Using Pulse Secure Virtual Traffic Manager in Docker

Deployment Guide

Published 15 July, 2020

Document Version 1.4

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

www.pulsesecure.net

Using Pulse Secure Virtual Traffic Manager in Docker

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

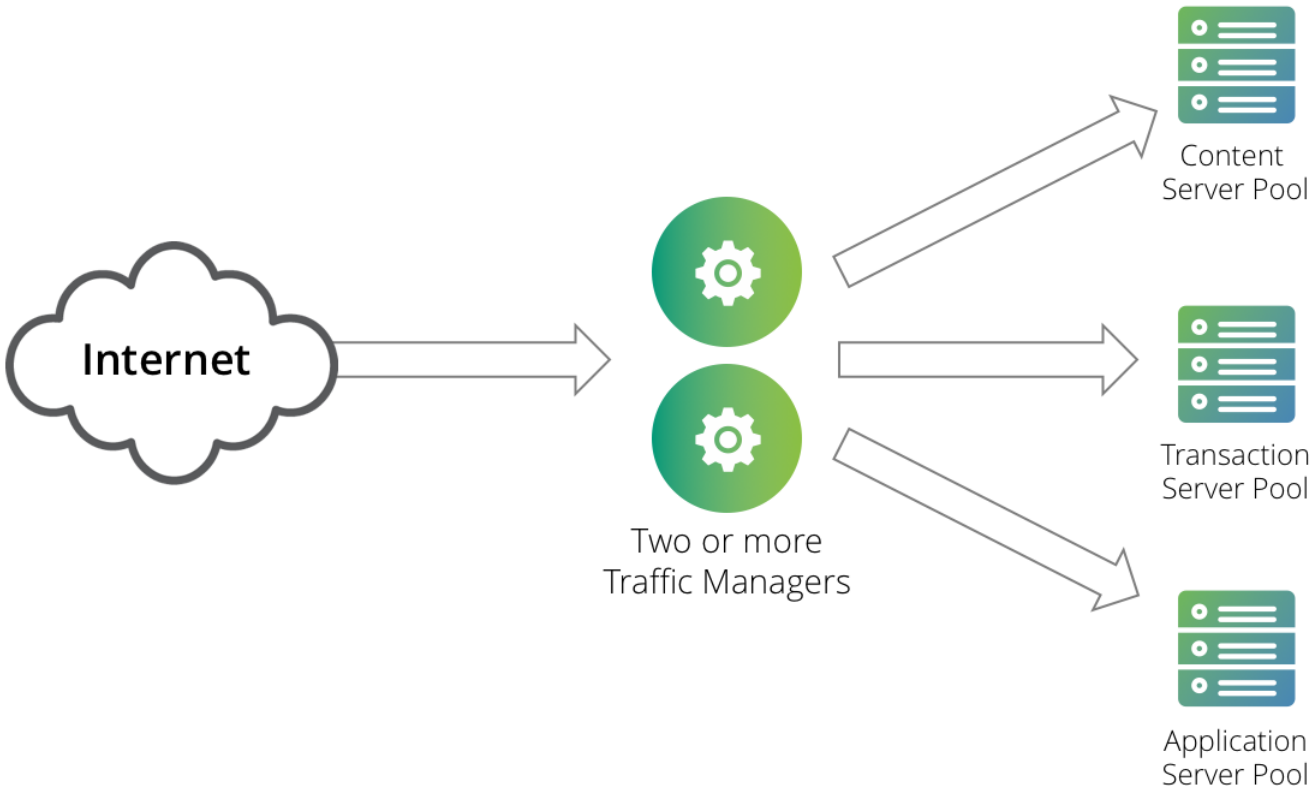
Getting Started with Docker

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

Network Architecture for a Typical Deployment

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 1 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.

Using the Traffic Manager with Docker

Docker provides a light-weight virtualization environment under which an administrator can launch one or more Traffic Manager instances in complete isolation from each other, on the same physical host hardware. Each instance is launched as a *container* image, containing the Traffic Manager application and all operating system components required for it to run independently. For information on the steps required to obtain a Docker-ready Traffic Manager container image, see "Launching the Traffic Manager in a Docker Container" on page 5.

