



Pulse Secure Virtual Traffic Manager: Cloud Services 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

© 2020 by Pulse Secure, LLC. All rights reserved.

Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Pulse Secure Virtual Traffic Manager: Cloud Services Installation and Getting Started Guide

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

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at <http://www.pulsesecure.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Contents

PREFACE	1
DOCUMENT CONVENTIONS	1
TEXT FORMATTING CONVENTIONS.....	1
COMMAND SYNTAX CONVENTIONS.....	1
NOTES AND WARNINGS.....	2
REQUESTING TECHNICAL SUPPORT	2
SELF-HELP ONLINE TOOLS AND RESOURCES.....	2
OPENING A CASE WITH PSGSC	3
OVERVIEW	5
ABOUT THIS GUIDE.....	5
INTRODUCING THE TRAFFIC MANAGER.....	5
PRODUCT VARIANTS	6
GETTING STARTED.....	7
NETWORK ARCHITECTURE	7
PREREQUISITES.....	8
ADDITIONAL PREREQUISITES FOR AMAZON EC2.....	8
ADDITIONAL PREREQUISITES FOR MICROSOFT AZURE	9
ADDITIONAL PREREQUISITES FOR GCE	9
SUPPORT FOR AMAZON VPC	10
INSTALLING THE TRAFFIC MANAGER SOFTWARE ON EC2 OR GCE	11
TRAFFIC MANAGER SOFTWARE SPACE REQUIREMENTS.....	11
UNPACKING THE TRAFFIC MANAGER SOFTWARE DOWNLOAD FILE	11
INSTALLING THE TRAFFIC MANAGER SOFTWARE	12
PERFORMING AN UNATTENDED TRAFFIC MANAGER SOFTWARE INSTALLATION	13
CONFIGURING THE TRAFFIC MANAGER SOFTWARE	13
ADMINISTRATION USER INTERFACE AUTHENTICATION.....	16
UPGRADING THE TRAFFIC MANAGER SOFTWARE	16
UPGRADING A CLUSTER OF TRAFFIC MANAGERS.....	17
PERFORMING AN UPGRADE	17
REVERTING TO AN EARLIER VERSION	18
RECONFIGURING OR UNINSTALLING THE TRAFFIC MANAGER SOFTWARE.....	20
RECONFIGURING THE TRAFFIC MANAGER SOFTWARE.....	20
UNINSTALLING THE TRAFFIC MANAGER SOFTWARE	21

CREATING A TRAFFIC MANAGER INSTANCE ON AMAZON EC2.....	23
BEFORE YOU BEGIN	23
USING IAM ROLES	25
ADDING A PORT TO THE DEFAULT SECURITY GROUP	26
LAUNCHING A VIRTUAL MACHINE INSTANCE	27
CONNECTING TO THE ADMIN UI	28
CONFIRMING THE TRAFFIC MANAGER'S IDENTITY	29
USING THE INITIAL CONFIGURATION WIZARD	29
ENTERING THE ADMIN USER PASSWORD	30
ACCEPTING THE LICENSE AGREEMENT.....	31
SETTING THE DATE AND TIME	31
SETTING SYSTEM SECURITY.....	32
PROVIDING A LICENSE KEY.....	32
VIEWING THE SUMMARY PAGE.....	33
CONFIGURING AN INSTANCE FROM THE COMMAND LINE	35
PERFORMING AN UNATTENDED CONFIGURATION.....	37
REMOVING AN INSTANCE	38
PRECONFIGURING THE TRAFFIC MANAGER AT LAUNCH TIME	38
UPGRADING YOUR TRAFFIC MANAGER.....	40
BEFORE YOU START.....	40
PERFORMING AN UPGRADE	41
UPGRADING USING THE REPLACE-AND-TERMINATE METHOD.....	43
UPGRADING AN EC2 CLUSTER USING THE BACKUP AND RESTORE METHOD	44
REVERTING TO AN EARLIER VERSION	45
CHANGING YOUR TRAFFIC MANAGER VERSION MANUALLY	47
EXPANDING THE LOG FILE PARTITION.....	47
 CREATING A TRAFFIC MANAGER INSTANCE ON GOOGLE COMPUTE ENGINE.....	49
BEFORE YOU BEGIN	49
LAUNCHING A VIRTUAL MACHINE INSTANCE.....	51
CONNECTING TO THE ADMIN UI	53
CONFIRMING THE TRAFFIC MANAGER'S IDENTITY	54
USING THE INITIAL CONFIGURATION WIZARD	54
ENTERING THE ADMINISTRATOR PASSWORD.....	55
ACCEPTING THE LICENSE AGREEMENT.....	55
SETTING THE DATE AND TIME	56
SETTING SYSTEM SECURITY.....	56
UPLOADING THE LICENSE KEY.....	57
VIEWING THE SUMMARY PAGE.....	58
CONFIGURING AN INSTANCE FROM THE COMMAND LINE	58
PERFORMING AN UNATTENDED CONFIGURATION.....	61

REMOVING AN INSTANCE	61
UPGRADING YOUR TRAFFIC MANAGER	61
BEFORE YOU START	61
PERFORMING AN UPGRADE	62
UPGRADING A CLUSTER USING THE BACKUP AND RESTORE METHOD	64
REVERTING TO AN EARLIER VERSION	65
CHANGING YOUR TRAFFIC MANAGER VERSION MANUALLY	66
EXPANDING THE LOG FILE PARTITION	67
CREATING A TRAFFIC MANAGER CLUSTER ON MICROSOFT AZURE	69
BEFORE YOU BEGIN	69
CREATING A TRAFFIC MANAGER CLUSTER IN THE AZURE PORTAL	69
CONFIGURING YOUR RESOURCE GROUP TO USE MORE THAN ONE SERVICE PORT	75
CONNECTING TO THE ADMIN UI	78
USING THE INITIAL CONFIGURATION WIZARD	79
ENTERING THE ADMINISTRATOR PASSWORD	79
ACCEPTING THE LICENSE AGREEMENT	80
SETTING THE DATE AND TIME	80
SETTING SYSTEM SECURITY	81
UPLOADING THE LICENSE KEY	82
REVIEWING THE SETTINGS SUMMARY	83
FINISHING THE INITIAL CONFIGURATION	83
CONFIGURING AN INSTANCE FROM THE COMMAND LINE	84
PERFORMING AN UNATTENDED CONFIGURATION	86
REMOVING A TRAFFIC MANAGER	87
UPGRADING YOUR TRAFFIC MANAGER	87
BEFORE YOU START	87
PERFORMING AN UPGRADE	88
UPGRADING A CLUSTER USING THE BACKUP AND RESTORE METHOD	90
REVERTING TO AN EARLIER VERSION	91
CHANGING YOUR TRAFFIC MANAGER VERSION MANUALLY	92
ADDITIONAL SYSTEM INFORMATION	93
SSH	93
SECURING COMMUNICATION WITH AMAZON EC2 ENDPOINTS	93
THE TRAFFIC MANAGER SOFTWARE INSTALLATION DIRECTORY (ZEUSHOME)	94
STARTING AND STOPPING THE TRAFFIC MANAGER SOFTWARE	94
FREEING UP DISK SPACE	94
LICENSE KEYS	95
THE COMMUNITY EDITION	95

BASIC CONFIGURATION INFORMATION	97
VIRTUAL SERVERS, POOLS, AND RULES	97
MANAGING YOUR FIRST SERVICE	98
ABOUT CREATING A TRAFFIC MANAGER CLUSTER	99
MULTI-REGION AND MULTI-VPC CLUSTERS ON AMAZON EC2	99
JOINING A CLUSTER	99
TRAFFIC IP GROUPS AND FAULT TOLERANCE ON AMAZON EC2	103
KEY DIFFERENCES BETWEEN TRAFFIC IP GROUPS ON AN EC2 AND TRAFFIC IP GROUPS ON OTHER PLATFORMS.....	103
USING ELASTIC IP ADDRESSES IN TRAFFIC IP GROUPS.....	103
USING PRIVATE IP ADDRESSES IN TRAFFIC IP GROUPS.....	104
FAULT TOLERANCE.....	105
TRAFFIC IP ADDRESSES AND TRAFFIC IP GROUPS.....	105
IP ADDRESS TRANSFERENCE WITHIN A TRAFFIC IP GROUP	105
CREATING A TRAFFIC IP GROUP.....	105
ALLOCATING A NEW ELASTIC IP ADDRESS	106
CREATING A TRAFFIC IP GROUP	106
DISABLING A TRAFFIC IP GROUP.....	108
RELEASING AN ELASTIC IP ADDRESS	108
ASSIGNING ELASTIC IP ADDRESSES TO SPECIFIC NETWORK CARDS	109
UNDERSTANDING A TRAFFIC MANAGER'S FAULT TOLERANCE CHECKS	109
LOCAL HEALTH CHECKS	110
HEALTH BROADCASTS	110
DETERMINING THE HEALTH OF A TRAFFIC MANAGER CLUSTER.....	110
TRAFFIC MANAGER FAILOVER	111
RECOVERING FROM TRAFFIC MANAGER FAILURES	111
DEBUGGING AND MONITORING FAULT TOLERANCE ACTIVITY.....	111
TRAFFIC IP GROUPS AND FAULT TOLERANCE ON GCE.....	113
USING TRAFFIC IP GROUPS FOR FAULT TOLERANCE.....	113
GCE NETWORK INTERFACES AND EXTERNAL IP ADDRESSES	114
CREATING A TRAFFIC IP GROUP.....	114
OPEN SOURCE SOFTWARE NOTICE	117

Preface

- [Document conventions](#) 1
- [Requesting Technical Support](#) 2

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
<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.
<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.

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](#) 5
- [Introducing the Traffic Manager](#) 5
- [Product Variants](#) 6

About This Guide

The *Pulse Secure Virtual Traffic Manager: Cloud Services Installation and Getting Started Guide* describes the cloud variant of the Traffic Manager.

Read this guide for an introduction to the functionality available in the Traffic Manager cloud variant, and for instructions on how to configure the Traffic Manager on each of the cloud computing platforms supported by this version of the Traffic Manager.

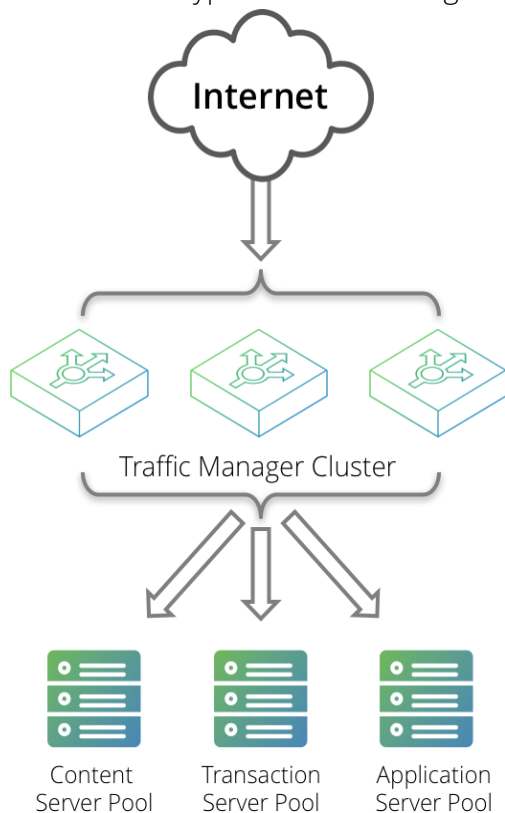
For a detailed description of the Traffic Manager and its full feature set, see the *Pulse Secure Virtual Traffic Manager: User's Guide*.

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 a software application, with versions for supported Linux and UNIX operating systems.
- 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

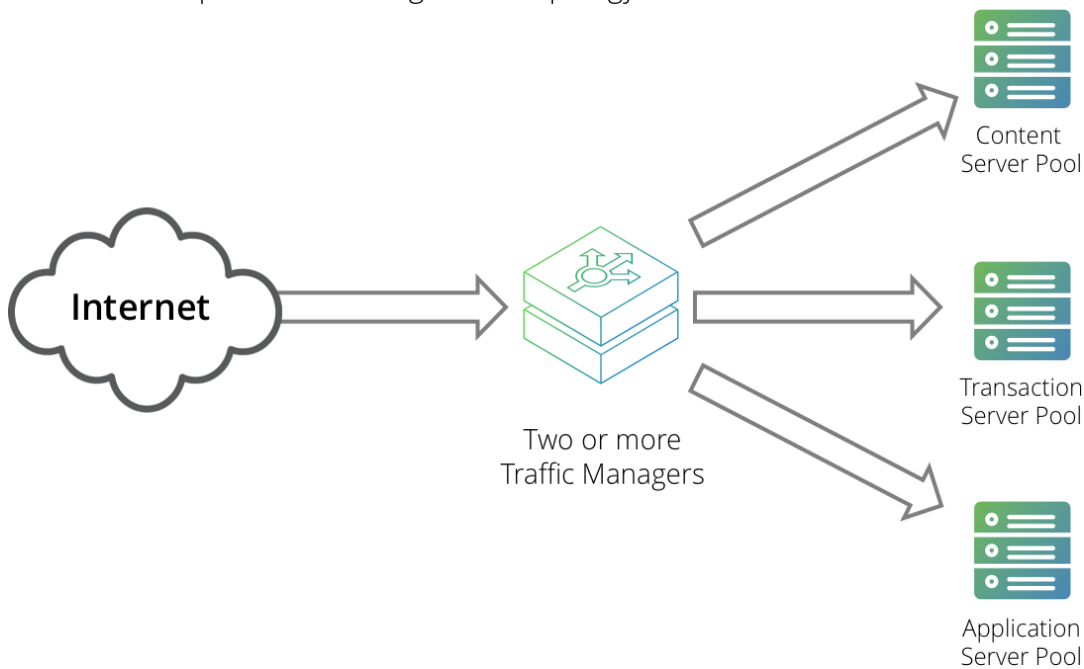
This chapter contains information about getting started using the Traffic Manager. This chapter contains the following sections:

- [Network Architecture](#) 7
- [Prerequisites](#) 8
- [Support for Amazon VPC](#) 10

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.

Note: For Amazon EC2 configurations, these clusters cannot directly span EC2-Classic regions or span beyond the network boundary of a VPC.

Prerequisites

You administer all Traffic Manager variants through a Web-enabled user interface known as the Admin UI. 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

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.

ATTENTION

If you are installing the Traffic Manager software on an preexisting Linux or UNIX virtual machine, make sure your virtual machine firewall rules allow access to the Traffic Manager Admin UI on TCP port 9090. If you also require access to the Traffic Manager REST API, enable access to TCP port 9070.

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

Additional Prerequisites for Amazon EC2

The Traffic Manager is available on EC2 as a software-only package (for use with existing Linux and UNIX virtual machines) or as a fully packaged Amazon Machine Image (AMI), from which you can create virtual machine instances. To install the software variant, see [“Installing the Traffic Manager Software on EC2 or GCE” on page 11](#). To create instances from the Traffic Manager AMI, see [“Creating a Traffic Manager Instance on Amazon EC2” on page 23](#)

To use either variant of the Traffic Manager on EC2, you need the following items:

- An Amazon Web Services (AWS) user account.
- A subscription to the EC2 version of the Traffic Manager software you want to use, or a valid Traffic Manager software license.
- Management tools that allow you to create and delete EC2 instances, such as Amazon's EC2 command line tools, Amazon's AWS management console, or the ElasticFox Firefox extension.

Note: To install the Traffic Manager software on an existing EC2 Linux or UNIX virtual machine, you must ensure that the target machine includes the “netcat” package. Standard Amazon Linux and Ubuntu virtual machines typically include netcat by default, although others might not. Consult your vendor specifications or support provider for more information.

For more information on setting up an AWS account, including EC2 subscriptions, see the Pulse Secure Community Web site (<https://community.pulsesecure.net>).

Amazon's EC2 command line tools are available in a standard software package (ec2-api-tools) on most common Linux variants. You can also download the software package from the Amazon Web Services Developer Tools website (<http://aws.amazon.com/developertools>). The commands described in this guide are based on API version 2011-02-28.

Additional Prerequisites for Microsoft Azure

To use the Traffic Manager with Microsoft Azure, you need the following items:

- A Microsoft Azure user account.
- Access to the Microsoft Azure Web management portal.
- A subscription for an applicable Traffic Manager image, or a valid license for use with non-subscription unlicensed Traffic Manager images.
- If you intend to use command line tools to manage your Azure deployment, Pulse Secure recommends you install the Azure Command Line Interface (CLI) Tool package (for OSX and Linux), or Windows Azure PowerShell (for Microsoft Windows). To install and use the Azure CLI Tool, see the documentation on the Microsoft Azure website: <http://azure.microsoft.com/en-us/documentation/articles/command-line-tools/>.

Additional Prerequisites for GCE

The Traffic Manager is available on GCE as a software-only package (for use with existing Linux and UNIX virtual machines) or as a fully packaged virtual machine image, from which you can create virtual machine instances. To install the software variant, see [“Installing the Traffic Manager Software on EC2 or GCE” on page 11](#) To create instances from the virtual machine image, see [“Creating a Traffic Manager Instance on Google Compute Engine” on page 49](#)

Note: When installing the Traffic Manager software on an existing Linux or UNIX virtual machine, you must first ensure your host virtual machine has Read/Write permission set for “Compute” API access. The Traffic Manager requires this access to interact with the *gcloud compute* API.

To use either variant of the Traffic Manager on GCE, you need the following items:

- A GCE user account and subscription.
- A subscription to the GCE version of the Traffic Manager software you want to use.
- Access to the GCE Web management portal.
- A suitable GCE project in which to launch your GCE-based Traffic Manager instances.

The Traffic Manager supports the use of GCE External IP addresses to implement front-end fault tolerance within your Traffic Manager cluster. To use External IP addresses for fault tolerance on a Traffic Manager, add extra network interfaces (one per IP address) to the host virtual machine at launch time and configure a Traffic IP Group to handle the traffic distribution.

Note: All Traffic Managers require a single network interface reserved for administration and management, so any further interfaces you add must be in addition to the primary interface.

GCE supports a maximum of 8 network interfaces per virtual machine. Consequently, the Traffic Manager can support a maximum of 7 External IP addresses per instance. GCE also requires that virtual machines must be specified with 1 CPU core per network interface, including the primary management address. Therefore, to use fault tolerance on a Traffic Manager deployment in GCE, make sure you perform the following actions before launching your virtual machines:

- Create as many GCE External IP addresses in the GCE console as required for your fault tolerant service (up to a maximum of 7).
- For every new Traffic Manager virtual machine you are creating (or host virtual machine, in the case of Traffic Manager software variants), add an additional network interface and CPU core for each External IP address you want to use. Make sure that the total number of interfaces attached to a virtual machine, and the total number of CPU cores, is at least equal to the number of External IP addresses you want to use plus one more for management.

ATTENTION

You must create additional network interfaces at launch time. GCE does not allow you to add further interfaces to an existing instance.

To learn more about fault tolerance on GCE, see [“Traffic IP Groups and Fault Tolerance on GCE” on page 113](#).

Support for Amazon VPC

Amazon Virtual Private Cloud (VPC) lets you provision a private, isolated section of the Amazon Web Services (AWS) Cloud where you can launch AWS resources in a virtual network that you define. Instances launched within the VPC have private addresses assigned from a range you define.

Traffic Manager AMIs can be deployed either inside or outside of a VPC. Traffic Manager AMIs deployed outside of a VPC are sometimes referred to as EC2-Classic. There are, however, a number of differences in the way that the Traffic Manager handles IP addressing and Traffic IP groups when deployed inside a VPC. These differences are covered in more detail in [“Traffic IP Groups and Fault Tolerance on Amazon EC2” on page 103](#)

Note: References to EC2 instances within this guide should be taken to mean all Traffic Manager instances launched into Amazon EC2, regardless of whether this is a VPC or an EC2-Classic deployment. Differences in functionality are noted in this guide.

This guide assumes you are familiar with VPC functionality in Amazon EC2. For more details about the VPC capabilities, implementation and deployment, see <http://aws.amazon.com/vpc>.

