Pulse Secure

Pulse Secure Virtual Traffic Manager: Software Installation and Getting Started Guide

Supporting Pulse Secure Virtual Traffic Manager 20.1

Product Release	**20.1**
Published	**16 March, 2020**
Document Version	**1.0**

Pulse Secure, LLC
2700 Zanker Road,
Suite 200 San Jose
CA 95134

www.pulsesecure.net

Pulse Secure Virtual Traffic Manager: Software Installation and Getting Started Guide

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

Contents

Preface

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Pulse Secure 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
italic text	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.
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.

Convention	Description
{ **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.

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

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

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

Requesting Technical Support

Technical product support is available through the Pulse Secure 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, Pulse Secure 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.pulsesecure.net/techpubs

- 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). This chapter contains the following sections:

About This Guide

The *Pulse Secure Virtual Traffic Manager: Software Installation and Getting Started Guide* describes the software variant of the Traffic Manager.

Read this guide for an introduction to the functionality available in the Traffic Manager software variant, and for instructions on how to install and configure the Traffic Manager on supported Linux and UNIX operating systems.

For a detailed description of the Traffic Manager and it's full feature set, see the *Pulse Secure Virtual Traffic Manager: User's Guide*.

Introducing the Traffic Manager

The Traffic Manager product family provides high-availability, application-centric traffic management and load balancing solutions in a range of software, hardware-ready, virtual appliance, and cloud-compute product variants. 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.

FIGURE 1   A Typical Cluster Configuration
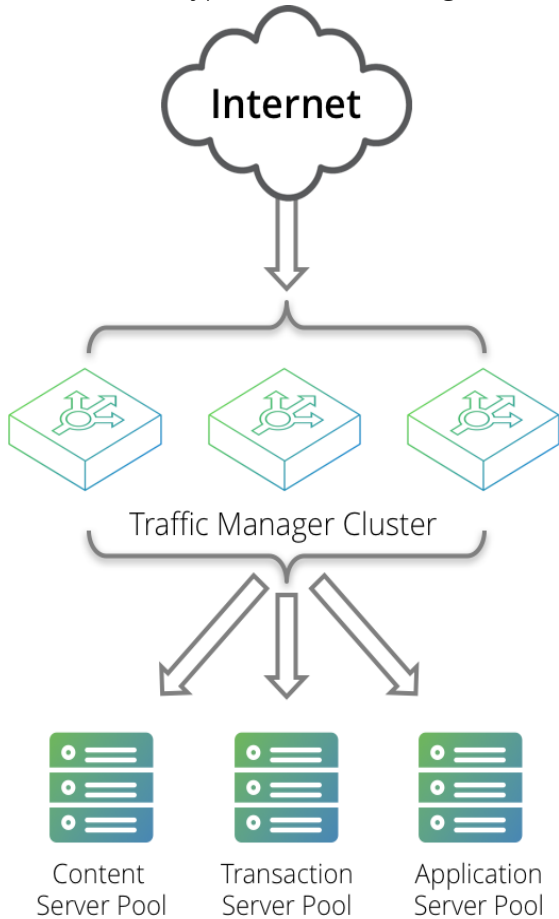
Product Variants

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). Pulse Secure 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.

Pulse Secure 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. This chapter contains the following sections:

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.

FIGURE 2   Simple Traffic Management Topology
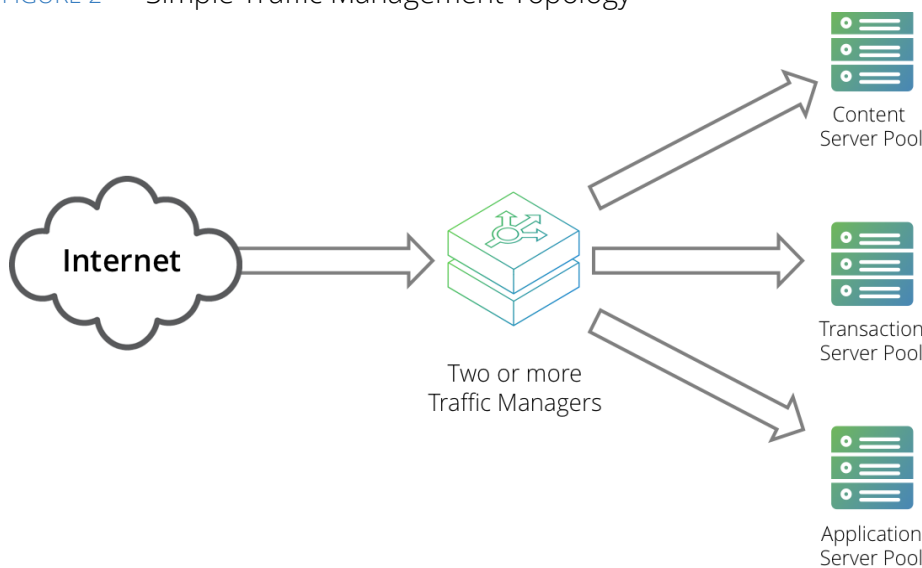
You can install two or more Traffic Managers in a clustered configuration to provide full fault-tolerance for individual software failures. A typical configuration contains at least two Traffic Managers, and at least two servers hosting the load-balanced application.