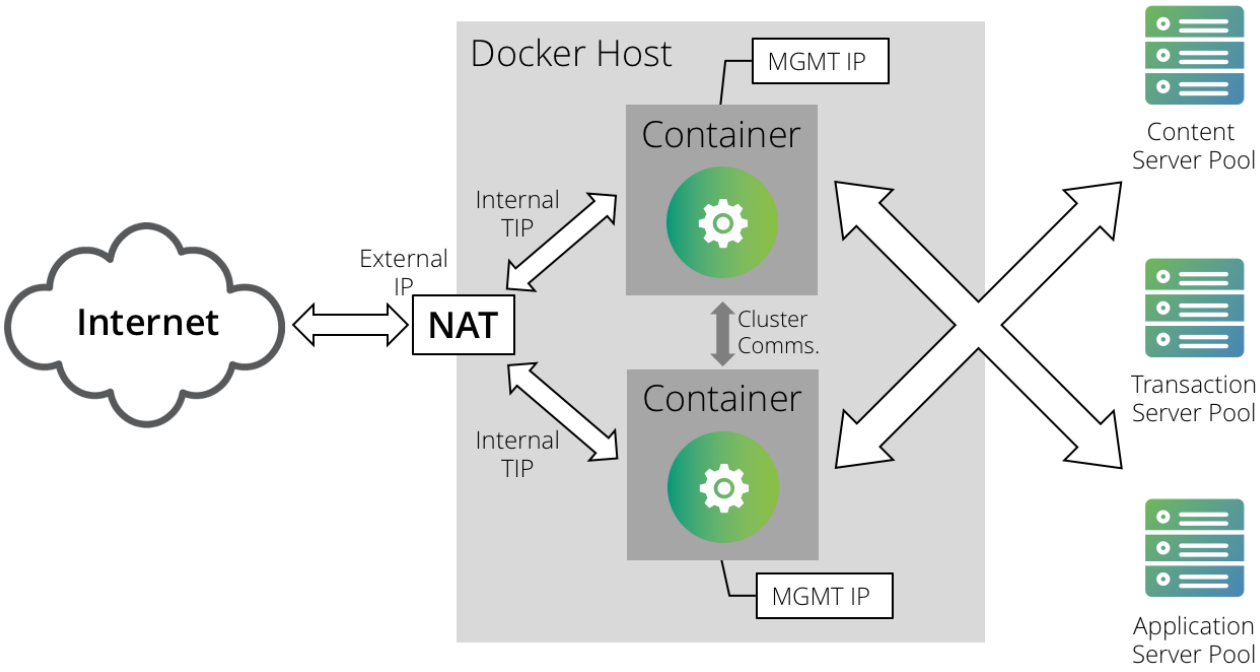
To operate a fault-tolerant cluster of Traffic Manager containers on a single Docker host, you must enable external access to the front-end IP addresses hosted by your Traffic Managers. To achieve this, Pulse Secure supports two deployment types. Which type is most suitable depends on your wider network topology and requirements.

Note: To use clustering inside Docker, you must also use the Traffic Manager's *nameip* feature. That is, you can only cluster Traffic Manager instances that are identified using the IP address of a network interface configured for the container. For further information, see "Changing the Traffic Manager Name" on page 15.

Deployment A - Using Network Address Translation

Configure your Traffic Manager container instances with a Traffic IP Group containing a single Traffic IP address. Then, configure Network Address Translation (NAT) on the Docker host to map an externally-available IP address on the host to the internal Traffic IP address raised on your Traffic Manager cluster.