Installing the Traffic Manager Software on EC2 or GCE

This chapter documents how to install and configure the Traffic Manager software variant on an existing Linux-based or UNIX-based virtual machine running on Amazon EC2 or Google Compute Engine (GCE). It contains the following sections:

• Traffic Manager Software Space Requirements	11
• Unpacking the Traffic Manager Software Download File	11
• Installing the Traffic Manager Software	12
• Configuring the Traffic Manager Software	13
• Administration User Interface Authentication	16
• Upgrading the Traffic Manager Software	16
• Reconfiguring or Uninstalling the Traffic Manager Software	20

Note: To create a new instance of the Traffic Manager virtual machine image, see instead “[Creating a Traffic Manager Instance on Amazon EC2](#)” on page 23 for EC2 based instances, or “[Creating a Traffic Manager Instance on Google Compute Engine](#)” on page 49 for GCE based instances.

Note: To install the Traffic Manager software variant on non-cloud platforms, see instead the *Pulse Secure Virtual Traffic Manager: Software Installation and Getting Started Guide*, available from the Pulse Secure website:

www.pulsesecure.net

Before you begin, make sure you have met the requirements listed in “[Prerequisites](#)” on page 8.

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.

For EC2:

```
./zinstall --ec2
```

For GCE:

```
./zinstall --gce
```

You should observe the following initial output:

```
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
```

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

Note: In the command samples that follow, `<variant>` must be either `ec2` or `gce` depending on your deployment type.

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

```
./zinstall --<variant> --record-to=bvtm_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 --<variant> --replay-from=bvtm_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 be prompted for the password later (unless you specified the `--noninteractive` option at the command line).

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 a Traffic 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 13](#).

To run the configure script

1. If you are installing the Traffic Manager software, 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 --<variant>
```

<variant> must be either `ec2` or `gce` depending on your deployment type.

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

2. The license agreement displays. Please read the entire agreement and 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. 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.

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

Type "N" to license this Traffic Manager directly.

4. 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 95](#).

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

5. 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 comprising the Traffic Manager's system security.

The default user with no privileges is usually called `nobody` and the default group with no privileges is usually called `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 you can specify them here.

6. 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.

(For EC2 deployments only) If you restrict management traffic on a Traffic Manager instance inside AWS, administrative access to the Traffic Manager is restricted to clients in the same network or VPC.

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 machine, 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.

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

Specify a cluster for the Traffic Manager to join, or create a new cluster with this Traffic Manager as the first member. Select one of the following choices:

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

- C) Create a new cluster
- S) Specify another machine to contact

Select C to create a new cluster.

When you join an existing cluster, your Traffic Manager automatically receives the configuration settings used by the cluster. Changes that you subsequently make to this Traffic Manager are replicated out to the other cluster members.

Note: To provide front-end fault tolerance, your Traffic Managers must be in the same 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.

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

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 6:3E:4E:22:D8:B6:83:04:F9:57
vtm2.mysite.com:9090 E9:61:36:FE:0B:F5:0A:E4:77:96 3:D8:35:8F:54:5F:E3:2C:71:ED
```

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

10. 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 software starts and 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 its unconfigured state. For more information, see [“Reconfiguring or Uninstalling the Traffic Manager Software” on page 20](#).

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 virtual machine command line using the following command:

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

Upgrading the Traffic Manager Software

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 17](#)).

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> [<args>]
```

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

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).

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 --<variant>
```

`<variant>` is either “ec2” or “gce” depending on your deployment type.

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

Reverting to an Earlier Version

The upgrade process preserves all previously used Traffic Manager versions to facilitate a reversion capability. To revert to a previous version, the Traffic Manager includes a *Switch Versions* facility in the Admin UI and a *rollback* program from the command line.

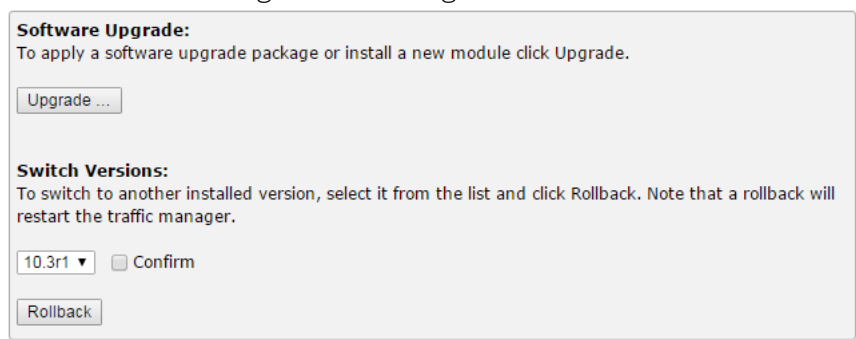
Note: This procedure does not retain any configuration you have made since upgrading to the current version. It is strictly a roll-back procedure that reinstates the selected software version and reinstates the previous configuration settings. Therefore, Pulse Secure strongly recommends that you make 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:

FIGURE 3 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.

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 20](#).

To uninstall the Traffic Manager software, see [“Uninstalling the Traffic Manager Software” on page 21](#).

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 root user and run the `configure` script from the virtual machine command line:

```
$ZEUSHOME/zxtm/configure --<variant>
```

<variant> is either `ec2` or `gce` depending on your deployment type.

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

```
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 on to the Traffic Manager and select “Perform the post-install configuration again”.
2. 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]:

3. 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 20](#).

## 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 --<variant>
```

<variant> is either `ec2` or `gce` depending on your deployment type.

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).

# Creating a Traffic Manager Instance on Amazon EC2

This chapter describes how to install and configure the Traffic Manager virtual machine on Amazon EC2. To install the Traffic Manager software variant on an existing EC2-based Linux or UNIX virtual machine, see instead [“Installing the Traffic Manager Software on EC2 or GCE” on page 11](#).

To create a Traffic Manager virtual machine, create one or more instances from the Traffic Manager AMI. No other installation procedure is necessary. All you need to do is login to the instance and configure it.

This chapter contains the following sections:

|                                                                           |    |
|---------------------------------------------------------------------------|----|
| • <a href="#">Before You Begin</a> .....                                  | 23 |
| • <a href="#">Using IAM Roles</a> .....                                   | 25 |
| • <a href="#">Adding a Port to the Default Security Group</a> .....       | 26 |
| • <a href="#">Launching a Virtual Machine Instance</a> .....              | 27 |
| • <a href="#">Connecting to the Admin UI</a> .....                        | 28 |
| • <a href="#">Using the Initial Configuration Wizard</a> .....            | 29 |
| • <a href="#">Configuring an Instance From the Command Line</a> .....     | 35 |
| • <a href="#">Removing an Instance</a> .....                              | 38 |
| • <a href="#">Preconfiguring the Traffic Manager at Launch Time</a> ..... | 38 |
| • <a href="#">Upgrading Your Traffic Manager</a> .....                    | 40 |
| • <a href="#">Expanding the Log File Partition</a> .....                  | 47 |

## Before You Begin

**Note:** Make sure you have met the requirements listed in [“Prerequisites” on page 8](#).

Your Traffic Manager software is primarily controlled through a web-based administration interface served by the Traffic Manager Admin Server. This interface provides the Admin UI, and handles communications with the core Traffic Manager software.

To access the Admin UI, connect to TCP port 9090 on the virtual machine instance, and optionally, connect to port 22 if you require SSH command line access. However, traffic to these ports is blocked by EC2's default firewall rules.

To access the Admin UI or command line, you must create a new EC2 Security Group that allows traffic for these ports to pass through the firewall. You only need to create the security group once, but you must remember to apply it every time you launch a new virtual machine instance. With EC2-Classic, a security group cannot be added to a virtual machine instance after it is launched.

The following example shows how you can use Amazon's command line tools to create a security group called vtm-admin-server, which permits connections to the specified ports from any address in the 131.111.0.0/16 subnet:

```
ec2-create-group vtm-admin-server -d "Virtual Traffic Manager Admin Server"
ec2-authorize vtm-admin-server -P tcp -p 9090 -s 131.111.0.0/16
and, optionally, for SSH access:
```

```
ec2-authorize vtm-admin-server -P tcp -p 22 -s 131.111.0.0/16
```

**Note:** The above arguments are used for example purposes only. You should specify your own security group and subnet when running these commands. However, ports 9090 and 22 should be used in all cases.

Intercluster communications must also be enabled, using the same method. To allow a Traffic Manager cluster to operate within a single EC2 region, use the following commands:

```
ec2-authorize vtm-admin-server -o vtm-admin-server
-u <AWS Account Number> -P tcp -p 9090
```

```
ec2-authorize vtm-admin-server -o vtm-admin-server
-u <AWS Account Number> -P udp -p 9090
```

```
ec2-authorize vtm-admin-server -o vtm-admin-server
-u <AWS Account Number> -P tcp -p 9080
```

```
ec2-authorize vtm-admin-server -o vtm-admin-server
-u <AWS Account Number> -P udp -p 9080
```

These commands ensure that the vtm-admin-server security group opens up UDP and TCP ports 9090 and 9080 for connections from other instances in the same vtm-admin-server group, launched with the specified <AWS Account Number>.

In addition, Pulse Secure Virtual Web Application Firewall (vWAF) users require using the following commands in order to authorize communication with the vWAF user interface and system processes:

```
ec2-authorize vtm-admin-server -o vtm-admin-server
-u <AWS Account Number> -P tcp -p 8083
```

```
ec2-authorize vtm-admin-server -o vtm-admin-server
-u <AWS Account Number> -P tcp -p 8086
```

```
ec2-authorize vtm-admin-server -o vtm-admin-server
-u <AWS Account Number> -P tcp -p <AdminMasterPort>
```

```
ec2-authorize vtm-admin-server -o vtm-admin-server
-u <AWS Account Number> -P tcp -p <AdminSlavePort>
```

```
ec2-authorize vtm-admin-server -o vtm-admin-server
-u <AWS Account Number> -P tcp -p <UpdaterSlavePort>
```

For these commands, <AdminMasterPort> (default value 11000), <AdminSlavePort> (default value 11002), and <UpdaterSlavePort> (default value 11007) refer to configurable ports listed on the **System > Application Firewall** page in the Admin UI. If you make changes to any of these settings in the Admin UI or through one of the Traffic Manager external APIs, you must also update your security group settings accordingly.

If you want to use the REST API, you must allow connections to the TCP port used by the Traffic Manager REST service (the default port is 9070):

```
ec2-authorize vtm-admin-server -o vtm-admin-server
-u <AWS Account Number> -P tcp -p 9070
```

If you have multiple Traffic Manager clusters spanning multiple EC2-Classic regions or VPCs, you must open those ports to hosts connecting from the internet by using the following commands:

```
ec2-authorize vtm-admin-server -P tcp -p 9090 -s 0.0.0.0/0
```

```
ec2-authorize vtm-admin-server -P udp -p 9090 -s 0.0.0.0/0
```

```
ec2-authorize vtm-admin-server -P tcp -p 9080 -s 0.0.0.0/0
```

```
ec2-authorize vtm-admin-server -P udp -p 9080 -s 0.0.0.0/0
```

**Note:** Multiple Traffic Manager clusters are typically managed by the Traffic Manager's multi-site cluster management feature. For more information about this feature, see the *Pulse Secure Virtual Traffic Manager: User's Guide*.

If your security policy requires it, you can limit these authorizations to the subnets corresponding to the different EC2 regions used, rather than 0.0.0.0/0 as used in the examples above. However, there is a risk that new instances may start up in alternative subnets and thus be unable to communicate with the cluster.

You also need to open ports for each virtual server you create on your Traffic Manager. For instance, the following command creates a group that allows traffic to HTTP (port 80) and HTTPS (port 443) servers from any Internet address:

```
ec2-create-group http-https -d "HTTP and HTTPS servers"
```

```
ec2-authorize http-https -p 80
```

```
ec2-authorize http-https -p 443
```

You can also create security groups using graphical management tools. In ElasticFox, security groups are managed in the Security Groups tab. In Amazon's AWS management console, click the Security Groups link in the Networking & Security section of the Navigation panel.

## Using IAM Roles

The Traffic Manager supports the use of EC2 Identity and Access Management (IAM) roles. IAM roles are required for deployments involving Traffic IP addresses, auto-scaling, or appliance network management.

To create an IAM role, use the AWS Console or equivalent management tool. When you launch a new Traffic Manager virtual machine instance, specify the IAM role you want the instance to assume.

During normal communication with EC2, the Traffic Manager executes a range of API calls to perform various functions. When you create an IAM role, you must attach an IAM policy to the role with the correct level of authority to execute the desired functions. EC2 provides various predefined IAM policies, together with the ability to create custom policies to meet specific needs. If you require one of the following functional areas in your deployment, make sure your chosen IAM policy has permission to execute the associated API calls.

For general Traffic Manager functioning:

- DescribeRegions
- DescribeInstances
- DescribeAddresses
- DescribeNetworkInterfaces

For Fault Tolerance:

- AssociateAddress
- DisassociateAddress
- AllocateAddress
- ReleaseAddress
- AssignPrivateIPAddresses
- UnAssignPrivateIpAddresses

For Autoscaling:

- RunInstances
- CreateTags
- TerminateInstances

For more information on IAM roles and policies, see the AWS documentation at: <http://aws.amazon.com/documentation/>.

## Adding a Port to the Default Security Group

If you want all virtual machine instances that you create to have a specific port open by default, you can add that port to the default security group. The default security group is used if no other group is specified at launch time.

To specify a port to open by default, use the following command:

```
ec2-authorize default -p 80
```

**Note:** The example above allows connections to port 80 on any virtual machine instance you launch, not just Traffic Manager instances. Allowing these connections may have unintended consequences for the security of your other virtual machines. For this reason, add the ports you need to task-specific security groups, and only apply those groups to the instances that need them.



## Launching a Virtual Machine Instance

Using your EC2 management tool, launch a new instance of the Traffic Manager virtual machine image you purchased. To do this, you need the AMI's ID code, which you should have received when you purchased the Traffic Manager software.

If you are using Amazon's EC2 command line management tools, you can start a new instance using the following command:

```
ec2-run-instances <ami_id> --user-data password=<secret> --group vtm-admin-server
```

where <ami\_id> is the ID of the Traffic Manager AMI you purchased and <secret> is the password you would like to use to access the Admin UI. If you do not supply a password, one is assigned randomly, as described in [“Entering the Admin User Password” on page 30](#).

If you are using a graphical management tool, such as ElasticFox, select your Traffic Manager product in the list of available AMIs and create an instance by clicking the launch button. To set the password, add the following line to the user data field in the launch dialogue box:

```
password=<secret>
```

For more details, see the documentation for the management tool you are using.

Amazon VPC users additionally require a previously created VPC with enough free private IP capacity to run the new instance. Your VPCs can be viewed (and created and deleted as appropriate) by using the VPC section of the Amazon AWS management console.

**Note:** Make note of the VPC ID you intend to use and its associated CIDR range. This information is required when selecting the VPC in which to launch the new instance.

There are several configuration options that you can use to control how and where your EC2 instances are created. One option is to specify the Availability Zone in which the instance should be created.

Availability Zones are independent parts of Amazon's network, isolated from each other so that the failure of one Availability Zone does not affect the others. To improve fault tolerance, you should ensure that your EC2 instances are located in different availability zones.

Depending on the Traffic Manager product you purchased, you may also be able to select the CPU power and memory for your instance. For more details on EC2 instance parameters and how to set them, see the Amazon's EC2 documentation, or the documentation for the management tool you are using.

VPC instances are initially specified with a primary IP address within the subnet used by the VPC, and optionally, the secondary addresses on the same interface. The primary address is mandatory for management traffic. The primary address cannot be removed. Secondary addresses are used to load-balance your services and can be added as necessary.

You can add and remove secondary addresses from the AWS console or from the **System > Networking** page of the Traffic Manager Admin UI once the instance has launched.

**Note:** Adding new private IP addresses to the default network interface might trigger a warning/error condition while the address is being raised. This is to be expected, and refreshing the browser page after a few seconds should show that the Traffic Manager health status has returned to normal. If you are still experiencing warning/error conditions after a few minutes, please see the Diagnose page for further details or contact your support provider for assistance.

## Connecting to the Admin UI

When you create a new EC2 instance, the new EC instance is initially listed as pending while the instance starts up. You can view the status of an instance using the following command:

```
ec2-describe-instances
```

Wait until the instance is listed as running and note the public DNS name or public IP address associated with the instance. This is the address of the Traffic Manager Admin UI.

For instances running inside a VPC, if you did not assign a public IP to the Traffic Manager instance when the Traffic Manager was launched, confirm you can connect to the Admin UI using a direct connection to the private address range in the VPC through, for example, a secure VPN or NAT (Network Address Translation) based infrastructure.

If you are still unable to access the Admin UI, you must associate a public IP address with one of the private IPs defined in your instance. To do this, allocate a new Elastic IP Address through the AWS Console and associate it with the primary private IP in your instance. If you do not associate the Elastic IP address with an instance, the address remains attached to your EC2 account until you release it.

**Note:** Elastic IP addresses are allocated for use with instances in EC2-Classical or a VPC, but not both. When allocating a new Elastic IP address for use with a VPC-based instance, select VPC when prompted.

When the instance is running and publicly accessible, access the following URL in your Web browser:

```
https://<admin_ui_address>:9090/
```

where <admin\_ui\_address> is either the public DNS name or public IP address listed by your management tool.

Verify that you can connect to the Admin UI using a Web browser and then proceed to configure your Traffic Manager instance through the Initial Configuration Wizard. For more details, see [“Using the Initial Configuration Wizard” on page 29](#).

## Confirming the Traffic Manager's Identity

Before you connect to the Admin UI of a newly configured Traffic Manager instance, 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). You can safely ignore this warning as the certificate is self-signed, and the hostname in the certificate might not match the URL you have used to access it (an instance's public DNS name and IP address are different to the private DNS name and IP address the instance uses within the EC2 network).

To verify the identity of the instance you are connecting to, check that the SHA-1 fingerprint of the self-signed SSL certificate matches the fingerprint of the Traffic Manager instance you want to configure. Consult the documentation for your Web browser for instructions on how to display the SSL certificate and associated SHA-1 fingerprint information for a Web site you are visiting.

To view the SHA-1 fingerprint for a Traffic Manager instance configured in EC2, check the instance EC2 console log. Click "Console output" in your graphical EC2 management tool, or run the following command:

```
ec2-get-console-output <instance_id>
```

<instance\_id> is the unique ID of the instance you are trying to configure.

**Note:** There might be a delay of several minutes after instance creation before the console output is available from EC2.

## Using the Initial Configuration Wizard

A newly created Traffic Manager instance requires some basic information to function normally. The Traffic Manager gathers this information over a series of steps that form the Initial Configuration wizard.

Access the first page of the wizard by entering the URL of the Admin UI into your Web browser:

FIGURE 4 Step-by-step Configuration Process

### Initial configuration, step 1 of 7

#### 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 EC2 Appliance for basic operation. This should only take a few minutes.

◀ Back

Next ▶

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

**Note:** The number and order of the wizard steps varies by product variant. The number and order of the wizard steps you see may differ from the ones shown in this chapter.

## Entering the Admin User Password

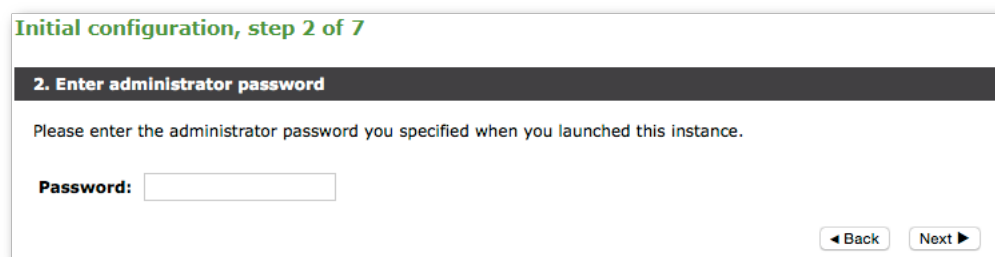
**Note:** This step applies only to Amazon EC2 instances.

The Traffic Manager uses the password you specify in this step to verify that you are the person who launched the instance. Verifying the identity helps prevent an unauthorized user from gaining control of a newly launched instance.

Note the following points about entering the admin user password:

- For EC2 instances where you preconfigured an admin user password, enter that password here. For more information, see [“Launching a Virtual Machine Instance” on page 27](#).

**FIGURE 5** Enter the Preconfigured Admin Password



Initial configuration, step 2 of 7

**2. Enter administrator password**

Please enter the administrator password you specified when you launched this instance.

**Password:**

◀ Back   Next ▶

- For EC2 instances where you did not preconfigure an admin user password, EC2 generates a random password for you.

You can find this EC2-generated password in the instance's EC2 console log for the instance. As an additional security measure, and to ensure that you are authorized to configure the instance, the console log is only available to the Amazon user who created the instance.

To view the console log, click Console output in your graphical EC2 management tool or run the following command:

```
ec2-get-console-output <instance_id>
```

The <instance\_id> variable is the unique ID of the instance you are trying to configure. There can be a delay of several minutes after the instance is created before the console output is available from EC2.

If you did not preconfigure an admin password, you can set one later using the configuration wizard.

Retrieve the randomly generated password from the console log and enter it in the wizard. Then click **Next**.

FIGURE 6 Enter the Randomly Generated Admin Password

**Initial configuration, step 2 of 7**

**2. Enter administrator password**

You did not provide any user data when you created the instance. This traffic manager has therefore been configured using default settings. To ensure it remains secure, a random password has been generated which has been printed to the EC2 instance console (note that it can take EC2 several minutes to update the console output).

You can view this instance's console output from the EC2 Management Console using 'Instance Settings > Get System Log', or by using the standard EC2 command line tools or the aws cli:

```
ec2-get-console-output i-9ce2d036 --region eu-west-1
```

```
aws ec2 get-console-output --instance-id i-9ce2d036 --region eu-west-1 --output text
```

**Password:**

◀ Back   Next ▶

## Accepting the License Agreement

Read and accept the Pulse Secure Terms and Conditions of Sale:

FIGURE 7 Terms and Conditions of Sale

**Initial configuration, step 3 of 7**

**3. 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 ▶

Please read the entire agreement. If you agree to its terms, click the I accept the license agreement check box and click Next to continue.

**Note:** You cannot use the Traffic Manager software until you accept the license agreement and you have completed the installation wizard.

## Setting the Date and Time

Set the date and time for your Traffic Manager instance. Setting this correctly ensures that any logs and diagnostic messages generated by the Traffic Manager have the correct timestamps:

FIGURE 8 Set the Date and Time

**Initial configuration, step 4 of 7**

**4. Date and Time Settings**

Please specify the time settings for this appliance.

**Time Zone:** America/Los Angeles ▼

**Date:** 3 September 2019

**Time:** 02 : 44 : 30

◀ Back Next ▶

## Setting System Security

If you did not preconfigure an admin password when you launched the instance, enter one now. Use the password you set here when you configure an instance through a Web browser. If you enable password authentication for SSH, you can also use the admin password when you log in to an instance using SSH (with the username “admin”).

The Traffic Manager also contains an SSH intrusion prevention tool to help prevent brute-force SSH attacks on your Traffic Manager instance. Pulse Secure strongly recommends you enable this option.

**Note:** If you preconfigured an admin password, the Traffic Manager displays only the option to enable SSH intrusion prevention.

FIGURE 9 Setting System Security

**Initial configuration, step 5 of 7**

**5. 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

◀ Back Next ▶

## Providing a License Key

The Traffic Manager is available as a range of set-frequency billing subscriptions where the license is built in, and as a Community Edition/Bring Your Own License (BYOL) instance. For the Community Edition/BYOL instance, the Initial Configuration Wizard provides an additional step to configure your instance with the required licensing.

For set-frequency billing subscriptions, this step does not appear.

FIGURE 10 Uploading a license key file

**Initial configuration, step 6 of 7**

The screenshot shows a web interface titled "6. License Key". Below the title, it states: "To use the traffic manager, you will need a valid license key. You have the following licensing options:". There are three radio button options: "Upload a license key for this traffic manager" (which is selected), "Register for flexible licensing using **Services Director**", and "Skip licensing for now (the traffic manager will run as the **Community Edition** until licensing is configured)". Below these options, it says "Upload a new license key:" followed by "Key file:". Under "Key file:", there is a button labeled "Choose File" and the text "No file chosen". At the bottom of the form, it says "If you need to obtain a license key, please visit the **Pulse Secure vTM website**". At the bottom right, there are two buttons: "Back" and "Next".

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.

**Note:** 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**.

To learn more about the Community Edition, see ["The Community Edition" on page 95](#).

## Viewing the Summary Page

The Summary page displays the configuration settings for you to review.

FIGURE 11 Summary Page

**Initial configuration, step 7 of 7**

**7. Summary**

Your date and time settings are:

|                   |                     |
|-------------------|---------------------|
| <b>Date:</b>      | 3 September 2019    |
| <b>Time:</b>      | 02:46:17            |
| <b>Time Zone:</b> | America/Los_Angeles |

Additional settings:

|                                  |                         |
|----------------------------------|-------------------------|
| <b>SSH Intrusion Protection:</b> | Enabled                 |
| <b>License key:</b>              | No license key provided |

To pre-configure another Pulse Secure vTM EC2 instance using these settings, specify the following user data at launch:

```
password=<Admin Password>
timezone=America/Los_Angeles
accept_license=Yes
```

To make a new Pulse Secure vTM EC2 instance cluster with this one, use the following user data:

```
cluster_host=ip-10-0-1-65
cluster_fingerprint=FB:1F:9F:5C:FC:CF:58:83:5C:99:4F:00:0B:B5:3A:20:E7:3D:8E:7D
password=<Admin Password for this Instance>
```

*The information above can be found on the 'System > Traffic Managers' page after completing the wizard.*

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

◀ Back
Finish

Click **Back** to make changes or click **Finish** to complete the installation.

**Note:** The Traffic Manager settings shown here are replicated on the **System > Traffic Managers** page after you have completed initial configuration.


After clicking the **Finish** button, a status message appears while the Traffic Manager is configured.



FIGURE 12 Initial Configuration is Progressing

**Initial configuration, finished****Setup finished**

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

 Please wait while your traffic manager is configured

You will be automatically redirected to the administration server when it is available. **Click here if you are not redirected.** You can log in with the username 'admin' and the password that you chose.

After a short wait, you are redirected to the login page of the Admin UI. Log in using the username (admin) and the admin password. The password is either the password you preconfigured when you launched the instance, or the password you set during the installation wizard.

## Configuring an Instance 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” on page 29](#).

To start the configuration program, login to the instance 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) 2020, Pulse Secure, LLC. 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 Traffic Manager.
```

```

Use of this software is subject to the Pulse Secure 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 Pulse Secure 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.

**Note:** The Traffic Manager is available as a range of set-frequency billing subscriptions where the license is built in, and as a Community Edition/Bring Your Own License (BYOL) instance. The following two steps concern software licensing options for the Community Edition/BYOL instance only, and might not appear if you are running the configuration program on an instance with a built-in license.

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 instance for remote licensing in a Pulse Secure Services Director deployment, type "Y" at the prompt. To instead license this instance individually, type "N". For further information on Pulse Secure Services Director, see the relevant product pages on the Pulse Secure website ([www.pulsesecure.net](http://www.pulsesecure.net)).

If you do not register this instance for remote licensing, the configuration program prompts you for a license key file.

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](#)" on page 95. For information about paid licensing, contact Pulse Secure Technical Support.

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 instance 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. Pulse Secure 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*.

Please provide the port on which the REST API should  
listen for requests (default 9070).

REST port [9070]:

If you enable the REST API, enter the port number on which you want the REST service to listen for requests.

**Note:** The REST API is enabled by default if you chose to register this Traffic Manager instance with a Pulse Secure Services Director.

You have specified the following settings:

|                         |                                                       |
|-------------------------|-------------------------------------------------------|
| No license file:        | The traffic manager will run as the Community Edition |
| Timezone:               | UTC                                                   |
| SSH protection enabled: | Yes                                                   |
| REST enabled:           | Yes                                                   |
| REST port:              | 9070                                                  |

Proceed with configuration? Y/N:

Before you finish, check through the summary to confirm your intended settings. To configure your Traffic Manager with these settings, type “Y” at the prompt.

## 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>
```

## Removing an Instance

You can terminate a Traffic Manager instance by clicking the Terminate... button in the Hardware Restart section of the **System > Traffic Managers** page. You are asked to confirm this action.

**Note:** If you terminate an instance, the instance is shut down and is permanently destroyed. You lose all configuration and data associated with that Traffic Manager instance.

## Preconfiguring the Traffic Manager at Launch Time

EC2 allows you to create new instances quickly, for example, to respond to a sudden increase in website traffic. To take advantage of this ability, you can preconfigure all the settings requested by the Initial Configuration Wizard when you launch the instance, avoiding the need to go through the wizard manually. You can also instruct the new instance to join an existing Traffic Manager cluster automatically after it starts up.

Specify your configuration settings as parameter=value pairs in the user data field. Enter each configuration pair, separated by whitespace, to correspond to the different questions in the wizard.

The following table lists the basic wizard parameters:

| Parameter      | Value or Description                                                                                  |
|----------------|-------------------------------------------------------------------------------------------------------|
| password       | The admin user password                                                                               |
| accept_license | Accept the Traffic Manager End User License Agreement? (y/n)                                          |
| timezone       | The Traffic Manager instance timezone (for example, Europe/London)<br>Defaults to America/Los Angeles |

If you do not provide values for at least the password and accept\_license parameters, the Initial Configuration Wizard prompts you to set the missing parameters manually.

The following table lists parameters used for cluster joining:

| Parameter    | Value or Description                                                                              |
|--------------|---------------------------------------------------------------------------------------------------|
| cluster_host | The private DNS name of a member of an existing cluster that the new Traffic Manager should join. |
| user         | The admin username for the cluster (defaults to admin).                                           |
| password     | The admin password for the cluster.                                                               |

| Parameter           | Value or Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| join_tips           | <p>Should the new Traffic Manager host Traffic IP addresses when it joins the cluster? (y/n, default n)</p> <p>For clusters with only one Traffic IP group configured in the cluster, enter <b>Y</b>.</p> <p>For clusters with multiple Traffic IP groups configured in the cluster, enter <b>N</b> and manually configure the Traffic IP group(s) that this new instance should join.</p> <p><b>Note:</b> For Amazon VPC instances, setting join_tips=y is ignored if the instance does not have a secondary IP address assigned while launching.</p> |
| cluster_fingerprint | Specifies the SHA-1 fingerprint of the machine you entered for the cluster_host parameter. You can accept any fingerprint by entering unsafe as this key's value. It is required if using cluster_host.                                                                                                                                                                                                                                                                                                                                                |
| cluster_location    | Specifies the configuration location this instance should join when clustering. If the location does not exist, it is created. For more details on configuration locations, see the <i>Pulse Secure Virtual Traffic Manager: User's Guide</i> .                                                                                                                                                                                                                                                                                                        |

The following table lists parameters used for Pulse Secure Services Director self-registration:

| Parameter           | Value or Description                                                                                                                                                                                                                                                                                                        |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| sd_address          | <p>The address to which this Traffic Manager instance sends a Services Director self-registration request at startup.</p> <p>Use the format &lt;IP address/FQDN&gt;:&lt;REST API port&gt;</p>                                                                                                                               |
| sd_cert             | The PEM-encoded certificate of the Services Director's REST API server, with begin/end comment lines removed, and newlines removed.                                                                                                                                                                                         |
| registration_policy | The identifier of an auto-registration policy resource in the Services Director that can be used to automatically accept a registration request from this Traffic Manager instance.                                                                                                                                         |
| owner               | The identifier of an Owner resource to associate with the registration request from this Traffic Manager instance.                                                                                                                                                                                                          |
| owner_secret        | <p>The secret token associated with the Owner, if one is provided.</p> <p>If an owner is specified then, by default, the Services Director requires that the matching secret is also included for a registration request to be auto-accepted. This behavior can be globally toggled on or off in the Services Director.</p> |

The Traffic Manager additionally supports the use of CloudFormation reference templates in Amazon EC2. To use reference templates, specify your CloudFormation stack, resource, and region in the user data field using the parameter names listed in the following table:

| Parameter    | Value or Description                  |
|--------------|---------------------------------------|
| cfn_stack    | The CloudFormation stack name.        |
| cfn_resource | A CloudFormation logical resource ID. |
| cfn_region   | The CloudFormation region.            |

The Cloud Formation **cfn-init** script runs when the Traffic Manager instance boots up for the first time. The parameters you specify form the arguments provided to the script: “-s <cfn\_stack>”, “-r <cfn\_resource>”, and “--region <cfn\_region>”.

To set user-data with the **ec2-run-instances** command line tool, use one of the following methods:

- as a string on the command line, using the --user-data argument
- in a file, passed using the --user-data-file argument

Graphical tools, such as ElasticFox, typically provide a text box in the new instance launch window, into which you can paste the configuration data. For more details, see your management tool's documentation.

## Upgrading Your Traffic Manager

This section contains details of how to upgrade and, where necessary, revert your Traffic Manager instance when a new version is released.

### Before You Start

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.

#### CAUTION

If you are upgrading from Traffic Manager versions earlier than 9.9, you must install a new instance of the Traffic Manager and import your configuration into it. This is due to the underlying operating system on earlier versions 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 2GB 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 700MB must be free on the / (root) partition, and at least 600MB must be free on the /logs partition. To confirm the available free disk space, use the **System > Traffic Managers** page of the Admin UI.

**Note:** Pulse Secure 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

**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 appliance platform. 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, EC2 instances), 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 EC2 instances), 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

**Note:** This procedure is applicable to versions 11.1 and later. If you are upgrading from a version prior to 11.1, use instead the replace-and-terminate method described in **“Upgrading Using the Replace-And-Terminate Method” on page 43**.

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 instance.

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” on page 45](#)).

**Note:** 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 instance 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>_EC2-Appliance-Upgrade-x86_64.tgz
```

Perform the upgrade through the Admin UI or from the instance 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 41](#)).

### To upgrade using the command line

1. Copy the package file to the instance 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

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

2. Connect to the Traffic Manager 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.

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

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

## Upgrading Using the Replace-And-Terminate Method

This procedure is offered as an alternative to the standard upgrade procedure.

The specific steps for upgrading your Traffic Manager in this way depends on whether you are upgrading a single Traffic Manager instance or a cluster of Traffic Manager instances.

### Upgrading a Single Traffic Manager Instance

When an AMI containing a newer version of the Traffic Manager software is made available, create a separate instance of the newer Traffic Manager AMI, migrate the configuration over from the existing instance, and then terminate the earlier version. For more information about creating and importing configuration backups, see the *Pulse Secure Virtual Traffic Manager: User's Guide*.

### Upgrading a Cluster of Traffic Manager Instances

Using clustering and fault tolerant Traffic IP addresses, you can upgrade a cluster in place, replacing each Traffic Manager with one running the newer version of the software, while continuing to serve application traffic.

In accordance with standard configuration replication rules, when you add a newer version Traffic Manager instance to your existing cluster, it automatically receives a copy of the cluster configuration. The new instance performs an automatic upgrade of the configuration it receives to ensure compatibility.

You can then terminate the older Traffic Manager instance it replaces, repeating the process with each cluster member in turn.

#### CAUTION

Configuration backup files are specific to the Traffic Manager instance on which they are created, and are not included in the cluster configuration replication mechanism. To avoid losing configuration backups when you terminate a Traffic Manager instance, Pulse Secure strongly recommends you download all stored configuration backups and then reimport them manually to the new Traffic Manager.

Due to the nature of the replace-and-terminate process described here, there is no direct roll back path should you need to return to the previous version. If you need to return to the previous version, complete a full configuration backup first and then preserve a copy of each existing Traffic Manager instance that you intend to remove.

To upgrade using this method, your cluster must be at least one Traffic Manager instance smaller than the maximum size that your license key permits. This is because you must add a new Traffic Manager running the upgraded version of the software to your cluster before removing one of the older instances. If your total number of instances is already at a maximum, use the alternative method described in [“Upgrading an EC2 Cluster Using the Backup and Restore Method” on page 44](#).

**Note:** When the cluster is in a mixed state (for example, the Traffic Managers are using different software versions) do not make any configuration changes until all Traffic Managers in the cluster are running the upgraded version.

### For configurations using the Pulse Secure Virtual Web Application Firewall (vWAF)

For cluster synchronization to succeed during the following procedure, you must ensure that your cluster members are using the same vWAF version as the new instance you are adding. If the Traffic Manager indicates that there is a vWAF configuration synchronization issue between your cluster members, Pulse Secure recommends using the Updater tool included with vWAF on all your cluster members (including the newly added instance) before continuing.

For each Traffic Manager in your cluster, perform the following steps:

1. Start an instance of the new AMI.
2. Using the Admin UI, or the userdata preconfiguration parameters, join the new instance to your cluster. You should ensure that `join_tips` is set according to the rules shown in the parameter list contained in [“Preconfiguring the Traffic Manager at Launch Time” on page 38](#).

For Traffic Manager instances, note that the Traffic Manager hostname mappings (configured using the **System > Networking** page) are not migrated automatically. You must set these manually on each new instance. Traffic Manager software instances do not manage hostname mappings directly. You must ensure that the host virtual machine is correctly configured with the desired hostname mappings.

3. Terminate one of the existing instances in your cluster.
4. Repeat these steps until all the Traffic Managers in your cluster have been replaced. Replace instances one by one. Do not terminate an existing instance until its replacement has successfully joined the cluster.

### Upgrading an EC2 Cluster Using the Backup and Restore Method

You can also upgrade a cluster by taking a backup of its configuration, creating a new cluster using a new AMI, and applying the backup to the new cluster. You might need to use this method if your license does not permit you to add extra instances to your cluster, or if you want to run an upgraded cluster alongside your existing one for testing.

To upgrade using this method, perform the following steps:

1. Log in to the existing cluster and download a configuration backup from the **System > Configuration Backups** page.
2. Create a new cluster of the same size as the existing one, using the new AMI. Make each new instance join the new cluster, but do not perform any additional configuration procedures.

Upload the configuration backup to the new cluster, and navigate to the Restore section on the Backup detail page. The Admin UI allows you to choose which instance in your new cluster takes the place of each instance in the existing one. In most cases, if the new cluster is the same size as the existing one, the software maps existing instances to new ones appropriately.

**FIGURE 13** Mapping the Traffic Manager in a Backup

**Restore Configuration**

Restore this backup to be the current configuration. NOTE: this will replace the current configuration and all unsaved changes will be lost.

This backup contains machine specific information, such as networking configuration and Traffic IP groups.  
Do you want to:

- ☒ Replace the Traffic Managers in the backup with the machines in the current cluster...
- ☐ Restore backup without replacing Traffic Managers.

| Original Traffic Manager                  |   | New Traffic Manager                       |
|-------------------------------------------|---|-------------------------------------------|
| domU-12-31-39-00-12-F1.compute-1.internal | ➔ | domU-12-31-39-07-80-42.compute-1.internal |
| domU-12-31-39-00-3D-D2.compute-1.internal | ➔ | domU-12-31-39-00-3D-D2.compute-1.internal |

☐ Confirm

You should only need to alter the default mapping if your new cluster is larger or smaller than the existing one, or if you need to ensure that an instance in the existing cluster is replaced by a particular instance in the new one.

## 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.

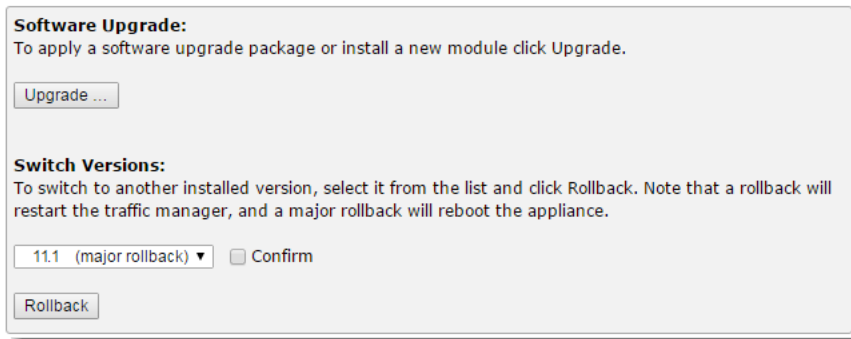
**Note:** This procedure does not retain any configuration you have made since upgrading to the current version. It is strictly a roll-back procedure that reinstates the selected software version and reinstates the previous configuration settings. Therefore, Pulse Secure strongly recommends that you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

**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 forward again to a later release, 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:

FIGURE 14 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. Connect to the Traffic Manager 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) 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]:
```

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 appliance reboots continue to use the version you select from the rollback program.

