



**Pulse Secure Virtual Traffic Manager: Virtual
Appliance Installation and Getting Started
Guide**

21.3

Copyright Notice

This document is provided strictly as a guide. No guarantees can be provided or expected. This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as "Ivanti") and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein. For the most current product information, please visit www.ivanti.com.

Copyright © 2021, Ivanti. All rights reserved.

Protected by patents, see <https://www.ivanti.com/patents>.

Contents

Preface	5
Document conventions	5
Requesting Technical Support	6
Overview	8
Introducing the Traffic Manager	8
Product Variants	8
Getting Started	10
Network Architecture	10
Prerequisites	10
Security Considerations for New Virtual Appliances	11
Network Configurations	12
Management Network	14
Installing the Traffic Manager Virtual Appliance on Microsoft Hyper-V	16
System Requirements	16
Installing the Virtual Appliance	17
Checking the Initial IP Address	19
Connecting to the Admin UI	20
Expanding the Log File Partition	20
Installing the Traffic Manager Virtual Appliance on VMware	22
System Requirements	22
Importing the OVF package	24
Checking the Initial IP Address	25
Connecting to the Admin UI	27
Expanding the Log File Partition	27
Installing the Traffic Manager Virtual Appliance on Xen Based Systems	29
System Requirements	29
Installing the Virtual Appliance XVA Package	29
Checking the Initial IP Address	31
Connecting to the Admin UI	32
Expanding the Log File Partition	32
Bootting your Virtual Appliance into Recovery Mode	34
Installing the Traffic Manager Virtual Appliance on QEMU/KVM	35
System Requirements	35
Installing the Virtual Appliance	36
Accessing the Virtual Appliance Console	42
Checking the Initial IP Address	43
Connecting to the Admin UI	44
Expanding the Logs Partition	44
Using Multi-Hosted Traffic IPs	45
Configuring the Traffic Manager Virtual Appliance	46
Administration User Interface Authentication	46
Using the Initial Configuration Wizard	46

Configuring a Virtual Appliance From the Command Line	56
NTP Settings	63
Upgrading Your Traffic Manager	63
Useful System Information	71
Basic Configuration Information	75
Virtual Servers, Pools, and Rules	75
Managing Your First Service	76
Creating a Traffic Manager Cluster	77
Open Source Software Notice	81

Preface

Document conventions

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

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
<i>italic text</i>	Identifies emphasis
	Identifies variables
	Identifies document titles
Courier Font	Identifies command 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.

Convention	Description
<i>italic text</i>	Identifies a variable.
[]	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.
x y	A vertical bar separates mutually exclusive elements.
< >	Non-printing 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.

Notes and Warnings

Note, Attention, and Caution statements might be used in this document.



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

ATTENTION

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

CAUTION

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

Requesting Technical Support

Technical product support is available through the Ivanti Global Support Center (PSGSC). If you have a support contract, file a ticket with PSGSC.

- Product warranties—For product warranty information, visit <https://support.pulsesecure.net/product-service-policies/>

Self-Help Online Tools and Resources

For quick and easy problem resolution, Ivanti provides an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://support.pulsesecure.net>
- Search for known bugs: <https://support.pulsesecure.net>
- Find product documentation: <https://www.ivanti.com/support/product-documentation>
- Download the latest versions of software and review release notes: <https://support.pulsesecure.net>
- Open a case online in the CSC Case Management tool: <https://support.pulsesecure.net>
- To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://support.pulsesecure.net>

For important product notices, technical articles, and to ask advice:

- Search the Pulse Secure Knowledge Center for technical bulletins and security advisories: <https://kb.pulsesecure.net>
- Ask questions and find solutions at the Pulse Community online forum: <https://community.pulsesecure.net>

Opening a Case with PSGSC

You can open a case with PSGSC on the Web or by telephone.

- Use the Case Management tool in the PSGSC at <https://support.pulsesecure.net>.
- Call 1-844 751 7629 (Toll Free, US).

For international or direct-dial options in countries without toll-free numbers, see <https://support.pulsesecure.net/support/support-contacts/>

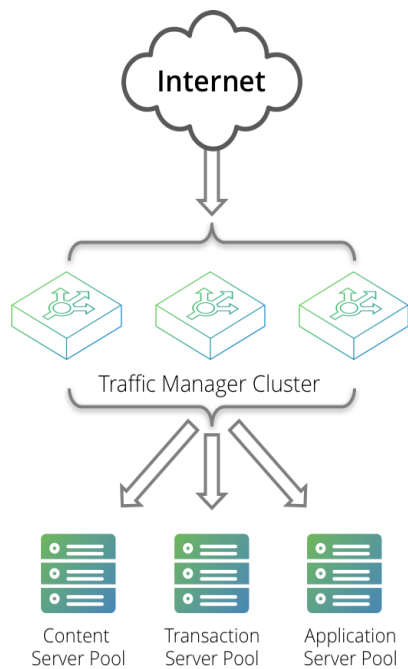
Overview

This chapter provides an overview of Pulse Secure Virtual Traffic Manager (the Traffic Manager).

Introducing the Traffic Manager

The Traffic Manager product family provides high-availability, application-centric traffic management and load balancing solutions. They provide control, intelligence, security and resilience for all your application traffic.

The Traffic Manager is intended for organizations hosting valuable business-critical services, such as TCP-based and UDP-based services like HTTP (web) and media delivery, and XML-based services such as Web Services.



Product Variants

The Traffic Manager product line is available in a variety of forms on different platforms:

- As software, with versions for supported Linux and UNIX operating systems (including support for virtual machine instances running on Amazon's Elastic Compute Cloud (EC2) platform).

- As a virtual appliance, with versions for VMware vSphere, Citrix XenServer, Microsoft Hyper-V, and QEMU/KVM.
- As a cloud computing platform machine image, with versions for Amazon's Elastic Compute Cloud (EC2), Rackspace, Microsoft Azure, and Google Compute Engine (GCE). Ivanti additionally supports installing the Traffic Manager software variant on supported Linux and UNIX virtual machine instances running on EC2 and GCE.
- As an appliance disk image, suitable for deployment on compatible server hardware platforms.

Ivanti provides a separate edition of this guide for each of the above product variants.

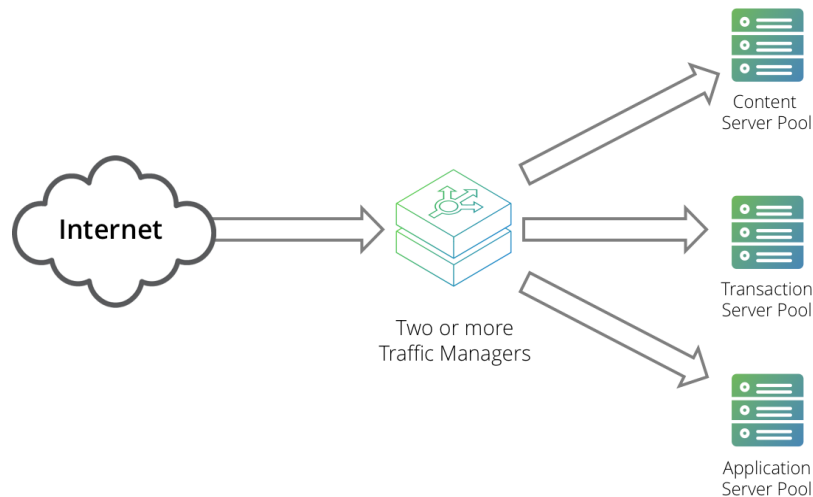
For detailed information concerning supported platforms and versions, see the release notes included with your product variant.

Getting Started

This chapter contains information about getting started using the Traffic Manager.

Network Architecture

The Traffic Manager sits between the Internet and your back-end servers, acting as a reverse proxy. It can be used in conjunction with a standalone firewall if desired. Traffic received from the Internet is passed on to the most appropriate back-end server to respond to the request.



You can install two or more Traffic Managers in a clustered configuration to provide full fault-tolerance for individual software failures. A typical configuration contains at least two Traffic Managers, and at least two servers hosting the load-balanced application.

Prerequisites

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

Make sure that you have the following information:

- Hostnames for each of the virtual appliance instances that you are creating.
- IP addresses for each of the interfaces that you intend to use on each virtual appliance.
- Subnet masks for each of the IP addresses you are using.

- The domain name to which your appliances belong (optional)
- The IP address for the default gateway.
- The IP address for each name server that the virtual appliance uses to resolve your internal network addresses (optional).
- The DNS search path (the "local part" of your machine hostnames) (optional). This item is commonly the same as the domain name.
- An Admin password for the Admin UI.

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.11 or newer
- Microsoft Edge: latest version
- Mozilla Firefox: latest version
- Apple Safari: latest version
- Google Chrome: latest version

Ivanti does not warrant the use of browser versions older than those listed here due to potential discontinuation of security updates by the vendor.

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



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

Security Considerations for New Virtual Appliances

A newly-created, un-configured, Traffic Manager virtual appliance does not itself include password protection or other security measures against hijacking or malicious intent.

Make sure you perform initial configuration on a secure internal network, accessible only by designated administrators, before attaching the Traffic Manager to the network on which it is intended to be deployed. Alternatively, use a network firewall (or switch setup) to prevent unauthorized access.

After you have successfully deployed and configured your Traffic Manager virtual appliances, you can increase administration security by implementing client IP address access restrictions. For more details, see the “Administration Security” chapter of the Pulse Secure Virtual Traffic Manager: User’s Guide.

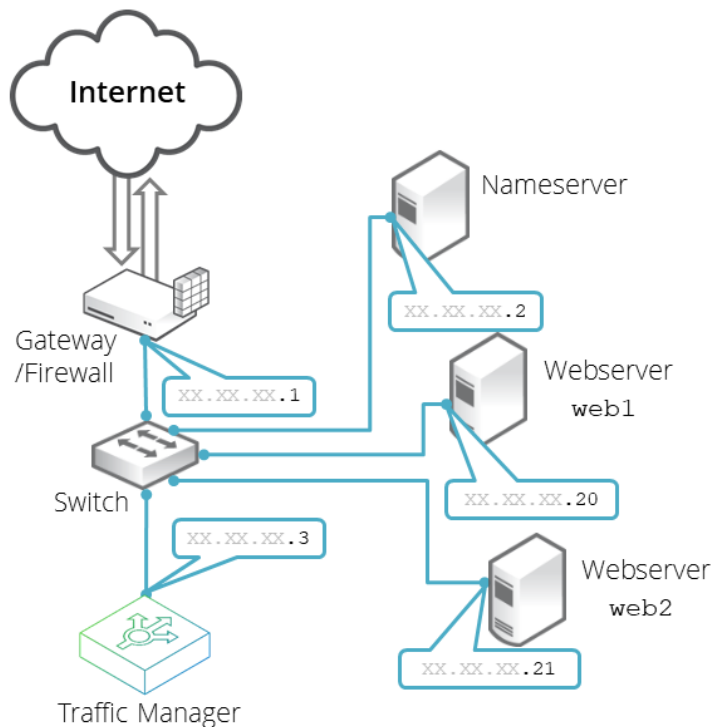
Network Configurations

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 Web site. All IP addresses run on a publicly addressable network (represented by xx.xx.xx in the diagram, with a netmask of 255.255.255.0).

Without the Traffic Manager, clients connecting to the Web site 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).

