Traffic Manager rejects any clustering attempt where the joining Traffic Manager does not fully meet all Data Plane Acceleration mode clustering requirements.

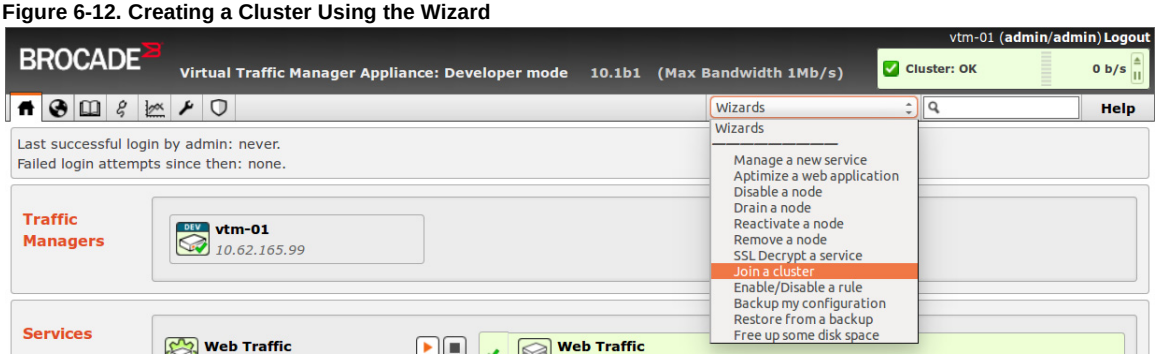
Finally, before making any further changes, join the instances together to form a cluster by using the "Join a cluster" wizard on the first Traffic Manager to join with the second Traffic Manager.

Note: In a Traffic Manager cluster, all instances are considered equal. You can access the Admin UI on any of the Traffic Managers to view the cluster configuration. Any configuration changes you make are automatically replicated across the cluster. All Traffic Managers function together to provide fault tolerance and simplified management.

To join a cluster

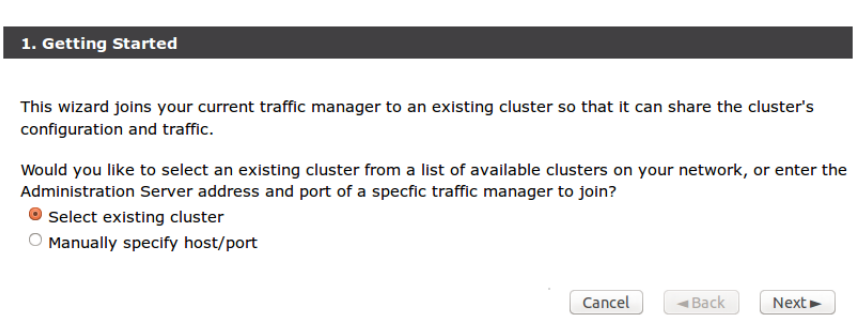
1. Log in to the Admin UI on one of your Traffic Managers and select **Join a cluster** from the **Wizards** list in the tool bar.

Figure 6-12. Creating a Cluster Using the Wizard



2. Choose whether to scan for existing clusters or specify the cluster details manually from the Getting Started page of the "Join a cluster" wizard.

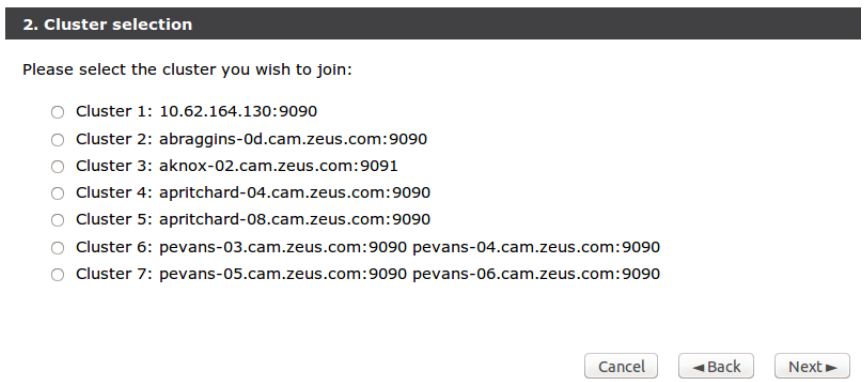
Figure 6-13. Getting Started with the cluster joining wizard



To instruct the Traffic Manager to automatically scan the network for contactable Traffic Managers, click **Select existing cluster**. Alternatively, to enter a specific host name and port you want to join, click **Manually specify host/port**. Click **Next** to continue.

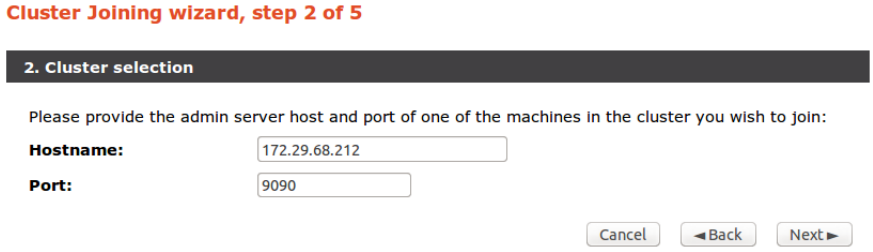
3. If you clicked **Select existing cluster**, the Traffic Manager presents a list of discovered Traffic Manager instances and clusters. Select the cluster you want to join and click **Next** to continue.

Figure 6-14. Select an existing Traffic Manager cluster to join



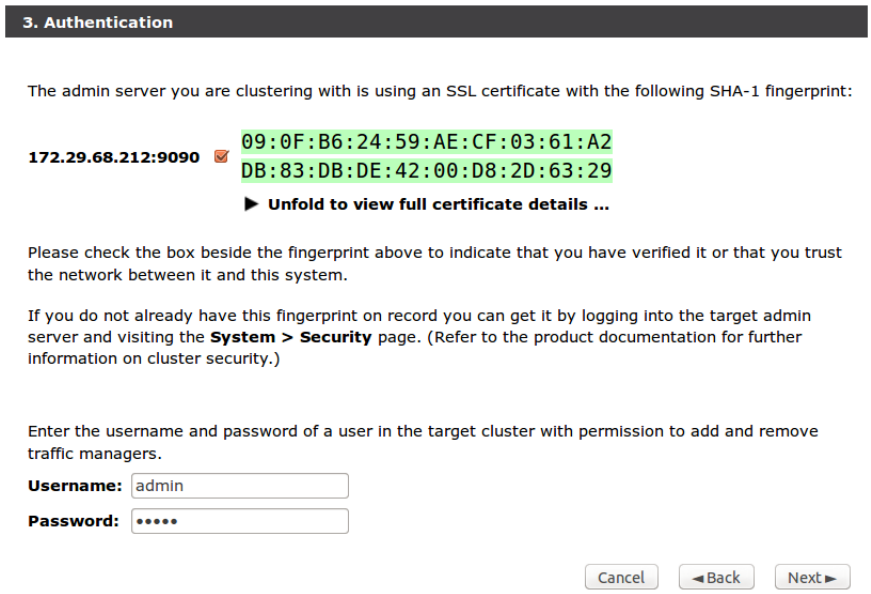
If you clicked **Manually specify host/port**, enter your host name and port number in the fields provided. Click **Next** to continue.

Figure 6-15. Specifying a host name and port



4. To connect to the specified instance, first verify the identity of the Traffic Manager instance and provide the administration credentials the Traffic Manager uses.

Figure 6-16. Authenticating the Cluster

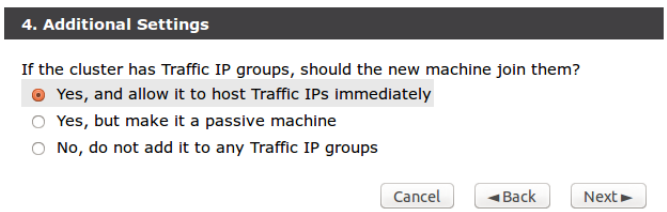


Check the displayed SHA-1 fingerprint against the fingerprint shown in the target Traffic Manager's Admin UI, in **System > Security**.

Click the check box next to the Traffic Manager host name to confirm you trust its identity, and then enter the cluster admin username and password. Click **Next** to continue.

5. If the cluster already has one or more Traffic IP groups configured, you can elect to add the new Traffic Manager to these Traffic IP groups so that it starts handling traffic immediately.

Figure 6-17. Assigning Traffic IP Group Membership



To add the Traffic Manager to existing Traffic IP groups, click **Yes, and allow it to host Traffic IPs immediately**. However, this can result in a number of connections being dropped at the instant the new Traffic Manager is added to the Traffic IP group, because allocations of traffic need to be transferred to the new Traffic Manager.

To avoid the potential for dropped connections, click **Yes, but make it a passive machine** to add the new Traffic Manager as a "passive" member of the Traffic IP group. This way, the Traffic Manager does not accept any traffic until another member of the group fails.

To leave the new Traffic Manager out of all existing Traffic IP groups, click **No, do not add it to any Traffic IP groups**.

Click **Next** to continue.

6. Check your settings on the Summary page and then click **Finish** to join the cluster.

   Provided the other Traffic Manager instance can be contacted, the Traffic Manager software reconfigures itself and presents a new home page showing both connected Traffic Manager instances in the Traffic Managers list.

Note: When you join a Traffic Manager to another Traffic Manager, the first Traffic Manager takes on the entire configuration that the second Traffic Manager is using, including the administration password you specified in the Initial Configuration wizard.

Clusters consisting of Traffic Managers on different platforms are possible, although you might find that product capabilities present on one of your Traffic Managers are not present on the other. For example, network and time settings are configurable only for certain Traffic Manager variants.