**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.

## 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 Traffic Manager “boot menu” from the command line.

**Note:** 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 complete a manual version change, perform the following steps:

1. Log in to the instance command line 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 instance.

## Expanding the Log File Partition

If you want to allocate more space for your log files, expand the virtual machine disk and then resize the Traffic Manager’s file system to take advantage of the extra space.

### ATTENTION

Before you begin, make sure you have performed a backup of your Traffic Manager configuration and log files.

To increase disk capacity for an existing virtual machine, EC2 requires you to instead create a new disk volume at the increased size and then migrate your data to it. You then discard the old disk volume. For more details, see the AWS Documentation website:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-expand-volume.html>

After you have increased the disk capacity, resize the Traffic Manager log partition to take advantage of the additional space.

**To resize the log partition**

1. Start the instance using the AWS Console or command line tools.
2. Engage the instance 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
```

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

# Creating a Traffic Manager Instance on Google Compute Engine

---

This chapter describes how to install and configure the Traffic Manager virtual machine on Google Compute Engine (GCE). To install the Traffic Manager software variant on an existing GCE-based Linux or UNIX virtual machine, see instead [“Installing the Traffic Manager Software on EC2 or GCE” on page 11](#).

To create a Traffic Manager virtual machine, launch one or more instances of the Traffic Manager image available from the GCE package launcher. No other installation procedure is necessary. All you need to do is login to the instance and configure it.

This chapter contains the following sections:

- [Before You Begin](#) ..... 49
- [Launching a Virtual Machine Instance](#) ..... 51
- [Connecting to the Admin UI](#) ..... 53
- [Using the Initial Configuration Wizard](#) ..... 54
- [Configuring an Instance From the Command Line](#) ..... 58
- [Removing an Instance](#) ..... 61
- [Upgrading Your Traffic Manager](#) ..... 61
- [Expanding the Log File Partition](#) ..... 67

## Before You Begin

**Note:** Make sure you have met the requirements listed in [“Prerequisites” on page 8](#).

Your Traffic Manager software is primarily controlled through a Web-based administration interface served by the Traffic Manager Admin Server. This interface provides the Admin UI, and handles communications with the core Traffic Manager software.

To access the Admin UI, you connect to TCP port 9090 on the external IP address of the virtual machine instance. However, traffic to most ports is blocked by default in GCE's firewall rules and must be explicitly enabled through the creation of new firewall rules.

The Traffic Manager also requires additional ports to be made accessible in certain situations. The following table lists all ports and their use:

| Port  | Protocol  | Reason                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9090  | TCP + UDP | For Web-based Admin UI access and intercluster communication.                                                                                                                                                                                                                                                                                                                                                                                                         |
| 22    | TCP       | For SSH command line access.<br><br><b>Note:</b> Port 22 is allowed by default in GCE, though Pulse Secure recommends restricting access through suitable firewall rules to prevent unauthorized access. To further prevent unauthorized SSH intrusion to specific instances, Pulse Secure recommends enabling the <i>SSH intrusion prevention</i> feature during initial configuration. For more details, see <a href="#">“Setting System Security” on page 56</a> . |
| 9080  | TCP + UDP | For intercluster communications between multiple Traffic Manager instances when one or more instances are outside the GCE network.<br><br>For example, where multiple Traffic Manager clusters are managed by the Traffic Manager’s multi-site cluster management feature. For more information about this feature, see the <i>Pulse Secure Virtual Traffic Manager: User’s Guide</i> .                                                                               |
| 9070  | TCP       | Access to the Traffic Manager REST API.                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 8083  | TCP       | Required for Pulse Secure Virtual Web Application Firewall internal communications. Typically, instances within the same GCE network do not require these ports to be enabled through firewall rules. However, where you are managing multiple Traffic Managers across different networks, such firewall rules must be created.                                                                                                                                       |
| 8086  | TCP       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 11000 | TCP       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 11002 | TCP       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 11007 | TCP       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

**Note:** The ports given in this table are the default values and can be modified through the Admin UI after you have completed initial configuration of your Traffic Manager software. You should ensure you update your firewall rules if you modify any of the ports shown. For more details, see the *Pulse Secure Virtual Traffic Manager: User’s Guide*.

#### ATTENTION

Further to the above, you must also create firewall rules applicable to any services you intend to configure in the Traffic Manager, if such services use ports or protocols not already allowed within GCE.

To create a firewall, use either the GCE management console or the “gcloud compute” command line API.

#### To create firewall rules in the GCE console

1. Login to GCE (<https://cloud.google.com>) and click **My console**.
2. In the navigation bar, click **Networking > Firewall rules**.
3. To add a new firewall rule, click **New firewall rule**.
4. Type a name for your rule, and optionally type a description.
5. Select the network you want this rule to apply to.



- For **Source filter**, select “IP range” and then type the IP address range you want this rule to apply to.

**Note:** If you need to also add Source tags to this rule, to determine which instances outbound traffic is allowed from, use instead the gcloud compute API method described later in this section.

- Choose the protocol and port that you want to allow through the firewall.
- Type a target tag name for this rule, if applicable. When a tag is applied to a virtual machine instance, the instance allows inbound connections in accordance with all firewall rules marked with that tag.
- Click **Create** to create the rule.

**Note:** For full details of each field and applicable values, see the Google Cloud Platform Help documentation. Click the *question-mark* icon in the title bar to access the help.

### To create firewall rules using the gcloud compute API

- To create a new firewall rule, execute the following command:

```
gcloud compute firewall-rules create <name> [--network <network>] --allow
<protocol>:<port> --source-ranges <ip network> --source-tags <tag1>[,<tag2>,...] --target-
tags <tag1>[,<tag2>,...]
```

Substitute the variables in angled brackets (<>) with your desired settings:

- <name>: The firewall rule name.
- <network>: (optional) The GCE network this rule should apply to. If you are operating within a single GCE network, no value is necessary here so you can leave this argument out.
- <protocol>: The protocol to allow. Typically “TCP” or “UDP”.
- <port>: The port to allow.
- <ip\_network>: The IP address range from which traffic is allowed. “0.0.0.0/0” enables all IP addresses for the given protocol and port.
- <tag1>,<tag2>,...: The source and target tags to associate with this rule. Set a source tag to control whether outbound traffic is allowed from Traffic Manager instances using this tag, and set a target tag to control whether Traffic Manager instances using this tag can accept inbound traffic.

- To confirm that your firewall rule has been successfully added, use the following command:

```
gcloud compute firewall-rules list
```

**Note:** To learn more about the gcloud compute API, see <https://cloud.google.com/sdk/gcloud>.

## Launching a Virtual Machine Instance

To launch a new instance of the Traffic Manager virtual machine, use the *GCP Marketplace* Web site:

<https://console.cloud.google.com/marketplace>

Browse or use the search tool to locate the **Pulse Secure Virtual Traffic Manager** package applicable to your requirements.

Click the package icon to show the package detail screen, and then click **Launch on Google Cloud Platform** to create a new instance.

**FIGURE 15** Creating a new Traffic Manager virtual machine instance

The screenshot shows the Google Cloud Platform console configuration for a new virtual machine instance. The form is organized into several sections:

- Deployment name:** A text input field containing "brocade-~~vtm~~-01".
- Zone:** A dropdown menu showing "us-central1-f".
- Machine type:** A dropdown menu showing "n1-standard-2 (2 vCPUs, 7.5 GB memory)".
- Boot Disk:** A section containing:
  - Disk type:** A dropdown menu showing "Standard Persistent Disk".
  - Disk size in GB:** A text input field containing "16".
- Networking:** A section containing:
  - Firewall:** A section with the text "Add tags and firewall rules to allow specific network traffic from the Internet". It includes three checked checkboxes: "Allow HTTP traffic", "Allow HTTPS traffic", and "Allow TCP 9090 traffic". A "More" link is also present.
- API Access:** A section containing:
  - Compute API:** A checked checkbox with the text "Allow read write access to Google Compute Engine APIs on the VM."

A blue "Deploy" button is located at the bottom left of the form.

Your new instance requires a number of standard configuration items before it can finally launch. The following table describes these options:

| Field           | Description                                                                                                                                                                                                                              |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Deployment Name | The identifying name for your Traffic Manager instance.                                                                                                                                                                                  |
| Zone            | The geographic zone into which your Traffic Manager instance is to be launched. Individual zones might have differing computing resources available and specific access restrictions. Contact your service provider for further details. |
| Machine type    | The specification of the computing resources allocated to your Traffic Manager virtual machine. For example, CPU core count and RAM.                                                                                                     |
| Disk type       | The disk image or snapshot your Traffic Manager instance is to launch from.                                                                                                                                                              |
| Disk size in GB | The disk size for your Traffic Manager instance.                                                                                                                                                                                         |
| Firewall        | The basic traffic types you want to allow for this Traffic Manager instance. By default, GCE creates firewall rules for HTTP and HTTPS traffic, and access to the Web-based Traffic Manager Admin UI on TCP port 9090.                   |

| Field         | Description                                                               |
|---------------|---------------------------------------------------------------------------|
| IP forwarding | Use IP forwarding with this Traffic Manager instance.                     |
| API access    | Whether to allow API access to Google Cloud services in the same project. |

To create a new Traffic Manager instance

1. Type an identifying name for the instance.
2. Select the desired geographic zone and machine type for the instance.
3. Ensure the boot disk corresponds to your computing resource requirements.
4. Pulse Secure recommends not changing the default disk size as this might affect the performance and functionality of your Traffic Manager.
5. Pulse Secure recommends leaving the firewall rules in their default enabled state. In particular, if you disable access to TCP port 9090, you cannot access the Traffic Manager Admin UI to configure the instance. For more information, see [“Before You Begin” on page 49](#).
6. To use IP Forwarding with this Traffic Manager instance, click **More** in the Networking section and set IP forwarding to "On":

FIGURE 16 Setting IP forwarding for your Traffic Manager instance



7. The Traffic Manager needs access to the Google Cloud *Compute API*, as indicated in the API Access section. Keep this option enabled to ensure your instance can function correctly.

**Note:** Without ComputeAPI access, the Traffic Manager cannot produce complete Technical Support Reports. It also cannot display various statistical and diagnostic information concerning the instance.

8. Click **Deploy** to launch the Traffic Manager instance.

## Connecting to the Admin UI

After your new Traffic Manager instance has been created, click through to the instance details page and locate the *External IP* field. Type this address into your Web browser, together with port 9090, to access the Admin UI for your instance:

`https://<admin_ui_address>:9090/`

**Note:** While the internal IP address of an instance remains constant over its lifetime regardless of state, the external IP address is allocated at run time and therefore might not remain the same after an instance restart.

When you connect to the Admin UI for the first time, the Traffic Manager requires you to complete the initial configuration wizard. See [“Using the Initial Configuration Wizard” on page 54](#).

During initial configuration, you must enter a one-time generated password to confirm your ownership of the instance. Obtain this password from the instance serial console output, a link to which is displayed on the instance details screen, and apply it when requested during the initial configuration wizard.

Alternatively, run the following gcloud compute API command:

```
gcloud compute instances get-serial-port-output <instance_name>
<instance_name> is the unique name of the instance you are configuring.
```

**Note:** The same link is provided in the initial configuration wizard.

## Confirming the Traffic Manager's Identity

Before you connect to the Admin UI of a newly configured Traffic Manager instance, 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). You can safely ignore this warning as the certificate is self-signed, and the hostname in the certificate might not match the URL you have used to access it (an instance's external IP address is different to the private IP address the instance uses within the GCE network).

To verify the identity of the instance you are connecting to, check that the SHA-1 fingerprint of the self-signed SSL certificate matches the fingerprint of the Traffic Manager instance you want to configure. Consult the documentation for your Web browser for instructions on how to display the SSL certificate and associated SHA-1 fingerprint information for a Web site you are visiting.

To view the SHA-1 fingerprint for a Traffic Manager instance configured in GCE, check the instance console. Click "Serial console output" in the instance details page in the GCE Web portal, or run the following gcloud compute API command:

```
gcloud compute instances get-serial-port-output <instance_name>
<instance_name> is the unique name of the instance you are configuring.
```

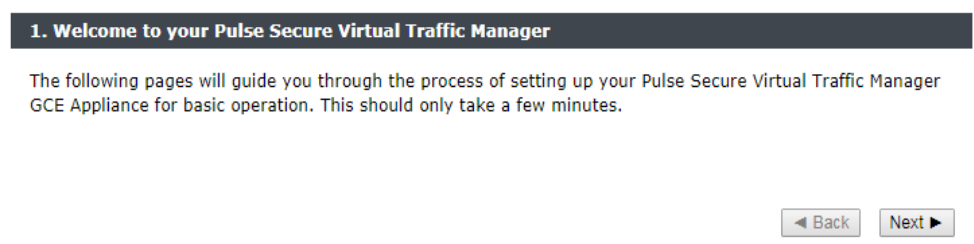
**Note:** There might be a delay of several minutes after instance creation before the console output is available.

## Using the Initial Configuration Wizard

A newly created Traffic Manager instance requires some basic information to function normally. The Traffic Manager gathers this information over a series of steps that form the initial configuration wizard.

Access the first page of wizard by entering the URL of the instance Admin UI into your Web browser:

FIGURE 17 Step-by-step Configuration Process

**Initial configuration, step 1 of 6**


**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 GCE Appliance for basic operation. This should only take a few minutes.

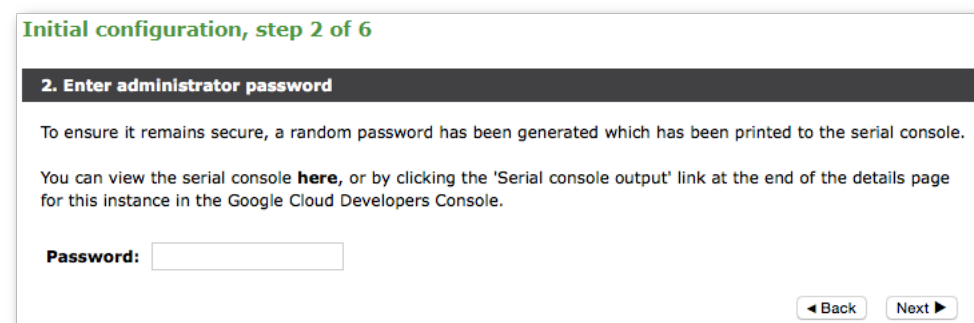
◀ Back   Next ▶

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

## Entering the Administrator Password

The Traffic Manager uses the password you specify in this step to verify that you are the person who launched the instance. Verifying the identity helps prevent an unauthorized user from gaining control of a newly launched instance.

FIGURE 18 Enter the Preconfigured Administrator Password



**Initial configuration, step 2 of 6**

**2. Enter administrator password**

To ensure it remains secure, a random password has been generated which has been printed to the serial console.

You can view the serial console [here](#), or by clicking the 'Serial console output' link at the end of the details page for this instance in the Google Cloud Developers Console.

**Password:**

◀ Back   Next ▶

You can find the password in the instance's serial console. As an additional security measure, and to ensure that you are authorized to configure the instance, the console log is only available to the GCE user who created the instance or a user in the same GCE project with adequate permissions.

To view the serial console, click the link shown. Alternatively, use the link provided in the instance details screen in the GCE Web management portal, or the gcloud compute API command:

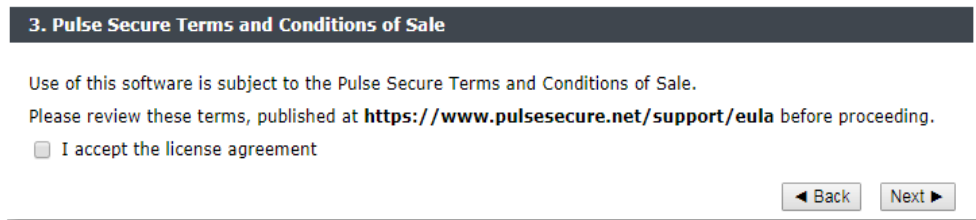
```
gcloud compute instances get-serial-console-output <instance_name>
```

Retrieve the randomly generated password from the console log and enter it in the wizard. Then click **Next**.

## Accepting the License Agreement

Read and accept the Pulse Secure Terms and Conditions of Sale:

FIGURE 19 Terms and Conditions of Sale

**Initial configuration, step 3 of 6**

**3. 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 ▶

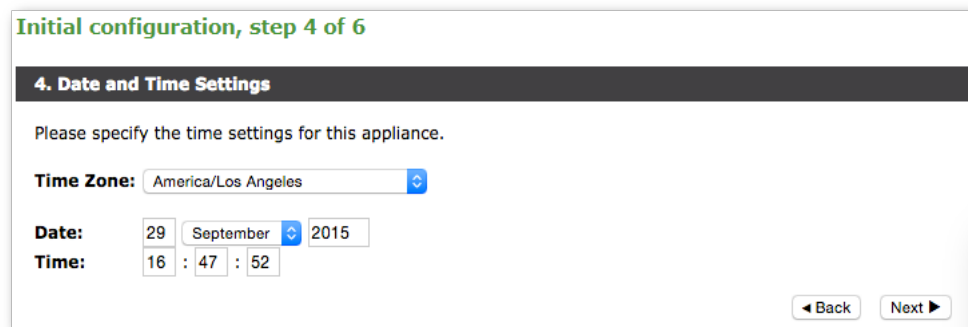
Please read the entire agreement. If you agree to its terms, click the “I accept the license agreement” check box and click **Next** to continue.

**Note:** You cannot use the Traffic Manager software until you accept the license agreement and you have completed the wizard.

## Setting the Date and Time

Set the date and time for your Traffic Manager instance. Setting this correctly ensures that any logs and diagnostic messages generated by the Traffic Manager have the correct timestamps:

FIGURE 20 Select the Time Zone



**Initial configuration, step 4 of 6**

**4. Date and Time Settings**

Please specify the time settings for this appliance.

**Time Zone:** America/Los Angeles

**Date:** 29 September 2015

**Time:** 16 : 47 : 52

◀ Back   Next ▶

## Setting System Security

Use the password you set here when you log in to the Traffic Manager Admin UI through a Web browser. If you enable password authentication for SSH, you can also use this password when you log in to an instance using SSH (with the username “admin”).

For all newly created GCE virtual machines, TCP port 22 (used for SSH command line access) is open by default for connections through the firewall. The Traffic Manager contains an SSH intrusion prevention tool to help prevent brute-force SSH attacks on your Traffic Manager instance. Pulse Secure strongly recommends you enable this option.

**Note:** You can additionally create a new GCE firewall to disable port 22 if so desired. For more information, see “Before You Begin” on page 49.

FIGURE 21 Setting System Security

**Initial configuration, step 5 of 6**

### 5. 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

◀ Back   Next ▶

## Uploading the License Key

The Traffic Manager is available as a range of set-frequency billing subscriptions where the license is built in, and as a Community Edition/Bring Your Own License (BYOL) instance. For the Community Edition/BYOL instance, the Initial Configuration Wizard provides an additional step to configure your instance with the required licensing.

For set-frequency billing subscriptions, this step does not appear.

FIGURE 22 Uploading the License Key

**Initial configuration, step 6 of 7**

### 6. 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**. This option is available for KVM, VMware and EC2 platforms only
- ☐ 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**

◀ Back   Next ▶

Click one of the following options:

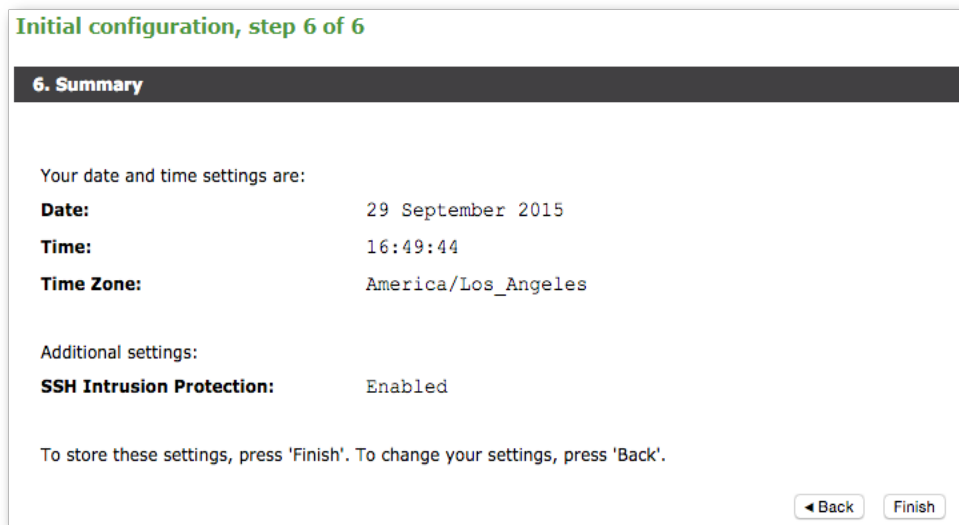
- To upload a license key now, click “Upload a license key for this traffic manager” and then click **Choose file** to select a suitable key file from your local workstation. Click **Next** to verify.
- To add a license key later, or to use the Traffic Manager as the Community Edition, click “Skip licensing for now” and then click **Next**.

To learn more about the Community Edition, see [“The Community Edition” on page 95](#).

## Viewing the Summary Page

The Summary page displays the configuration settings for you to review.

FIGURE 23 Summary Page



The screenshot shows a web interface titled "Initial configuration, step 6 of 6". Below the title is a dark header bar with the text "6. Summary". The main content area displays the following information:

Your date and time settings are:

|                   |                     |
|-------------------|---------------------|
| <b>Date:</b>      | 29 September 2015   |
| <b>Time:</b>      | 16:49:44            |
| <b>Time Zone:</b> | America/Los_Angeles |

Additional settings:

|                                  |         |
|----------------------------------|---------|
| <b>SSH Intrusion Protection:</b> | Enabled |
|----------------------------------|---------|

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

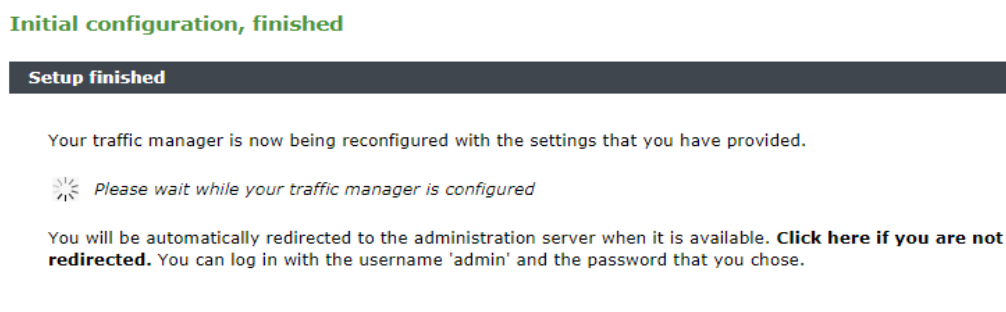
At the bottom right, there are two buttons: "Back" and "Finish".

Click **Back** to make changes or click **Finish** to complete the installation.

**Note:** The Traffic Manager settings shown here are replicated on the **System > Traffic Managers** page once you have completed initial configuration.


After clicking the Finish button, status message appear as the Traffic Manager is being configured.

FIGURE 24 Initial configuration is progressing



The screenshot shows a web interface titled "Initial configuration, finished". Below the title is a dark header bar with the text "Setup finished". The main content area displays the following information:

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

 Please wait while your traffic manager is configured

You will be automatically redirected to the administration server when it is available. **Click here if you are not redirected.** You can log in with the username 'admin' and the password that you chose.

After a short wait, you are redirected to the login page of the Admin UI. Log in using the username (admin) and the admin password you set during the installation wizard.

## Configuring an Instance 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” on page 54.](#)



To start the configuration program, login to the instance 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) 2020, Pulse Secure, LLC. 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 Traffic Manager.
```

```

Use of this software is subject to the Pulse Secure 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 Pulse Secure 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.

**Note:** The Traffic Manager is available as a range of set-frequency billing subscriptions where the license is built in, and as a Community Edition/Bring Your Own License (BYOL) instance. The following step concerns software licensing options for the Community Edition/BYOL instance only, and might not appear if you are running the configuration program on an instance with a built-in license.