Prerequisites

Before you begin the installation of your Traffic Manager software, make sure you have the correct software version for your operating system and suitable license keys for each Traffic Manager instance you want to install.

Verify also that your installation target host systems conform to the following:

- The correct IP addresses are configured and raised automatically at boot time.

- All hosts can ping each other on the configured IP addresses.

- All hosts can route traffic to external networks.If you plan to use a separate management network, make sure it is correctly configured and that all hosts can communicate with each other and with your own management Web browser across this network.

Note: Traffic IP addresses automatically raised by the Traffic Manager should not be raised by the operating system. For more information on Traffic IP addresses, see the *Pulse Secure Virtual Traffic Manager: User's Guide*.

You administer all Traffic Manager variants through a Web-enabled user interface known as the Admin UI. Host firewall programs or similar traffic restriction mechanisms might initially be configured to deny access to the port used by the Admin UI (by default, TCP port 9090). Before you can configure the Traffic Manager, ensure you have enabled access to this port, and any other ports necessary to your requirements. See the *Pulse Secure Virtual Traffic Manager: User's Guide* for full information on the ports used by the Traffic Manager.

The Traffic Manager Admin UI supports the following browsers:

- Internet Explorer: v.11 or newer

- Microsoft Edge: latest version

- Mozilla Firefox: latest version

- Apple Safari: latest version

- Google Chrome: latest version

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

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

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

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).

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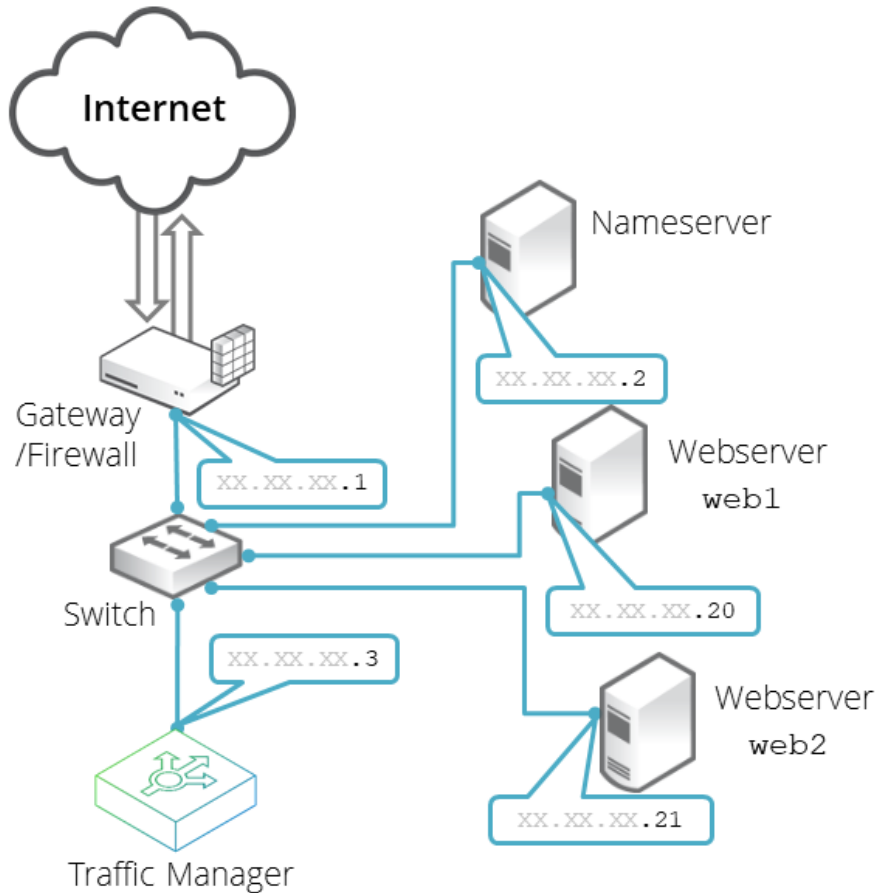
By installing a Traffic Manager, configured to receive traffic over a single network port and IP address xx.xx.xx.3, you can alter your DNS record to instead direct clients to xx.xx.xx.3. In this way, the Traffic Manager receives the Web page requests and responds with content from one of the available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