For instructions on upgrading an existing cluster to a later software version, refer to "Upgrading and Downgrading" on page 58.

Upgrading and Downgrading

To upgrade your Traffic Manager software version, use the instructions contained in this section. To downgrade your Traffic Manager software to a previously used version, see "Downgrading to an Earlier Version" on page 62.

Before You Start

Caution: If you are upgrading from version 9.1 and earlier, you must install a new instance of the Traffic Manager and import your configuration into it. This is due to the underlying operating system on earlier Traffic Manager versions missing packages required in version 9.9 and later. For more information on creating and importing configuration backups, refer to the *Brocade Virtual Traffic Manager: User's Guide*.

Caution: If you are upgrading from version 9.6 and earlier, your Traffic Manager instance has a root partition size of 1.9 GB. To obtain the larger root partition of 3.7 GB required for version 9.7 and later, Brocade recommends installing a new instance of the Traffic Manager and importing your configuration into it. For more information on creating and importing configuration backups, refer to the *Brocade Virtual Traffic Manager: User's Guide*.

Caution: 32-bit instances of the Traffic Manager (software, appliance, and cloud variants) are deprecated from version 9.6. To upgrade an earlier 32-bit instance to version 9.6 or later, you must install a new 64-bit instance and import your configuration into it. For more information on creating and importing configuration backups, refer to the *Brocade Virtual Traffic Manager: User's Guide*.

Before you start, make sure you have enough system resources to perform the upgrade:

- **Available memory:** A Traffic Manager instance running in Data Plane Acceleration mode requires a minimum of 3 GB of RAM to function normally. If your existing version of the Traffic Manager has fewer resources assigned to it, make sure you increase the RAM resource allocation before you start the upgrade. Additional RAM might be required depending on the CPU core allocation. For further information, refer to Chapter 2, "Prerequisites and Planning."
- **Free disk space:** For an incremental upgrade to succeed, a minimum of 700 MB must be free on the root (/) partition, and at least 600 MB must be free on the /logs partition. To confirm the available free disk space, use the **System > Traffic Managers** page of the Admin UI. A full upgrade installs the new version into a separate partition on the instance. After the new version has been installed, the upgrade process applies a copy of your configuration from the previous version. Space requirements are therefore different for incremental revision upgrades. You should only encounter problems if you have unusually large amounts of data in your configuration directories (specifically /root and $ZEUSHOME). For further guidance, contact Brocade Support.

Note: Brocade recommends you back up your configuration as a precaution before upgrading a Traffic Manager. Use the **System > Backup** page to create a snapshot of your current configuration that you can restore later if necessary.

For further information on upgrading and space requirements, refer to the Brocade Community website at http://community.brocade.com.

Caveats for VMware Users

Certain earlier versions of the Traffic Manager were built for VMware platforms that have since been updated or changed. Before upgrading to the latest version of the Traffic Manager, Brocade recommends you check your virtual machine settings for any of the following out-of-date configuration values:

Setting	Out-of-date Value	Correct Value
Virtual Hardware	"VM Version" set to 4	Set to VM Version 7 or later (depending on the ESX version you are running, you might be offered more than one virtual hardware version)
Guest OS	Other Linux	Ubuntu Linux 64
Network Adapter Type	VMXNET	VMXNET3

Note: If you have configured your Traffic Manager with additional network adapters, make sure you update the adapter type for each one.

You must correct all virtual machine settings before performing an upgrade.

To correct your VMware configuration

1. Shut down the Traffic Manager.
2. Edit the virtual machine settings.
3. Change your settings to the up-to-date values.
4. Save your settings, and restart the Traffic Manager.

Note: If your Traffic Manager has several network adapters defined with distinct configuration differences, such as with connections to different virtual networks, deleting and re-creating them might disrupt the expected interface assignment order within your virtual machine (eth0, eth1, and so on). You must confirm that the newly created adapters are connected to your virtual machine as per your original configuration.

Installing Incremental Software Revisions

Installing a software revision (for example, 11.0 to 11.0r1) involves replacement of the Traffic Manager software and a small number of operating system packages.

Any previously installed revisions of the current version, including the original unrevised version, are retained in case you need to cancel or revert the upgrade. For more details, refer to "Downgrading to an Earlier Version" on page 62.

To complete the upgrade, a restart of the Traffic Manager software is required, but a system reboot is not generally needed.

To install a software revision

1. Obtain the appropriate upgrade package. Packages are named according to the following convention:

```
ZeusTM_<version>_VMware-Appliance-Upgrade-x86_64.tgz
ZeusTM_<version>_kvm-Appliance-Upgrade-x86_64.tgz
ZeusTM_<version>_Appliance-Upgrade-x86_64.tgz
```

2. Log in to the Admin UI, and go to the **System > Upgrade** page.
3. Follow the instructions to upload and apply the upgrade package.

Upgrading a Cluster From One Revision to Another

The procedure for upgrading a cluster of several Traffic Managers is the same as upgrading a single Traffic Manager instance. Note that when the cluster is in a mixed state (cluster members are using different software versions), Brocade strongly advises against making any configuration changes.

To upgrade a cluster, upgrade each Traffic Manager in turn. All Traffic Managers in the cluster continue to run their configured services.

Installing Full Upgrades (Version Number Changes)

Full version upgrades (for example 10.4 to 11.0) involve installation of a new operating system image and a full system restart. To enable the installation of a new operating system image, the Traffic Manager maintains a secondary disk partition into which the new image is installed. The Traffic Manager then applies a copy of the configuration from the previous version to the new version, marks the partition as primary, and restarts the instance.

The previous partition is not deleted, but is marked as dormant. This dual-partition mechanism facilitates a rollback capability, should you need to revert to the previous version (refer to "Downgrading to an Earlier Version" on page 62).

Caution: Only one previous full version, with installed incremental revisions, can be maintained on the Traffic Manager in addition to the current version. If you have previously upgraded to a new full version, a subsequent full version upgrade overwrites the oldest version held. This operation is permanent; the overwritten version cannot be retrieved once the upgrade is applied.

If you are upgrading from a currently installed Traffic Manager version of 9.0 or later, you can perform the upgrade through the Admin UI or from the Traffic Manager console.

To upgrade using the Admin UI

1. Obtain the relevant Traffic Manager installation package for the platform you are using. Packages are named according to the following convention:

```
ZeusTM_<version>_VMware-Appliance-Upgrade-x86_64.tgz
ZeusTM_<version>_kvm-Appliance-Upgrade-x86_64.tgz
ZeusTM_<version>_Appliance-Upgrade-x86_64.tgz
```

2. Log in to the Admin UI, and go to the **System > Upgrade** page.

3. Follow the instructions to upload and apply the upgrade package.

To upgrade using the command line interface

Note: The command line interface method is mandatory where the currently installed Traffic Manager version is prior to 9.0

---

1. Obtain the relevant Traffic Manager installation package for the platform you are using. Packages are named according to the following convention:

```
ZeusTM_<version>_Appliance-x86_64-vmware.zpkg
ZeusTM_<version>_Appliance-x86_64-kvm.zpkg
ZeusTM_<version>_Appliance-x86_64.zpkg
```

2. Copy the upgrade package to the Traffic Manager, using the Linux scp command, or Windows-based pscp program (http://www.chiark.greenend.org.uk/~sgtatham/putty/) or WinSCP (http://winscp.net/eng/index.php).

Caution: Brocade recommends the installation package is copied to the /logs partition to avoid any disk space issues during the upgrade process.

---

3. Connect to the Traffic Manager command line using PuTTY or some other suitable terminal emulator.

4. Run the following command:

```
z-upgrade-appliance <package_filename>
```

5. Follow the instructions provided. The upgrade program copies your configuration data to the new version, but a reboot is required before you can start to use it.

Note: Subsequent configuration changes in the original version are not migrated to the new version.

---

6. Reboot the instance when convenient from the Admin UI or use the **reboot** command from the command line interface.

Upgrading a Cluster From One Full Version to Another

Follow the advice in "Upgrading a Cluster From One Revision to Another" on page 60 to upgrade each Traffic Manager instance in turn, taking care to not make any configuration changes during the cluster upgrade process.

Downgrading to an Earlier Version

The upgrade process preserves the previous full Traffic Manager software version, and any applied revisions, in a separate disk partition to facilitate a downgrade capability. To revert to an earlier revision of the current software version, or to any installed revision of the previous full software version, the Traffic Manager includes a *rollback* facility in the Admin UI and the instance console.

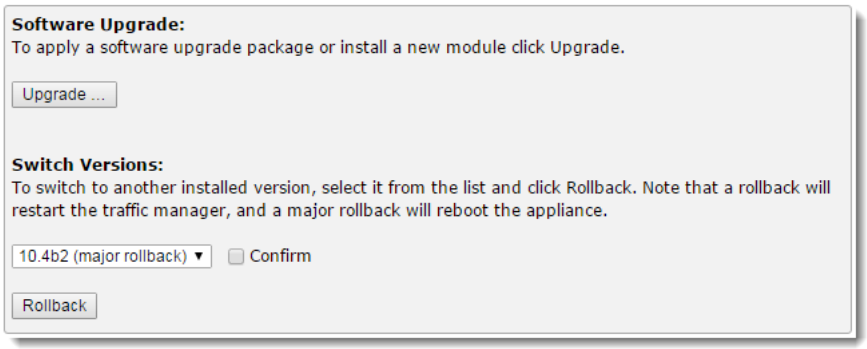
Note: Rollback can access all installed revisions of the current software version, but can only initially access the last used revision of the previous full version. If you want to revert to a different revision of the earlier software version, you must run rollback twice: first to switch to the alternate disk partition containing the earlier software, and then once more to access the other revisions of the software on that partition.