```
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” on page 95](#).

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

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 instance 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. Pulse Secure 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*.

Please provide the port on which the REST API should listen for requests (default 9070).

REST port [9070]:

If you enable the REST API, enter the port number on which you want the REST service to listen for requests.

You have specified the following settings:

|                         |                                                       |
|-------------------------|-------------------------------------------------------|
| No license file:        | The traffic manager will run as the Community Edition |
| Timezone:               | UTC                                                   |
| SSH protection enabled: | Yes                                                   |
| REST enabled:           | Yes                                                   |

REST port: 9070

Proceed with configuration? Y/N:

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

## 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>
```

## Removing an Instance

To remove a Traffic Manager instance, delete it from the GCE Web management portal.

**Note:** If you delete an instance, the instance is shut down and is permanently destroyed. You lose all configuration and data associated with that Traffic Manager instance.

## Upgrading Your Traffic Manager

This section contains details of how to upgrade and, where necessary, revert your Traffic Manager instance when a new version is released.

### Before You Start

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.

#### CAUTION

If you are upgrading from Traffic Manager versions earlier than 9.9, you must install a new instance of the Traffic Manager and import your configuration into it. This is due to the underlying operating system on earlier versions 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 2GB 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 700MB must be free on the / (root) partition, and at least 600MB must be free on the /logs partition. To confirm the available free disk space, use the **System > Traffic Managers** page of the Admin UI.

**Note:** Pulse Secure 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

**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 appliance platform. 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, GCE instances), 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 GCE instances), 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

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 instance.

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” on page 65](#)).

**Note:** 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 instance 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.

To upgrade the Traffic Manager, use either the Admin UI or the Traffic Manager instance command line. For either method, first obtain the Traffic Manager GCE upgrade package file. Packages are named according to the following convention:

```
ZeusTM_<version>_GCE-Appliance-Upgrade-x86_64.tgz
```

In the above filename, <version> corresponds to the Traffic Manager version you want to install.

### 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 62](#)).

### To upgrade using the command line

1. Copy the package file to the instance 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

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

2. Connect to the Traffic Manager 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`.

- 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.

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

- Reboot the Traffic Manager when convenient from the Admin UI or command line (type "reboot").

## Upgrading a Cluster Using the Backup and Restore Method

You can also upgrade a cluster by taking a backup of its configuration, creating a new cluster based on the more recent Traffic Manager version, and applying the backup to the new cluster. Use this method if you want to run an upgraded cluster alongside your existing one for testing purposes.

### To upgrade using the backup and restore method

- Login to the Admin UI of an existing cluster member and download a configuration backup from the **System > Backups** page.
- Deploy a new cluster of the same size as the existing one, using the newer Traffic Manager GCE virtual machine. Make each new instance join the new cluster, but do not perform any additional configuration procedures.
- Import the configuration backup into the new cluster using the **System > Backups** page, and navigate to the "Restore Configuration" section on the Backup detail page. The Admin UI allows you to choose which instance in your new cluster takes the place of each instance in the existing one. In most cases, if the new cluster is the same size as the existing one, the software maps existing instances to new ones appropriately.

FIGURE 25 Mapping the Traffic Manager in a Backup

**Restore Configuration**

Restore this backup to be the current configuration. NOTE: this will replace the current configuration and all unsaved changes will be lost.

This backup contains machine specific information, such as networking configuration and Traffic IP groups.  
Do you want to:

- ☒ Replace the Traffic Managers in the backup with the machines in the current cluster...
- ☐ Restore backup without replacing Traffic Managers.

| Original Traffic Manager                  |   | New Traffic Manager                       |
|-------------------------------------------|---|-------------------------------------------|
| domU-12-31-39-00-12-F1.compute-1.internal | ➔ | domU-12-31-39-07-80-42.compute-1.internal |
| domU-12-31-39-00-3D-D2.compute-1.internal | ➔ | domU-12-31-39-00-3D-D2.compute-1.internal |

☐ Confirm

You should only need to alter the default mapping if your new cluster is larger or smaller than the existing one, or if you need to ensure that an instance in the existing cluster is replaced by a particular instance in the new one.

## 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:

FIGURE 26 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. Connect to the Traffic Manager 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) 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]:

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 appliance reboots continue to use the version you select from the rollback program.

**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.

## 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 Traffic Manager "boot menu" from the command line.

**Note:** 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 complete a manual version change, perform the following steps:

1. Log in to the instance command line 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 instance.



## Expanding the Log File Partition

If you want to allocate more space for your log files, expand the instance disk and then resize the Traffic Manager's file system to take advantage of the extra space.

### ATTENTION

Before you begin, make sure you have performed a backup of your Traffic Manager configuration and log files.

GCE allows you to increase the size of the persistent disk associated with your Traffic Manager instance as necessary, even if the instance is running. For full details, see the GCE Documentation website:

[https://cloud.google.com/compute/docs/disks/add-persistent-disk#resize\\_pd](https://cloud.google.com/compute/docs/disks/add-persistent-disk#resize_pd)

After you have increased the disk capacity, resize the Traffic Manager log partition to take advantage of the additional space.

### To resize the log partition

1. Engage the instance 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
```

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



# Creating a Traffic Manager Cluster on Microsoft Azure

To use the Pulse Secure Virtual Traffic Manager (Traffic Manager) on the Microsoft Azure platform, you create one or more virtual machine “instances” using the Azure Certified Traffic Manager template available from the Azure marketplace. Each instance is a version of the Traffic Manager Virtual Appliance variant, optimized for Azure. No other installation is necessary, although you must log into a newly deployed instance to configure the Traffic Manager software before it can be used to manage your services.

This chapter contains the following sections:

|                                                                                |    |
|--------------------------------------------------------------------------------|----|
| • <a href="#">Before You Begin</a> .....                                       | 69 |
| • <a href="#">Creating a Traffic Manager Cluster in the Azure Portal</a> ..... | 69 |
| • <a href="#">Connecting to the Admin UI</a> .....                             | 78 |
| • <a href="#">Using the Initial Configuration Wizard</a> .....                 | 79 |
| • <a href="#">Configuring an Instance From the Command Line</a> .....          | 84 |
| • <a href="#">Removing a Traffic Manager</a> .....                             | 87 |
| • <a href="#">Upgrading Your Traffic Manager</a> .....                         | 87 |

## Before You Begin

**Note:** Make sure that you have met the requirements listed in [“Prerequisites” on page 8](#).

To achieve high availability (HA), deploy a cluster of at least two Traffic Manager instances. Azure implements high availability through automatically load-balancing traffic to the public service IP address and port that you specify when you deploy your instances. To add specific load balancer and network security rules, see the instructions at [“Configuring Your Resource Group to use More Than One Service Port” on page 75](#). If you do not need HA, select a cluster size of 1 during the deployment process.

A cluster of Traffic Managers created inside the Azure portal cannot be joined to other non-Azure Traffic Manager instances.

## Creating a Traffic Manager Cluster in the Azure Portal

Use the Azure Management portal to create a cluster of virtual machine instances based on the Traffic Manager template contained in the Azure marketplace.

### To create a Traffic Manager cluster using the Azure Management portal

1. Login to the Azure Management portal (<https://portal.azure.com>).
2. On the main portal page, locate the Traffic Manager template using one of the following methods:

- Click **+ Create a resource** and type “Pulse Secure” into the search bar.
  - Click the Marketplace icon in the main window, ensure **Everything** is highlighted in the category list, and then type “Pulse Secure” into the search bar.
  - Click the Marketplace icon in the main window and scroll through the list to manually locate the Traffic Manager.
3. The Traffic Manager is available under a range of licensing options. Click the desired variant to display the product information blade.
  4. Click Create to display the “Create” blade.

FIGURE 27 The Create blade

The screenshot shows the 'Create Brocade Vi...' blade with the 'Basics' configuration step selected. The left sidebar lists the following steps:

- 1 Basics: Configure basic settings
- 2 Service Configuration: Configure settings for the service ...
- 3 Network Settings: Configure Virtual Network
- 4 Instance Configuration: Configure Instance settings
- 5 Summary: Brocade Virtual Traffic Manager (S...
- 6 Buy

The main configuration area for 'Basics' includes the following fields:

- Cluster Name**: vtmtest1 (with a green checkmark)
- License**: Standard Edition - 1 Gbps (dropdown)
- Version**: 10.4 LTS (dropdown)
- Instance Count**: 2 (with a green checkmark)
- Authentication type**: Password (selected), SSH public key (available)
- Password**: [Redacted] (with a green checkmark)
- Confirm password**: [Redacted] (with a green checkmark)
- Subscription**: Pay-As-You-Go (dropdown)
- Resource group**: Create new (radio button selected), vTM-rg1 (with a green checkmark)
- Location**: East US (dropdown)

An 'OK' button is located at the bottom of the configuration area.

The steps needed to create your Traffic Manager cluster are displayed in the main “Create” blade, with the individual settings applicable to each highlighted step displayed in a sub-blade to the right.

5. For the “Basics” blade, ensure the following items are configured as listed below:
  - Cluster Name: Type a descriptive name for your Traffic Manager cluster.

- **License:** Choose your desired license type from the drop-down list.
- **Version:** Choose the product version you want to use.
- **Instance count:** The number of Traffic Manager instances you want to launch.

**Note:** Instances you create here are not automatically joined together to form a cluster. To create your cluster, you must first perform initial configuration on each Traffic Manager instance you create, and then use the “Join a cluster” wizard to join them together. For information about configuring an instance, see [“Using the Initial Configuration Wizard” on page 79](#). For information about creating a cluster, see [“About Creating a Traffic Manager Cluster” on page 99](#).

- **Authentication Type:** Your password or SSH Public Key. If you click Password, enter your password in the boxes provided. If you instead choose to authenticate using an SSH Public Key, enter your key in the text box provided.

**Note:** If you choose to use an SSH Public Key, you must connect to the virtual machine console of a newly created Traffic Manager instance and set an authentication password before you can perform initial configuration.

- **Subscription:** Choose your Azure subscription.
- **Resource Group:** Type a descriptive name for a new resource group for this cluster.
- **Location:** Choose the geographic location into which your Traffic Manager virtual machines are launched.

6. Click **OK** to continue to the Service Configuration blade:

**FIGURE 28** The service configuration blade.

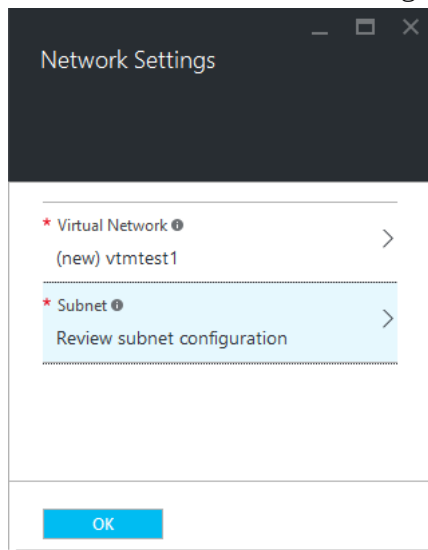
The screenshot shows the 'Service Configuration' blade with the following details:

- IP Address Name:** (new) vtmtest1
- DNS Label:** vtmtest1 (with a green checkmark and the domain eastus.cloudapp.azure.com)
- Service Port Number:** 80
- Service Protocol:** TCP (selected over UDP)
- OK button:** Located at the bottom left of the configuration area.

7. Ensure the following items are configured as listed below:

- **IP Address Name:** Choose a name to describe the public IP address Azure assigns to your cluster for service traffic (and for administrative access to your cluster members). Azure pre-populates this setting with the same name as your cluster. To change the IP address name, or to select an existing IP address, click the currently selected IP Address Name to display the “Choose Public IP Address” blade. Select an existing available IP Address, or type your new name into the box provided.
  - **DNS Label:** Type the domain name you want to use for the cluster. Azure pre-populates this field with the name of your cluster. The fully qualified domain name (FQDN) becomes a concatenation of the DNS label, the region selected, and “cloudapp.azure.com”. For example, “vtmtest1.eastus.cloudapp.azure.com”.
  - **Service Port Number:** Type the port number for the service your cluster is going to manage. To add further ports, modify the resource group settings after you have created the cluster.
  - **Service Protocol:** Choose the protocol for your service.
8. Click **OK** to continue to the Network Settings blade:

FIGURE 29 The Network Settings blade



9. Choose a *Virtual Network* for your Traffic Manager cluster to reside on. Azure assumes you want to create a new virtual network, using the cluster name as an identifier. To instead select a previously created virtual network, or to make changes to the address space being allocated to the new virtual network, click the virtual network name to reveal the “Choose Virtual Network” and “Create Virtual Network” blades.

FIGURE 30 Changing the virtual network

The figure consists of three side-by-side screenshots of the Pulse Secure web interface, illustrating the process of changing a virtual network.

- Left Screenshot (Network Settings):** Shows the 'Virtual Network' section with '(new) myvtmtest' selected. Below it, the 'Subnet' section has a red exclamation mark icon and a 'Configure subnets' link. An 'OK' button is at the bottom.
- Middle Screenshot (Choose virtual network):** Displays a message: 'These are the virtual networks in the selected subscription and location 'East US'.' Below this is a 'Create new' button and a list of existing virtual networks, including 'vtmtest1' and 'vTM-rg1'.
- Right Screenshot (Create virtual network):** Shows the configuration form for a new virtual network. The 'Name' field contains 'myvtmtest'. The 'Address space' field contains '10.0.0.0/16' and '10.0.0.0 - 10.0.255.255 (65536 addresses)'. An 'OK' button is at the bottom.

10. To save your changes and return to the “Network Settings” blade, click **OK**.

11. After you have selected your virtual network, you must configure the subnet your Traffic Manager cluster uses. Click **Configure Subnets** to choose the desired subnet:

FIGURE 31 Configuring the network subnet

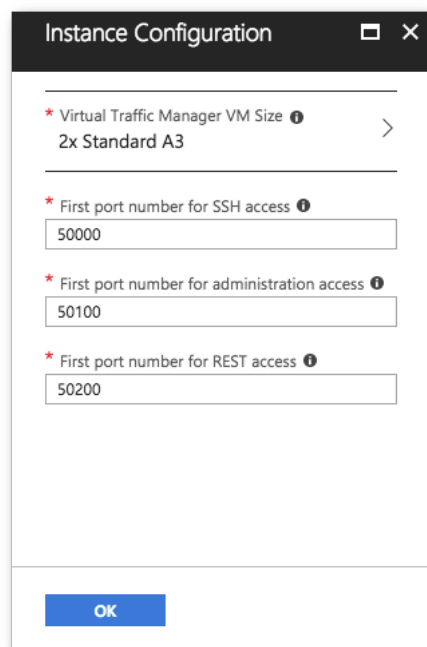
The figure consists of two side-by-side screenshots of the Pulse Secure web interface, illustrating the process of configuring a network subnet.

- Left Screenshot (Network Settings):** Shows the 'Virtual Network' section with '(new) myvtmtest' selected. Below it, the 'Subnet' section has a red exclamation mark icon and a 'Configure subnets' link. An 'OK' button is at the bottom.
- Right Screenshot (Subnet):** Displays the configuration form for a subnet. The 'Traffic Manager Subnet name' field contains 'vtm' with a green checkmark. The 'Traffic Manager Subnet address prefix' field contains '10.0.0.0/24' with a green checkmark. An 'OK' button is at the bottom.

12. If you configured a new virtual network, enter a subnet name and address prefix in the “Subnet” blade. If you instead selected an existing virtual network, choose a subnet. Click **OK** to save your changes.

13. Click **OK** to continue to the Instance Configuration blade:

FIGURE 32 The Instance Configuration blade



The screenshot shows a window titled "Instance Configuration" with a close button (X) in the top right corner. The window contains three configuration sections, each with a red asterisk icon and an information icon (i):

- Virtual Traffic Manager VM Size**: A dropdown menu showing "2x Standard A3" with a right-pointing chevron.
- First port number for SSH access**: A text input field containing "50000".
- First port number for administration access**: A text input field containing "50100".
- First port number for REST access**: A text input field containing "50200".