FIGURE 4   Using the Traffic Manager to separate a public network from a private network
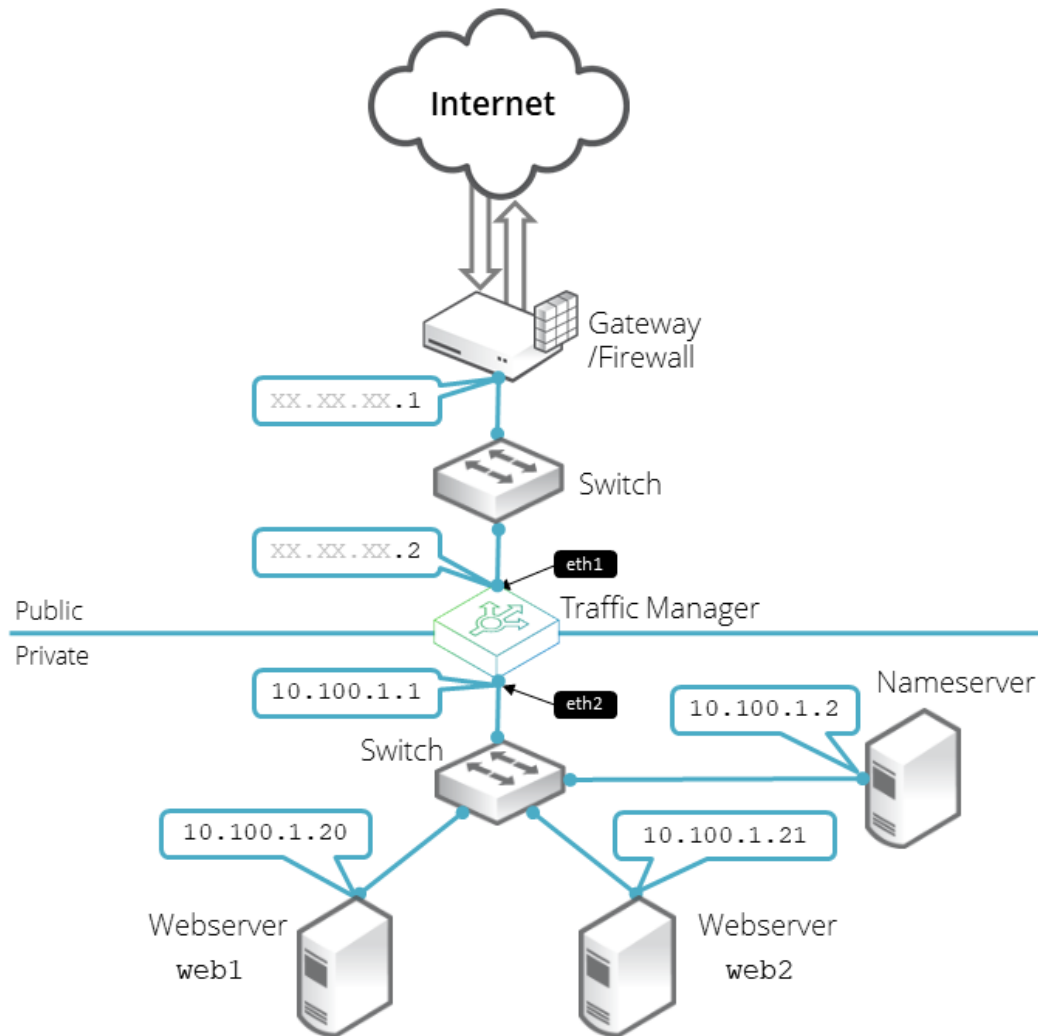
Scenario 3: Multiple Traffic Managers

This scenario deploys two Traffic Managers in a public/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*.