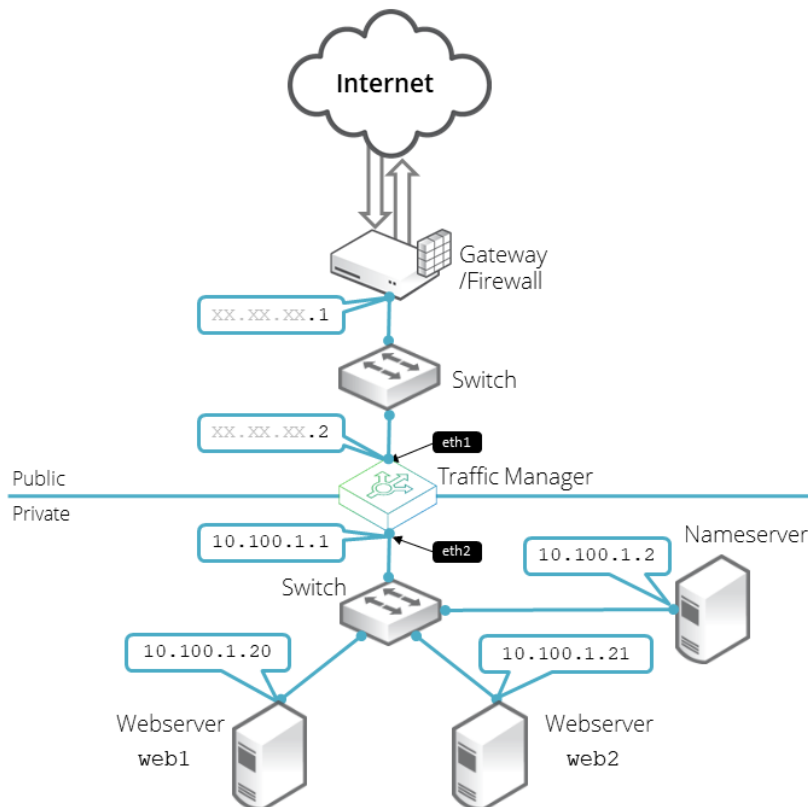


By installing a Traffic Manager, configured to receive traffic over a single network port and IP address `xx.xx.xx.3`, you can alter your DNS record to instead direct clients to `xx.xx.xx.3`. In this way, the Traffic Manager receives the Web page requests and responds with content from one of the available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

Scenario 2: Public/Private Networks

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

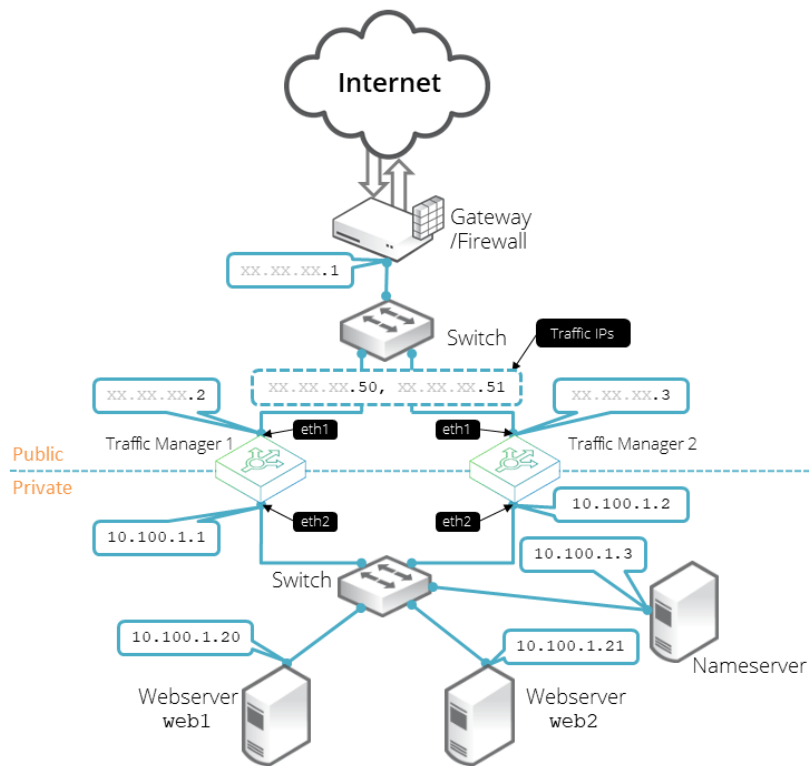
The diagram shows how you can configure the network gateway and the Traffic Manager's front-end (`eth1`) interface with publicly routable IP addresses (the `xx.xx.xx` network, netmask `255.255.255.0`). You then configure the Traffic Manager's back-end interface (`eth2`) on the internal network (`10.100.xx.xx`,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



Scenario 3: Multiple Traffic Managers

This scenario deploys two Traffic Managers in a public/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 Traffic Manager's Web-based Admin UI, and you set them up after the initial low-level networking is complete. For more information, see the Pulse Secure Virtual Traffic Manager: User's Guide.



Management Network

By default, the Traffic Manager accepts management traffic on all of its network interfaces. All management traffic is encrypted or secured

Management traffic includes the following types:

- Access to the Web-based administration interface (also known as the Admin UI).

- Connections through the SOAP-based Control API, the REST API, and Command-Line Interface (CLI).
- Internal health and state sharing traffic.

You typically use a network firewall to prevent external clients from attempting to access any of the management interfaces.

For heightened security, the Traffic Manager enables you to nominate a particular network interface for management traffic. This interface can reside on a secure internal management network.

Installing the Traffic Manager Virtual Appliance on Microsoft Hyper-V

This chapter describes how to install the Traffic Manager Virtual Appliance on the Microsoft Hyper-V platform.

System Requirements

The Traffic Manager virtual appliance is supported for production use on the Microsoft Hyper-V hypervisor, running on the Windows Server platform. The Traffic Manager is available on Hyper-V as a 64-bit version only.

Refer to the release notes included with your virtual appliance package for a full list of the supported platforms and versions.

The virtual appliance software is provided as a ZIP archive file. This file contains a VHD disk image file suitable for use within a Hyper-V environment. The software can be installed and configured through the Hyper-V Manager component in the Server Manager application.

The minimum resource requirements for the virtual appliance are:

- Allocated Memory (RAM): 2 GB
- Disk allocation: 16 GB



For instances intended to include Pulse Secure Virtual Web Application Firewall (vWAF), use a minimum allocated memory (RAM) of 4 GB.

The Traffic Manager uses a dynamically expanding virtual hard disk format. A freshly installed appliance starts with a minimal disk size and expands automatically with usage up to the defined maximum allocation shown above. Such usage includes stored configuration and log file entries. Should you reach this maximum, it is possible to increase the disk size through tools provided in the Hyper-V manager. For more details, see [Expanding the Log File Partition](#).

ATTENTION

A newly-created, but un-configured, Traffic Manager virtual appliance can be vulnerable to hijacking or malicious use if not deployed in a secure environment. For pre-deployment security considerations, see [Network Architecture](#).

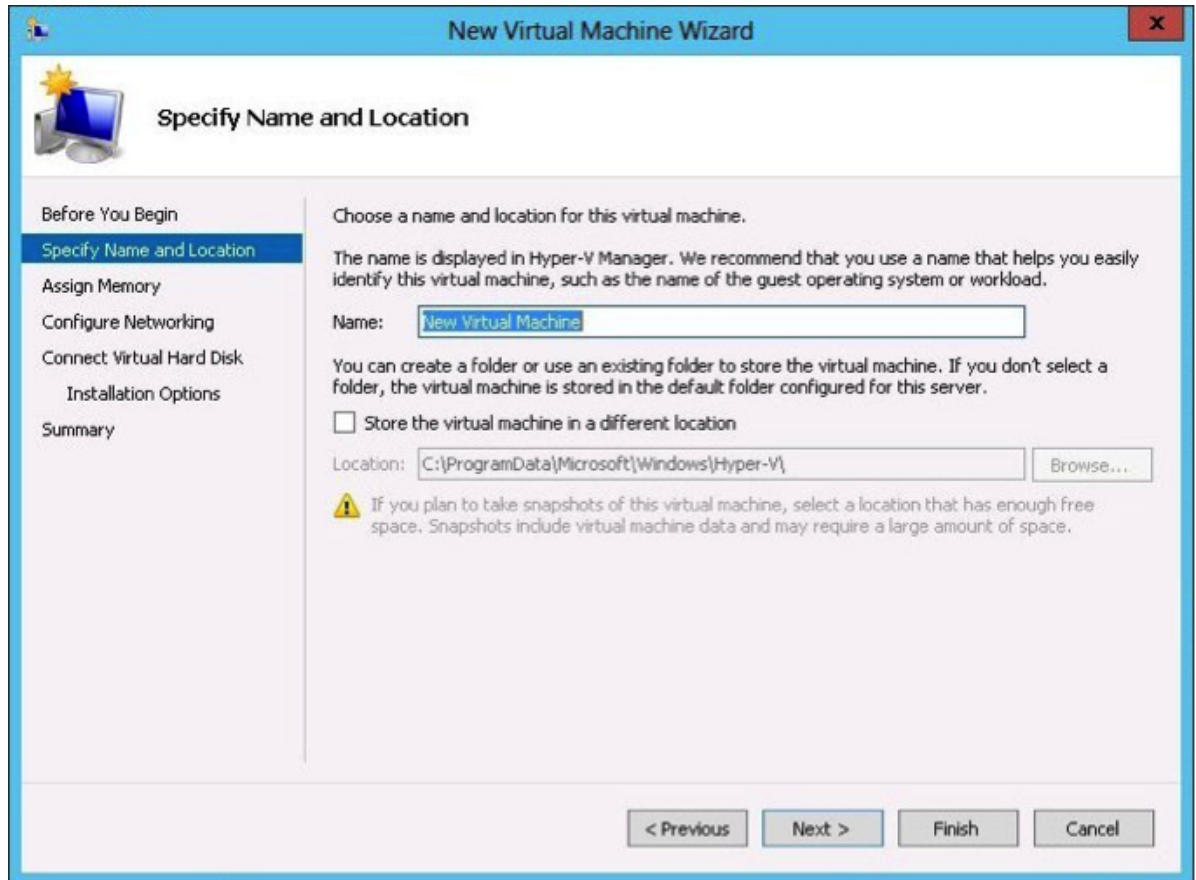
Installing the Virtual Appliance

Microsoft provides a Windows Server-based Hyper-V Manager application for managing your virtual infrastructure. This application can be used to install and administer the Traffic Manager virtual appliance on Hyper-V.

First obtain the appropriate virtual appliance disk image in VHD format. If the virtual appliance is delivered in a compressed archive file (for example, .zip), unpack this archive to your Windows server first.

To install the Virtual Appliance on Hyper-V

1. Launch the Hyper-V Manager application.
2. Connect to the Hyper-V host server you intend to create the virtual machine on.
3. From the Actions command list, choose **New > Virtual Machine...**
4. The New Virtual Machine wizard is displayed. The individual steps to follow are shown on the left, with the current step displayed in the main part of the window. The **Previous** and **Next** buttons allow navigation between the various steps.



5. *Specify Name and Location*: Enter a suitably identifying name for your virtual machine. Optionally enter an alternative location for the virtual machine to be stored.
6. *Assign Memory*: Enter the total amount of allocated memory (RAM) to be made available to the virtual machine. This should be equal to the amount specified in [System Requirements](#).
7. *Configure Networking*: A suitable connection needs to be created between the network interfaces within your Hyper-V virtual infrastructure and the interface on the Traffic Manager virtual appliance. Select the virtual switch interface from the drop-down list you want this connection to use.
8. *Connect Virtual Hard Disk*: Ivanti provides the necessary virtual hard disk as part of the Traffic Manager virtual appliance package. Click **Use an existing virtual hard disk** and provide the full path to the .vhd file from your unpacked virtual appliance archive. Alternatively click **Browse...** to locate it in the file explorer dialog.
9. *Summary*: Click **Finish** to complete the process.



Some variants of Hyper-V Manager contain an additional wizard step to specify which *Generation* your virtual machine belongs to. For this step, choose "Generation 1".

Your Traffic Manager virtual appliance appears in the Virtual Machines pane of the main window. To start the appliance, click **Start** in the Actions pane below the virtual machine name.

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 192.168.1.101 (on the 192.168.1.0/24 network). With either case, the chosen IP address is displayed on the console.

```
Pulse Secure Virtual Traffic Manager, version 17.4 (patchlevel 17420170921)

Welcome to Pulse Secure Virtual Traffic Manager.

The appliance has now booted. To manage, please use a web browser
to access this URL:

Administration interface: https://10.62.165.97:9090/
                        Username: admin
SSL(SHA-1) fingerprint: B6:35:68:29:76:56:15:C0:FF:76
                        69:89:DA:30:7A:DB:02:60:2A:89

SSH(RSA) fingerprint: BF:A7:A6:0F:17:8A:0D:15
                        FE:BA:00:A0:99:5D:05:BC

SSH(ECDSA) fingerprint: E3:8E:AF:CA:F0:D0:04:01
                        3B:97:07:C8:25:1F:CB:1A

Support can be obtained from your reseller, or online assistance
is available at https://forums.pulsesecure.net/
```

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

To set the initial IP address

1. Engage the Traffic Manager virtual appliance console interface.
2. Type 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. Type an IP address and netmask at the prompt.
6. Once the command terminates, type `logout` to log out of the console.
7. Switch back to "tty1" by typing `Alt+F1`.
8. Observe that the IP address in the URL for the Traffic Manager administration interface (Admin UI) has changed to your new IP address.

Connecting to the Admin UI

To connect to the Traffic Manager Admin UI, type the URL displayed on the appliance console into your Web browser.

By default, this URL is "https://<appliance_IP>:9090/", where <appliance_IP> is either:

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



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 hostname in the certificate does not match the hostname in the URL). These problems can safely be ignored: the certificate is a self-signed certificate, and the hostname 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.