At the bottom of the window is a blue button labeled "OK".

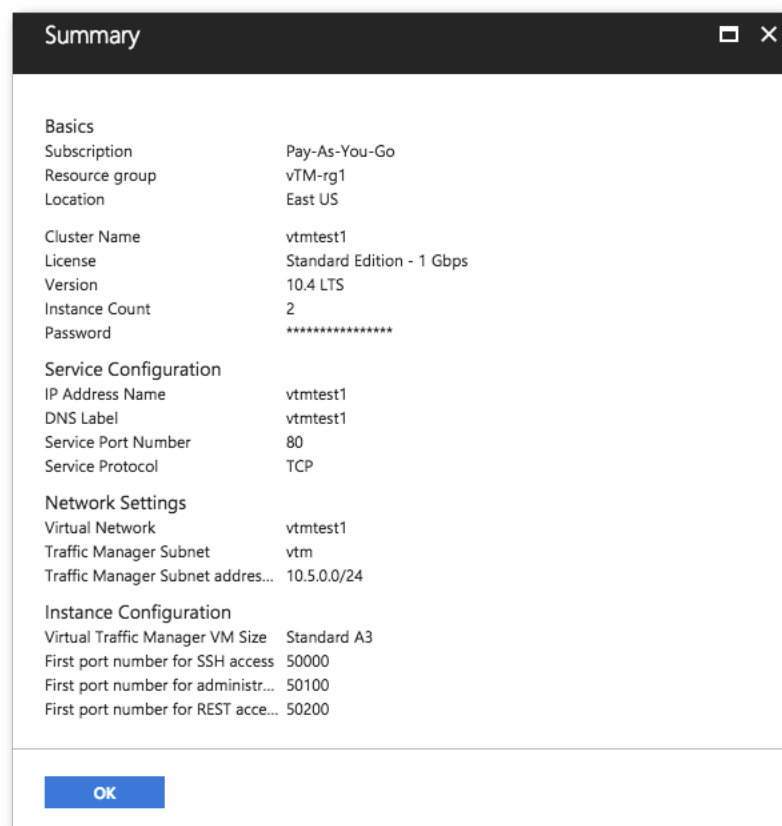
14. Configure the settings as described below:

- **Virtual Traffic Manager VM Size:** Choose the resource and pricing model for your Traffic Manager instances.
- **First port number for SSH access:** Azure uses Network Address Translation (NAT) to enable access to your individual Traffic Manager instances through specific ports on the public IP address for the service. Use this setting to determine the base port for SSH access to your Traffic Manager instances. Each instance in the cluster has SSH enabled at an incremental port number, starting at the base port you specify here. For example, choosing the default port of 50000 means that a cluster of 4 Traffic Managers uses ports 50000 to 50003 (one port per Traffic Manager).
- **First port number for Administration access:** As above, but for access to the Admin UI on each Traffic Manager instance in the cluster.
- **First port number for REST access:** As above, but for access to the REST interface on each Traffic Manager instance in the cluster.

15. Click **OK** to continue to the Summary blade:



FIGURE 33 Instance summary



The screenshot shows a 'Summary' dialog box with the following configuration details:

| Basics                             |                           |
|------------------------------------|---------------------------|
| Subscription                       | Pay-As-You-Go             |
| Resource group                     | vtm-rg1                   |
| Location                           | East US                   |
| Cluster Name                       | vtmtest1                  |
| License                            | Standard Edition - 1 Gbps |
| Version                            | 10.4 LTS                  |
| Instance Count                     | 2                         |
| Password                           | *****                     |
| Service Configuration              |                           |
| IP Address Name                    | vtmtest1                  |
| DNS Label                          | vtmtest1                  |
| Service Port Number                | 80                        |
| Service Protocol                   | TCP                       |
| Network Settings                   |                           |
| Virtual Network                    | vtmtest1                  |
| Traffic Manager Subnet             | vtm                       |
| Traffic Manager Subnet address...  | 10.5.0.0/24               |
| Instance Configuration             |                           |
| Virtual Traffic Manager VM Size    | Standard A3               |
| First port number for SSH access   | 50000                     |
| First port number for administr... | 50100                     |
| First port number for REST acce... | 50200                     |

An 'OK' button is located at the bottom left of the dialog box.

16. Verify the settings you have provided, and then click OK to display the Purchase blade.

17. Review the purchase terms and click Purchase to create your Traffic Manager instances.

After your Traffic Manager instances have been created, the Azure portal displays a blade showing the details for your newly created Resource Group. You can use the information shown here to obtain access to your Traffic Manager instances.

## Configuring Your Resource Group to use More Than One Service Port

To manage an additional service in your Traffic Manager cluster, or if the existing service uses multiple ports or protocols, add load balancer and network security rules after creating the cluster.

### To add load balancer and network security rules

1. Login to the Azure Management portal (<https://portal.azure.com>), then click the **Resource Groups** link in the menu bar.
2. Click the name of your Resource Group to show the resources it includes.
3. Click the name of the *Network Security Group* resource (typically named "<clustername>-vtmNSG"). If the Settings blade does not appear, click **All Settings**.
4. Click **Inbound Security Rules**.

5. Click **+Add**:

FIGURE 34 Adding an Inbound Security Rule

The screenshot shows a dialog box titled "Add inbound security rule" with the subtitle "vtmtest1-vtmNSG". It contains the following fields and options:

- Name:** An empty text input field.
- Priority:** A text input field containing the value "1310".
- Source:** Three radio button options: "Any" (selected), "CIDR block", and "Tag".
- Protocol:** Three radio button options: "Any" (selected), "TCP", and "UDP".
- Source port range:** A text input field containing the value "\*".
- Destination:** Three radio button options: "Any" (selected), "CIDR block", and "Tag".
- Destination port range:** A text input field containing the value "80".
- Action:** Two radio button options: "Deny" and "Allow" (selected).

An "OK" button is located at the bottom left of the dialog.

6. Configure the settings as shown:

- **Name:** Type a descriptive name for this rule.
- **Priority:** Enter the desired priority number. The higher the priority number, the lower the priority over other rules.
- **Source:** Select "Any".
- **Protocol:** Select your traffic protocol.
- **Source Port Range:** Leave this setting as the default "\*".
- **Destination:** Select "Any".
- **Destination Port Range:** Enter the port number or range for your traffic.
- **Action:** Select "Allow".

7. Click **OK** to save your rule.

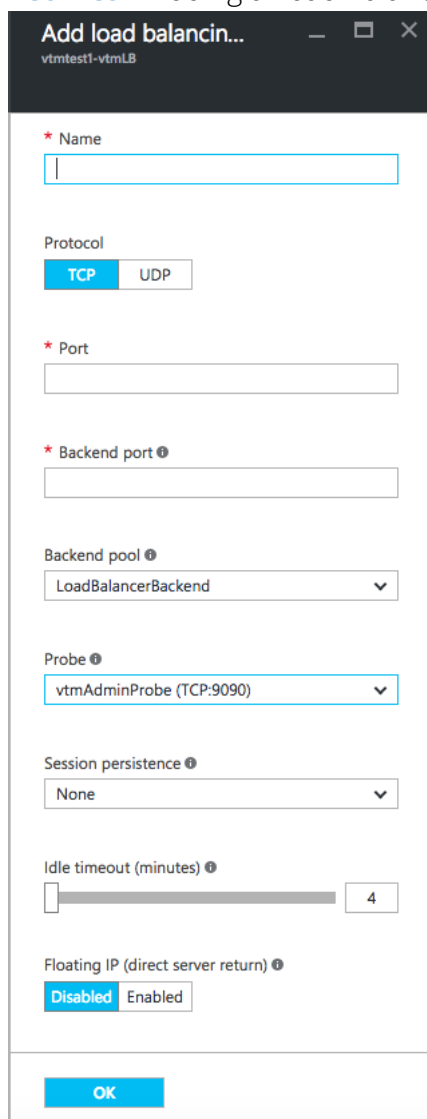
8. Navigate back to the blade for your resource group.

9. Click the *Load Balancer* resource name (typically named "<clustername>-vtmLB").

10. From the load balancer settings blade, click **Load balancing rules**.

11. Click **+Add**.

FIGURE 35 Adding a Load Balancing Rule



The screenshot shows a dialog box titled "Add load balancin..." with a subtitle "vtmtest1-vtmLB". The dialog contains the following fields and controls:

- Name:** A text input field with a red asterisk indicating it is required.
- Protocol:** Two buttons, "TCP" (selected) and "UDP".
- Port:** A text input field with a red asterisk indicating it is required.
- Backend port:** A text input field with a red asterisk indicating it is required.
- Backend pool:** A dropdown menu showing "LoadBalancerBackend".
- Probe:** A dropdown menu showing "vtmAdminProbe (TCP:9090)".
- Session persistence:** A dropdown menu showing "None".
- Idle timeout (minutes):** A slider control set to 4 minutes.
- Floating IP (direct server return):** Two buttons, "Disabled" (selected) and "Enabled".
- OK:** A blue button at the bottom left.

12. Configure the settings as shown:

- **Name:** Type a descriptive name for this rule.
- **Protocol:** Select your traffic protocol.
- **Port:** Enter the port number for your traffic.
- **Backend Port:** Set to the same value as **Port**.
- **Backend Pool:** Leave as the default value.
- **Probe:** Leave as the default value.
- **Session Persistence:** Select "None".

- **Idle Timeout (minutes):** Set to a timeout value suitable for your service.
- **Floating IP (direct server return):** Select "Disabled".

13. Click **OK** to save your rule.

## Connecting to the Admin UI

After your cluster has been created, use the fully qualified public DNS name or public IP address for this deployment in your Web browser to access the Admin UI on one of your Traffic Manager instances. For example, to access the Admin UI for the first instance in your cluster using the details shown in this guide, enter the following URL:

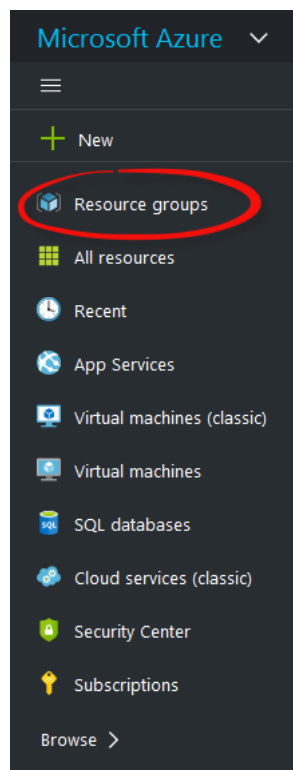
```
https://vtmtest1.eastus.cloudapp.net:50100
```

To view the full connection details for your cluster, see the Resource Group you created as part of the cluster deployment process.

### To locate the connection details for your cluster

1. Login to the Azure Management portal (<https://portal.azure.com>), then click the **Resource Groups** link in the menu bar:

FIGURE 36 The Azure portal menu bar (Resource Groups link highlighted)



2. Click the name of your Resource Group to show the resources it includes.

3. Click the name of the *Load Balancer* resource. If the load balancer settings blade does not automatically appear, click **All Settings**.
4. Click **Inbound NAT rules**. This shows 3 rules for each instance: adminNatPool.N, restNatPool.N and sshNatPool.N (where N is the instance number).
5. Pick the rule for the desired type of access and note the associated port number in the “Service” column.
6. To access the Traffic Manager instance, use the public IP address shown in the “Destination” column with the selected port number. Alternatively, use the DNS name for the service (listed in the *Public IP Address* resource).

**Note:** REST API access is initially disabled in your instances. To enable REST access, configure your Traffic Manager instances and enable REST through the Admin UI. For more details, see the *Pulse Secure Virtual Traffic Manager: User's Guide*.

To learn more about resource groups, see <https://azure.microsoft.com/en-gb/documentation/articles/resource-group-overview/>.

If your Traffic Manager instance has not yet been configured, first complete the Initial Configuration wizard. This wizard allows you to specify the initial time and security settings for your Traffic Manager. For more information, see [“Using the Initial Configuration Wizard” on page 79](#).

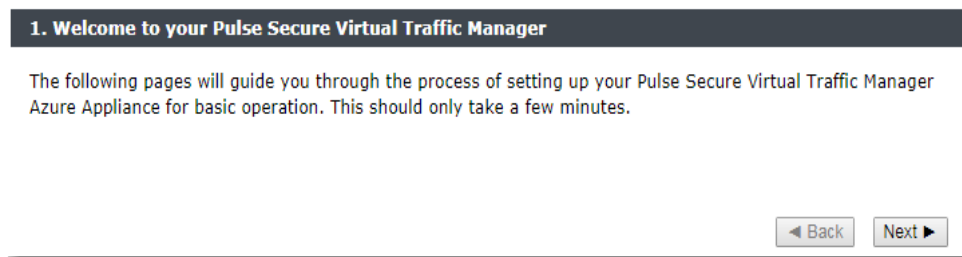
## Using the Initial Configuration Wizard

A newly created or reset Traffic Manager virtual machine requires some basic information to function normally. The Traffic Manager gathers this information over a series of steps that form the Initial Configuration wizard.

You can access the first page of the wizard by entering the URL of the Admin UI into your Web browser. The first window of the Initial Configuration wizard appears.

FIGURE 37 Initial Configuration Wizard

### Initial configuration, step 1 of 7



- Click Next to begin using the Initial Configuration wizard.

## Entering the Administrator Password

To authenticate yourself as the person who launched the instance, enter your administrator password on this page to proceed.

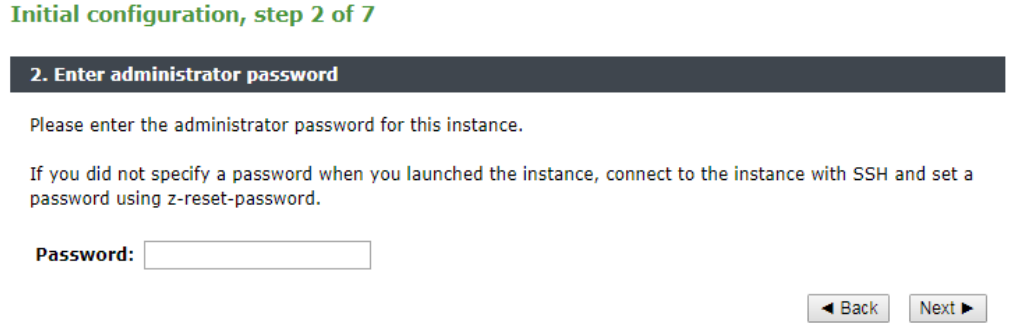
**Note:** If you provided an SSH key instead of a password when you created the cluster, you must first connect to the instance through SSH and use the `z-reset-password` command to set an administrator password before you can complete the Initial Configuration wizard.

### To enter the administrator password

1. Enter your password.
2. Click Next.

FIGURE 38 Enter Your Password for Authentication

Initial configuration, step 2 of 7



The screenshot shows a window titled "2. Enter administrator password". Below the title bar, it says "Please enter the administrator password for this instance." and "If you did not specify a password when you launched the instance, connect to the instance with SSH and set a password using `z-reset-password`." There is a text input field labeled "Password:" and two buttons at the bottom right: "Back" and "Next".

## Accepting the License Agreement

This step requires you to read and accept the Pulse Secure End User License Agreement.

### To accept the license agreement

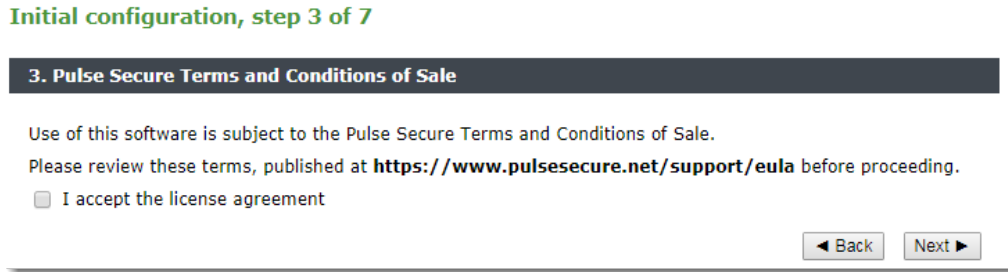
1. Read the entire license agreement located at the URL shown below.
2. Click the I Accept the License Agreement check box.

**Note:** The Traffic Manager software is usable only after you have accepted the license and completed the wizard.

3. Click **Next**.

FIGURE 39 End User License Agreement

Initial configuration, step 3 of 7



The screenshot shows a window titled "3. Pulse Secure Terms and Conditions of Sale". Below the title bar, it says "Use of this software is subject to the Pulse Secure Terms and Conditions of Sale." and "Please review these terms, published at <https://www.pulsesecure.net/support/eula> before proceeding." There is a checkbox labeled "I accept the license agreement" and two buttons at the bottom right: "Back" and "Next".

## Setting the Date and Time

Set the date and time for your Traffic Manager instance. Setting this correctly ensures that any logs and diagnostic messages generated by the Traffic Manager have the correct timestamps.

## To set the date and time

1. Specify the appropriate time zone.
2. Enter the date and time in the fields shown.
3. Click **Next**.

FIGURE 40 Set Date and Time

Initial configuration, step 4 of 7

**4. Date and Time Settings**

Please specify the time settings for this appliance.

**Time Zone:** America/Los Angeles ▼

**Date:** 3 October 2017

**Time:** 10 : 04 : 47

◀ Back Next ▶

## Setting System Security

The Traffic Manager requires a password for the primary (admin) user. This password overrides the administrator password you specified, if applicable, when you created the virtual machine.

Use the admin password to configure an instance through a Web browser, or when you log in to an instance using SSH (with the username admin).

The Traffic Manager also contains an SSH intrusion prevention tool to help prevent brute-force SSH attacks on your Traffic Manager instance. Pulse Secure strongly recommends you enable this option.

## To enable system security settings

1. Enter the admin user password you want to use.
2. Confirm the password by entering it again.
3. Click **Enable SSH Intrusion Prevention** if required.
4. Click **Next**.

FIGURE 41 Setting System Security

**Initial configuration, step 5 of 7**

**5. 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

◀ Back   Next ▶

## Uploading the License Key

**Note:** This step applies only to unlicensed Traffic Manager variants and does not appear for set-frequency billing subscriptions where the license is built in.

### To upload the license key

1. Click **Upload a license key for this traffic manager**
2. Click the Choose File button to select the license key to want to upload.
3. Click **Next**.

FIGURE 42 Uploading the License Key

**Initial configuration, step 6 of 7**

**6. 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**. This option is available for KVM, VMware and EC2 platforms only
- ☐ 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**

◀ Back   Next ▶

This page includes the option to skip uploading a license key and instead run the Traffic Manager software as the Community Edition. For further information, see [“The Community Edition” on page 95](#).

You can upload a full license key file using the following methods:



- When you first log in to the Admin UI of an unlicensed Traffic Manager instance.
- At any time, through the **System > Licenses** page.

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

## Reviewing the Settings Summary

The Summary page displays the settings you configured when you were using the Initial Configuration wizard.

### To review the settings summary

1. Review the information displayed.
2. Click **Finish** or click **Back** to make changes.

FIGURE 43 Summary Page  
Initial configuration, step 7 of 7

**7. Summary**

Your date and time settings are:

|                   |                     |
|-------------------|---------------------|
| <b>Date:</b>      | 3 October 2017      |
| <b>Time:</b>      | 10:05:34            |
| <b>Time Zone:</b> | America/Los_Angeles |

Additional settings:

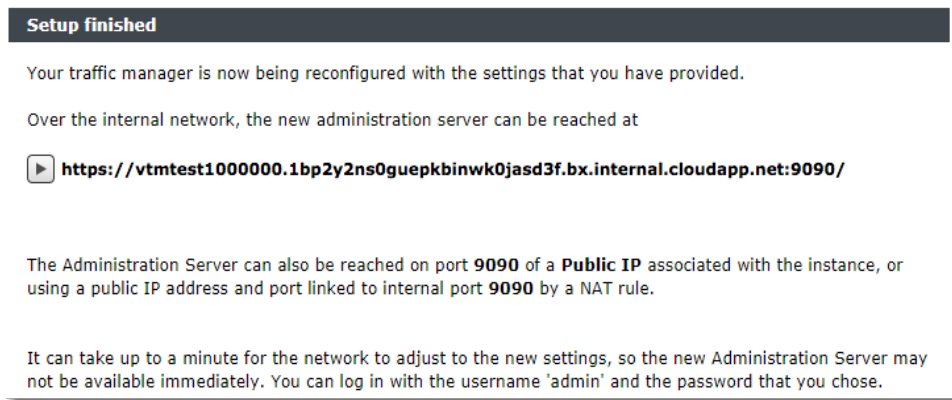
|                                  |                         |
|----------------------------------|-------------------------|
| <b>SSH Intrusion Protection:</b> | Enabled                 |
| <b>License key:</b>              | No license key provided |

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

## Finishing the Initial Configuration

After clicking **Finish** at the Summary page, the Initial Configuration, Finished step appears.