To revert the Traffic Manager to a previous version using the Admin UI

1. Login to the Admin UI of the Traffic Manager you want to revert.

2. Click **System > Traffic Managers** and locate the "Switch Versions" section:

Figure 6-18. Switching Traffic Manager versions



Note: The Switch Versions section is hidden if there are no applicable software revisions to revert to.

---

3. Select a software version to use from the drop-down list.

4. Tick **Confirm** and then click **Rollback** to start the roll back process.

Note: Traffic Manager versions earlier than 10.4 do not contain a switch feature in the Admin UI. If you roll back to a version earlier than 10.4 and then want to switch again to a different revision, or even to return to the newest software version, you must use the command line "rollback" program until you reach version 10.4 or later.

To revert the Traffic Manager to a previous version using the "rollback" program

1. Connect to the Traffic Manager instance console using PuTTY or some other suitable terminal emulator.

2. Ensure you are the root user.

3. Run the following command:

```
$ZEUSHOME/zxtm/bin/rollback
```

This starts the rollback program:

```
Rollback
Copyright (C) 2017, Brocade Communications, Inc. All rights reserved.

This program allows you to roll back to a previously installed version of the software. Please note
that the older version will not gain any of the configuration changes made since upgrading.

To delete obsolete versions of the software, use the --delete option.

Do you want to continue? Y/N [N]:
```

4. Type **Y** and press Enter to continue. The program lists all the versions of the software it can restore:

```
Which version of the Traffic Manager would you like to use?
  1) 10.3r1
  2) 10.4 (current version)
Select a version [2]
```

5. Select the version of the software you want to restore, and press Enter.

6. The Traffic Manager stops the current version and restarts itself with the selected version.

If you need to cancel this process and return to the latest software version, rerun rollback and select the later version to restore. You do not need to reinstall the latest version of the Traffic Manager to achieve this. The change in software version is applied permanently; subsequent Traffic Manager reboots continue to use the version you select from the rollback program.

The rollback program includes a `--delete` option to delete unneeded software revisions for the version you are currently using. Run the following command from the console:

```
$ZEUSHOME/zxtm/bin/rollback --delete
```

Follow the instructions to permanently delete a selected software revision. You cannot delete the revision you are currently using, and you cannot delete revisions from other dormant Traffic Manager versions.

Caution: Deleting a software revision is permanent and cannot be reversed. Brocade recommends making a configuration backup first.

Downgrading a Traffic Manager Manually

If the rollback program is unable to complete a version change, you can perform the operation manually by editing the Traffic Manager "boot menu" from the console.

To edit VMware and bare-metal appliance instances

1. Ensure you have access to the instance console.

2. Reboot the instance from the **System > Traffic Managers** page of the Admin UI or use the **reboot** command from the command line interface.

3. During the reboot process, press ESC when you view the following message on the console:

```
GRUB loading, please wait...
Press 'ESC' to enter the menu...
```

4. Select the required version from the list provided.

To edit QEMU/KVM instances

1. Log in to the instance console as the "admin" user.

2. Edit the file /boot/grub/menu.lst.

3. Locate the `default 0` line and replace it with `default 2`.

4. Save the changes to the file.

5. Use the **reboot** command to reboot your instance.

CHAPTER 7

Configuring Your L4Accel Services

In a typical Traffic Manager deployment, you configure a virtual server object to manage connections from remote clients, and configure a pool object to manage connections to your local servers.

After you have installed and configured your Traffic Manager system on the network, you can access the Admin UI to set up a pool and a virtual server.

This chapter describes L4Accel service configuration and introduces the main conceptual differences in the Traffic Manager while Data Plane Acceleration mode is enabled. For a complete description of all Traffic Manager functionality available in all modes, refer to the *Brocade Virtual Traffic Manager: User's Guide*.

This chapter contains the following sections:

- "Structure of a Basic L4Accel Service," next
- "L4Accel Virtual Server Settings" on page 68
- "Pools and Load Balancing" on page 75
- "Traffic IP Groups and Fault Tolerance" on page 77
- "System Settings" on page 80
- "Troubleshooting" on page 83

Structure of a Basic L4Accel Service

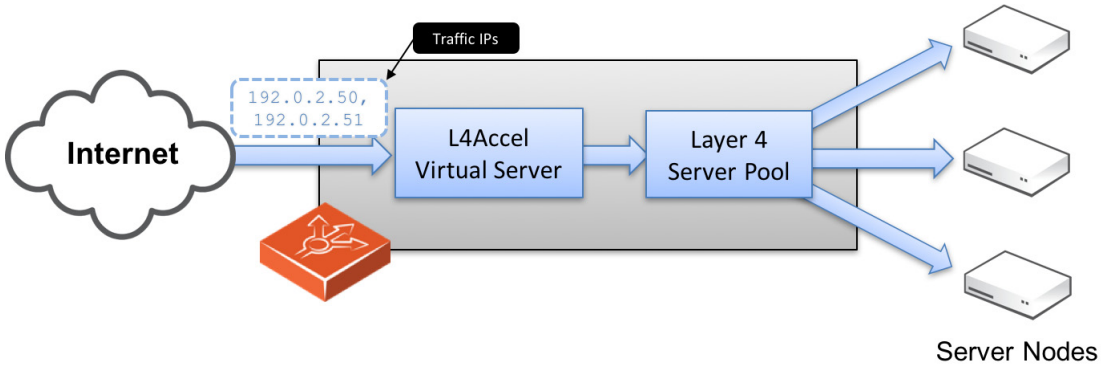
The virtual server listens for incoming network traffic on one or more dedicated traffic IP addresses, and typically handles all of the traffic for a certain protocol (for example, "L4Accel TCP" or "L4Accel UDP"). The Traffic Manager then balances traffic across the server nodes defined in the selected pool.

A pool is a collection of nodes. Each node corresponds to a back-end server and port, such as server1.mysite.com:80. You can set up several pools with nodes in common. For further information on pool configuration with an L4Accel service, refer to "Pools and Load Balancing" on page 75.

You can create a cluster of two Traffic Manager instances running the same services, and both cluster members cooperate to ensure the advertised traffic IP addresses are always available. If a particular Traffic Manager fails, the other Traffic Manager ensures that the advertised IP addresses remain available. For further information about traffic IP addresses, refer to "Traffic IP Groups and Fault Tolerance" on page 77.

The following figure illustrates the relationship between a virtual server and a pool.

Figure 7-1. Relationship Between a Virtual Server and a Pool



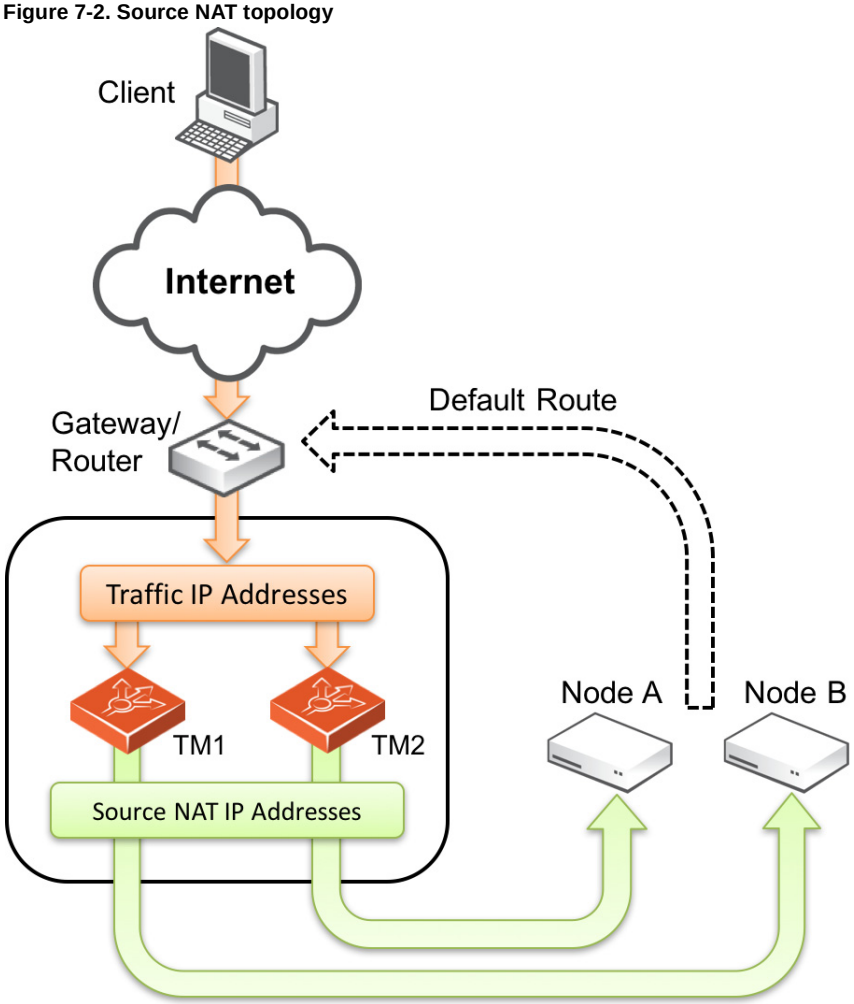
Source Network Address Translation

For Layer 4 services, the Traffic Manager provides a nonterminating load-balanced session flow between a client and your back-end server nodes. With this architecture, the Traffic Manager passes the source IP address of the client to the selected back-end node unchanged (known as IP Transparency). As a result, the node automatically views the client's request as originating from the remote client rather than the Traffic Manager.

To learn more about IP Transparency in the Traffic Manager, refer to the *Brocade Virtual Traffic Manager: User's Guide*.

In Data Plane Acceleration mode, your Traffic Manager cluster can use Source Network Address Translation (Source NAT) to use a specific configured IP address as the source IP address in data packets sent to back-end server nodes. This allows you to operate with separate front-end and back-end networks, while providing transparent failover for your Layer 4 services. For Layer 7 services, Source NAT is enabled by default.