Resizing the Virtual Hard Disk

In the Hyper-V Manager application, edit the settings of the desired Traffic Manager virtual machine to set a new size for the hard disk.

To resize the virtual hard disk

1. To edit the virtual machine settings, click **Settings...** in the Actions pane, use the right-click context menu over the virtual machine name, or use the Action menu in the toolbar.
2. In the Settings dialog, select the hard drive you want to expand in the Hardware pane (the relevant .vhd virtual hard disk file is listed here), and click **Edit** in the right hand details pane. This launches the Edit Virtual Hard Disk wizard.
3. Choose "Expand" and click **Next**.
4. Enter the new disk size (in GB) in the box provided.
5. Click **Next** to view a summary of the changes, or **Finish** to expand the disk immediately.
6. Click **OK** to close the Settings dialog, and click **Start** to restart the virtual machine.

Once the virtual machine has started, resize its log partition to take advantage of the newly allocated disk size.

Resizing the Virtual Appliance Log Partition

To expand the Traffic Manager's log partition into a newly resized virtual hard disk, use the virtual appliance console interface.

To expand the log partition

1. Engage the virtual appliance console, or connect using SSH.
2. Log in as the "admin" user.
3. Resize the /logs partition by typing the following command:

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



Be aware that SSH Intrusion Prevention is disabled temporarily during the resize process.

Installing the Traffic Manager Virtual Appliance on VMware

This chapter describes how to install the Traffic Manager Virtual Appliance on VMware.

System Requirements

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

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

CAUTION

If you are upgrading your virtual appliance from a previous Traffic Manager version, you can find information specific to VMware users in [Upgrading Your Traffic Manager](#).

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

The minimum resource requirements for the virtual appliance are:

- Allocated Memory (RAM): 2 GB
- Disk allocation: 16 GB



For instances intended to include Pulse Secure Virtual Web Application Firewall (vWAF), use a minimum allocated memory (RAM) of 4 GB.

To ensure the full performance of your deployment, Ivanti recommends you set the memory resource reservation for your new virtual machine at least equal to its allocated RAM. To achieve this, configure the "Reservation" setting on the **Resources > Memory** tab of your Virtual Machine settings.



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

ATTENTION

A newly-created, but un-configured, Traffic Manager virtual appliance can be vulnerable to hijacking or malicious use if not deployed in a secure environment. For pre-deployment security considerations, see [Network Architecture](#).

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.

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 in vSphere Client to be used as a template.
2. Navigate to the Admin UI and complete the Initial Configuration Wizard. For more information, see [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 system cannot successfully resolve your Traffic Manager hostname, *nameip* allows you to configure the Traffic Manager to instead use its IP address to identify itself to other cluster members.

CAUTION

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

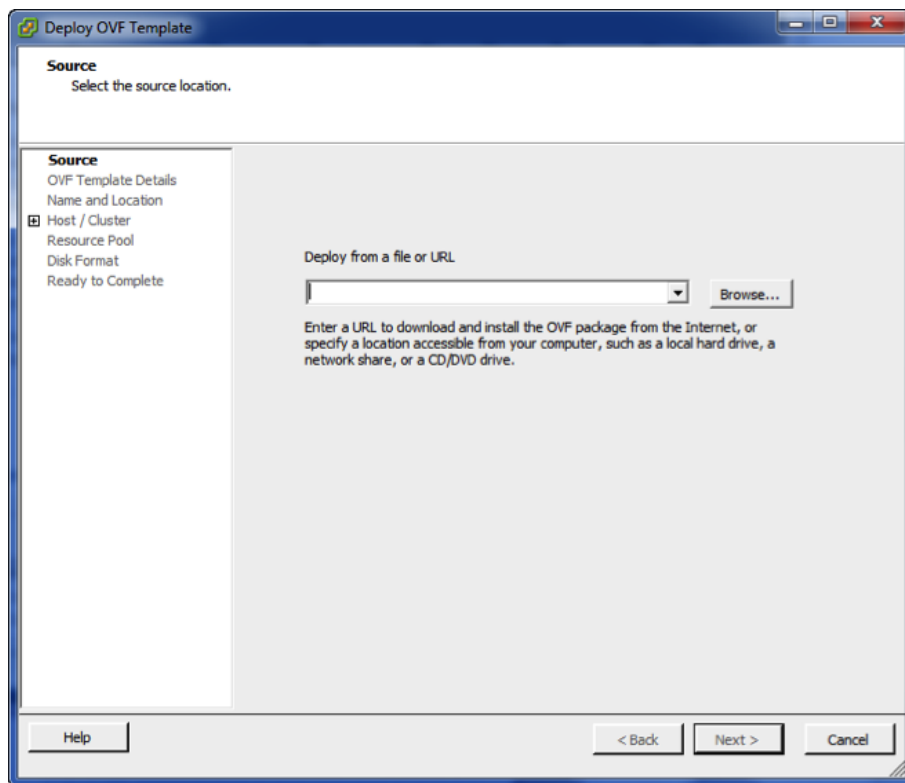
For further information on cloning and Guest OS Customization, see the VMware documentation Web site: <http://www.vmware.com/support/pubs>.

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



3. *Source*: 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.

4. *OVF Template Details*: Displays the details of your successfully validated virtual appliance package.
5. *End User License Agreement*: To continue importing the OVF template, you must read and accept the Ivanti Terms and Conditions of Sale. To view the agreement, use the URL provided.
6. *Name and Location*: 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 appliance. If you are connected directly to the host, the location is not applicable.
7. *Host / Cluster*: Select the appropriate host or cluster on which you intend to install and run the virtual appliance.
8. *Resource Pool*: If you have multiple resource pools, hosts, or clusters set up within your infrastructure, use this page to select the resource within which you want your virtual appliance to reside.
9. *Disk Format*: Select either "thin" or "thick" disk provisioning according to your organizational policy or requirements.
10. *Ready to complete*: 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-side pane.

The Traffic Manager virtual appliance is supplied preconfigured with one network interface. If you require more than one interface, edit the virtual machine settings of the newly imported appliance before starting it and add new Ethernet adapters as required.



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. Ivanti recommends that you select the same network driver for each defined interface if MAC address preservation is required across your network interfaces.

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 192.168.1.101 (on the 192.168.1.0/24 network). With either case, the chosen IP address is displayed on the console.

```
Pulse Secure Virtual Traffic Manager, version 17.4 (patchlevel 17420170921)

Welcome to Pulse Secure Virtual Traffic Manager.

The appliance has now booted. To manage, please use a web browser
to access this URL:

Administration interface: https://10.62.165.97:9090/
                        Username: admin
SSL(SHA-1) fingerprint: B6:35:68:29:76:56:15:C0:FF:76
                        69:89:DA:30:7A:DB:02:60:2A:89

SSH(RSA) fingerprint: BF:A7:A6:0F:17:8A:0D:15
                        FE:BA:00:A0:99:5D:05:BC

SSH(ECDSA) fingerprint: E3:8E:AF:CA:F0:D0:04:01
                        3B:97:07:C8:25:1F:CB:1A

Support can be obtained from your reseller, or online assistance
is available at https://forums.pulsesecure.net/
```

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

To set the initial IP address

1. Engage the Traffic Manager virtual appliance console interface.
2. Type 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. Type an IP address and netmask at the prompt.
6. Once the command terminates, type logout to log out of the console.
7. Switch back to "tty1" by typing Alt+F1.
8. Observe that the IP address in the URL for the Traffic Manager administration interface (Admin UI) has changed to your new IP address.

Connecting to the Admin UI

To connect to the Traffic Manager Admin UI, type the URL displayed on the appliance console into your Web browser.

By default, this URL is "https://<appliance_IP>:9090/", where <appliance_IP> is either:

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



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 hostname in the certificate does not match the hostname in the URL). These problems can safely be ignored: the certificate is a self-signed certificate, and the hostname 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. Engage the virtual appliance console, or connect using SSH.

3. Log in as the "admin" user.
4. Resize the /logs partition by typing the following command:

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



Be aware that SSH Intrusion Prevention is disabled temporarily during the resize process.

Installing the Traffic Manager Virtual Appliance on Xen Based Systems

This chapter describes how to install the Traffic Manager Virtual Appliance on Xen based hypervisors.

System Requirements

The Traffic Manager virtual appliance is supported for production use on Citrix XenServer.

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

The minimum resource requirements for the virtual appliance are:

- Allocated Memory (RAM): 2 GB
- Disk allocation: 16 GB



For instances intended to include Pulse Secure Virtual Web Application Firewall (vWAF), use a minimum allocated memory (RAM) of 4 GB.

Installing the Virtual Appliance XVA Package

Ivanti recommends using Citrix XenCenter for managing your XenServer virtual infrastructure. These instructions refer to importing the Traffic Manager virtual appliance using this method.

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

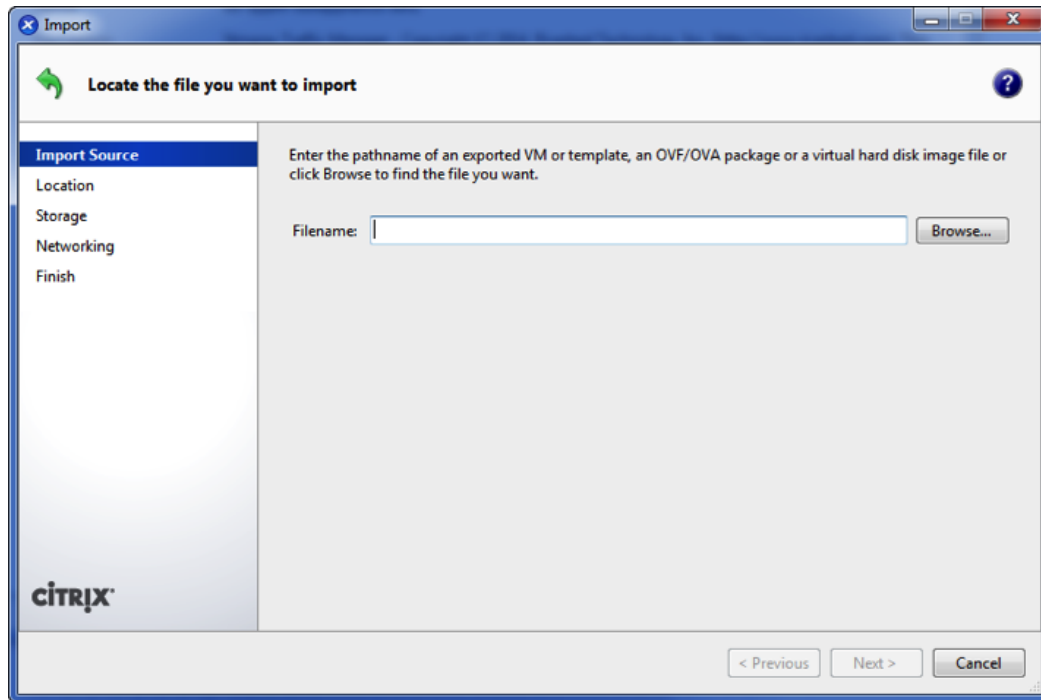
ATTENTION

A newly-created, but un-configured, Traffic Manager virtual appliance can be vulnerable to hijacking or malicious use if not deployed in a secure environment. For pre-deployment security considerations, see [Network Architecture](#).

To install the Traffic Manager, obtain the appropriate Traffic Manager virtual appliance package in XVA format. If the virtual appliance is delivered in a compressed archive format (for example, ZIP) unpack this archive to your local hard disk before starting the installation procedure.

To install the Traffic Manager using XenCenter

1. Log in to XenCenter and connect to your designated XenServer.
2. Click **File > Import** to launch the Import wizard. The individual steps to follow are shown on the left of the wizard window, with the current step displayed in the main section. Click **Previous** and **Next** to navigate between steps, and **Cancel** to exit the wizard without deploying the virtual appliance.



3. *Import source*: Type the full name and path of the .xva file from your unpacked virtual appliance archive package into the Filename box, or click **Browse...** to locate the file on your hard disk. Click **Next** to proceed.
4. *Home server*: Click the XenServer name you want to install the virtual appliance on, or click **Add New Server** to add a new XenServer. Click **Next** to proceed.
5. *Storage*: Select the storage repository you want XenCenter to use for the Traffic Manager's virtual disk. Click **Import** to proceed.
6. *Networking*: Use this step to create one or more network connections between the interfaces in your Xen virtual infrastructure and the interface on the Traffic Manager virtual appliance. Click **Add** to create a new connection, and under the Network column select the XenServer interface from the drop-down list you want this connection to use. Click **Delete** to remove connections as necessary. Click **Next** to proceed.

7. *Finish*: Check the configuration summary of your virtual appliance deployment and click **Finish** to proceed. Click **Previous** to go back and modify any step of the wizard. Click **Start VM(s) after import** to instruct XenCenter to start the virtual appliance automatically upon completion.