FIGURE 44 Initial Configuration Finished

**Initial configuration, finished**

To access the Admin UI of your configured Traffic Manager, use the public IP address or fully qualified DNS name with the dedicated administration port assigned to the instance when you created the cluster. To obtain these details, see [“Connecting to the Admin UI” on page 78](#).

If you are connected to the same internal network as the cluster you created, you can use the URL shown on the “Setup finished” page.

Log in using the username “admin” and the admin password you set when you used the Initial Configuration wizard.

## Configuring an Instance 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” on page 79](#).

To start the configuration program, login to the instance 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) 2020, Pulse Secure, LLC. 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 Traffic Manager.

```

Use of this software is subject to the Pulse Secure 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 Pulse Secure 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.

**Note:** The Traffic Manager is available as a range of set-frequency billing subscriptions where the license is built in, and as a Community Edition/Bring Your Own License (BYOL) instance. The following step concerns software licensing options for the Community Edition/BYOL instance only, and might not appear if you are running the configuration program on an instance with a built-in license.

Enter the license key file name, or leave blank to use 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" on page 95](#).

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

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 instance 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. Pulse Secure 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*.

```
Please provide the port on which the REST API should
listen for requests (default 9070).
```

```
REST port [9070]:
```

If you enable the REST API, enter the port number on which you want the REST service to listen for requests.

You have specified the following settings:

|                         |                                                       |
|-------------------------|-------------------------------------------------------|
| No license file:        | The traffic manager will run as the Community Edition |
| Timezone:               | UTC                                                   |
| SSH protection enabled: | Yes                                                   |
| REST enabled:           | Yes                                                   |
| REST port:              | 9070                                                  |

```
Proceed with configuration? Y/N:
```

Before you finish, check through the summary to confirm your intended settings. To configure your Traffic Manager with these settings, type “Y” at the prompt.

## 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>
```

## Removing a Traffic Manager

To remove an individual Traffic Manager instance from your cluster, use the APIs for virtual machine scale sets. You cannot remove an instance through the Azure management portal.

To remove an entire cluster, delete the resource group associated with it. All resources, including any Traffic Managers connected to the resource group, are permanently removed.

### To remove a Traffic Manager cluster

1. Login to the Azure management portal.
2. Select Resource Groups from the navigation bar.
3. Scroll to the right of the blade and click the three dots that correspond to your Resource Group, then click **Delete** from the pop-up menu. Alternatively, click the name of your Resource Group and then click the **Delete** option at the top of the Resource Group Settings blade.
4. In the “Are you sure you want to delete <Resource Group>” blade, type the name of your Resource Group into the text box provided.
5. Click **Delete** to confirm the action.

**Note:** The Traffic Manager cluster is shut down and is permanently destroyed. You lose all configuration and data associated with each instance in the cluster.

## Upgrading Your Traffic Manager

This section contains details of how to upgrade and, where necessary, revert your Traffic Manager instance when a new version is released.

### Before You Start

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.

#### CAUTION

If you are upgrading from Traffic Manager versions earlier than 9.9, you must install a new instance of the Traffic Manager and import your configuration into it. This is due to the underlying operating system on earlier versions 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 2GB 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 700MB must be free on the / (root) partition, and at least 600MB must be free on the /logs partition. To confirm the available free disk space, use the **System > Traffic Managers** page of the Admin UI.

**Note:** Pulse Secure 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

**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 appliance platform. 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, Azure instances), 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 Azure instances), 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

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 instance.

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” on page 91](#)).

**Note:** 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 instance 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>_Azure-Appliance-Upgrade-x86_64.tgz
```

Perform the upgrade through the Admin UI or from the instance 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 88](#)).

### To upgrade using the command line

1. Copy the package file to the instance 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

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

2. Connect to the Traffic Manager 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.

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

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

## Upgrading a Cluster Using the Backup and Restore Method

You can also upgrade a cluster by taking a backup of its configuration, creating a new cluster based on the more recent Traffic Manager version, and applying the backup to the new cluster. Use this method if you want to run an upgraded cluster alongside your existing one for testing purposes.

### To upgrade using the backup and restore method

1. Login to the Admin UI of an existing cluster member and download a configuration backup from the **System > Backups** page.
2. Deploy a new cluster of the same size as the existing one, using the newer Traffic Manager Azure virtual machine. Make each new instance join the new cluster, but do not perform any additional configuration procedures.
3. Import the configuration backup into the new cluster using the **System > Backups** page, and navigate to the "Restore Configuration" section on the Backup detail page. The Admin UI allows you to choose which instance in your new cluster takes the place of each instance in the existing one. In most cases, if the new cluster is the same size as the existing one, the software maps existing instances to new ones appropriately.

FIGURE 45 Mapping the Traffic Manager in a Backup

**Restore Configuration**

Restore this backup to be the current configuration. NOTE: this will replace the current configuration and all unsaved changes will be lost.

This backup contains machine specific information, such as networking configuration and Traffic IP groups.  
Do you want to:

- ☒ Replace the Traffic Managers in the backup with the machines in the current cluster...
- ☐ Restore backup without replacing Traffic Managers.

| Original Traffic Manager                  |   | New Traffic Manager                       |
|-------------------------------------------|---|-------------------------------------------|
| domU-12-31-39-00-12-F1.compute-1.internal | ➔ | domU-12-31-39-07-80-42.compute-1.internal |
| domU-12-31-39-00-3D-D2.compute-1.internal | ➔ | domU-12-31-39-00-3D-D2.compute-1.internal |

☐ Confirm

You should only need to alter the default mapping if your new cluster is larger or smaller than the existing one, or if you need to ensure that an instance in the existing cluster is replaced by a particular instance in the new one.



## 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:

FIGURE 46 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. Connect to the Traffic Manager 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) 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]:

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 appliance reboots continue to use the version you select from the rollback program.

**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.

## 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 Traffic Manager "boot menu" from the command line.

**Note:** 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 complete a manual version change, perform the following steps:

1. Log in to the instance command line 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 instance.

# Additional System Information

The chapter contains additional system information about using the Traffic Manager software. This chapter contains the following sections:

|                                                                        |    |
|------------------------------------------------------------------------|----|
| • SSH.....                                                             | 93 |
| • Securing Communication with Amazon EC2 Endpoints .....               | 93 |
| • The Traffic Manager Software Installation Directory (ZEUSHOME) ..... | 94 |
| • Starting and Stopping the Traffic Manager Software.....              | 94 |
| • Freeing Up Disk Space .....                                          | 94 |
| • License Keys .....                                                   | 95 |
| • The Community Edition .....                                          | 95 |

## SSH

You normally administer the Traffic Manager through the Web-based Admin UI. However, you can also access the instance through the command line interface to access files stored on the system. To do this, log in to the instance using an SSH client.

## Securing Communication with Amazon EC2 Endpoints

**Note:** This section does not apply to Traffic Manager instances running on Microsoft Azure.

To ensure secure communication with Amazon EC2 endpoints, the Traffic Manager can optionally use a Certificate Authority (CA) certificate to verify the identity of your endpoints.

### To import the CA certificate into your Traffic Manager instance

1. First obtain the CA certificate from Amazon for the top level EC2 endpoint, ec2.amazonaws.com.
2. Copy the certificate to a temporary location on your Traffic Manager instance (for example, by using the scp or similar command).
3. Verify the certificate by using the httpclient command:

```
httpclient --verify --CA=<certificate> https://ec2.amazonaws.com/
```

4. In the Admin UI, click **SSL > CAs and CRLs > Import**. Use this page to upload the certificate file to the Traffic Manager's Certificate Authorities catalog.
5. Click **System > Global Settings > EC2 Account Settings**.
6. Set ec2!verify\_query\_server\_cert to Yes to enable verification using the imported CA certificate.

## The Traffic Manager Software Installation Directory (ZEUSHOME)

The Traffic Manager software installation directory (referred to throughout this documentation as `ZEUSHOME`) varies depending on whether you install a virtual machine instance or software variant on an EC2 Linux or UNIX instance.

For EC2, Rackspace, and Azure instances:

```
/opt/zeus
```

For a software installation:

```
/usr/local/zeus
```

## 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 or restart the software on an appliance or cloud variant, use the buttons on the **System > Traffic Managers** page of the Admin UI.

For software variants, you can stop the Traffic Manager software from the command line using the following (as the root user):

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

To start the software again, use the following:

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

## Freeing Up Disk Space

**Note:** This section is applicable only to appliance and cloud variants.

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 top navigation 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.

**Note:** This operation is irreversible. You should ensure 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 last time you used the wizard

## License Keys

For Traffic Manager virtual machine instances (excluding software based variants running on Linux or UNIX instances), a license key might be prebuilt into the Traffic Manager machine image. You do not need to request a license key for new Traffic Manager instances launched from these images. Equally, you cannot delete the built-in license key for these product variants.

For Traffic Manager software deployments and virtual machine images without built-in licenses, you apply a valid software license key during installation.

For questions about license keys, contact Pulse Secure Technical Support.

## 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.



# 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.

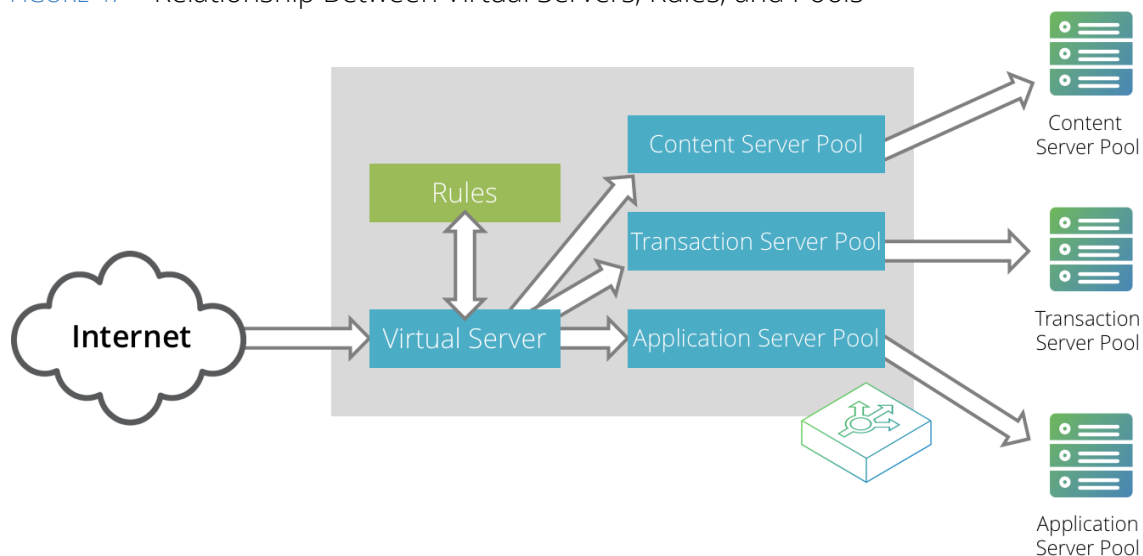
This chapter describes the basic Traffic Manager configuration and contains the following sections:

- [Virtual Servers, Pools, and Rules](#) ..... 97
- [Managing Your First Service](#) ..... 98
- [About Creating a Traffic Manager Cluster](#) ..... 99

## Virtual Servers, Pools, and Rules

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

FIGURE 47 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.

**Note:** To allow a virtual server to listen on an EC2 Elastic IP address, first make sure the Elastic IP has been associated to your Traffic Manager instance.

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 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.

## About Creating a Traffic Manager Cluster

If you are configuring two or more Traffic Managers in a cluster, you should 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.

For more information, see [“Joining a Cluster” on page 99](#).

**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.

## Multi-region and Multi-VPC Clusters on Amazon EC2

While Traffic Manager clusters cannot directly span multiple EC2-Classic regions or span outside of a VPC, it is possible to enable communications between clusters in different locations by using the Traffic Manager's multi-site cluster management capability. For more details, see the *Pulse Secure Virtual Traffic Manager: User's Guide*.

To use multi-site communications, you need to assign each Traffic Manager instance an external IP address which can be used by each cluster member to enable communication. To assign an external IP address, use the **System > Traffic Manager** page of the Admin UI. Clustering is not possible beyond an EC2-Classic region or VPC until you have performed this task.

**Note:** Elastic IP addresses are per-region only.

## Joining a Cluster

### 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. Click Next to begin.

3. Enter the public DNS hostname and port of the Traffic Manager machine you want to join, then click **Next** to continue.

FIGURE 48 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.

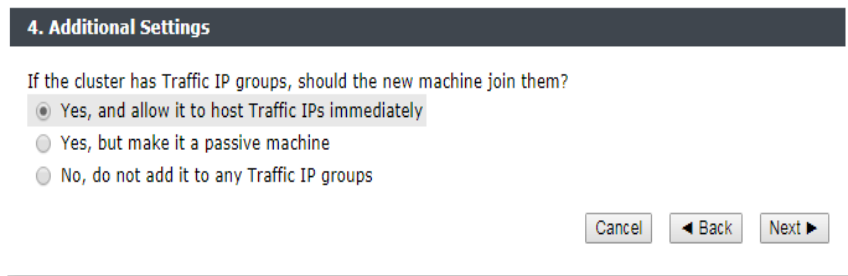
**Username:**

**Password:**

4. Pulse Secure recommends that you verify the identity of each Traffic Manager in the cluster you want to join. To verify a Traffic Manager's identity, 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.

FIGURE 49 Assigning Traffic IP Group Membership

## 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

Cancel Back Next

5. 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.

6. Check your settings in the summary step and then click Finish to join the cluster.  
Provided the other Traffic Manager instance can be contacted, the Traffic Manager software reconfigures itself and presents a new home page showing 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.



# Traffic IP Groups and Fault Tolerance on Amazon EC2

A cluster of Traffic Managers on EC2 can transfer Elastic IP Addresses from one to another if a Traffic Manager fails. Traffic distribution is configured by means of Traffic IP groups, as defined on the **Services > Traffic IP Groups** page of the Admin UI.

This chapter highlights the differences in traffic distribution capabilities between the Amazon EC2 platform and other software, hardware, virtual, or cloud Traffic Manager variants. The chapter contains the following sections:

- [Key Differences Between Traffic IP Groups on an EC2 and Traffic IP Groups on Other Platforms](#) 103
- [Fault Tolerance](#) ..... 105
- [Creating a Traffic IP Group](#)..... 105
- [Understanding a Traffic Manager's Fault Tolerance Checks](#)..... 109
- [Traffic Manager Failover](#)..... 111
- [Debugging and Monitoring Fault Tolerance Activity](#) ..... 111

For more complete information about the features available to all product variants, see the *Pulse Secure Virtual Traffic Manager: User's Guide*.

## Key Differences Between Traffic IP Groups on an EC2 and Traffic IP Groups on Other Platforms

Traffic IP groups on EC2 variants are implemented using either AWS Elastic IP addresses or private IP addresses (VPCs only).

**Note:** To use Traffic IP addresses on EC2 you must launch an instance with an assigned IAM role.

### Using Elastic IP Addresses in Traffic IP Groups

An Elastic IP Address is a public IP address that can be reserved and assigned manually to a virtual machine instance, replacing the randomly-assigned public IP address that the instance was allocated when it was created (or, in the case of VPCs, to map to the private IP addresses raised when the instance is created). The instance's private IP address and private DNS name do not change when the Elastic IP Address is assigned. Amazon places some restrictions on Elastic IP Addresses that are reflected in the behavior and capabilities of Traffic IP groups on EC2. These restrictions vary depending on whether you are using EC2-Classical or VPC for your deployment.

For EC2-Classical:

- A Traffic IP group can only contain one public Traffic IP Address (default or Elastic) at any one time;

- A Traffic Manager instance can only be a member of one Traffic IP group;
- When a Traffic Manager raises a Traffic IP address its Admin UI is only available outside the EC2-Classical network on that address;
- All traffic sent to the Elastic IP address is delivered to the same Traffic Manager instance.
- Instances created inside a VPC differ in that they can have two or more Elastic IP Addresses assigned to them at once; one to map to the primary private IP for management traffic, and the rest to map to free secondary private IP addresses for use in Traffic IP groups.

**Note:** Traffic IP address failover might be slower on EC2 than on other platforms.

**Note:** When a Traffic Manager running on EC2 lowers a Traffic IP address, the Traffic Manager receives a new public IP address. Amazon does not charge for Elastic IP addresses that are in use; that is, the Elastic IP addresses that are assigned to running instances. However, Amazon does charge for unused Elastic IP addresses. There is also a charge for moving an Elastic IP address from one instance to another, but the first 100 such moves in each billing period are currently free of charge. Therefore, create only as many Elastic IP addresses as you need to avoid unnecessary charges and failovers.

For up to date information on EC2 pricing policies, see Amazon's EC2 documentation.

## Using Private IP Addresses in Traffic IP Groups

Private IP addresses differ from Elastic IP addresses in that they are not chargeable on an individual basis by Amazon, and are limited in quantity by your subnet size and the type of instance you have. Private IP addresses are also, in contrast to Elastic IP addresses, not assigned to a specific AWS account.

Traffic IP groups based on private IP addresses are single-hosted in nature. To use private IP addresses in a Traffic IP group, your Traffic Manager instances must be inside a VPC, in the same "availability zone" (within a region), and must have Elastic Network Interfaces (ENIs) in the same subnet. Additionally, you must be able to raise a free secondary IP address on the ENI for this purpose - the primary IP address on the ENI remains as-is.

While using private Traffic IP addresses, the Traffic Manager operates with the following functionality:

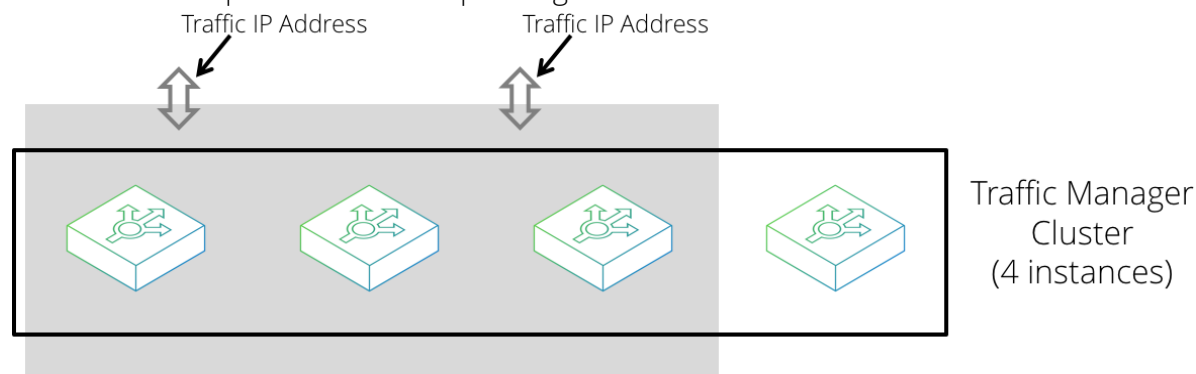
- You can use multiple ENIs configured on different subnets. The Traffic Manager selects the correct ENI to use for the Traffic IP group.
- A Traffic Manager can be in a private IP address Traffic IP group and an elastic IP address Traffic IP group simultaneously.
- Multihomed and Route Health Injection (RHI) based fault tolerance is not supported as private IP addresses cannot be assigned to multiple Traffic Manager instances.

## Fault Tolerance

### Traffic IP Addresses and Traffic IP Groups

A Traffic IP address is an IP address that must remain highly available. You assign Traffic IP addresses to Traffic IP groups, and each group is managed by some of (or all of) the Traffic Managers in your cluster. A Traffic IP group contains either a single Traffic IP address (for EC2-Classic configurations) or one or more Traffic IP addresses (for VPC configurations).

FIGURE 50 Example Traffic IP Group Configuration



#### Traffic IP Group (2 IP Addresses, 3 Traffic Managers)

In [Figure 50](#), a Traffic IP group has been configured, spanning 3 of the 4 Traffic Managers in the cluster. These Traffic Managers ensure that any Traffic IP address assigned to the group is always available. If multiple addresses are assigned to the group, each is raised on a different Traffic Manager, distributed as evenly as possible.

For example, a web service might be published on IP address 34.56.78.90. You can ensure that the service is always available by adding this IP address to a Traffic IP group. The Traffic Manager cluster raises this IP address and manage all of the traffic to it. You typically configure the DNS entry for your service to resolve to one or more Traffic IP addresses, although you must use a VPC where more than one address is used.

### IP Address Transference Within a Traffic IP Group

All traffic destined for a particular Traffic IP address is handled by the Traffic Manager with the raised address. Any other Traffic Managers in the group run as hot spares, ready to take over if the active machine fails.

Each Traffic Manager reports periodically to the other Traffic Managers. If the Traffic Manager currently hosting the Traffic IP address fails, one of the remaining Traffic Managers takes over its share of traffic. In this way, services that depend on the Traffic IP addresses are always available.

### Creating a Traffic IP Group

To create a new Traffic IP group, click **Services > Traffic IP Groups**. Use this page to view and edit your existing Traffic IP groups, and to create new Traffic IP groups.

Decide whether you want to create a Traffic IP group based on Elastic IP addresses or private IP addresses. To create a Traffic IP group using an Elastic IP address, you must first allocate a new Elastic IP address to your AWS account.

## Allocating a New Elastic IP Address

**Note:** This section does not apply to Traffic IP groups based on private IP addresses.

You manage the Elastic IP addresses allocated to your EC2 account using the “Manage Elastic IPs” section in the Traffic IP Groups page. You can use allocated Elastic IP addresses in your Traffic IP groups.

FIGURE 51 Allocating new Elastic IPs

| Elastic IP     | Instance ID | Domain   | Network Interface ID | Private IP | Traffic Manager | Traffic IP Group | Release IP                          |
|----------------|-------------|----------|----------------------|------------|-----------------|------------------|-------------------------------------|
| 107.23.144.184 | i-cef375b0  | vpc      | eni-58c63832         | 10.0.0.28  |                 |                  | <input type="checkbox"/>            |
| 107.23.146.3   | i-168a0c68  | vpc      | eni-cbc33da1         | 10.1.0.120 | 10.1.0.84       | Web TIP 1        | <input checked="" type="checkbox"/> |
| 107.23.148.185 | i-168a0c68  | vpc      | eni-cbc33da1         | 10.1.0.84  | 10.1.0.84       |                  | <input type="checkbox"/>            |
| 107.23.159.178 | i-1cab2d62  | vpc      | eni-9336c8f9         | 10.0.0.79  |                 |                  | <input type="checkbox"/>            |
| 184.73.224.108 | i-7af37504  | standard |                      |            |                 |                  | <input checked="" type="checkbox"/> |

☐ Confirm

**Note:** For EC2-Classic, you must have at least one Traffic Manager in your cluster that is not already part of an existing Traffic IP group, as a Traffic Manager cannot be a member of more than one Traffic IP group. This restriction does not apply to VPC configurations.

### To allocate an elastic IP address to your account

1. Click Allocate new Elastic IP.
2. Select whether you need to allocate the address for use with EC2-Classic or VPC instances.

**Note:** Addresses allocated for use with EC2-Classic instances are not available to VPC instances, and vice versa.

3. Since allocating an Elastic IP address might incur a charge, click the Confirm check box to confirm this action.

The new Elastic IP address appears in the table.

## Creating a Traffic IP Group

To create a new Traffic IP group using an EC2 based Traffic Manager, use the "Create a new Traffic IP Group" section.






FIGURE 52 Creating a new Traffic IP group on a VPC based instance

**Create a new Traffic IP Group**

**Name:**

**Traffic Managers:**

|                                                                                   | Traffic Manager | Passive                  | Add                                 |
|-----------------------------------------------------------------------------------|-----------------|--------------------------|-------------------------------------|
|  | 10.0.0.14       | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
|  | 10.0.0.185      | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
|  | 10.0.0.86       | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

**EC2 IP Address Type** ☒ Elastic ☐ Private

**VPC Elastic IP Addresses:**

54.171.54.162  
 54.171.180.145  
 54.171.183.83  
 54.194.208.99

The EC2 account used to manage Elastic and Private IP addresses is configured on the Global settings page.

**Modify the EC2 account in the Global Settings section.**

**Note:** Clusters outside of a VPC can use only Elastic IP addresses in a Traffic IP group. In these circumstances, EC2 IP Address Type is not shown.

### To create a Traffic IP group and associate it with an Elastic or private IP address

1. Enter a group name and select the Traffic Managers you want to include as members of the group.
2. If your Traffic Manager cluster resides in a VPC, choose whether to create the Traffic IP group based on either Elastic IP addresses or private IP addresses.

**Note:** This step is not applicable to clusters based outside of a VPC; in which case, the only option is Elastic IP addresses.

3. Enter the following information based on whether you are using Elastic IP addresses or private IP addresses:
  - For Elastic IP addresses, choose one or more Elastic IP addresses from the list.
  - For private IP Addresses, type one or more private IP addresses into the text box.

For Elastic IP addresses on VPC-based instances, you must have a free secondary private IP address raised (that is, an address not currently associated with an Elastic IP address or without a virtual server bound specifically to it) before they can be joined to a Traffic IP group.

**Note:** For Traffic IP groups based on Elastic IP addresses, Pulse Secure recommends that a VPC-based Traffic Manager has the same number of spare secondary private IP addresses as there are Elastic IP addresses in the Traffic IP groups to which the Traffic Manager belongs.

For example, if your Traffic Manager is part of two Traffic IP groups, each containing two Elastic IP addresses, the Traffic Manager should have four spare secondary private IP addresses so that all Elastic IP addresses can move to it at the same time.

**Note:** The Traffic (Elastic) IP is raised using this secondary Private IP on the default network interface. The primary Private IP is used for Traffic Manager administration and multi-site cluster management support and is not available for this purpose.

4. Click **Create Traffic IP Group** to create the new group.

**Note:** (EC2-Classic only) If the Traffic Manager you are currently logged into is part of the new Traffic IP group, the Traffic IP address may be raised. This causes the Admin UI address to change. If the Admin UI address changes, you are redirected and connected to the new Admin UI address as soon as the address is available. You may see a certificate warning from the new address. Receiving this warning is normal and you can ignore it. (For more information, see the [“Connecting to the Admin UI” on page 28](#)).

## Disabling a Traffic IP Group

You can disable a Traffic IP group using the **Enabled** setting on the edit page for that group. You can temporarily disable a group if it is not currently required but may be required in the future.

You cannot release an Elastic IP address assigned to a disabled Traffic IP group. You also cannot lower a private IP address that has been assigned to a disabled Traffic IP group. Furthermore, for EC2-Classic, Traffic Managers in a disabled Traffic IP group remain assigned to that group and cannot be assigned to another group.

**Note:** (EC2-Classic only) If the Traffic Manager you are currently logged into is hosting the Traffic IP address associated with the group you are disabling, your connection to the Admin UI is dropped. This connection is then unavailable for several minutes while Amazon allocates a new public IP address. For this reason, change Traffic IP group settings from the Admin UI of a machine that is not a member of the group you are changing.

## Releasing an Elastic IP Address

### To release an Elastic IP address

1. Make sure the Elastic IP address is not associated with a Traffic IP group. If this is the case, first delete the Traffic IP group. It may take a few seconds for the Traffic Manager hosting the IP address to release the address.
2. Click the **Release IP** check box next to each IP address to be released.
3. Click **Confirm**.
4. Click **Release Selected Elastic IPs** to complete the action.

## Assigning Elastic IP Addresses to Specific Network Cards

The Traffic Manager allows you to use multiple network cards with your Traffic IP groups on an instance running inside a VPC. By increasing your Traffic Manager network connections, a greater degree of fault tolerance is provided.

**Note:** For Traffic Manager software variants running inside a Linux virtual machine, use only those Linux AMIs that automatically support, and can configure, multiple network cards. Refer to your support provider for further information.

### To assign Elastic IPs to specific network cards

1. To assign the network cards for your Elastic IP associations, click **Services > Traffic IP Groups** to display the EC2 Traffic IP Network Cards page.
2. Select the network card you want to use.
3. Click Update Public ENIs. The next EC2 Traffic IP Network Cards page appears.
4. Select the network card you want to use.
5. Click **Add**.

### About Configuring Multiple Network Cards

For each of your Elastic IP (Traffic IP) addresses, you can specify more than one network card for the Traffic Manager to use. However, select only those network cards in a subnet that has access to the Internet (that is, your public subnets).

**Note:** Pulse Secure recommends that you make changes to the network cards you are using at a time of least disruption to your services.

For EC2 appliance variants, the Traffic Manager automatically configures the card settings (such as routes, IP addresses, and routing rules). To add or remove secondary private IP addresses, use the **System > Networking** page.

For software instances running on an EC2 virtual machine, the Traffic Manager does not maintain or configure the network cards it uses.

If you do not specify a network card for your Elastic IP addresses, the Traffic Manager uses the default network card.

The Traffic Manager only uses secondary private IP addresses to associate with the Elastic IP. For this reason, make sure you have enough secondary private IP addresses available on the network cards you intend to use.

## Understanding a Traffic Manager's Fault Tolerance Checks

The Traffic Managers in a cluster periodically check that they can communicate with the network using ICMP pings through each active network interface. They then broadcast a message describing their health as good or failed.

If the Traffic Manager hosting the Traffic IP address in a cluster fails, one of the other Traffic Managers takes over the address.

To configure fault tolerance checks, use the settings in **System > Fault Tolerance**.

## Local Health Checks

Each Traffic Manager checks that its network interfaces are operating correctly. It does this by periodically pinging each of the back-end nodes in the pools that are in use, to ensure that its back-end network interfaces are functioning. The Traffic Manager concludes that it has failed if it cannot ping any of the nodes in any of the currently used pools.

**Note:** If your pools contain nodes that are hosted outside the EC2 network, you might see warnings about node failures when Traffic IP addresses fail over. These warnings occur because an EC2 instance loses all external connectivity while its public IP address is changed, which causes back-end connectivity checks to fail. These warnings can safely be ignored and are cleared when the instance regains external connectivity. Backend nodes hosted inside the EC2 network are not affected by this issue.

## Health Broadcasts

Each Traffic Manager machine regularly broadcasts the results of its local health checks, whether it is healthy or not.

By default, each machine broadcasts these heartbeat messages every 2 seconds. You can configure this behavior with the `flipper!monitor_interval` setting.

**Note:** The `tcpdump` program is a useful debugging tool. You can capture heartbeat messages in your Traffic Manager clusters by running the following commands on each Traffic Manager:

```
tcpdump -i eth0 udp and port 9090
```

## Determining the Health of a Traffic Manager Cluster

Each Traffic Manager listens for the health messages from all of the other Traffic Managers in the cluster. A Traffic Manager concludes that one of its peers has failed if:

- It receives an “I have failed” health message from the peer.
- It does not receive any messages from the peer within the value set in `flipper!monitor_timeout`.
- The peer reports that one of its child process is no longer servicing traffic. This occurs if any child process fails to respond within the value set in `flipper!child_timeout`.

The Traffic Manager concludes that a peer has recovered when it starts receiving “I am healthy” messages from the peer.

## Traffic Manager Failover

When each Traffic Manager in a cluster determines that one of its peers has failed, the Traffic Manager may take over some or all of the traffic shares for which that failed system was responsible.

Each Traffic Manager in a cluster uses its knowledge of which machines are active to determine which Traffic IPs it should be using. The cluster uses a fully deterministic algorithm to determine which Traffic Manager should host the traffic IP address. Because the algorithm is deterministic, the Traffic Managers do not need to negotiate when one of their peers fails or recovers.

## Recovering From Traffic Manager Failures

When a failed Traffic Manager recovers, it announces that it is able to host a Traffic IP address again but does not automatically take over the address, even if it was hosting it when it failed. Instead, message displays indicating that the Traffic Manager has recovered and can take back the Traffic IP addresses. To reactivate the Traffic Manager, go to the Diagnose page and click the Reactivate this Traffic Manager link.

This behavior exists because each time traffic shares are transferred from one Traffic Manager to another, any connections currently in that share are dropped. Dropped connections are inevitable when a transfer occurs because a Traffic Manager fails, but might not be desirable when a Traffic Manager recovers.

If you would prefer recovering Traffic Manager to take back the Traffic IP addresses automatically, enable the flipper!autofailback setting on the **System > Fault Tolerance** page.

## Debugging and Monitoring Fault Tolerance Activity

All state changes and IP address transfers are logged in the event logs of each relevant Traffic Manager. If email alerting is correctly configured on your Traffic Manager system, an email message is sent to the system administrator describing the state change and any IP address transfers that resulted.

For detailed debugging, you can enable the flipper!verbose setting. This setting causes each Traffic Manager to log each connectivity test, broadcast message sent and received, and is useful when determining why the fault tolerance behavior is not working as expected.

You can also view the Cluster Diagnosis section of the Diagnose page. This page contains information about broadcast messages not received correctly, and summarizes the system status if an error has occurred.



# Traffic IP Groups and Fault Tolerance on GCE

This chapter describes how to implement front-end fault tolerance on Traffic Managers running in Google Compute Engine (GCE) through the use of External IP addresses and Traffic IP Groups. It should be read as an introduction to the capability and how it pertains to GCE in particular. For full details of fault tolerance and Traffic IP Groups, see the *Pulse Secure Virtual Traffic Manager: User's Guide*.

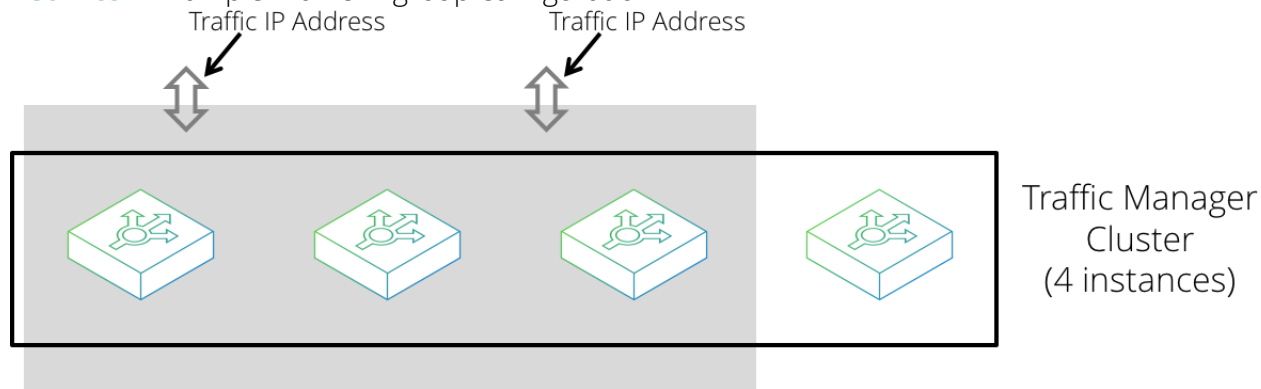
This chapter contains the following sections:

- [Using Traffic IP Groups for Fault Tolerance](#) ..... 113
- [GCE Network Interfaces and External IP Addresses](#) ..... 114
- [Creating a Traffic IP Group](#) ..... 114

## Using Traffic IP Groups for Fault Tolerance

The Traffic Manager can implement fault tolerance through the use of Traffic IP Groups and GCE External IP addresses. You configure a Traffic IP Group to contain two or more of the Traffic Managers in your cluster, together with one or more pre-reserved GCE External IP addresses. In a Traffic IP Group, such addresses are referred to as Traffic IP Addresses.

**FIGURE 53** Example Traffic IP group configuration



Traffic IP Group (2 IP Addresses, 3 Traffic Managers)

A Traffic IP Address is a permanent, externally-visible IP address that must remain highly available, and the Traffic Managers in the group share responsibility for keeping the Traffic IP Address raised regardless of individual instance failure. In other words, if a Traffic Manager that is currently receiving traffic over a Traffic IP Address suffers a failure, the remaining Traffic Managers in the group take on responsibility for maintaining the service and raise the relevant Traffic IP Address between themselves.

You can configure Traffic IP Groups on GCE as either active/active or active/passive. Furthermore, all Traffic IP Addresses hosted by the group are single-hosted. That is, responsibility for hosting Traffic IP Addresses is spread evenly between the Traffic Managers assigned to the group. Each Traffic IP Address is hosted on only one Traffic Manager, and transferred to another group member should the original host fail.

## GCE Network Interfaces and External IP Addresses

Fault tolerance with Traffic IP Groups in a GCE environment requires the use of External IP addresses. GCE associates External IP addresses to Traffic Managers through adding additional network interfaces to the host. For each External IP address, you require one extra network interface to be attached to your Traffic Manager virtual machine. This is in addition to the first network interface which is reserved for Traffic Manager administration and management. Thus, to use 3 External IP addresses with your Traffic Manager, you require a total of 4 network interfaces to be added when you first create the host virtual machine.

GCE supports a maximum of 8 network interfaces per instance. Therefore, with a single interface reserved for management use, the Traffic Manager can use a maximum of 7 further network interfaces.

**Note:** You cannot add network interfaces to a pre-existing virtual machine.

Only one External IP address can be associated per network interface. Network interfaces that already have an External IP address association (static or ephemeral) are not used by the Traffic Manager for Traffic IP Groups. If a Traffic Manager is already included in a Traffic IP Group for a Traffic IP Address raised on another instance in the cluster, an interface on the local Traffic Manager is considered reserved for use by that Traffic IP Group in case it is required for failover. Therefore, that interface cannot be used by a different Traffic IP Group.

**Note:** GCE uses two types of External IP address: "regional" and "global". For Traffic IP groups, the Traffic Manager supports the use of regional IP addresses only.

### ATTENTION

Traffic Manager virtual machines automatically configure network interface policy routing and rules at startup. For Traffic Manager software variants running on a virtual machine host, you must manually configure policy routing for secondary network interfaces on the host. See the Google Cloud documentation for "Configuring Policy Routing" at <https://cloud.google.com/docs> for more details.

## Creating a Traffic IP Group

To create a new Traffic IP Group, log into the Admin UI of one of your cluster members and click **Services > Traffic IP Groups**. Use this page to view and edit your existing Traffic IP Groups, and to create new Traffic IP Groups.



FIGURE 54 Viewing and creating a Traffic IP Group

**Traffic IP Groups**



A Traffic IP group contains a selection of traffic managers and a set of one or more IP addresses that are to be raised at all times on at least one traffic manager in the group.

*You have not created any traffic IP groups yet.*

**Create a new Traffic IP Group**

**Name:**

**Traffic Managers:**

|                                                                                   | Traffic Manager                                | Passive                  | Add                                 |
|-----------------------------------------------------------------------------------|------------------------------------------------|--------------------------|-------------------------------------|
|  | vtm-2.c.vtm-development.internal<br>10.0.1.195 | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
|  | vtm-3.c.vtm-development.internal<br>10.0.1.196 | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

**GCE External IP Address:**

jlm-06 (35.210.41.52)  
jlm-07 (35.210.231.110)  
jlm-08 (35.195.28.89)  
jlm-09 (35.210.74.154)

### To create a Traffic IP Group and associate it with GCE External IP addresses

1. Enter a group name and select the Traffic Managers you want to include as members of the group.
2. To use an active/passive traffic distribution model, tick the "Passive" checkbox next to those Traffic Managers you want to start in a passive state.
3. Select one or more of the pre-reserved CGE External IP addresses you want this group to host.
4. To create the Traffic IP Group based on these settings, click **Create Traffic IP Group**.



# 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.