FIGURE 5   Using multiple Traffic Managers in fault-tolerant mode
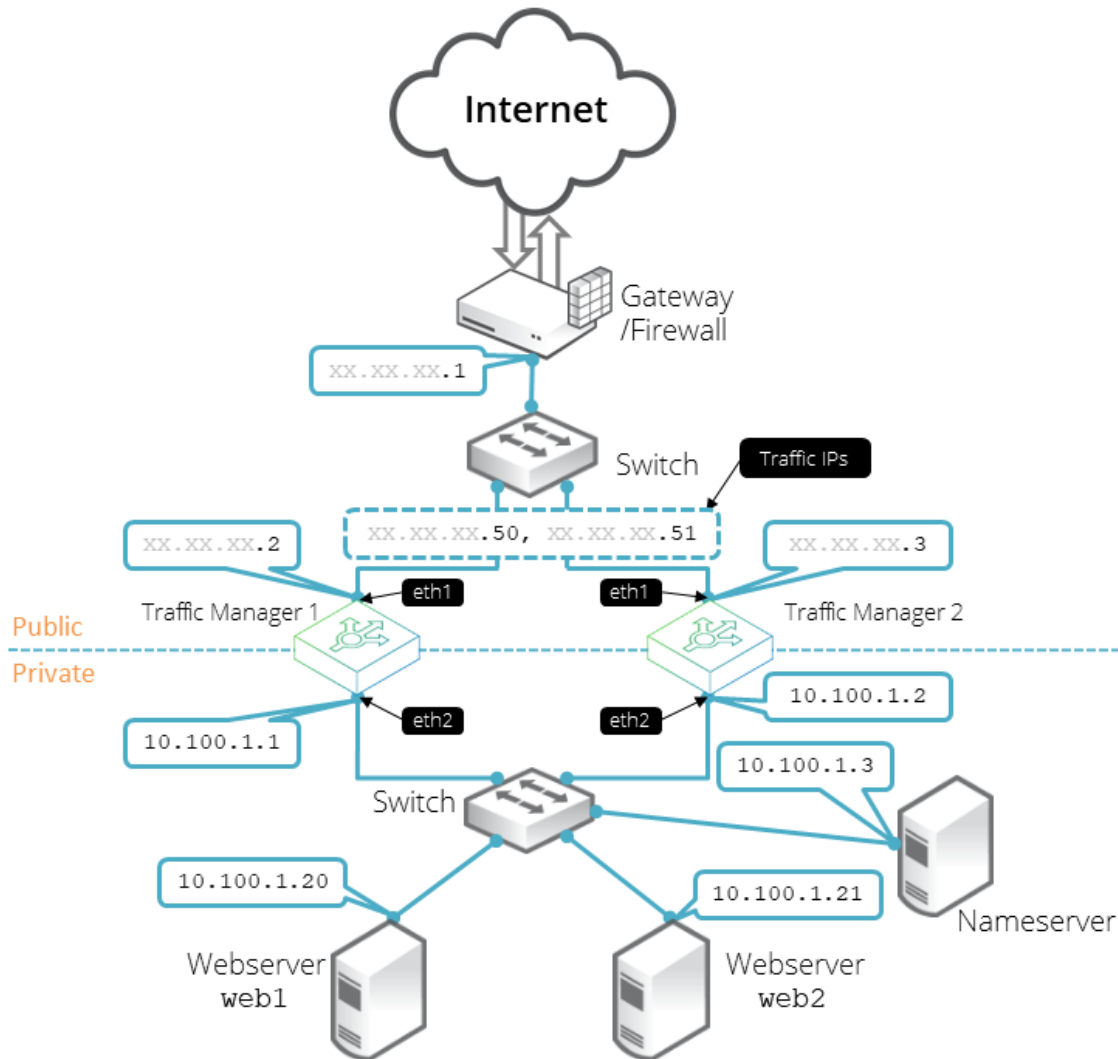
Management Network

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 Software

This chapter documents how to install the Traffic Manager software on a valid supported Linux or UNIX platform.

You can find instructions for Amazon EC2-based software installations in the *Pulse Secure Virtual Traffic Manager: Cloud Services Installation and Getting Started Guide*, available from the Pulse Secure Web site at http://www.pulsesecure.net.

It contains the following sections:

Note: Before you begin, make sure you have met the requirements listed in "Prerequisites" on page 7.

Traffic Manager Software Space Requirements

The Traffic Manager software requires approximately 250 MB of disk space during installation. After installation, clear the intermediate directory created when the compressed file was unpacked, so that the software takes up approximately 100 MB.

Unpacking the Traffic Manager Software Download File

The Traffic Manager software is distributed as a compressed tar archive directory. The software download file is called ZeusTM_ProductVersion_OS.tgz, where ProductVersion is the version number and OS is the operating system where the software is to be installed.

Decompress and extract the files contained in this archive directory to a temporary directory using your system gzip and tar tools. Use the following command:

```
$ gzip -dc ZeusTM_ProductVersion_OS.tgz | tar -xvf -
```

This command unpacks the archive directory and creates a new destination directory for the installation files. As it does so, it displays the name of each extracted file.

Installing the Traffic Manager Software

Note: The Traffic Manager software must be installed, configured and started as root. Root privileges are necessary to bind to ports lower than 1024 (for example, port 80 for HTTP) and to provide front-end fault tolerance.

To install the Traffic Manager software

1. Become the system superuser (also known as the "root" user). For instructions on how to become the superuser, see your host operating system documentation.

2. Change directories to the directory to where the tar archive was extracted (for example, ZeusTM_ProductVersion_OS).

3. Start the installation program (zinstall) by using the following command:

```
# ./zinstall
You are installing a package built for Linux-x86_64

Pulse Secure Installation Program - Copyright (C) 2020, Pulse Secure, LLC. All rights
reserved.

Checking distribution ... all packages match checksums
```

Note: Installing the software on an EC2-based Linux machine sends a request to the host instance for the EC2-specific parameters.

4. Read the Pulse Secure End User License Agreement. If you agree with these terms, type **accept** at the prompt.

5. When prompted, specify a destination directory for the Traffic Manager software or use the default destination directory (/usr/local/zeus).

   You can install the Traffic Manager software anywhere on your file system, but you must not install it in the same directory as any other Traffic Manager products. The Traffic Manager software installation directory is called $ZEUSHOME.

Note: The Traffic Manager Admin UI accesses the configuration and stores state information and lock files under the $ZEUSHOME directory. Pulse Secure strongly recommends that you locate $ZEUSHOME on a local file system with sufficient disk space, or on a fast, reliable, shared file system. The Traffic Manager Admin UI might be slow or unresponsive if the file system it uses is slow or unresponsive.