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 192.168.1.101 (on the 192.168.1.0/24 network). With either case, the chosen IP address is displayed on the console.

```
Pulse Secure Virtual Traffic Manager, version 17.4 (patchlevel 17420170921)

Welcome to Pulse Secure Virtual Traffic Manager.

The appliance has now booted. To manage, please use a web browser
to access this URL:

Administration interface: https://10.62.165.97:9090/
Username: admin
SSL(SHA-1) fingerprint: B6:35:68:29:76:56:15:C0:FF:76
                        69:89:DA:30:7A:DB:02:60:2A:89

SSH(RSA) fingerprint: BF:A7:A6:0F:17:8A:0D:15
                      FE:BA:00:A0:99:5D:05:BC

SSH(ECDSA) fingerprint: E3:8E:AF:CA:F0:D0:04:01
                        3B:97:07:C8:25:1F:CB:1A

Support can be obtained from your reseller, or online assistance
is available at https://forums.pulsesecure.net/
```

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

To set the initial IP address

1. In XenCenter, select the required Traffic Manager from the list of virtual appliances and click the **Console** tab to engage the console interface.
2. Press Enter to display the login prompt.
3. Log in as "admin" with the default password of "admin".
4. Run the following command:

`z-set-initial-address`

5. Type an IP address and netmask at the prompt.
6. Once the command terminates, type `logout` to log out of the console.
7. Observe that the IP address in the URL for the Traffic Manager administration interface (Admin UI) has changed to your new IP address.

Connecting to the Admin UI

To connect to the Traffic Manager Admin UI, type the URL displayed on the appliance console into your Web browser.

By default, this URL is "`https://<appliance_IP>:9090/`", where `<appliance_IP>` is either:

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



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 hostname in the certificate does not match the hostname in the URL). These problems can safely be ignored: the certificate is a self-signed certificate, and the hostname 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

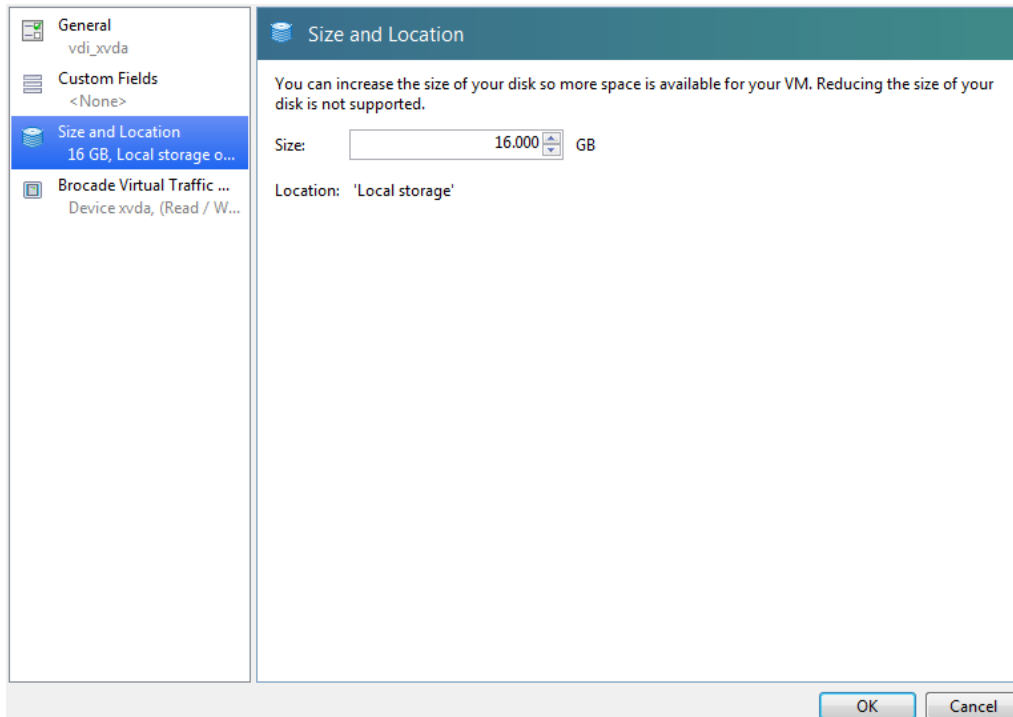
To increase the disk space for your virtual appliance log files, expand the virtual disk and then resize the file system from the virtual appliance's console interface.

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 using XenCenter.

To resize the virtual disk

1. In XenCenter, select the required Traffic Manager from the list of virtual appliances and click the **Storage** tab. A standard Traffic Manager virtual appliance installation contains one virtual disk, displayed in this tab.
2. Select the Traffic Manager virtual disk and click **Properties**.
3. In the virtual disk properties window, click **Size and Location**.



4. Expand the disk to the required size (the default is 16 GB). Click **OK** to make the change.
5. Start the Traffic Manager virtual appliance.
6. After it has finished booting, log in to the console using SSH or the Console tab in XenCenter.
7. To resize the "/logs" partition, type the following command into the console:

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



Be aware that SSH Intrusion Prevention is disabled temporarily during the resize process.

Booting your Virtual Appliance into Recovery Mode

If your Traffic Manager ever becomes unresponsive, or if you suffer some other failure that cannot be resolved from the XenCenter console, it might be necessary to boot your virtual appliance into Recovery Mode.

To use Recovery Mode

1. Log in to the command console of the XenServer that contains your Traffic Manager virtual appliance.
2. Find the "UUID" of the virtual appliance you are interested in using this command:

```
xe vm-list
```

3. After you have obtained the UUID, run the following command:

```
xe vm-param-set PV-bootloader-args="--entry=1" uuid=<UUID>
```

4. Restart the Traffic Manager virtual appliance.

To reset the virtual appliance boot mode back to the default, perform the same operation again, inserting this command in place of [step 3](#):

```
xe vm-param-set PV-bootloader-args="" uuid=<UUID>
```

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.

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, see the release notes included with your virtual appliance package.

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 "virt-manager" and the CLI is provided by "virt-install".

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

The minimum resource requirements for the virtual appliance are:

- Allocated Memory (RAM): 2 GB
- Disk allocation: 16 GB



For instances intended to include Pulse Secure Virtual Web Application Firewall (vWAF), use a minimum allocated memory (RAM) of 4 GB.

ATTENTION

A newly-created, but un-configured, Traffic Manager virtual appliance can be vulnerable to hijacking or malicious use if not deployed in a secure environment. For pre-deployment security considerations, see [Network Architecture](#).

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, basing it 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:
 - **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"). As each `.qcow2` file corresponds to a specific virtual appliance, this step ensures that your disk image files remain unique within the storage pool.
5. You can use the following command to ensure this 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. Issue a `virt-install` command to install the virtual appliance:

```
virt-install --import --cpu=host
             --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
             --ram=2048
             --graphics=vnc
```

In the above 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.

CAUTION

If the installation process fails with the error: "ERROR OS variant 'ubuntuprecise' does not exist in our dictionary for OS type 'linux'", Ivanti 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:

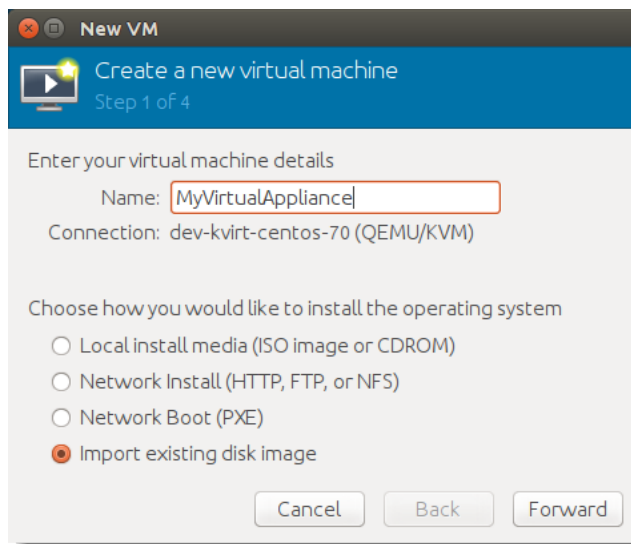
1. Start the VMM tool from a client machine, and connect to the host QEMU/KVM machine. The following command can be used to achieve this:

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

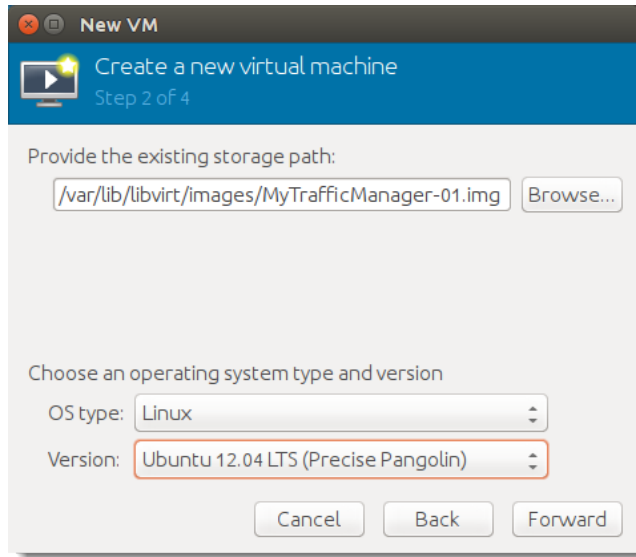
In the above command, my-kvm-host.com is the host machine name. An SSH tunnel is used to connect to the QEMU/KVM host. You must have an SSH account and corresponding public key stored on this host for authentication.

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

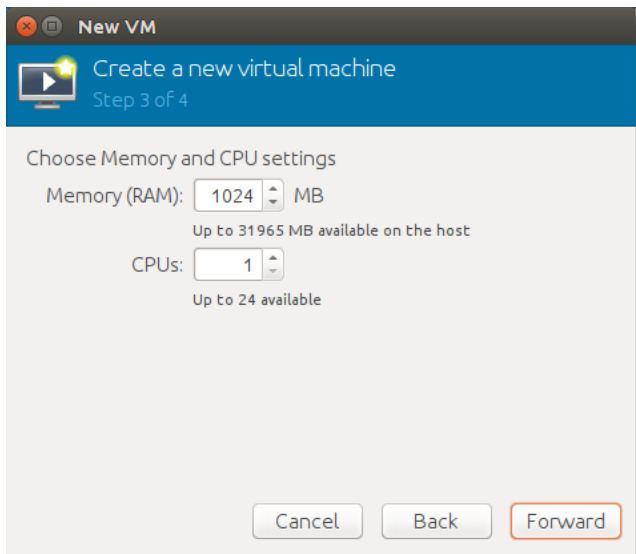
2. Click **New** to start the process of creating a new virtual machine.



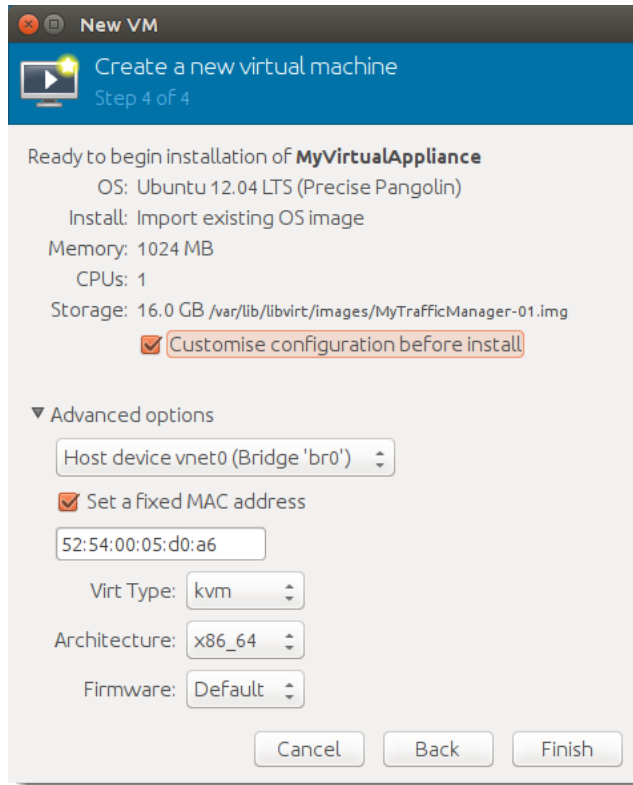
3. Enter a name for your virtual appliance that corresponds with the name used for the virtual machine disk file. From the list of options, click **Import existing image** and then click **Forward** to proceed.