Figure 7-2. Source NAT topology



With IP Transparency, your back-end nodes require dedicated routing configuration that sends traffic intended for all possible client IP addresses through the Traffic Manager. Source NAT removes this requirement; the back-end nodes send all their packets to the selected Source NAT IP address, which is raised as a secondary IP address in the Traffic Manager cluster.

To enable Source NAT for your L4Accel service, configure your pool's IP Transparency settings. For more details, refer to "Pools and Load Balancing" on page 75. You must also configure a list of back-end Traffic IP addresses in your Traffic IP Group. The Traffic Manager uses these back-end Traffic IP addresses as Source NAT IP addresses when sending packets to the back-end nodes to ensure seamless fail-over in the event of a Traffic Manager becoming unresponsive (refer to "Traffic IP Groups and Fault Tolerance" on page 77).

With Source NAT enabled, you must configure at least one back-end IP address for your Traffic IP Group when it is being used by a virtual server that has L4Accel State Synchronization enabled. If L4Accel State Synchronization is disabled, the Traffic Manager uses instead all primary and secondary IP addresses in a subnet as it's source IP address list.

Note: With Data Plane Acceleration mode disabled, only the primary IP address for a given subnet is used. Data plane acceleration mode enables the Traffic Manager to use all primary and secondary IP addresses in a subnet.

L4Accel Virtual Server Settings

With Data Plane Acceleration enabled, the Traffic Manager includes an additional "L4Accel" protocol type. This protocol supports several stateful modes and one stateless mode.

L4Accel Protocol Modes

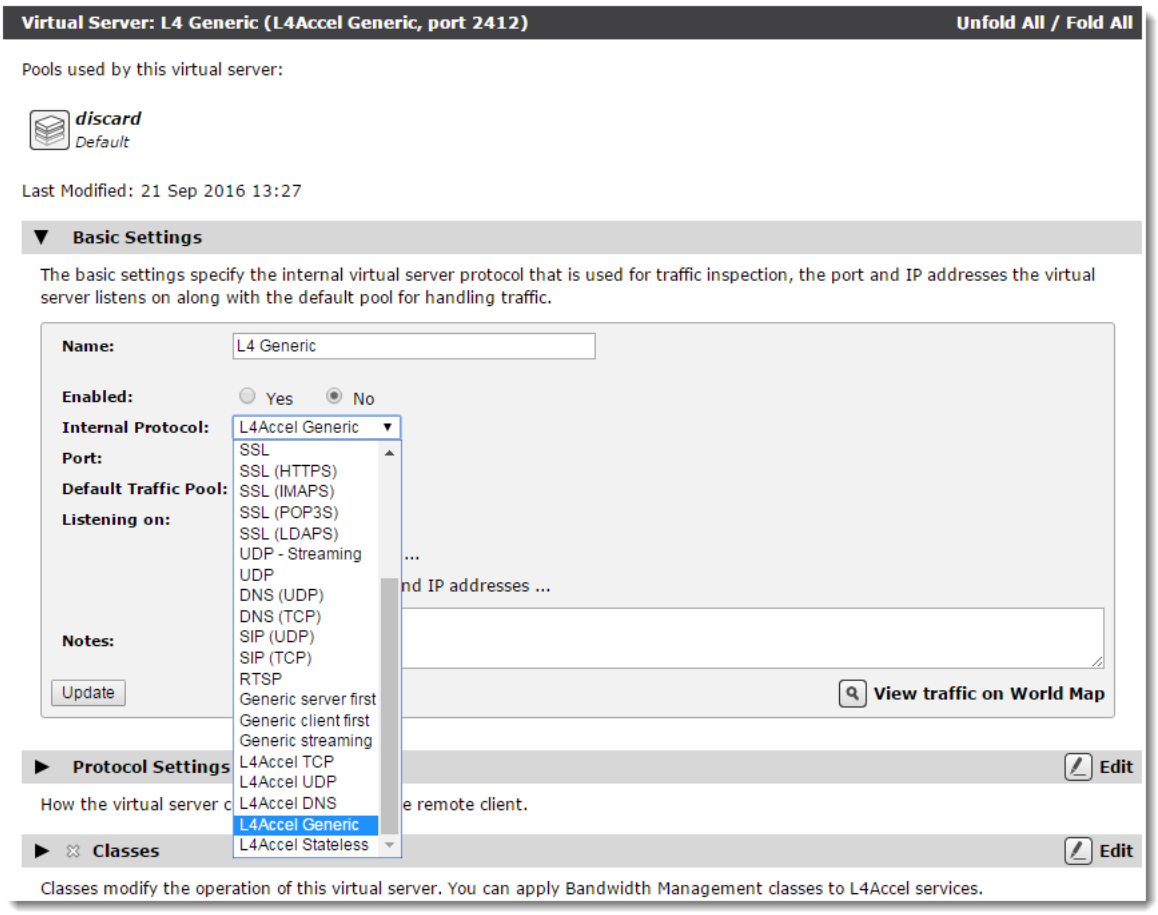
The L4Accel protocol modes are shown in the following table:

Protocol	Description
L4Accel TCP	Use for stateful Layer 4 services based on TCP connections. For each connection request, the Traffic Manager selects a back-end server node and creates corresponding forward and reverse sessions. For subsequent traffic, the Traffic Manager matches the incoming source IP address against these created sessions. The Traffic Manager modifies the packet accordingly and forwards it out to the other side.
L4Accel UDP	The same as L4Accel TCP, but for stateful Layer 4 services contained in UDP datagrams.
L4Accel DNS	Use for DNS traffic utilizing both TCP and UDP packets. To configure L4Accel DNS settings, click **Protocol Settings > L4Accel Settings**.

Protocol	Description
L4Accel Generic	The same as L4Accel TCP, where both TCP and UDP Layer 4 traffic is expected.
L4Accel Stateless	In L4Accel stateless mode, the Traffic Manager does not maintain per-flow session information. For each virtual server, the Traffic Manager maintains an internal lookup table populated with the healthy back-end server nodes in the associated pool. The Traffic Manager uses the client IP address and port of incoming connections as the table index so session persistence to server nodes is preserved. The Traffic Manager maintains the lookup table by using a consistent hashing algorithm that reduces the impact of a failed server node by redistributing the clients served by that failed node to adjacent nodes in the table. The number of clients allocated to each node is statistically evenly distributed. This arrangement offers an alternative solution for Layer4 load-balancing without consuming sessions for each incoming connection, but bypasses most of the Traffic Manager's high-level traffic inspection capabilities. Additionally, the following limitations apply to L4Accel Stateless services: • Source NAT and pass-through traffic are not supported. • You cannot set the nodes in a pool used by an L4Accel Stateless virtual server into a "Draining" state. • A node used by an L4Accel Stateless virtual server cannot be used by any other virtual server. • An L4Accel Stateless service can listen on only one IP address. You can configure a back-end Traffic IP address to be used as the default gateway for the back-end nodes to ensure seamless fail-over in the event of a Traffic Manager becoming unresponsive. • A node belong to a pool used by an L4Accel Stateless virtual server cannot exist in any other pool. • A port used only by a single L4Accel Stateless virtual server provides greater performance than if the port is shared with other L4Accel virtual servers using different IP addresses.

To configure a virtual server with an L4Accel protocol, click **Services > Virtual Servers** in the Admin UI. Create a new virtual server or edit an existing virtual server to use one of the L4Accel protocol types.

Figure 7-3. Setting the Internal Protocol



L4Accel Protocol Settings

The Traffic Manager includes a number of settings to control cluster behavior with L4Accel services. To view and configure these settings, click **Protocol Settings > L4Accel Settings**:

Setting	Description
l4accel!state_sync	**Note:** This setting applies only to L4Accel stateful protocol types. Whether the state of active connections will be synchronized across the cluster for L4Accel services, such that connections will persist in the event of a failover. Note that the service must listen only on Traffic IP Groups for this setting to be enabled. To learn more about state synchronization, refer to "L4Accel State Synchronization" on page 72.
l4accel!service_ip_snat	When Source NAT is enabled on the pool selected to load-balance a connection, the Traffic Manager selects an IP address hosted on the local machine to use as the source IP address for the connection established to the back-end server. Enable this setting to ensure the Traffic Manager always selects the IP address to which the client connected as the egress IP address for the back-end connection. To use this setting, the virtual server must be configured to use L4Accel State Synchronization (**l4accel!state_sync** is set to "Yes"). If the connection state is not synchronized across the cluster, a failover event could cause new client connections to fail.
l4accel!timeout	The number of seconds after which a connection will be closed if no further packets have been received on it.
l4accel!tcp_msl	**Note:** This setting applies only to L4Accel TCP virtual servers. The maximum segment lifetime, in seconds, of a TCP segment being handled by the Traffic Manager. This setting determines for how long information about a connection will be retained after receiving a two-way FIN or RST.
l4accel!rst_on_service_failure	Whether the virtual server should send a TCP RST packet or ICMP error message if a service is unavailable, or if an established connection to a node fails.
udp_end_transaction	**Note:** This setting applies only to L4Accel DNS virtual servers. DNS sessions are typically not expected to be long lived. For UDP DNS in particular, a connection serves only one request and is expected to close after one response. Use this setting to configure how the Traffic Manager should handle termination of DNS sessions. Choose one of the following options: • When they time out • After one response (default value) • When the number of responses matches the number of requests

Traffic Inspection Restrictions with L4Accel Services

To achieve the increased performance Data Plane Acceleration mode provides, the Traffic Manager does not inspect application data beyond the headers of any Layer 4 traffic handled by an L4Accel service. Therefore, a virtual server configured with any of the L4Accel protocols is subject to restrictions in the traffic inspection feature set available to typical virtual servers. The Admin UI lists all unavailable features in a separate disabled section at the bottom of the virtual server edit page.