   After you specify the destination directory, the following messages appear:

```
Pulse Secure Virtual Traffic Manager is now installed in /usr/local/zeus.
Are you ready to perform the initial configuration now ? (Y/N) [Y]:
```

6. Type **Y** to run the configuration script now, or type **N** to run it later.

7. Press Enter.

Performing an Unattended Traffic Manager Software Installation

In some situations, (for example, when rebuilding multiple machines) you may want to automate the installation of the Traffic Manager software. The zinstall script can record specific installation options to a replay file, and then use those options when installing the Traffic Manager software on a another machine.

To perform an unattended Traffic Manager software installation

1. To create a replay file, add the --record-to option to the zinstall script command, as shown below:

```
# ./zinstall --record-to=vtm_install.txt
```

Note: When prompted to run the configuration script, you must answer No. Otherwise, a replay file is not created. The installation and configuration steps have to be recorded and replayed separately.

2. To reuse the installation options, add the --replay-from option to the command, as shown below:

```
# ./zinstall --replay-from=vtm_install.txt
```

This command runs the zinstall script using the answers you provided in the replay file. For any unanswered questions, the zinstall script pauses until an answer is provided. To stop the zinstall script, enter the --noninteractive option at the command line.

You can also run the configure script automatically using the same method. Be aware that passwords appear in plain text inside the replay file. However, passwords are not printed in the output of the configure program.

Note: You can delete the password line in a newly generated replay file. You will prompted for the password later (unless you specified the --noninteractive option at the command line).

Configuring the Traffic Manager Software

This chapter describes how to configure a newly installed Traffic Manager software instance. It assumes you have already performed the installation procedure described in "Installing the Traffic Manager Software" on page 13

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

It contains the following sections:

Configuring the Traffic Manager Software

Before you can start the Traffic Manager and use the Web-based Admin UI, you must first run the configure script. The configure script handles the initial settings that must be in place before the software can start. These initial settings include creating passwords and choosing whether the Traffic Manager is a standalone instance or is included in aTraffic Manager cluster.

You can run the configure script at any time to change settings, or to restore your Traffic Manager to its unconfigured state.

Note: You must rerun the configure script whenever the name of the host virtual machine changes.

You can also run the configure script as part of an unattended (automated) installation process. For more information, see "Performing an Unattended Traffic Manager Software Installation" on page 14.

To run the configure script

1. If you are installing the Traffic Manager, the zinstall script prompts you to complete the initial configuration.

    Alternatively, you can complete the initial configuration directly by becoming the system superuser and typing the following at the command line:

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

    To become the system superuser (also known as the "root" user), see your host operating system documentation.

2. If this is a first time configuration, or a reconfiguration following a factory reset, you must agree to the Pulse Secure Terms and Conditions of Sale to continue, available from the URL shown. Read the agreement fully, then type **accept** at the prompt to confirm you agree with its terms. The configuration process stops if you do not accept the license agreement.

3. Enter the full path and file name of your license key. If you do not have a license key, you can leave this entry blank. License keys can also be added to your Traffic Manager through the Admin UI at any time after the script has completed.

   If you do not enter a license key, the Traffic Manager defaults to running as the Community Edition. For further information, see "The Community Edition" on page 20.

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

4. For new installations only, specify a UNIX user and group to run the Traffic Manager. Although the Traffic Manager must be configured and started as a root user, the Traffic Manager can be run as any user. Pulse Secure strongly recommends that you specify a user with no privileges, to avoid compromising the Traffic Manager's system security.

   The default user with no privileges is typically called "nobody" and the default group with no privileges is typically "nogroup" or "nobody", depending on which version of Linux or UNIX you are using. If you have set up other users and groups on the Traffic Manager host machine, specify them here.

5. Decide whether or not to restrict the software's internal management traffic to a single IP address. Management traffic includes access to the Traffic Manager Admin UI, external API access, and internal communications within a Traffic Manager cluster.

   If you decide to restrict the software's internal management traffic to a single IP address, you must specify the IP address. The Traffic Manager you are configuring accepts management traffic destined to this IP address only. Typically, this IP address would reside on a private or dedicated management network.

Note: You should only choose to use a single IP address for the internal traffic management traffic if you have a dedicated, reliable management network. Each IP address is a single point of failure for an entire Traffic Manager cluster; all IP addresses must always be available.

   If you intend to use a single IP address for the internal management traffic, and are running on a Linux host, Pulse Secure strongly recommends using the Linux kernel 2.6.12 or later. Earlier 2.6 Linux kernels cannot reliably restrict multicast or heartbeat messages to a single network card.

   To later modify the management IP address, either rerun the configure script or use the **System > Traffic Managers** page of the Admin UI. A software restart is required for this procedure.

6. If your DNS system cannot successfully resolve your hostname, you must use an IP address to identify the Traffic Manager to other cluster members. When prompted, enter **Y** to specify the IP address to use. If you have elected to restrict management traffic to a single IP address, this IP address is automatically selected. Entering **N** forces the software to use the unresolvable hostname, which could result in connectivity issues until the hostname is resolved.