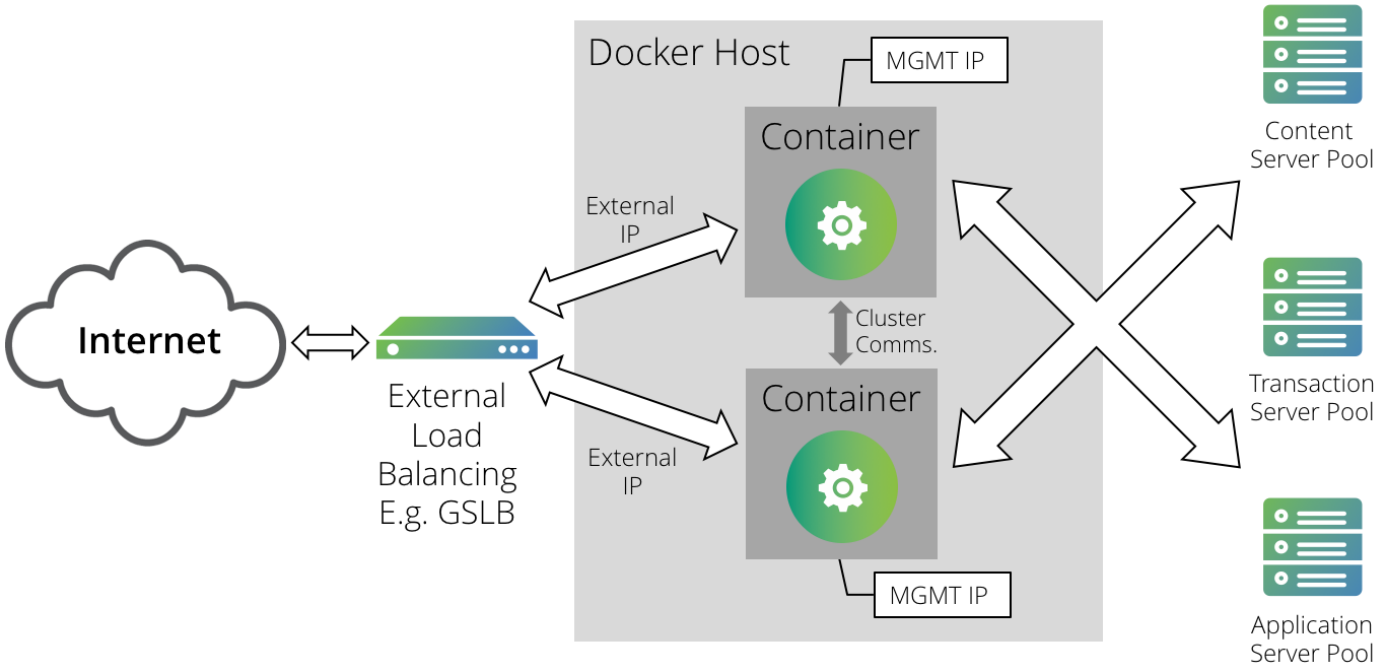
Figure 2 Using Network Address Translation



Deployment B - Using an External Load Balancer

Configure your Traffic Manager container instances to each raise a separate externally-visible front-end IP address, and use an external load-balancer or traffic management device to balance traffic across them. This method can be useful if you have multiple Traffic Manager deployments across geographically-separated data centers and want to balance traffic through Global Server Load Balancing (GSLB) techniques.

Figure 3 Using an external load balancer



Container Networking Overview

To use the Traffic Manager in Docker, make sure your containers are configured to use bridge networking mode. This mode allows the deployment of multiple Traffic Manager containers on a single Docker host, with each container having its own network stack.

Bridge networking mode ensures that every container receives an IP address from the internal subnet range of the default "docker0" host interface. It also ensures that individual Traffic Manager containers can communicate between themselves when creating a cluster.

For external access to the Traffic Manager Admin UI, raise an externally-routeable IP address for the container on an external host interface. Then, start the container with the optional argument "`-p <external IP>:9090:9090`" to map an external IP address to the container's internal Traffic Manager management address. For more information on launch-time command line arguments, see "Launching the Traffic Manager in a Docker Container" on page 5.

For full information concerning Docker networking principles, see the documentation available from the Docker website:

https://docs.docker.com

Prerequisites

The Traffic Manager is supported for use with Docker 1.13.0 or later.

This guide assumes you have deployed a Docker host, and are familiar with Docker administration and networking concepts.

Use only Pulse Secure Virtual Traffic Manager 17.4 or later as part of a Docker-based container deployment.

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

Launching the Traffic Manager in a Docker Container

This chapter documents how to install and configure the Traffic Manager software inside a Docker container. It contains the following sections:

Before you begin, make sure you have met the requirements listed in "Prerequisites" on page 4.