Layer 4 Request Logging

With Data Plane Acceleration enabled, you can configure a Layer 4 virtual server to log connection information to a disk file and/or remote syslog server. Each destination can have its own log format.

To use request logging, click **Services > Virtual Servers > Edit > Request Logging**.

The Traffic Manager logs each connection made to a stateful L4Accel virtual server (L4Accel TCP, L4Accel UDP, L4Accel Generic, or L4Accel DNS) on a separate line. For an L4Accel Stateless virtual server, the Traffic Manager creates one log line for each data packet. In addition, for each packet, the Traffic Manager logs the TCP flag to facilitate identification of the packet type.

You define the log line format using the **log!format** and **syslog!format** settings. For each log line, you can include macros that represent the parameters of the connection being logged. As Layer 4 services manage traffic at a connection level, macros used for Layer 7 services (for example, HTTP parameters) are not shown.

The following table shows the macros available for Layer 4 services:

Macro	Description
%a	The client's IP address
%A	The IP address to which the client connected
%d	The full 4-tuple for the front-end connection between the client and the Traffic Manager, in the format: `client_ip:client_port=virtual_server_ip:virtual_server_port`
%e	The full 4-tuple for the back-end connection between the Traffic Manager and the server, in the format: `traffic_manager_ip:traffic_manager_port=server_ip:server_port`
%h	The client's IP address (same as %a)
%l	The remote log name
%n	The node used for the connection
%N	The node required to handle this connection (because of session persistence)
%o	The pool used
%p	The port number to which the client connected
%P	The PID of the Traffic Manager child process
%{Time-String}t	The current time
%v	The virtual server name

Note: Log file naming and rotation is handled automatically on a Traffic Manager virtual or hardware appliance. For more information, refer to the *Brocade Virtual Traffic Manager: User's Guide*.

L4Accel State Synchronization

When state synchronization is enabled in your L4Accel services, the Traffic Managers in a cluster begin to share information about the state of connections being processed. This sharing of connection state allows each Traffic Manager to take over Layer 4 connection processing from its peer during a failover event. This provides a robust option for services that have long-lived TCP connections.

For a clustered pair of Traffic Managers with L4Accel state synchronization enabled, each cluster member takes on one of two logical roles, Active and Backup. The Active Traffic Manager raises Traffic IP addresses and handles all incoming connections. The virtual servers on this Traffic Manager send state information to the Backup Traffic Manager over a defined link interface.

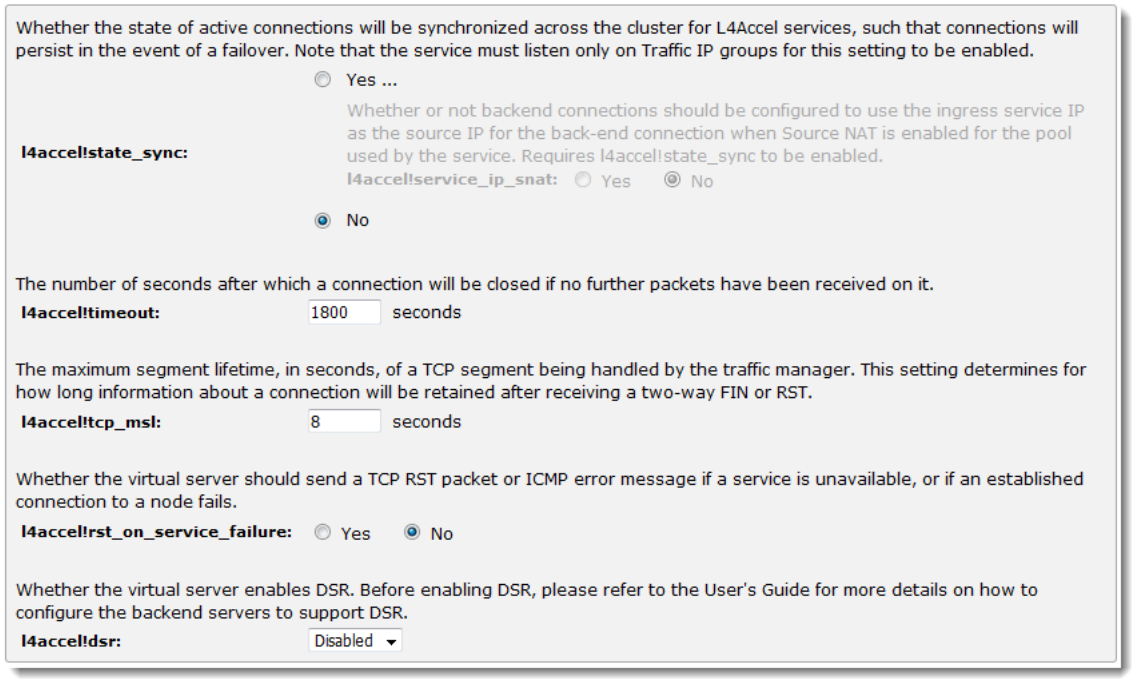
In the event the Active Traffic Manager fails, the Backup Traffic Manager takes over responsibility for raising Traffic IP addresses. Using the state information it has been receiving from the Active Traffic Manager, the Backup Traffic Manager begins to handle connections in a seamless manner. The Backup Traffic Manager now effectively becomes the Active Traffic Manager.

When the original Active Traffic Manager recovers, it returns to being the Active role. To ensure a seamless handover, the recovered Traffic Manager explicitly requests all state information from the currently Active Traffic Manager to ensure it is prepared ahead of the failback of Traffic IP addresses.

L4Accel state synchronization is available for all stateful L4Accel protocol types (L4Accel TCP, L4Accel UDP, L4Accel Generic, and L4Accel DNS), and is only available with Data Plane Acceleration mode enabled. Additionally, your Traffic IP Groups must use the Single-Hosted distribution mode and be configured with the "keeptogether" option enabled.

To enable L4Accel state synchronization, click **Services > Virtual Servers > Edit > Protocol Settings** and set **l4accel!state_sync** to **Yes**.

Figure 7-4. L4Accel Protocol Settings page



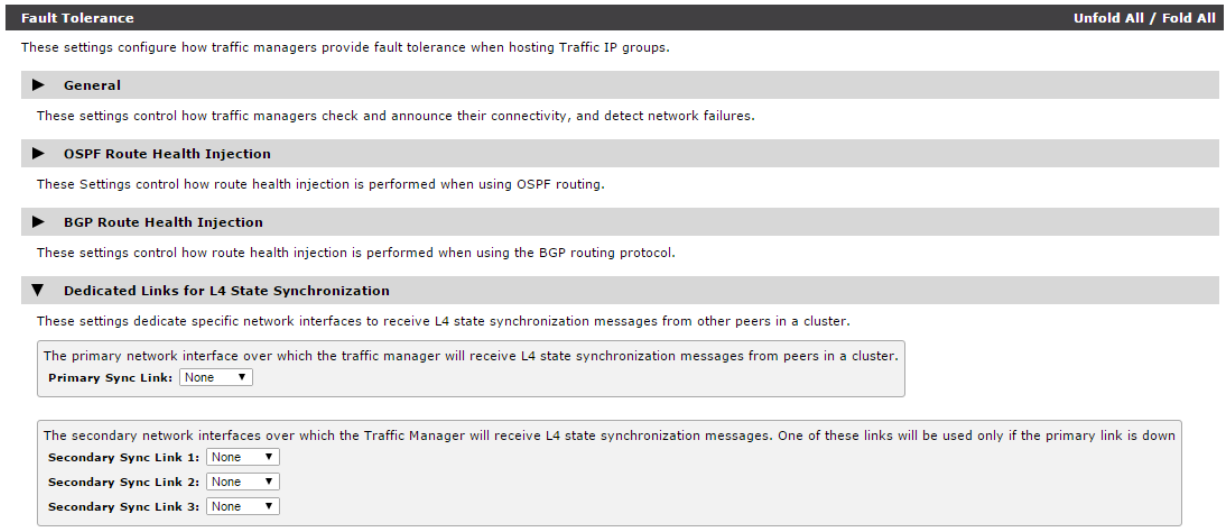
L4Accel state synchronization requires a reasonable amount of bandwidth and low latency between Traffic Manager cluster partners. Before engaging state synchronization, it is important to ensure that your Traffic Managers have good connectivity.

The synchronization process is performed using UDP, with Traffic Manager peers optionally using one of a series of user-defined link interfaces over which to synchronize L4Accel state messages. By using a dedicated interface, state synchronization does not then consume bandwidth on network interfaces reserved for normal system operation. If you choose not to define dedicated link interfaces, the Traffic Manager defaults to sending L4Accel state synchronization messages over one of the IP addresses currently active in your cluster.

You can configure the Traffic Manager with a single primary link interface, and up to three secondary link interfaces. If the primary link is unavailable, a secondary link is randomly selected by the active Traffic Manager. If the primary link recovers, the Traffic Manager returns to prioritizing this interface.

To define L4Accel state synchronization link interfaces, click **System > Fault Tolerance** and locate the "Dedicated Links for L4 State Synchronization" section.

Figure 7-5. Defining dedicated link interfaces for L4Accel state synchronization



For each link field, use the drop-down list to select a network interface. Select the default value of "None" to clear the previous selection.

Note: VLANs are included in the list of available network interfaces. To define a VLAN, use the **System > Networking** page of the Admin UI.

The following restrictions apply:

- You cannot define secondary link interfaces without first defining a primary link interface.
- You cannot select an interface used already in another link field.
- An interface must have an IP address associated with it.
- The Admin UI does not differentiate between interfaces defined within any of the three secondary link fields. Each is considered equal, and can be used if the primary link becomes unavailable.