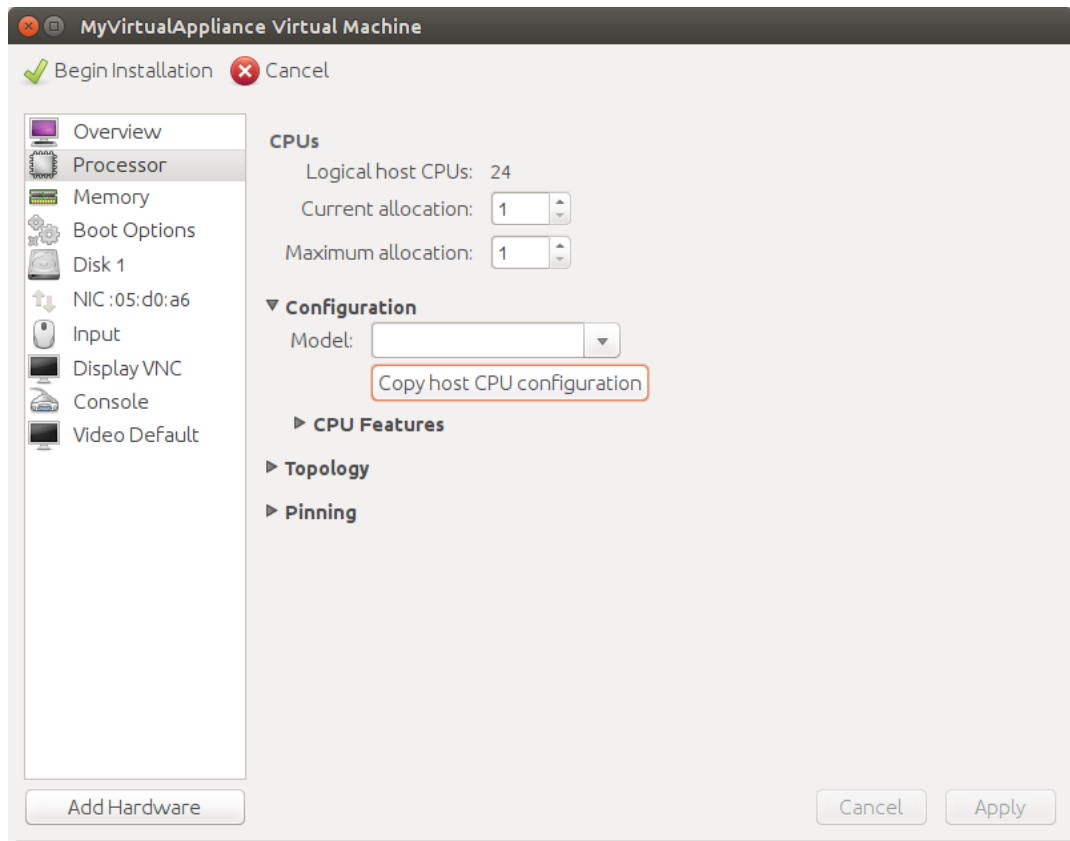
4. Click **Browse** to select the storage pool location and disk file for this virtual machine.
5. Select an OS type of "Linux" and set Version to a supported Linux variant. Click **Forward** to proceed.
6. Enter the RAM and CPU resource settings required for your virtual machine. For recommended settings, see [System Requirements](#) or in the release notes provided with your virtual appliance package. Click **Forward** to proceed.



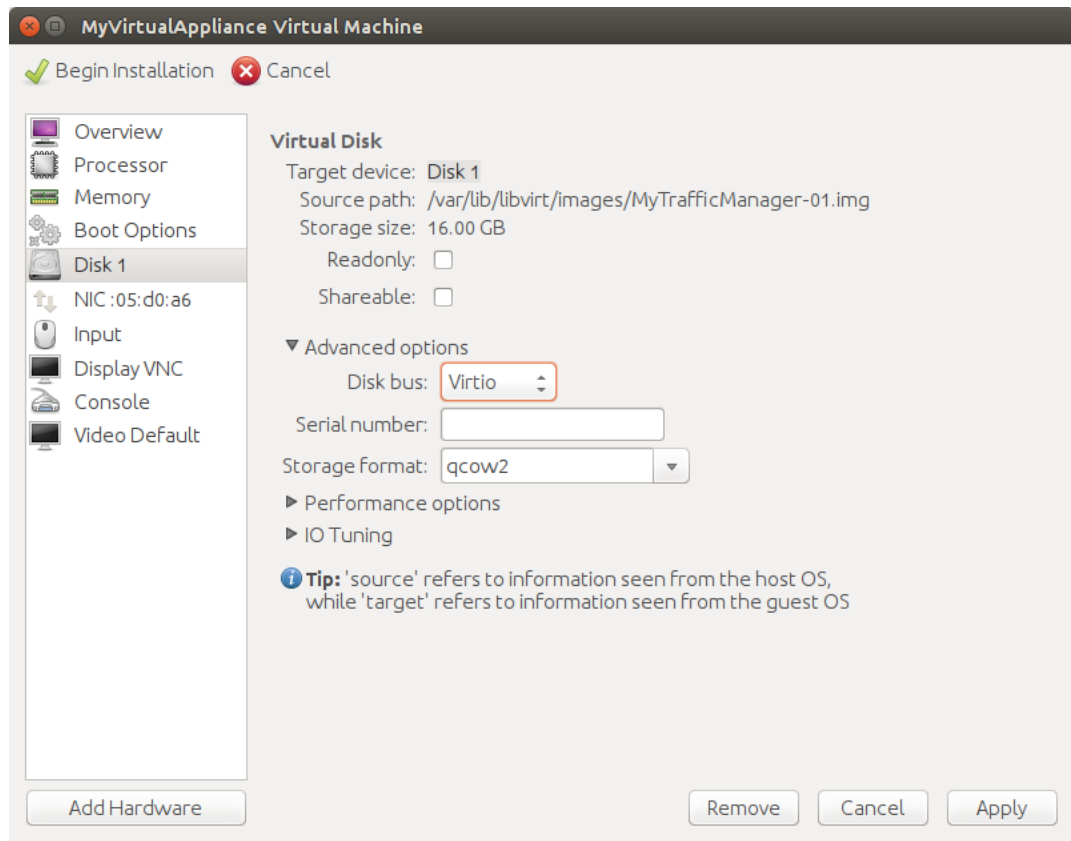
7. Under Advanced options, choose any further settings that you want to apply. Ivanti recommends that you select bridged networking using the drop-down list provided.



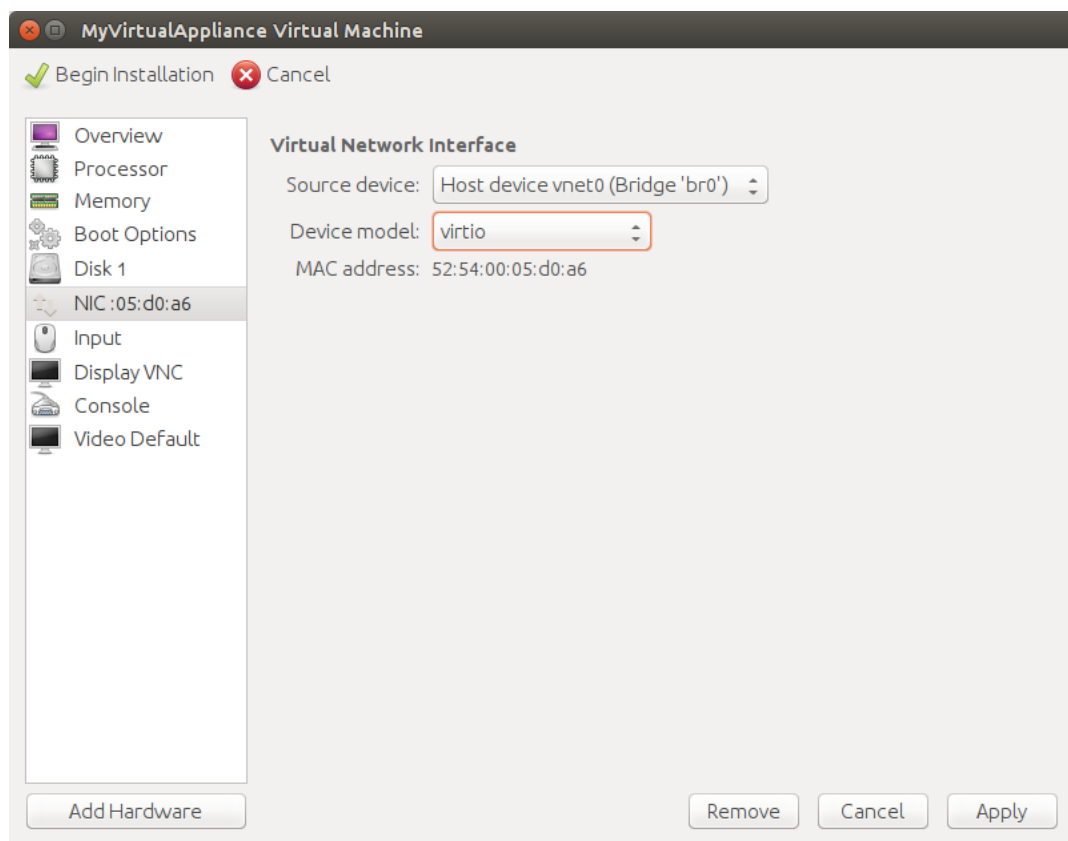
8. Tick **Customise configuration before install**, and then click **Finish**.
9. Before your Traffic Manager virtual machine is installed, VMM displays the hardware configuration page. Click **Processor** in the left hand category list and then click **Copy host CPU configuration** to set the CPU model to match the host hardware.



10. Click **Apply** to save your changes.
11. Click **Disk 1** in the left hand category list and then click the fold-down arrow next to Advanced options. For Disk bus, select "Virtio" from the drop-down list.



12. Click **Apply** to save your changes.
13. Click **NIC** in the left hand category list and then select "Virtio" from the Device model drop-down list.



14. Click **Apply** to save your changes 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 192.168.1.101 (on the 192.168.1.0/24 network). With either case, the chosen IP address is displayed on the console.

```
Pulse Secure Virtual Traffic Manager, version 17.4 (patchlevel 17420170921)

Welcome to Pulse Secure Virtual Traffic Manager.

The appliance has now booted. To manage, please use a web browser
to access this URL:

Administration interface: https://10.62.165.97:9090/
Username: admin
SSL(SHA-1) fingerprint: B6:35:68:29:76:56:15:C0:FF:76
                        69:89:DA:30:7A:DB:02:60:2A:89

SSH(RSA) fingerprint: BF:A7:A6:0F:17:8A:0D:15
                      FE:BA:00:A0:99:5D:05:BC

SSH(ECDSA) fingerprint: E3:8E:AF:CA:F0:D0:04:01
                        3B:97:07:C8:25:1F:CB:1A

Support can be obtained from your reseller, or online assistance
is available at https://forums.pulsesecure.net/
```

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

To set the initial IP address

1. Engage the Traffic Manager virtual appliance console interface.
2. Type Alt+F2 to switch to the alternative console display "tty2".
3. Log in as "admin" with the default password of "admin".
4. Run the command z-set-initial-address.
5. Type an IP address and netmask at the prompt.
6. Once the command terminates, type logout to log out of the console.

7. Switch back to "tty1" by typing Alt+F1.
8. Observe that the IP address in the URL for the Traffic Manager administration interface (Admin UI) has changed to your new IP address.

Connecting to the Admin UI

To connect to the Traffic Manager Admin UI, type the URL displayed on the appliance console into your Web browser.

By default, this URL is "https://<appliance_IP>:9090/", where <appliance_IP> is either:

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



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 hostname in the certificate does not match the hostname in the URL). These problems can safely be ignored: the certificate is a self-signed certificate, and the hostname 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, choose 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, type the following command:

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



Be aware that SSH Intrusion Prevention is disabled temporarily during the resize process.

Using Multi-Hosted Traffic IPs

By default, multi-hosted Traffic IP Groups cannot be used on a QEMU/KVM-based Traffic Manager virtual appliance. To enable support for this feature, enter the following command on the QEMU/KVM host server command line:

```
echo >/sys/devices/virtual/net/<iface>/bridge/multicast_snooping 0
```

In this command, "<iface>" is the name of the bridge network interface used by your virtual machines.

Configuring the Traffic Manager Virtual Appliance

This chapter describes how to configure a newly installed Traffic Manager virtual appliance. It assumes you have already performed the installation procedure described the preceding chapter applicable to your virtualization platform.

This chapter also documents further configuration tasks such as reconfiguring, uninstalling, and upgrading the virtual appliance.

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 virtual appliance 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.