To deploy a Traffic Manager in Docker, download and run the Traffic Manager image directly from Docker Hub

Deploying the Traffic Manager

To deploy the Traffic Manager from Docker Hub, first log in to the service from your Docker host. Run the command:

```
docker login
```

Provide your user credentials when prompted. If you are deploying the Traffic Manager from a locally-prepared image, this step is not necessary.

To install the Traffic Manager, run the following command on your Docker host:

```
docker run --name=<container_name> \
   -e ZEUS_EULA=accept \
   -e ZEUS_PASS=admin \
   --privileged \
   --init \
   -t \
   -d \
   <image_ID>
```

In the above command, set <container_name> to a suitably descriptive name for the container, and <image_ID> to the location and identifier of your Traffic Manager image (see "Setting the Image Identifier" on page 6).

Note that this command sets a password of "admin" for the Traffic Manager administrative user account. For further information on administrator passwords, see "Customizing your Traffic Manager Container" on page 6.

Use the mandatory argument "ZEUS_EULA=accept" to indicate that you accept the Pulse Secure license agreement at https://www.pulsesecure.net/support/eula. You must include this argument to install and use the Traffic Manager software.

The container uses ports TCP:9070, TCP:9080, TCP:9090, UDP:9080, and UDP:9090.

To access the Admin UI, use TCP port 9090.

To specify a DNS search path for your instance, use the "--dns-search <search domain>" argument. For example, `--dns-search example.com`.

Setting the Image Identifier

To install the Traffic Manager from an image held in Docker Hub, use the value:

```
pulsesecure/vtm:<version>
```

where <version> corresponds to the Traffic Manager version number (for example, 20.2).

Alternatively, if you are installing the Traffic Manager from a locally-built image, use the details of the public repository containing the image. Specify your repository details in the format:

```
<domain>[:<port>]/<image_tag>
```

where <domain> is the domain name or IP address of the repository, followed by an optional <port> number. Provide the identifying Traffic Manager image tag in <image_tag>. For example, a valid image identifier for a local repository might be "registry.mycompany.com:9999/pulse-vtm-20.2".

Customizing your Traffic Manager Container

The command syntax from the previous section shows the typical usage designed to launch a Traffic Manager instance in a Docker container. The Docker "run" command can be customized to introduce additional configuration for your Traffic Manager container using the syntax "-e <ARGUMENT>=<VALUE>". The following table describes common optional arguments.

Argument	Description
ZEUS_LIC	Use ZEUS_LIC=<license_file> to add a software license to your Traffic Manager instance. Set <license_file> to an HTTP URL from which the license file is downloaded. For example: ZEUS_LIC=http://192.0.2.0/fla.lic If you omit this argument, the Traffic Manager is considered unlicensed.
ZEUS_COMMUNITY_EDITION	If you do not provide a software license through the ZEUS_LIC argument, on first start the Traffic Manager presents a unlicensed warning page. Use "ZEUS_COMMUNITY_EDITION=yes" to bypass this warning and instead use the Community Edition. For more information, see "Licensing" on page 16.

Argument	Description
ZEUS_PASS	Use ZEUS_PASS=<password> to set the administrator password. If this argument is omitted, or if you specify "ZEUS_PASS=RANDOM" or "ZEUS_PASS=SIMPLE", the Traffic Manager generates a random password using a combination of alphanumerics, commas (,), periods (.), hyphens (-), underscores (_), and plus (+) characters. Alternatively, use "ZEUS_PASS=STRONG" to request a cryptographically stronger (and longer) random password constructed from a wider range of characters. To view the generated password, view the log file `/var/log/provision.log` inside the container.
ZEUS_PACKAGES	Use ZEUS_PACKAGES=<package list> to include a space-separated list of software packages for installation on first run of the container. For example: ZEUS_PACKAGES="openjdk-7-jre-headless"
ZEUS_CLUSTER_NAME	Use ZEUS_CLUSTER_NAME=<DNS_name> to join this new instance to an existing Traffic Manager cluster. Set <DNS_name> to the DNS name of one of the cluster members. The Traffic Manager then attempts to contact this cluster member at https://<DNS_name>:9090.
ZEUS_CLUSTER_PORT	If you have set ZEUS_CLUSTER_NAME, but your cluster peer is listening on a port other than 9090, set the alternative port with ZEUS_CLUSTER_PORT=<port>.