The Traffic Manager constantly monitors the health and availability of the network interfaces used for L4Accel state synchronization. By pinging the IP address associated with each interface (at an interval of 0.5 seconds), the Traffic Manager is able to make a decision over whether or not to use a particular link at the point state synchronization is attempted.

If you are using dedicated links for L4Accel state synchronization and one or more links become unavailable, the Traffic Manager reports the failed links through the event log. If all defined interfaces links are unavailable, the Traffic Manager reports an error stating that L4Accel state synchronization cannot take place.

To set the port used for synchronization messages, configure **flipper!l4accel_sync_port** in the "General" section.

Pools and Load Balancing

A pool is a logical group of back-end server nodes. Each node is a combination of a server name or IP address and a port, for example, server1.brocade.com:80 or 192.0.2.1:1234.

A pool becomes Layer 4-specific or Layer 7-specific based on the type of virtual server to which it is assigned. Once the pool is assigned, features not supported by the virtual server protocol or Traffic Manager license are presented separately and unselectable at the bottom of the pool edit page.

Note: Mixing IPv4 addresses and IPv6 addresses for your nodes is not supported in Layer 4 pools.

Note: Binding applications that create additional connections on service ports that are different from the original listening ports (FTP, MMS, RTSP) are not allowed for Layer 4 virtual servers.

Pools assigned to L4Accel virtual servers are able to use only a restricted set of load balancing algorithms. To set a load balancing algorithm, click **Pools > Edit > Load Balancing** and configure the "Algorithm" setting with one of the selectable options. Click **Update** to save your changes.

The list of load balancing algorithms available to an L4Accel service is shown in the following table:

Algorithm	Description
Round Robin	Round Robin distributes traffic by assigning each request to a new node in turn. Over a period of time, all the nodes receive the same number of requests.
Weighted Round Robin	Weighted Round Robin works in a similar way to Round Robin, but assigns more requests to nodes with a greater weight. Over a period of time, nodes receive a number of requests in proportion to their weight. Specify the weights for your nodes using the entry boxes provided. You must use positive integer values; a node with a weight of "4" receives four times as many requests as a node with a weight of "1".
Least Connections	Least Connections sends each new request to the node with the fewest currently active connections. During periods of high traffic, each node should be handling a similar number of connections. Faster nodes should respond to requests faster, and so are given proportionally more requests to process over time.
Weighted Least Connections	Weighted Least Connections works in a similar way to the Least Connections algorithm, but assigns more requests to nodes with a greater weight. Specify the weights for your nodes using the entry boxes provided. Requests are distributed across nodes based on the number of active concurrent connections. However, the weightings affect the proportion of connections each node receives. A node with a weight of "4" is four times as likely to receive requests than a node with a weight of "1".

Node Deletion Behavior for L4Accel Services

With Data Plane Acceleration mode enabled, the **node_delete_behavior** setting (refer to **Services > Pools > Edit > Protocol Settings**) is unavailable. This setting typically specifies the behavior for nodes in this pool when a node is deleted: either closing all connections immediately when the node is deleted, or waiting for a connection to finish.

For all Layer 4 and Layer 7 services running with Data Plane Acceleration mode enabled, removing a node from a pool forces all connections to close immediately.

Session Persistence in L4Accel Services

Pools used in L4Accel services can use only IP-based session persistence classes. You can also specify an optional subnet mask within your session persistence class to ensure requests are sent from the same IPv4 or IPv6 subnet to the same node.

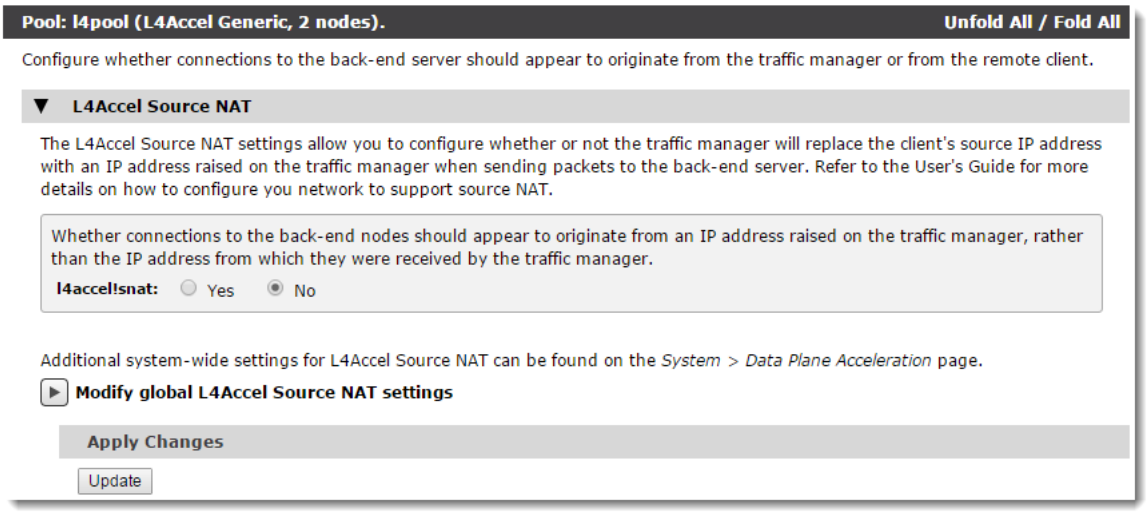
All other persistence methods are not applicable and as such cannot be selected on the **Catalogs > Session Persistence > Edit** page for a session persistence class assigned to a Layer 4 pool.

For full details on using session persistence with your services, refer to the *Brocade Virtual Traffic Manager: User's Guide*.

Configuring Source NAT for a Pool

To configure Source NAT for your Layer 4 pool, click **Services > Pools > Edit > IP Transparency**.

Figure 7-6. Configuring Source NAT for your Layer 4 pool



Set **l4accel!snat** to **Yes** and click **Update**.

Note: The IP Transparency page shows only the option that is applicable for your pool type. For Layer 4 pools, IP Transparency is non-switchable and is therefore not shown. Likewise, for Layer 7 pools, only IP Transparency is offered. If your pool is not yet assigned, both options are shown to allow preconfiguration.

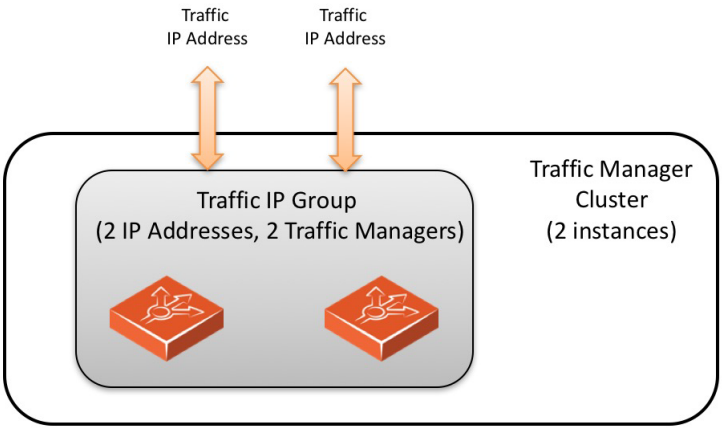
The Traffic Manager selects Source NAT IP addresses from the list of back-end Traffic IP addresses configured in the Traffic IP Group used by your L4Accel services. For more information about configuring back-end Traffic IP addresses, refer to "Traffic IP Groups and Fault Tolerance" on page 77.

Traffic IP Groups and Fault Tolerance

Traffic distribution across a cluster of Traffic Managers is configured by means of Traffic IP Groups. These groups consist of one or more Traffic IP addresses over which your services are advertised. A single Traffic IP Group is managed by some (or all) of the Traffic Managers in your cluster, and these Traffic Managers cooperate to ensure the Traffic IP addresses are always available.

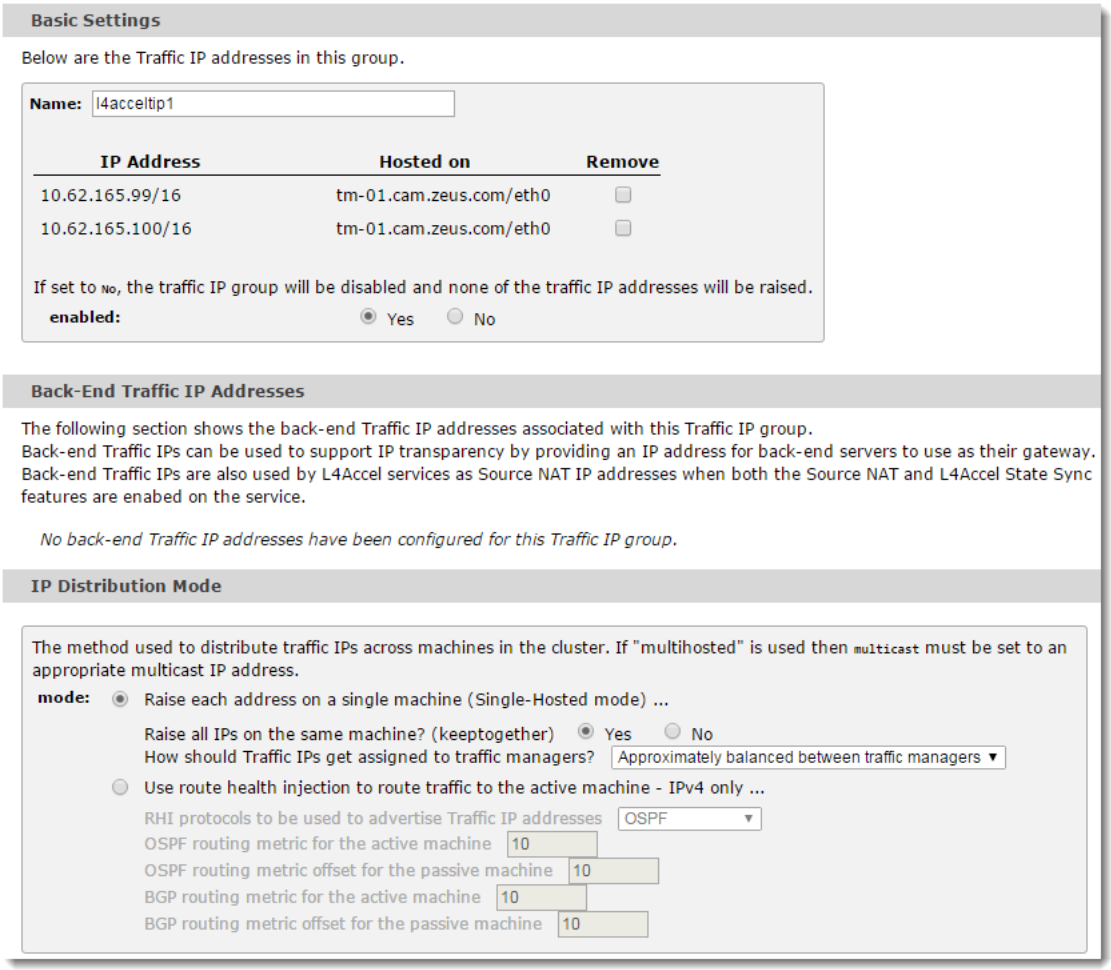
With Data Plane Acceleration mode enabled, your Traffic IP Groups must contain at most two Traffic Managers.