When you set up a new Traffic Manager, Ivanti 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
```

Using the Initial Configuration Wizard

Before you begin, make sure you have met all the requirements listed in [Prerequisites](#). Ivanti recommends that you read this chapter fully before continuing.

A newly installed virtual appliance 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 virtual appliance console.

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

Initial configuration, step 1 of 8**1. Welcome to your Pulse Secure Virtual Traffic Manager**

The following pages will guide you through the process of setting up your Pulse Secure 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.

◀ Back Next ▶

Click **Next** to begin the initial configuration of your virtual appliance.

Accept the Terms and Conditions of Sale

Read and accept the Ivanti Terms and Conditions of Sale, available from the URL shown:

Initial configuration, step 2 of 8**2. Pulse Secure Terms and Conditions of Sale**

Use of this software is subject to the Pulse Secure Terms and Conditions of Sale.
Please review these terms, published at <https://www.pulsesecure.net/support/eula> before proceeding.
 I accept the license agreement

◀ Back Next ▶

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

Configuring Networking

Use this page to set your virtual appliance basic network configuration. A summary of the network settings to be applied to your virtual appliance is given at the end of the wizard.

Initial configuration, step 3 of 8

3. Networking

Please provide the basic network configuration for this appliance. The configuration may be changed at a later date using the user interface.

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

Hostname:

Please enter a valid IPv4 address and netmask for at least one network card if all the cards are in static mode.

IPv6 addresses can be configured on the *System > Networking* page.

Interface	Mode	IP address	Netmask	Management IP address
eth0	<input type="radio"/> static <input checked="" type="radio"/> dhcp	<input type="text"/>	<input type="text"/>	<input type="radio"/>
eth1	<input type="radio"/> static <input checked="" type="radio"/> dhcp	<input type="text"/>	<input type="text"/>	<input type="radio"/>
eth2	<input checked="" type="radio"/> static <input type="radio"/> dhcp	10.62.165.99	18	<input checked="" type="radio"/>

The appliance can be configured to only allow management on one specific IP address. This restricts all admin server access, SOAP management, REST API access and other control information to this IP address. This setup is useful if you want to completely separate your public and private networks. If you wish to do this, tick the box below and select an IP address using the Management IP address option buttons above.

Use a single Management IP address

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.

The gateway IP address for this appliance.

Gateway:

Configure the following settings:

Setting	
Hostname	The hostname of 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 virtual appliances 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 flagged up later in the wizard.
Mode	The mode of the network interface. Choose one of the following options: <ul style="list-style-type: none"> static: manually configure the IP address and netmask for the interface. dhcp: use DHCP to automatically obtain network settings for the interface.

Setting	
	<p>To use DHCP with your Traffic Manager deployment, Ivanti recommends that your network infrastructure is configured with long-life IP reservations for each interface in your system. IP address renewal after lease expiry can cause service interruption and communication issues in your Traffic Manager cluster.</p> <p>If you select DHCP for at least one of your interfaces, the Traffic Manager attempts to automatically obtain a default gateway, name server, and search domain from the DHCP service. If successful, the Traffic Manager uses these settings in place of any values entered during the wizard.</p>
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.
Use a single Management IP	<p>Click to restrict management traffic to a single interface. Then click the Management IP radio button next to the interface you want to use.</p> <p>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.</p> <p>If you are cloning a VMware based virtual appliance using guest customization, this feature is disabled on the cloned instances to ensure they remain accessible. For further information, see Cloning and Guest OS Customization.</p> <p>Ivanti 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.</p> <p>To later modify the management IP address, use the System > Traffic Managers page of the Admin UI. Note that a software restart is required for this procedure.</p>

Setting	
Gateway	<p>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.</p> <p>A DHCP service configured to provide a gateway IP address takes precedence over the value manually specified here.</p>

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 Pulse Secure Virtual Traffic Manager: User's Guide.

CAUTION

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

For optimum performance, Ivanti recommends that you use separate interfaces for front and back end traffic. In other words, 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 Pulse Secure Virtual Traffic Manager: User's Guide helpful in planning your network. Additionally, the Pulse Community Web site (<https://community.pulsesecure.net>) contains several articles about configuring your Traffic Manager.

DNS Settings

Use this 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' hostnames rather than IP addresses. This can make subsequent configuration tasks easier.



If you selected DHCP for at least one of your network interfaces, the Traffic Manager attempts to automatically obtain a default gateway, name server, and search domain from the DHCP service. If successful, the Traffic Manager uses these settings in place of any values entered during the wizard.

Initial configuration, step 4 of 8

4. DNS/Search Domain Settings

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.

The Name Server(s) that the appliance will use. Please provide a space separated list of your Name Servers' IP addresses.

Name Servers:

System is currently using '10.62.128.30 10.62.129.32'

The search domains the appliance should use when looking up unqualified hostnames in the DNS.

Search Domain:

System is currently using 'cam.zeus.com brocade.com'

◀ Back

Next ▶

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, or manually enter the hostname to IP mappings, which can be done from the Admin UI (in the "DNS" section of the **System > Networking** page) after you have completed the Initial Configuration wizard.

Hostname Resolution

The Traffic Manager attempts to resolve your chosen hostname to an IP address using the Name Servers specified (or obtained through DHCP). Where the hostname 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:

Initial configuration, step 4 of 8

4. DNS/Search Domain Settings

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.

The Name Server(s) that the appliance will use. Please provide a space separated list of your Name Servers' IP addresses.

Name Servers:

The search domains the appliance should use when looking up unqualified hostnames in the DNS.

Search Domain:

'vtm-01' cannot be resolved using '10.62.128.30, 10.62.129.32'. The traffic manager will not work properly if it is identified by a name that is not resolvable. You can choose to identify this traffic manager with an IP address to fix the problem. If you wish to do this, select an IP address from the list below. Please tick the box before continuing.

Select IP Address

Ignore Warning I understand the traffic manager may not function as expected if I do not use either a resolved hostname/IP address pair or select a specific IP address to use

Select the desired IP address from the drop-down list, or select "None" to force the wizard to set the Traffic Manager name to be the unresolvable hostname. However, you can experience connectivity issues until the hostname successfully resolves to an IP address within your DNS. Read and confirm your acknowledgement of the Ignore Warning message by clicking the checkbox 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.



If you are cloning a VMware based virtual appliance using guest customization, this feature is disabled on the cloned instances. For further information, see [Cloning and Guest OS Customization](#).

Timezone Settings

Use this page to set the time zone for the virtual appliance. This ensures that any logs and diagnostic messages generated by the Traffic Manager have the correct timestamps:

Initial configuration, step 5 of 8

5. Date and Time Settings

Please specify the time settings for this appliance.

Time Zone:

Date:

Time: : :



Some Traffic Manager variants manage the date and time through the host environment. In these circumstances, this step contains only the time zone setting.

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

Admin Password

Use this page to set the password for the admin user. This is the master password that is used when configuring the virtual appliance 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").

Initial configuration, step 6 of 8

6. Security

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.

Enter Password:

Confirm Password:

Pulse Secure vTM Appliances come with a tool pre-installed to help prevent brute-force SSH attacks. This will block remote hosts that have made multiple failed connection attempts for a set time. The specific parameters, including the time spent blocked and the number of permissible failed attempts, can be configured on the Security page when you have completed the initial configuration.

Would you like to enable this tool now?

Enable SSH Intrusion Prevention

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

License Key

The Traffic Manager requires a license key to operate fully. 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 the Initial Configuration Wizard has completed.

Choose either to upload the license key now, to register for flexible licensing using Pulse Secure Services Director, or to skip licensing and instead run the Traffic Manager as the Community Edition (for more details, see [The Community Edition](#)).



Flexible licensing through the Services Director is available only for certain virtualization platforms. This option is marked inactive where it is not applicable.

Initial configuration, step 7 of 8

7. License Key

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

- Upload a license key for this traffic manager
- Register for flexible licensing using **Services Director**
- Skip licensing for now (traffic manager will run as the **Community Edition** until licensing is configured)

Upload a new license key:

Key file: No file chosen

If you need to obtain a license key, please visit the **Pulse Secure vTM website**

Click one of the following options:

- To upload a license key now, click “Upload a license key for this traffic manager” and then click **Choose file** to select a suitable key file from your local workstation. Click **Next** to verify.
- To license this Traffic Manager instance as part of a Pulse Secure Services Director deployment, click “Register for flexible licensing using Services Director” and follow the instructions contained in your Services Director documentation.



To use flexible licensing, make sure you are using Pulse Secure Services Director version 2.4 or later.

- To add a license key later, or to use the Traffic Manager as the Community Edition, click “Skip licensing for now” and then click **Next**.

For information about paid licensing options, contact Pulse Secure Technical Support.

Summary

Before your settings are applied to the virtual appliance, the Initial Configuration wizard displays a summary of the settings you have configured.

Initial configuration, step 8 of 8

8. Summary

You have specified the following network settings:

Management IP address (eth0):	dhcp
eth1:	dhcp
eth2:	10.62.165.99 (netmask 18)
Gateway:	10.62.128.1
Hostname:	vtm-01
Traffic Manager Name IP(Hostname was unresolved):	10.62.136.160
DNS Servers:	10.62.128.30 10.62.129.32
Search Domain:	cam.zeus.com

Your date and time settings are:

Date:	4 October 2017
Time:	03:55:43
Time Zone:	America/Los_Angeles

Additional settings:

SSH Intrusion Protection:	Enabled
License key:	No license key provided

To store these settings, press 'Finish'. To change your settings, press 'Back'.

◀ Back Finish


Review these settings, and in particular the specified network settings, since your virtual appliance 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**.

Initial configuration, finished**Setup finished**

Your traffic manager is now being reconfigured with the settings that you have provided.

Please make a note of the new Administration Server location:

 <https://10.62.142.27:9090/>

It can take up to a minute for the network to adjust to the new settings, so the new Administration Server may not be available immediately. You can log in with the username 'admin' and the password that you chose.

The Traffic Manager presents a page with a link to the new URL of the Admin UI. Ivanti recommends waiting a short period (typically 10 – 30 seconds) before clicking the link, to allow the virtual appliance time to reconfigure its network interfaces. You might also need to reconfigure your computer's network settings so that it can send packets to the IP address of the virtual appliance management interface.

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

Configuring a Virtual Appliance 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 [Using the Initial Configuration Wizard](#).

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

```
z-initial-config
```

Follow the on-screen instructions to proceed.

```
Pulse Secure Virtual Traffic Manager Installation Program  
Copyright (C) 2021, Ivanti, Inc. All rights reserved.
```

```
Welcome to your Pulse Secure Virtual Traffic Manager Appliance
```

```
This application will guide you through the process of setting up  
your Pulse Secure 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 virtual appliance.

Use of this software is subject to the Ivanti Terms and Conditions
of Sale.

Please review these terms, published at
<http://www.pulsesecure.net/support/eula/> before proceeding.

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

Read and accept the Ivanti 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 Pulse Secure Services Director deployment, type "Y" and follow the instructions contained in your Services Director documentation.



To use remote licensing, make sure you are using Pulse Secure Services Director version 2.4 or later.



Flexible licensing through the Services Director is available only for certain virtualization platforms. This option appears only where it is applicable.

Type "N" to license this Traffic Manager directly.

Enter the license key file name, or leave blank for the Community Edition.
Enter 'help' for more information.

License key file:

The Traffic Manager requires a license key to operate fully. 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 your instance.

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 defaults to running as the Community Edition. For further information, see [The Community Edition](#).

For information about paid licensing, contact Pulse Secure Technical Support.

```
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 virtual 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 Managers 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 eth3 eth4 eth5. 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]: y
Would you like to enable DHCP on eth1? Y/N [N]: y
Would you like to enable DHCP on eth2? Y/N [N]: n
```

For each interface, type "Y" to enable DHCP. The Traffic Manager then attempts to obtain address details from the DHCP service in your network. Type "N" to instead specify an IP address and netmask manually.

```
Enter eth2 IPv4 address or 'use_current' to use currently configured IP which is none.  
IP:
```

Type the IP address for the selected interface in dotted quad notation. For example, "192.168.1.101".

```
Enter eth2 netmask or 'use_current' to use currently configured netmask which is none.  
Netmask:
```

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

```
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.



If you selected DHCP for at least one of your network interfaces, the Traffic Manager attempts to automatically obtain a default gateway, as well as name servers and a search domain, from the DHCP service. If successful, the Traffic Manager uses these settings in place of any values entered during this step.

```
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

Ivanti 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 virtual 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 virtual appliance should use when looking up unqualified hostnames.



If you selected DHCP for at least one of your network interfaces, the Traffic Manager attempts to automatically obtain name servers and a search domain from the DHCP service. If successful, the Traffic Manager uses DHCP-derived settings in place of any values entered during this step.