Importing Configuration

From version 18.3, Traffic Manager containers can be deployed in a pre-configured state by using the *Configuration Importer* to import configuration documents copied or mounted into the container. The Traffic Manager can also continue to manage its configuration through watching for changes to mounted configuration documents. To learn more about the format of configuration documents and to see examples of how to manage the configuration of Docker containers using this mechanism, see the *Pulse Secure Virtual Traffic Manager: Configuration Importer Guide*.

Traffic Manager containers deployed with base configuration can be managed through the standard configuration interfaces, such as the Admin UI and the REST API. However, Pulse Secure recommends that Traffic Manager containers whose configuration is managed by watching for changes to configuration documents do not have their configuration updated through other mechanisms. Those updates are overridden if the watched configuration changes.

The following Docker "run" command arguments control whether the Traffic Manager imports a base configuration during deployment and whether it continues to manage its configuration through watching for changes to the supplied configuration:

Note: The following commands are applicable to Traffic Manager version 18.3 and later only.

Argument	Description
ZEUS_BASE_CONFIG	A directory path containing base configuration to apply to the Traffic Manager when the container is first deployed. To pick up any changes to the base configuration, you must re-deploy the container. This directory must contain a subdirectory named "config", under which your configuration documents are stored. To learn more about how to define the configuration documents, see the *Pulse Secure Virtual Traffic Manager: Configuration Importer Guide*.
ZEUS_WATCHED_CONFIG	A directory path containing configuration to be applied on top of the base configuration. The Traffic Manager watches for changes to the configuration in this directory and automatically applies the configuration whenever a change is detected. This directory must contain a subdirectory named "config", under which your configuration documents are stored. To learn more about how to define the configuration documents, see the *Pulse Secure Virtual Traffic Manager: Configuration Importer Guide*.
ZEUS_CONFIG_IMPORT_ARGS	Additional arguments to pass to the configuration importer tool when invoked. Applies to both ZEUS_BASE_CONFIG and ZEUS_WATCHED_CONFIG. Possible values are: • **--no-replicate**: Do not replicate configuration between cluster members after an import. • **--no-restart**: Do not automatically restart the Traffic Manager software if a setting changes that requires the software to be restarted to take effect. • **--restart-timeout**: The time to wait for remote Traffic Managers to restart before reporting a failure.

Auto-Registering with Pulse Secure Services Director

To license a Traffic Manager instance as part of a Pulse Secure Services Director deployment, the Traffic Manager first be configured with a Fully Qualified Domain Name (FQDN). To provide the container with a FQDN at launch, use the "-h" argument:

```
-h vtm1.mycompany.com
```

For the Traffic Manager to successfully register itself with a Services Director, include the following arguments in the Docker "run" command using the syntax "-e <ARGUMENT>=<VALUE>":

Argument	Description
ZEUS_REGISTER_HOST	The Host/IP and Port of your Services Director REST API. For example: `ZEUS_REGISTER_HOST=sd.mycompany.com:8100`
ZEUS_REGISTER_FP	A 20-byte, hex-encoded, colon-separated hash value, used to verify the SHA-1 fingerprint of the certificate of the Services Director. For example: `ZEUS_REGISTER_FP=aa:bb:cc:dd:ee:ff:11:22:33:44:55:66:77:88:99:00:aa:bb:cc:dd`
ZEUS_REGISTER_EMAIL	The contact email address for the registering Traffic Manager

Argument	Description
ZEUS_REGISTER_MSG	A short message to display to the Services Director administrator
Deployments of Pulse Secure Services Director release 2.6 and later include the ability to have Traffic Manager software licenses auto-accepted according to an approval policy. To use this feature, add the following arguments to the "run" command line:	
ZEUS_REGISTER_POLICY	The ID for the Auto-Accept approval policy to use for this Traffic Manager
ZEUS_REGISTER_OWNER	The associated Services Director owner ID
ZEUS_REGISTER_SECRET	The associated Services Director owner shared secret