7. Decide if you want the software to start automatically when the Traffic Manager restarts.

8. Specify a cluster for the Traffic Manager to join.

If this is the first Traffic Manager you are setting up, you are given the following choices:

```
Searching for Pulse Secure Virtual Traffic Manager clusters ... done

Which Pulse Secure Virtual Traffic Manager cluster should this installation be added
to?

C)  Create a new cluster
S)  Specify another machine to contact
R)  Refresh the cluster list

Select C to create a new cluster.
```

However, if you have already set up one or more other Traffic Managers, you are given the following additional choices:

```
C)  Create a new cluster
1)  Cluster 1: vtm1.mysite.com:9090
             vtm2.mysite.com:9090
2)  Cluster 2: vtm-test.mysite.com:9091
S)  Specify another machine to contact
R)  Refresh the cluster list
```

Note: To provide front-end fault tolerance, your Traffic Managers must be in the same cluster. The new Traffic Manager automatically shares the configuration settings already chosen for the cluster.

9. If you are creating a new cluster, specify a password for the admin server. The admin server provides the Web-based Admin UI and handles communications with the core Traffic Manager software. The password specified is used for the admin user when accessing the Admin UI of your Traffic Manager.

10. If you choose to join an existing cluster, verify the identity of the other cluster members. The host:port and SHA-1 fingerprint of each instance are displayed as shown:

```
Select option [C] : 1

Joining the cluster containing the following admin servers:

            Host:Port   SHA-1 Fingerprint
   vtm1.mysite.com:9090  72:BC:EE:A1:90:C6:1B:B6:6E:EB
   vtm2.mysite.com:9090  E9:61:36:FE:0B:F5:0A:E4:77:96

Have you verified the admin server fingerprints, or do you trust the network between
this machine and the other admin servers? Y/N [N]:
```

11. If the identities are accurate, type **Y** and specify the cluster administrator username and password. This is the user account used to access the Admin UI of each Traffic Manager in the cluster.

The Traffic Manager starts and the installer displays the following information:

```
**
** The SHA-1 fingerprint of the admin server's SSL certificate:
**   09:0F:B6:24:59:AE:CF:03:61:A2:DB:83:DB:DE:42:00:D8:2D:63:29
** Keep a record of this for security verification when connecting
** to the admin server with a web browser and when clustering other
** Pulse Secure Virtual Traffic Manager installations with this one.
**
```

```
** To configure the Pulse Secure Virtual Traffic Manager, connect to the admin server
at:
**   https://yourmachinename:port/
** and login as 'admin' with your admin password.
**
```

Note: Note the URL shown, as you need it to administer the Traffic Manager software. Also notice that the protocol is HTTPS (secure HTTP).

You can rerun the configuration script at any time to change settings or to restore your Traffic Manager to it's unconfigured state. For more information, see "Reconfiguring or Uninstalling the Traffic Manager Software" on page 21.

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.

Note: 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. Pulse Secure 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.

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 command line after you finish using the configure script and have completed the installation. The SHA-1 fingerprint is useful for the following purposes:

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

Note: When you set up a new Traffic Manager, Pulse Secure 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
```

Starting and Stopping the Traffic Manager Software

When you set up the Traffic Manager for the first time, the Traffic Manager software starts automatically after the initial configuration has been performed.

To manually shut down the software, type the following command at the host command line (as the root user):

```
$ZEUSHOME/stop-zeus
```

To start the software again, use the following command:

```
$ZEUSHOME/start-zeus
```

Reconfiguring or Uninstalling the Traffic Manager Software

The `configure` script is a utility that allows you to clear your Traffic Manager software configuration (and then reconfigure the software) or uninstall (remove) the Traffic Manager software entirely from the virtual machine.

To reconfigure the Traffic Manager software, see "Reconfiguring the Traffic Manager Software" on page 21.

To uninstall the Traffic Manager software, see "Uninstalling the Traffic Manager Software" on page 23.

Note: You can rerun the configure script at any time to change any or all of the settings you chose initially; or you can use the configure script to completely remove the software from your virtual machine (along with any clusters in which it was a member) before clearing the installation files from your machine.

Reconfiguring the Traffic Manager Software

To reconfigure the Traffic Manager software

1. Log in as the system superuser and run the configure script from the host machine command line:

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

   For instructions on how to become the system superuser, see your host operating system documentation.

   The Traffic Manager determines that your software has been previously configured and the following options display:

   ```
   Pulse Secure Configuration Program
   Copyright (C) 2020, Pulse Secure, LLC. All rights reserved.

   This program will perform the initial configuration of the
   Pulse Secure Virtual Traffic Manager.

   Initial configuration has already been performed on this
   Pulse Secure Virtual Traffic Manager installation.

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

```
H. Help

Choose option [1]:
```

2. To rerun the Traffic Manager configuration, type **2**. Each previously set value is displayed, allowing you to selectively make changes as applicable.

3. To clear your existing configuration and stop the software, type **3**. This resets the Traffic Manager to the unconfigured state (that is, the state it was in at the completion of the zinstall script). To reconfigure the Traffic Manager, run the configure script again (option 2), if necessary.