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 virtual appliance hostname is not resolvable, you must use the IP address of a configured network interface as the virtual 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 virtual 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 virtual 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 virtual appliance. Ivanti 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 *Pulse Secure Virtual Traffic Manager: REST API Guide*.

```
You have specified the following settings:
```

```
No license file:          the traffic manager will run as the Community Edition
Hostname:                vtm-01
DHCP enabled on:        eth0 eth1
eth2 IP address:        192.168.1.101
eth2 netmask:           16
Gateway:                192.168.1.1
Management IP:          192.168.1.99
Nameservers:            192.168.1.127 192.168.1.128
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.

Use your management IP address to log in again.

Proceed with configuration? Y/N:

Before you finish, check through the summary to confirm your intended settings. To configure your virtual 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:

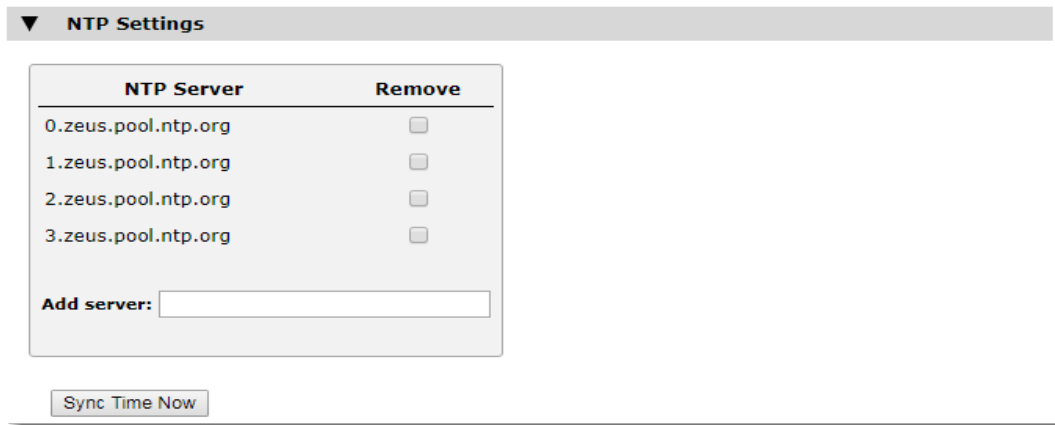
```
z-initial-config --record-to=<replay filename>
```

NTP Settings



This section is not applicable to Xen VA users, where the virtual appliance time is automatically synchronized from the host machine.

Ivanti recommends configuring your virtual appliances to use the Network Time Protocol (NTP) to synchronize their clocks. To do this, visit the **System > Time** page of the Admin UI and set your NTP servers accordingly. By default, the virtual appliance attempts to use the public NTP servers referenced by "pool.ntp.org".



If, for any reason, the time on your virtual appliance differs from the correct time by more than a few minutes, the NTP daemon is not able to adjust the time automatically. To correct the time difference in this case, click **Sync Time Now** on the **System > Time** page.

Traffic Manager virtual appliances also run a local NTP server that listens for NTP (time) requests on all interfaces. You can optionally use the Traffic Manager as a local time source for other servers on your network.

Unexpected time jumps by more than one second trigger a warning message in the Event Log and an SNMP Trap (where configured). Synchronize the time of your virtual appliance if such messages appear.

Upgrading Your Traffic Manager

This section contains details of how to upgrade and, if necessary, revert your Traffic Manager virtual appliance version.

Before You Start

These instructions describe the upgrade and reversion functionality available in version 21.3. For upgrades from an earlier release, use the Upgrading instructions in the Pulse Secure Virtual Traffic Manager: Installation and Getting Started Guide applicable to the former version. Functionality described here might not be present in earlier releases.

CAUTION

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

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

- **Available memory:** The Traffic Manager requires a minimum of 2 GB of RAM to function normally. If the Traffic Manager in question currently has less memory, assign more to the virtual machine before proceeding.
- **Free disk space:** For an upgrade to succeed, a minimum of 2.7 GB must be free on the /logs partition. To confirm your current disk usage, use the **System > Traffic Managers** page of the Admin UI.



Ivanti recommends you backup 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, see the Pulse Community Web site: <https://community.pulsesecure.net>

Upgrading a Cluster of Traffic Managers



This section is applicable to upgrades from version 17.4 and later only. Versions of the Traffic Manager earlier than 17.4 do not contain the cluster upgrade functionality described here. Instead, you must upgrade each cluster member individually. See the documentation applicable to the version you have for more details.

An upgrade initiated on one cluster member can optionally be rolled out to all other cluster members automatically.

To initiate an upgrade, you must first obtain the software package specific to your product variant. For clusters containing two or more Traffic Managers, one of the following scenarios must apply:

- Where a cluster contains Traffic Managers of only one variant (for example, VMware virtual appliances), the uploaded software package is applicable to all Traffic Managers in the cluster. Hence, an upgrade initiated on one Traffic Manager can upgrade all other Traffic Managers in the cluster without further user intervention.
- Where a cluster contains Traffic Managers spanning multiple platforms (for example, a mixed cluster of software instances and virtual appliances), a single uploaded software package applies only to a subset of your cluster. To upgrade all the Traffic Managers in your cluster, obtain software upgrade packages that cover all product variants used. Then, execute an upgrade for each product variant in turn from any cluster member (regardless of that cluster member's host platform).

In the event an upgrade fails on any Traffic Manager in the cluster, the default behavior is to roll-back the upgrade in progress and leave your entire cluster on the previous working software version.




Command line upgrades contain an additional option to not automatically roll-back *all* Traffic Managers in the event of an upgrade failure. You can instead instruct the cluster members which upgraded successfully to remain using the new version, and to only roll-back the Traffic Managers that failed. However, you must not make any configuration changes while your cluster is in a mixed-version state.

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, Ivanti recommends you check your virtual machine settings for any of the following out-of-date configuration values:

Setting		
Virtual Hardware	"VM Version" set to 10 or earlier	Set to 11 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


Setting		
Network Adapter Type	VMXNET or VMXNET2 (Enhanced)	VMXNET3

 If you have configured your virtual appliance with additional network adapters, make sure you update the adapter type for each one.

You must correct all of these settings before performing an upgrade.

To correct your VMware configuration

1. Shut down the virtual appliance.
2. Edit the virtual machine settings.
3. Make your changes according to the values in the table.
4. Save your settings, and restart the virtual appliance.

 If your virtual appliance has several network adapters defined with distinct configuration differences, such as with connections to different virtual networks, deleting and recreating 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.

Performing an Upgrade

Traffic Manager version upgrades involve installation of a new operating system image and a full system restart. To achieve this, the Traffic Manager maintains a secondary disk partition into which the new system 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 virtual appliance.

The previous partition is not deleted, but instead marked as dormant. This dual-partition mechanism facilitates a roll-back capability, should you need to revert to the previous version (see [Reverting to an Earlier Version](#)).



Traffic Manager releases earlier than 18.2 install maintenance releases inside the same partition as the parent release. For example, 17.2r1 and 17.2r2 are installed into the same partition holding feature release 17.2. From version 18.2 onwards, all Traffic Manager upgrades are treated equally, regardless of the type of change being attempted. In other words, each new feature release or maintenance release is installed to the alternate partition.

Only one previous version can be maintained on the virtual appliance in addition to the current version. If you have previously upgraded to a new version, upgrading a further time overwrites the oldest version held. Take note that this operation is permanent – the overwritten version cannot be retrieved after the upgrade is applied.

Before you begin, obtain the relevant Traffic Manager appliance installation package. Packages are named according to the following convention:

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

Perform the upgrade through the Admin UI or from the virtual appliance command line.

To upgrade using the Admin UI

1. Log in to the Admin UI, and click **System > Traffic Managers > Upgrade...**
2. Follow the instructions to upload and apply the upgrade package. Where you are upgrading a cluster of Traffic Managers, select which of your other cluster members should receive the upgrade package (subject to the platform rules in [Upgrading a Cluster of Traffic Managers](#)).

To upgrade using the command line

1. Copy the upgrade package to the virtual appliance using the Linux scp command, or Windows based pscp (<http://www.chiark.greenend.org.uk/~sgtatham/putty/>) or WinSCP (<http://winscp.net/eng/index.php>).

CAUTION

Ivanti recommends the package is copied to the /logs partition to avoid any disk space issues during the upgrade process.

2. Connect to the virtual appliance command line.
3. To upgrade the current Traffic Manager only, run the command:

```
ZEUSHOME/zxtm/bin/upgrade <package_filename> [<args>]
```

To upgrade a cluster of Traffic Managers, run the command:

```
ZEUSHOME/zxtm/bin/upgrade-cluster --package <package_filename> --mode <mode> [<args>]
```

To see the full list of optional arguments available for each command, add the `--help` argument.

For `upgrade-cluster`, `<mode>` is either "info" (just report on the potential upgrade) or "install" (perform the upgrade). Additionally, upgraded cluster members reboot automatically into the new software version by default. To override this behavior, use the option `--no-restart`.

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



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

5. Reboot the virtual appliance when convenient from the Admin UI or command line (type "reboot").

Reverting to an Earlier Version

The upgrade process preserves the previous Traffic Manager version in a separate disk partition to facilitate a reversion capability. To revert to the previous version, use the *Switch Versions* feature in the Admin UI or the *rollback* program from the command line.



This procedure does not retain any configuration you have made since upgrading to the current version. It is strictly a roll-back procedure that reinstates the selected software version and reinstates the previous configuration settings. Therefore, Ivanti strongly recommends that you make a backup copy of your configuration before reverting your virtual appliance.

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



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.

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:



i The Switch Versions section is hidden if there are no applicable versions to revert to.

3. Select a Traffic Manager version to use from the drop-down list.
4. Tick **Confirm** and then click **Rollback** to start the roll back process.

To revert the Traffic Manager to a previous version using the command line

1. Connect to the virtual appliance command line.
2. Ensure you are the root user.
3. Run the command:

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

This starts the rollback program:

```
Rollback
Copyright (C) 2021, Ivanti, 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.
```

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

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

```
Which version of the Traffic Manager would you like to use?
1) 18.2
2) 18.3 (current version)
```

Select a version [2]

5. Select the version 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 version, repeat the rollback procedure and select the newer version to restore. You do not need to reinstall the latest version of the Traffic Manager to achieve this. The change in version is applied permanently; subsequent virtual appliance reboots continue to use the version you select from the rollback program.



For rollbacks to 18.1 or earlier, be aware that if you subsequently decide to roll forward again to version 18.2 or later, the Admin UI "Switch Versions" feature is not supported. Use only the command line rollback program for this purpose.

Changing Your Traffic Manager Version Manually

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



Due to boot menu updates implemented in version 18.2, this process applies only if you want to switch between Traffic Manager versions from 18.2 onwards. For version changes between version 18.2 (or later) and version 18.1 (or earlier), use only the rollback program. For more information, contact Pulse Secure Technical Support.

To edit VMware and Hyper-V based virtual appliances

1. Ensure you have access to the virtual appliance console.
2. Reboot the virtual appliance from the **System > Traffic Managers** page of the Admin UI, or from the console (use the command "reboot").
3. During the reboot process, press Escape when you see the 5-second countdown on the console.
4. Select the required version from the list provided.

To edit Citrix Xen and QEMU/KVM based virtual appliances

1. Log in to the appliance console as the "admin" user.
2. Run the command:

```
grub-set-default <version>
```

where <version> is a string representing an available Traffic Manager release (for example, the string "zeus183" refers to the Traffic Manager 18.3 release). For the list of applicable releases and their associated version string, run the command:

```
/opt/zeus/zxtm/bin/rollback-helper --list-versions
```

3. Type "reboot" at the prompt to reboot your appliance.

Useful System Information

The Community Edition

If your license key expires (or if you actively select it the first time you log in), the Traffic Manager operates in a default state known as the Community Edition. In this state, the Traffic Manager operates normally and with full functionality, but with a bandwidth limit of 10Mb/second and cluster size limit of 4. The Community Edition is designed as a free, production-ready, variant of the Traffic Manager useful for system administrators and application developers wanting to try out advanced vADC (virtual Application Delivery Controller) capabilities in a production environment.

To upgrade the Traffic Manager from the Community Edition to incorporate a full license key, use the **System > Licenses** page of the Admin UI.

Where the Traffic Manager is operating inside a cluster, you must ensure that the proposed license key update is compatible with other fully licensed cluster instances to avoid unintended functionality impairment. Ivanti strongly recommends that you seek advice from your support provider before updating license keys in a mixed cluster of Community Edition and fully-licensed Traffic Managers.

SSH

You normally administer the virtual appliance through the Web-based Admin UI. However, you can also access the Traffic Manager through the console (command line) to access files stored on the system. To do this, use an SSH client to log in to the virtual appliance.

Freeing Up Disk Space

Over time, your appliance can run low on disk space. For example, your system logs can become large if you have configured your Traffic Manager to produce detailed request log information.

The Traffic Manager warns you if disk space is running low through the **Event Log** and **Diagnose > Cluster Diagnosis** page. You can also view disk space usage at any time through the **System > Traffic Managers** page.

To free up disk space, click **Free up some disk space** from the Wizards: drop-down menu in the main tool bar. You can also run the wizard from the "Free Disk Space" link on the **System > Traffic Managers** page at any time, and from the **Diagnose > Cluster Diagnosis** page when a low disk space warning appears.

CAUTION

This operation is irreversible. Make sure you have created a backup of any files you need to keep before running the wizard. Note also that any "Technical Support Reports" you create afterwards contain only those logs generated since the wizard was run.

Changing the Traffic Manager Name

Each Traffic Manager in your cluster uses a DNS resolvable hostname with which it can be identified and contacted by each other cluster member. If you are unable to use a resolvable name, you can instead use a contactable IP address. You set the hostname or IP address during the initial configuration of your Traffic Manager. See [Using the Initial Configuration Wizard](#).

To change the designated Traffic Manager hostname after you have completed the initial configuration, or to instead switch to using an IP address, run the Ivanti Configuration Program from the virtual appliance console:

```
$ZEUSHOME/zxtm/configure
```

This program displays the following options:

```
Ivanti Configuration Program
```

```
Copyright (C) 2021, Ivanti, Inc. All rights reserved.
```

```
This program will perform the initial configuration of the  
Traffic Manager.
```

```
Initial configuration has already been performed on this Traffic Manager installation.
```

1. Quit (default)
2. Perform the post-install configuration again
3. Clear all configuration
- H. Help

Choose option [1]:

Select **Perform the post-install configuration again** and then choose which action you want to perform from the further options provided:

```
Each traffic manager in your cluster must have a unique name,  
resolvable by each member of the cluster.
```

```
This traffic manager is currently called 'stm1.example.com'.  
Would you like to
```

1. Keep the current traffic manager name (default)
2. Specify a new resolvable hostname
3. Use an IP address instead of a hostname

Choose option [1]:

You can also switch to using an IP address from the Replace Traffic Manager Name section on the **System > Traffic Managers** page of the Admin UI. You cannot, however, switch back to using a resolvable name from this page. Instead, rerun `$ZEUSHOME/zxtm/configure` as previously described.

Resetting to Factory Defaults

If you would like to completely reset the virtual appliance back to its unconfigured state, use the following command. Be aware that this command completely erases your existing configuration, including the network configuration and any additional software modules you might have installed (such as the Pulse Secure Virtual Web Application Firewall).

```
z-reset-to-factory-defaults
```

After the virtual appliance has been reset, reconfigure the virtual appliance using the instructions in [Using the Initial Configuration Wizard](#) or [Configuring a Virtual Appliance From the Command Line](#).

Resetting the Admin Password

If you forget the admin user password, you can reset it from the virtual appliance console.

To reset the admin user password

1. Access the virtual appliance host management interface (for example, vSphere Client or XenCenter).

2. Reboot the virtual appliance, "forcefully" if required.
3. Access the virtual appliance console.
4. During startup, press Escape when you see the 5-second countdown.
5. Choose *Recovery mode* from the boot menu and press Enter.
6. At the prompt, enter the following command:

```
z-reset-password
```

7. Follow the instructions to change the password (enter a new admin password twice as directed).
 8. Type the following command to reboot the virtual appliance:
- ```
reboot
```
9. After the virtual appliance reboots, log in to the Admin UI using the username "admin" and your new admin password.



If your virtual appliance is a member of a cluster, the Diagnose page of the Admin UI might report a configuration conflict. Use this page to push the new admin password to the other Traffic Managers in the cluster.

---

# Basic Configuration Information

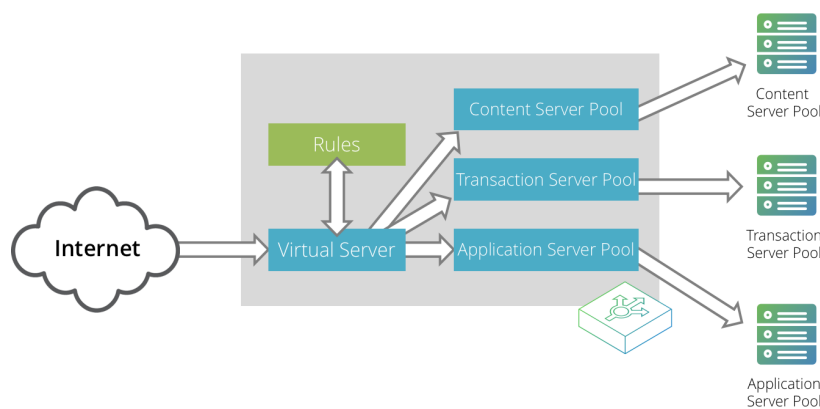
The Traffic Manager receives traffic from the Internet, makes decisions based on the traffic source, destination and content, and chooses a group of back-end servers to handle the traffic. Traffic is balanced across this group according to the network resources.

In a traffic management system, you configure a virtual server object to manage connections from remote clients, and configure a pool object to manage connections to your local servers.

Once 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.

## Virtual Servers, Pools, and Rules

The following figure illustrates the relationship between virtual servers, rules, and pools.



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.

A virtual server listens for and processes incoming network traffic, and typically handles all of the traffic for a certain protocol (for example, HTTP or FTP). In contrast, a virtual server in a Web server typically serves only one website. The Traffic Manager sends traffic to a default pool, although the virtual server first runs through any rules that you have associated with it. Each of these might select a different pool to use depending on the conditions satisfied within the rule. Traffic is balanced across the nodes in the selected pool.

A request rule can do much more than just select a pool. It can read an entire request, inspect and rewrite it, and control how the other traffic management features on the Traffic Manager are used to process that particular request. It can select the pool based on the contents of the request.

Response rules process responses. They can inspect and rewrite responses, control how the response is processed, or even instruct the Traffic Manager to try the request again against a different pool or node.

## Managing Your First Service

To manage your first service

1. Browse to the Admin UI and log in with the username “admin” and your password.
2. The Admin UI home page shows that you have not yet created any pools or virtual servers. From the Wizards drop-down menu, choose Manage a New Service to begin using the wizard.
3. Specify a name that identifies the virtual server, and choose a protocol and port (for example, HTTP and default port 80).
4. Click **Next** to continue.
5. Create a list of backend nodes, which form the default pool for the virtual server.

The nodes are identified by hostname and port. You can modify these later from the **Pools > Edit** page. Make sure that you can serve content directly from the hostname/port combinations you specify here.

6. Click **Next** to display the setting summary page.
7. Review the settings that you have chosen. Click **Back** to make changes or click Finish to set up the service.
8. Test your Traffic Manager setup by browsing to it, using the port you set up for your new service. Use one of the following paths:

```
http://<machine_name>:<port>
```

or

```
http://<ip_address>:<port>
```

9. (Optional) You can observe the traffic handled by the Traffic Manager to verify that the traffic was processed and routed correctly. To do so, click Activity in the Admin UI and select the Connections tab. This page lists connections that the Traffic Manager has recently managed. If the list is empty, reload pages from the Website that the Traffic Manager is managing and check that the connections list is modified accordingly.

You can also use the Current Activity graph to watch the activity of the Traffic Manager in real-time.

## Creating a Traffic Manager Cluster

If you are configuring two or more Traffic Managers in a cluster, first perform the initial configuration process for each instance. Then, before making any other changes, join the instances together to form a cluster using one of the following procedures:

- If you are creating a new Traffic Manager cluster, choose one Traffic Manager as the first cluster member. Log in to the Admin UI on each of the other instances, and use the Join a cluster wizard to join each of these with the first Traffic Manager.
- If you want to join an existing Traffic Manager cluster, log in to the Admin UI on each of the new instances and use the Join a cluster wizard to join each of these to the existing cluster.



In a Traffic Manager cluster, all systems are considered equal. You can access the Admin UI on any of the Traffic Managers. 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 drop down box menu in the tool bar.
2. Step 1 of the Join a cluster wizard requires you to choose whether to scan for existing clusters or manually specify the cluster details.

### Cluster Joining wizard, step 1 of 5

#### 1. Getting Started

This wizard joins your current traffic manager to an existing cluster so that it can share the cluster's configuration and traffic.

Joining a new cluster will remove this traffic manager from its current cluster.

Would you like to select an existing cluster from a list of available clusters on your network, or enter the Administration Server address and port of a specific traffic manager to join?

- Select existing cluster  
 Manually specify host/port

Cancel ◀ Back Next ▶

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

3. Click **Next** to continue.
4. Step 2 reflects the choice you make in step 1. If you clicked "Select existing cluster", the Traffic Manager presents a list of discovered Traffic Manager instances and clusters.

#### Cluster Joining wizard, step 2 of 5

**2. Cluster selection**

Please select the cluster you wish to join:

- Cluster 1: aknox-02.cam.zeus.com:9092
- Cluster 2: apritchard-12.cam.zeus.com:9090
- Cluster 3: coeus.cam.zeus.com:9090
- Cluster 4: fry:9090
- Cluster 5: rkistruck-2b:9090 rkistruck-2d.cam.zeus.com:9090
- Cluster 6: jmoore-01:9090
- Cluster 7: jsteele-00.cam.zeus.com:9090 jsteele-04.cam.zeus.com:9090

Cancel ◀ Back Next ▶

If you clicked "Manually specify host/port", enter your hostname and port number in the boxes provided.

5. Click **Next** to continue.
6. To connect to the specified instance or cluster, first verify the identity of the Traffic Managers within the cluster, and provide the administration credentials used by the cluster.

## Cluster Joining wizard, step 3 of 5

**3. Authentication**

The admin server you are clustering with is using an SSL certificate with the following SHA-1 fingerprint:

**10.62.165.97:9090**  **B6:35:68:29:76:56:15:C0:FF:76  
69:89:DA:30:7A:DB:02:60:2A:89**

▶ **Unfold to view full certificate details ...**

Please check the box beside the fingerprint above to indicate that you have verified it or that you trust the network between it and this system.

If you do not already have this fingerprint on record you can get it by logging into the target admin server and visiting the **System > Security** page. (Refer to the product documentation for further information on cluster security.)

Enter the username and password of a user in the target cluster with permission to add and remove traffic managers.

**Username:**

**Password:**

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

Tick the checkbox next to each Traffic Manager hostname to confirm you trust its identity, and then enter the cluster admin username and password. Click Next to continue.

- 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.

## Cluster Joining wizard, step 4 of 5

**4. Additional Settings**

If the cluster has Traffic IP groups, should the new machine join them?

Yes, and allow it to host Traffic IPs immediately  
 Yes, but make it a passive machine  
 No, do not add it to any Traffic IP groups

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 this situation, 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, it 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.

8. Check your settings in the summary step and then click Finish to join the cluster.

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

To add further Traffic Managers to the cluster, run the Join a cluster wizard on the Admin UI of each Traffic Manager instance you want to add.



When you join a Traffic Manager to an existing cluster, it takes on the entire configuration that the cluster is using, including the administration password you specify during the wizard.

---

Clusters consisting of Traffic Managers on different platforms is possible, although you might find that product capabilities present on one of your cluster members are not present on others. For example, Networking and Time settings are configurable only for certain Traffic Manager variants.



# Open Source Software Notice

This product includes software originating from third parties that are subject to one or more of the following:

- The GNU Library/Lesser General Public License (LGPL)
- The GNU General Public License (GPL)
- The Berkeley Software Distribution (BSD) License
- The OSI Artistic License
- Various GPL/BSD-like Distribution Licenses

All applicable third party software packages and accompanying licenses are listed in the Pulse Secure Virtual Traffic Manager: User's Guide and in the Pulse Secure Virtual Traffic Manager: Appliance License Acknowledgements, available from the Traffic Manager product pages on the Ivanti Web site.

Ivanti, Inc offers to provide a complete copy of the source code for the software under said licenses on a CD-ROM, for a charge covering the cost of performing such distribution, such as the cost of media, shipping, and handling, upon written request to Ivanti, Inc at the following address:

Source Code Requests VTM-APPLIANCE (GPL)

Ivanti, Inc

The Jeffreys Building

Cowley Road

Cambridge

CB4 0DS

United Kingdom

This offer is valid for a period of three (3) years from the date of the distribution of this product by Ivanti, Inc. Please refer to the exact terms of the appropriate license regarding your rights.