Figure 7-7. Basic Traffic IP Address Configuration



Additionally, your L4Accel services must use Traffic IP Groups based on the Single-Hosted distribution mode, while layer 7 services can use either Single-Hosted or Route Health Injection modes. To set the distribution mode for a Traffic IP group, use the Traffic IP Group edit page.

Figure 7-8. Setting the distribution mode on the Traffic IP Group edit page



In Single Hosted distribution mode, each Traffic IP address is raised on only one of the Traffic Managers in the group. If there are multiple IP addresses in the group, the addresses are raised as evenly as possible across both Traffic Managers. If a Traffic Manager fails, the other Traffic Manager takes over responsibility for traffic to all IP addresses in the group.

After you have defined your Traffic IP Group, configure your services to use the group in the virtual server basic settings.

The **System > Fault Tolerance** page contains a number of system settings for fine-tuning fault tolerance behavior across your cluster with your L4Accel services.

The fault tolerance settings are shown in the following table:

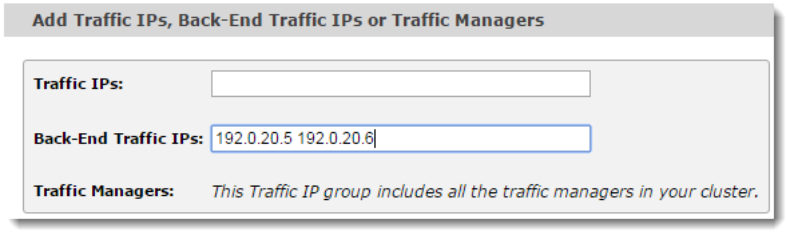
Setting	Description
flipper!l4accel_child_timeout	When running in Data Plane Acceleration mode, how long the Traffic Manager should wait for a status update from child processes handling L4Accel services before assuming it is no longer servicing traffic. Default: 2 seconds
flipper!l4accel_sync_port	The port on which cluster members will transfer state information for L4Accel services when running in Data Plane Acceleration mode. Default: 10240

Adding Back-end IP Addresses

Back-end Traffic IP addresses are shared between the Traffic Managers in your cluster, and are generally used to support IP transparency and Source NAT. If your virtual server is configured to use L4Accel State Synchronization and the associated pool has Source NAT enabled, at least one back-end Traffic IP address must be configured for the Traffic IP Group used by the service.

To add back-end Traffic IP addresses to your Traffic IP Group, make sure the Single-Hosted "keeptogether" option is enabled. Then, add your IP addresses as a space-separated list in the **Back-End Traffic IPs** text box.

Figure 7-9. Configuring a Back-end IP address list

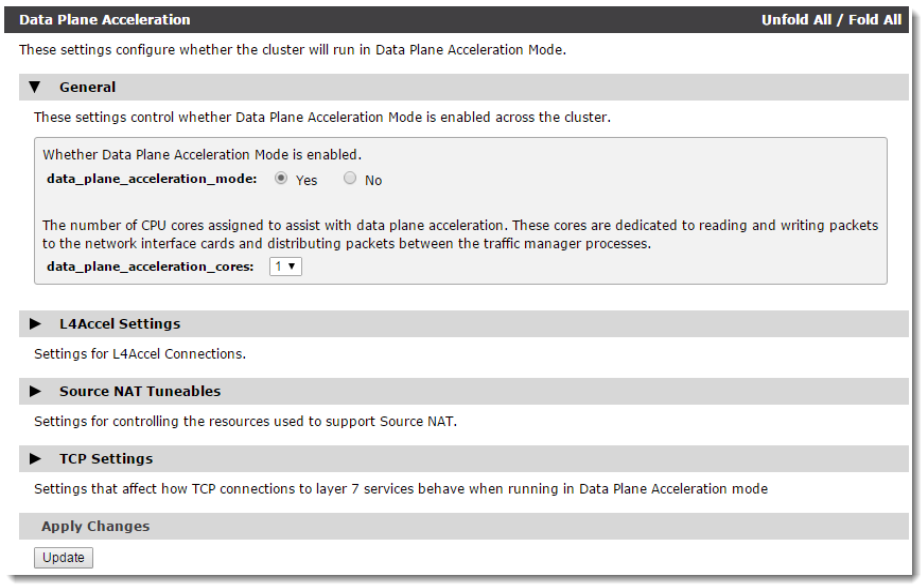


Click **Update** to save your changes.

System Settings

To enable or disable Data Plane Acceleration completely for your Traffic Manager, click **System > Data Plane Acceleration**.

Figure 7-10. Configuring Data Plane Acceleration



Set **data_plane_acceleration_mode** to **Yes** or **No** accordingly and then click **Update**.

Caution: You must reboot the Traffic Manager for the change to take effect.

If during reboot your Traffic Manager determines that it does not meet the minimum requirements necessary for Data Plane Acceleration (refer to Chapter 2, "Prerequisites and Planning"), the system falls back to having Data Plane Acceleration mode disabled with appropriate errors and warnings displayed in the Event Log, on the **Diagnose > Cluster Diagnosis** page, and in the menu bar status display.

Use the **data_plane_acceleration_cores** setting to configure the number of CPU cores on your Traffic Manager instance that are available to assist with Data Plane Acceleration mode.

CPU cores assigned to assist Data Plane Acceleration are dedicated to transferring packets between network interfaces and Traffic Manager's internal system processes. These CPU cores run in "poll mode" to ensure that incoming packets are processed as quickly as possible. As a result, CPU utilization on these cores appears close to 100%, even when no traffic is being handled.

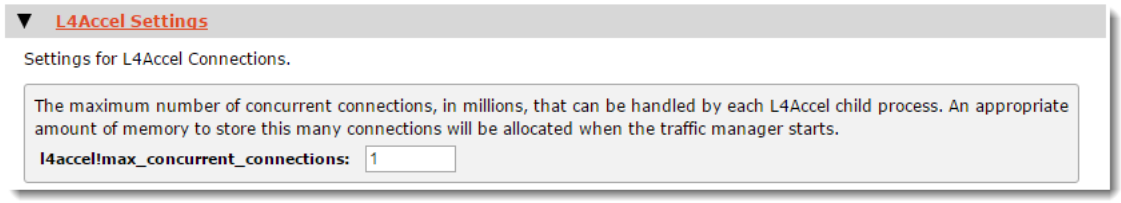
To monitor the true utilization of these cores, plot the SNMP counter "Data Plane Acceleration assist core utilization" on the Current Activity graph. If this counter measures the utilization as being over 80%, Brocade recommends that you increase the number of assigned CPU cores in **data_plane_acceleration_cores**.

Note: If your Traffic Manager instance does not have enough CPU cores available to enable you to increase the **data_plane_acceleration_cores** setting, the Traffic Manager dedicates as many cores as are available. In all cases, one CPU core is always reserved for running theTraffic Manager's internal system processes.

L4Accel Settings

Use the **System > Data Plane Acceleration > L4Accel Settings** section to configure system-wide connection settings for your L4Accel services.

Figure 7-11. Configuring the maximum number of concurrent connections to L4Accel services



Use the **l4accel!max_concurrent_connections** setting to configure an upper limit on the number of connections that can be processed concurrently by your L4Accel services. Type a value that corresponds to the number of millions of connections you want the Traffic Manager to use as a limit. For example, use a value of "4" to represent 4000000 concurrent connections.

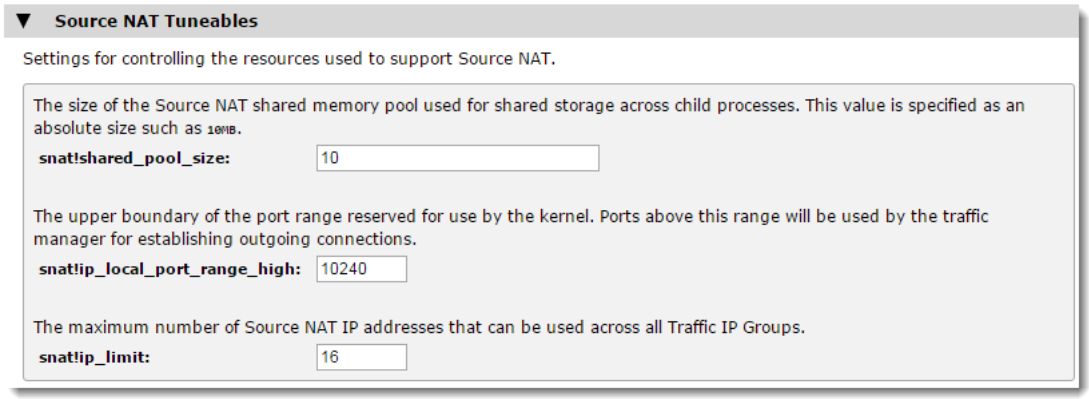
The Traffic Manager then preallocates enough system RAM to support handling the number of concurrent connections you specify in each L4Accel child process. The Traffic Manager typically requires approximately 336 MB of physical memory per L4Accel child process to support 1 million concurrent connections.