To obtain the argument values described here, contact your Services Director administrator. The following is an example command incorporating Services Director auto-registration:

```
docker run --name="vtm1" \
   -e ZEUS_EULA=accept \
   -e ZEUS_REGISTER_HOST="sd.mycompany.com:8100" \
   -e ZEUS_REGISTER_FP="A0:A1:A2:A3:A4:A5:A6:A7:A8:A9:B1:B2:B3:B4:B5:B6:B7:B8:B9:B0" \
   -e ZEUS_REGISTER_EMAIL="me@mycompany.com" \
   -e ZEUS_REGISTER_MSG="Success" \
   -e ZEUS_REGISTER_OWNER="jbloggs" \
   -e ZEUS_REGISTER_SECRET=qwerty1 \
   -e ZEUS_REGISTER_POLICY=Policy-9999-9999-9999-9999 \
   --privileged \
   --init \
   -t \
   -d \
   registry.mycompany.com:9999/pulse-vtm-20.2
```

For further details concerning the use of Pulse Secure Services Director, contact Pulse Secure Technical Support (support@pulsesecure.net).

Connecting to the Container

To attach to the Traffic Manager container, use the following command:

```
docker exec -i -t <container ID> /bin/bash
```

To locate the correct <container ID>, use the `docker ps` command to list all containers and their associated identifiers.

Configuring the Traffic Manager Software Manually

Depending on the arguments passed to the Docker "run" command, your Traffic Manager instance is fully installed and configured ready for use. To manually reconfigure the Traffic Manager software, use the procedure described in this section.

To re-configure your Traffic Manager software, use 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.

To run the configure script

1. Become the system superuser and type the following at the command line:

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

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

2. 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. 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 software starts as the Community Edition. For further information, see "Licensing" on page 16.

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

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

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

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

   If you intend to use a single IP address for the internal management traffic, and are running on a Linux 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.

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

7. Decide if you want the software to start automatically when the Traffic Manager container operating system 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.

8. 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]:
   ```

9. 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 the Traffic Manager Software" on page 14.

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 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 container command line using the following command:

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

Upgrading and Downgrading the Traffic Manager

Note: Pulse Secure strongly recommends you make a configuration backup before commencing any of the procedures described in this section. For information on creating configuration backups, see the *Pulse Secure Virtual Traffic Manager: User's Guide*.

Traffic Manager containers in Docker are designed to be transient. That is, to be created and terminated according to need. To upgrade or downgrade the Traffic Manager software version running in a particular container, replace it with a container based on the alternate Traffic Manager version.

To learn more about downgrading your Traffic Manager software version, see "Downgrading to an Earlier Version" on page 14.

The specific procedure for upgrading your Traffic Manager software version depends on whether you are upgrading a single Traffic Manager instance or a cluster of Traffic Manager instances.

Upgrading a Single Traffic Manager

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

Upgrading a Cluster of Traffic Managers

Using clustering and fault tolerant Traffic IP addresses, you can upgrade a cluster in place, replacing each Traffic Manager instance 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 container 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 a Cluster Using the Backup and Restore Method" on page 13.

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.

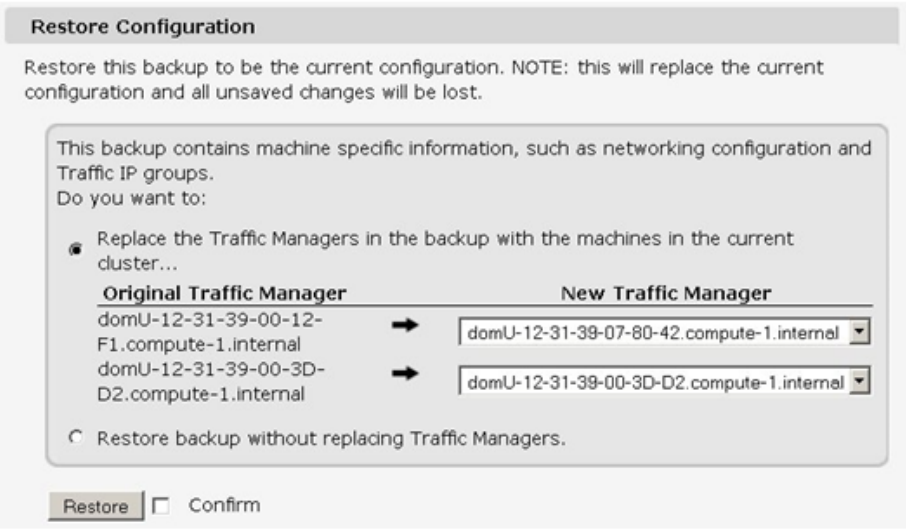
Upgrading a Cluster Using the Backup and Restore Method

You can also upgrade a cluster by taking a backup of its configuration, creating a new cluster using a new Docker container image, 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 container image. Make each new instance join the new cluster, but do not perform any additional configuration procedures.
3. 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 4 Mapping the Traffic Manager in a Backup



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.

Downgrading to an Earlier Version

The procedure to downgrade, or roll-back, your Traffic Manager software is based on the same replace and terminate procedure described earlier in this chapter for software upgrades.

While the upgrade procedure includes the facility to import configuration from an older Traffic Manager instance, and for that configuration to be automatically upgraded, Traffic Manager instances at earlier software versions cannot accept configuration created in later versions. For example, rolling back from 18.3 to 18.2.

Instead, create a new container based on the earlier Traffic Manager software version, and terminate any containers using the later software version. Pulse Secure recommends recreating the configuration for any required services manually.

Reconfiguring the Traffic Manager Software

The `configure` script is a utility that allows you to clear your Traffic Manager configuration and then reconfigure the software.

Note: You can rerun the configure script at any time to change any or all of the settings you chose initially.

To reconfigure the Traffic Manager software

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

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

   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 an unconfigured installation state. 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 typically uses a DNS resolvable name for identification and cluster communications. You set this name or IP address when you initially configure the Traffic Manager software.

To cluster multiple Traffic Manager container instances in Docker, each Traffic Manager must instead be identified using its IP address. To configure your Traffic Manager instance to be identified with an IP address instead of a hostname, perform the following steps:

1. Log on to the Traffic Manager command line and select "Perform the post-install configuration again".
2. To use an IP address instead of a hostname, choose the applicable option from the choices shown:

```
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 [3]:
```

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 back to using a resolvable name from this page. Instead, rerun the configure script.

Licensing

Traffic Manager deployments in Docker consist of a Linux/UNIX container image, with the Traffic Manager software variant installed within.

The Traffic Manager uses a license key to define its operating parameters and available feature set. If you intend to join two or more Traffic Managers together to form a fault-tolerant cluster, you must ensure your license keys provide the same level of functionality for all cluster members.

If your license key expires (or if you elect not to add a license during initial configuration), the Traffic Manager runs 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 add a license later, or to make changes to your Traffic Manager's existing licensing, refer to the guidance in the *Pulse Secure Virtual Traffic Manager: Software Installation and Getting Started Guide*. For further questions about licensing, or to obtain license keys, contact Pulse Secure Technical Support.

Including an Updated GeoIP Database in a Customized Docker Image

The following Dockerfile provides sample code to show how a `geoip_update_<date>.tgz` package can be applied to the standard Traffic Manager Docker image. Alternatively, the steps described here can be incorporated into other Dockerfiles being used to customize the Traffic Manager image.

```
FROM pulsesecure/vtm:20.2
ADD geoip_update*.tgz  /tmp/
RUN mkdir -p /usr/local/zeus/zxtm/etc/geo/ && \
    mv /tmp/geoip_upgrade/geo/* /usr/local/zeus/zxtm/etc/geo/
ENTRYPOINT [ "/usr/local/zeus/runzeus.sh" ]
EXPOSE 9070 9080 9080/udp 9090 9090/udp
```

The **FROM** step specifies the initial Traffic Manager image the subsequent steps are applied to, and should refer to the version specified by *dockerhub* or a local repository.

The **ADD** step requires that your new `geoip_update_<date>.tgz` file is present in the directory specified to the subsequent `docker build` command.

Note: To obtain updated GeoIP packages, see the Pulse Secure customer portal pages at: my.pulsesecure.net.

With this Dockerfile and a GeoIP update package in the current directory, the following command prepares an image containing the updated GeoIP database:

```
docker build --no-cache -t registry.mycompany.com:9999/vtm:withgeo ./
```

(replace references to `mycompany.com` with a value applicable to your organization)