Note: Clearing your configuration stops the Traffic Manager from handling traffic. Pulse Secure recommends you make sure this does not impact your external service availability.

Changing the Traffic Manager Name

Each Traffic Manager in your cluster uses a DNS resolvable name with which the Traffic Manager can be identified and contacted by each member of the cluster. If you are unable to use a resolvable name, you can use an IP address instead. You set this name or IP address when you initially configure the Traffic Manager.

To change the Traffic Manager name (or assign an IP address)

1. Log in as the system superuser and run the configure script from the host machine command line:

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

   For instructions on how to become the system superuser, see your host operating system documentation.

2. Type **2** to perform the post-install configuration again.

3. Choose the action you want to perform from the options listed below:

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

   This Traffic Manager is currently called 'vtm1.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]:
   ```

4. Press Enter.

Note: 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 to using a resolvable name from this page. Instead, rerun the configure script as described in "Reconfiguring the Traffic Manager Software" on page 21.

Uninstalling the Traffic Manager Software

To completely uninstall (that is, remove entirely) the Traffic Manager software from your host machine, complete the following steps:.

To uninstall the Traffic Manager software

1. Login as the system superuser, and enter the following command at the command line:

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

    For instructions on how to become the system superuser, see your host operating system documentation.

2. Choose option 3 to completely remove the Traffic Manager software from the host machine.

    The configuration for this Traffic Manager is removed. The Traffic Manager is no longer a member of a Traffic Manager cluster, and the Traffic Manager is not usable until you run the configuration program and the initial configuration script again.

3. Delete the $ZEUSHOME directory (the directory in which the software was installed).

Upgrading Your Traffic Manager

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

These instructions describe the upgrade and reversion functionality available in version 20.1. 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.

Note: Pulse Secure recommends you backup your configuration as a precaution before upgrading the 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

Note: This section is applicable to upgrades from version 17.4 and later only.

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 operating system. 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, the software edition), 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 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.

Note: 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.

Performing an Upgrade

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

```
ZeusTM_<version>_<OS>.tgz
```

where <version> is the Traffic Manager version and <OS> is the Operating System platform identifier.

Perform the upgrade through the Admin UI or from the 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" on page 23).

To upgrade using the command line

1. Copy the upgrade package to the Traffic Manager host 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).

2. Using ssh (Linux) or putty (Windows), login to your Traffic Manager machine as the system superuser. For instructions on using the system superuser (also known as the "root" user), see your host operating system documentation.

3. Change directories to the directory where you copied the installation package file.

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

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

In the above command syntax, <package_filename> refers to the upgrade package file in .tgz format, and <mode> is one of "info" (just report on the potential upgrade) or "install" (perform the upgrade). For full details of this command and all optional arguments, use the --help argument.

Alternatively, to upgrade the current Traffic Manager only, extract the contents of the tgz file by running the following command:

```
gzip -dc ZeusTM_<Version>_<OS>.tgz | tar –xvf –
```

Then, run the following command in the extracted directory:

```
./zinstall
```

5. Your Traffic Manager software is automatically stopped, upgraded, and restarted, while retaining its current configuration.

Note: When upgrading the software through the Admin UI from a significantly older version of the software, for example 4.2, you might see warning messages such as:

SERIOUS:monitors/SIP UDP: Unknown monitor scope: sip
SERIOUS:monitors/RTSP: Unknown monitor scope: rtsp
WARN:monitors/SIP UDP: Line 1: Unknown config key

These messages come from the older version of the software and warn you about the incompatibility with RTSP/SIP monitors of the newer version. The messages can be safely ignored.

For further information relating to upgrades and warnings, see the release notes provided with your software.

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.

Note: 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, Pulse Secure strongly recommends that you make a backup copy of your configuration before reverting your appliance.

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

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

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:

Switching Traffic Manager versions
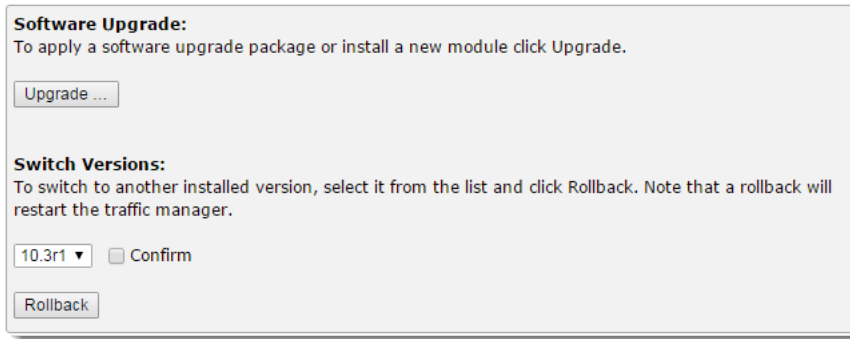
Note: The Switch Versions section is hidden if there are no applicable versions to revert to.

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. Using ssh (Linux) or putty (Windows), log in to your Traffic Manager machine as the system superuser.

    To become the system superuser (also known as the "root" user), see your host operating system documentation.

2. Run the command:

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

    This starts the rollback program:

    ```
    Rollback
    Copyright (C) 2020, Pulse Secure, LLC. 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]:
    ```

3. 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]
    ```

4. Select the version you want to restore, and press Enter.

5. 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.

Note: 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.

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.
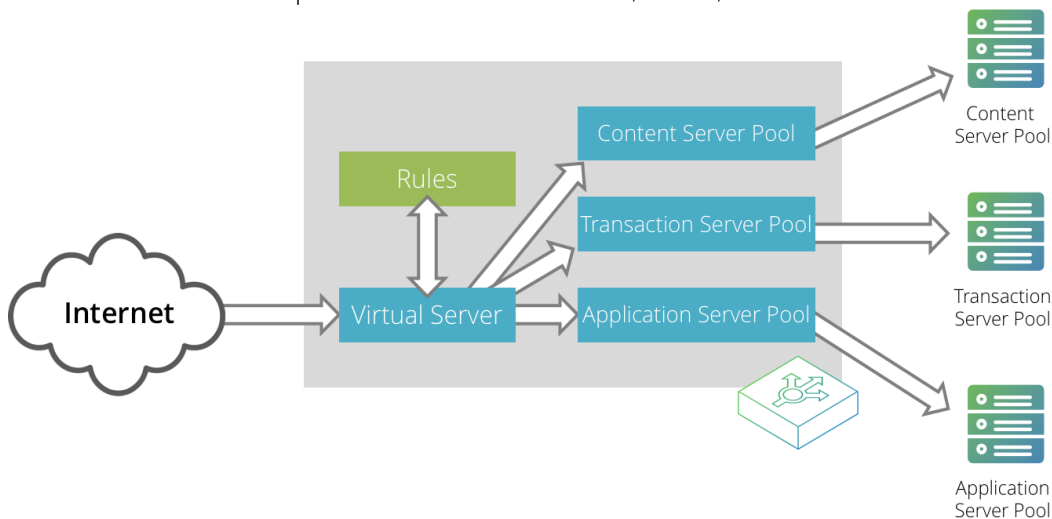
This chapter descibes the basic Traffic Manager configuration and contains the following sections:

Virtual Servers, Pools, and Rules

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

FIGURE 7   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.

Note: 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 manu 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.

FIGURE 8   Getting Started with the cluster joining wizard
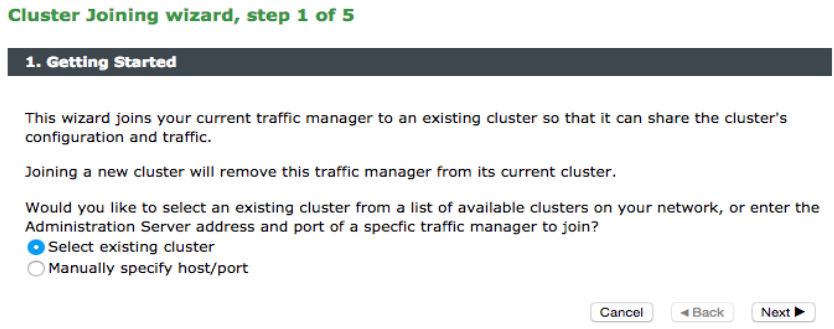
To instruct the Traffic Manager to automatically scan the network for contactable Traffic Managers, click "Select existing cluster". Alternatively, to enter a specific hostname and port you want to join, click "Manually specify host/port".

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.

FIGURE 9   Select an existing Traffic Manager cluster to join

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.

FIGURE 10   Authenticating 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: admin
Password: •••••

[Cancel] [◄ Back] [Next ►]

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 it's identity, and then enter the cluster admin username and password. Click Next to continue.

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

FIGURE 11   Assigning Traffic IP Group Membership
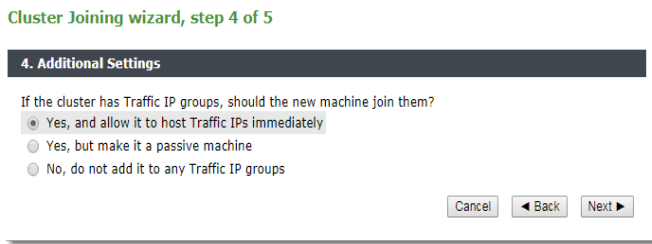
To add the Traffic Manager to existing Traffic IP groups, click "Yes, and allow it to host Traffic IPs immediately". However, this can result in a number of connections being dropped at the instant the new Traffic Manager is added to the Traffic IP group, because allocations of traffic need to be transferred to the new Traffic Manager.

To avoid 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 option ensures that the Traffic Manager does not accept any traffic until another member of the group fails.

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

Click Next to continue.

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.

Note: 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 Pulse Secure Web site.

Pulse Secure, LLC 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 Pulse Secure, LLC at the following address:

> Source Code Requests VTM-APPLIANCE (GPL)
>
> Pulse Secure, LLC
>
> 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 Pulse Secure, LLC. Please refer to the exact terms of the appropriate license regarding your rights.