If your Traffic Manager has insufficient system RAM available to support the value you configure, the Traffic Manager attempts to reserve enough RAM to support 1 million concurrent connections per L4Accel child process. If there is insufficient RAM available to support that number, 75% of the available physical memory is reserved.

Source NAT Tuneables

Use the **System > Data Plane Acceleration > Source NAT Tuneables** section to configure the resources used to support Source NAT behavior in your cluster.

Figure 7-12. Configuring Source NAT global settings



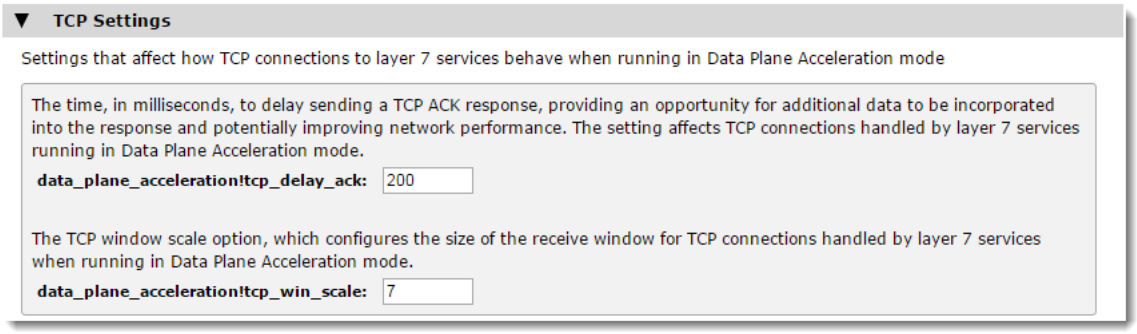
The available configuration options are described in the following table:

Setting	Description
snat!shared_pool_size	The size, in MB, of the Source NAT shared memory pool used for shared storage across child processes. This value is specified as an absolute size such as 10.
snat!ip_local_port_range_high	The upper boundary of the port range reserved for use by the kernel. Ports above this range will be used by the Traffic Manager for establishing outgoing connections.
snat!ip_limit	The maximum number of back-end Traffic IP addresses that can be used as Source NAT IP addresses across all Traffic IP Groups.

TCP Settings

Use the **System > Data Plane Acceleration > TCP Settings** section to configure the behavior of TCP connections to layer 7 services while your Traffic Manager is running in Data Plane Acceleration mode.

Figure 7-13. Layer 7 TCP connection settings while in Data Plane Acceleration mode



The available configuration options are described in the following table:

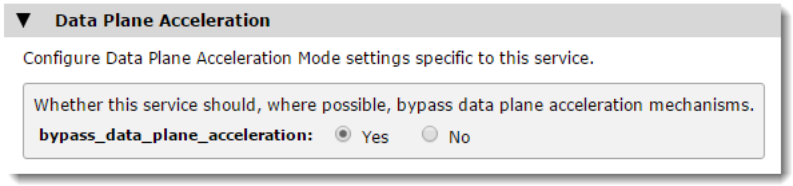
Setting	Description
data_plane_acceleration!tcp_delay_ack	The time, in milliseconds, to delay sending a TCP ACK response to a connection request for a layer 7 service while Data Plane Acceleration mode is enabled. This provides an opportunity for additional data to be incorporated into the response, potentially improving network performance.
data_plane_acceleration!tcp_win_scale	A value between 0 and 7 to represent the *TCP window scale* option, which configures the size of the receive window for TCP connections handled by layer 7 services while Data Plane Acceleration mode is enabled. The Traffic Manager uses the TCP window scale option to increase the TCP receive window size above its maximum value of 65,535 bytes. Reducing this value could negatively impact the performance of high-speed connections, although each connection then consumes fewer resources on the Traffic Manager.

Troubleshooting

Bypassing Data Plane Acceleration in a Layer 7 Virtual Server

With Data Plane Acceleration mode enabled in your Traffic Manager, all Layer 4 and Layer 7 virtual servers are able to take advantage of increased system performance. For troubleshooting purposes, the Traffic Manager can keep Data Plane Acceleration mode enabled at a system-wide level, but provides the ability for individual Layer 7 virtual servers to bypass the underlying data plane process model and instead revert back to using the traditional Traffic Manager Linux stack. To enable or disable the virtual server bypass setting, click **Virtual Servers > Edit > Protocol Settings > Data Plane Acceleration**:

Figure 7-14. Data plane acceleration bypass setting



Troubleshooting Failure to Enable Data Plane Acceleration

After you enable Data Plane Acceleration mode (refer to "System Settings" on page 80), you must restart the Traffic Manager system for the changes to take effect. If during system startup any component of Data Plane Acceleration mode fails to properly initialize, the Traffic Manager reverts back to its previous operating mode.

In most circumstances, the Traffic Manager records information about the failure in a temporary file:

```
/tmp/DataPlaneAccelerationInitStatus
```

The following table lists the possible status codes and their meanings:

Status Code	Status Message	Meaning
0	Data Plane Acceleration mode is not configured.	Your Traffic Manager is not running in Data Plane Acceleration mode. To correct this situation, enable Data Plane Acceleration mode and reboot the system. For more details, refer to "Enabling Data Plane Acceleration" on page 55.
1	Data Plane Acceleration initialization successful.	The Traffic Manager is successfully running in Data Plane Acceleration mode.
2	Data Plane Acceleration pre-init checks successful.	Data Plane Acceleration mode pre-initialization checks, including hardware compatibility, successfully passed. If Traffic Manager software initialization also completes successfully, the status changes to code 1. If Traffic Manager software initialization is not successful, this code is replaced with one of the error codes shown in this table.
-1	Data Plane Acceleration initialization failed during software initialization.	A Data Plane Acceleration software component could not be initialized correctly. To correct this situation, try rebooting the Traffic Manager. If a reboot fails to fix the problem, contact Brocade Support for assistance.

Status Code	Status Message	Meaning
-2	Reserving huge pages memory failed with errno <error_code>.	The Traffic Manager could not reserve sufficient *hugepages* memory for Data Plane Acceleration mode to operate correctly. To resolve this situation, perform a system reboot and/or increase the RAM allocated to your instance.
-3	Kernel I/O driver initialization failed with errno <error_code>.	The Traffic Manager instance is running on an unsupported kernel version. Contact Brocade Support for assistance.
-4	Kernel network interface driver initialization failed with errno <error_code>.	The Traffic Manager instance is running on an unsupported kernel version. Contact Brocade Support for assistance.
-5	No compatible network interface found.	The Traffic Manager instance does not have any network interface that is compatible with Data Plane Acceleration mode. For the list of compatible network interface drivers, refer to Chapter 2, "Prerequisites and Planning."
-6	Not all network interfaces are compatible.	At least one network interface in your Traffic Manager instance is not compatible with Data Plane Acceleration mode. For the list of compatible network interface drivers, refer to Chapter 2, "Prerequisites and Planning."
-7	Unsupported virtualization platform <hypervisor name>.	The virtualization hypervisor you are using does not support Data Plane Acceleration mode. For the list of currently supported virtualization platforms, refer to the release notes supplied with your product variant.
-8	System does not have any network interfaces.	The Traffic Manager must have at least one compatible network interface to run in Data Plane Acceleration mode. For the list of compatible network interface drivers, refer to Chapter 2, "Prerequisites and Planning."
-9	More than 16 network interfaces found.	The Traffic Manager does not support more than 16 network interfaces in Data Plane Acceleration mode. Remove excess network interfaces and reboot the Traffic Manager.
-10	A network interface with unsupported driver <driver_name> found.	A network interface using an unsupported driver was found. Remove the network interfaces that use the unsupported driver shown in the error message and reboot the Traffic Manager.
-11	Insufficient number of cores. Minimum of <number of cores> required.	The Traffic Manager instance does not have the minimum number of CPU cores required for Data Plane Acceleration mode. Add at least the minimum CPU cores specified in Chapter 2, "Prerequisites and Planning" and reboot the Traffic Manager.
-12	CPU does not support ssse3/sse4.2 instructions.	Data Plane Acceleration mode requires CPU support for ssse3/sse4.2 instructions. Check the CPU flag settings in your hypervisor platform or appliance hardware specifications.
-13	Minimum of <memory in GB> required.	The Traffic Manager instance does not have sufficient system RAM for Data Plane Acceleration mode to operate. Add additional RAM up to at least the amount specified in the error message and reboot the Traffic Manager.

Status Code	Status Message	Meaning
-14	Appliance does not support Data Plane Acceleration mode.	Data Plane Acceleration mode is enabled in your Traffic Manager configuration but the host appliance does not support this mode. This can happen when a software upgrade was performed with an incompatible Traffic Manager version or the configuration file was edited manually.
-15	Software does not support Data Plane Acceleration mode.	Data Plane Acceleration mode is enabled in your Traffic Manager configuration but the software does not support this mode. This can happen when a software upgrade was performed with an incompatible Traffic Manager version or the configuration file was edited manually.