Pulse Secure Virtual Traffic Manager: Release Notes

Supporting Pulse Secure Virtual Traffic Manager 21.1

Product Release	21.1
Published	26 April, 2021
Document Version	1.1

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

www.pulsesecure.net

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: Release Notes

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

Release Notes

This chapter contains the following topics:

Overview

Pulse Secure Virtual Traffic Manager 21.1 is a feature release of the Pulse Secure Virtual Traffic Manager product family, containing a number of performance and functionality enhancements and bug fixes.

New Features

The following table describes the major features that are introduced in the corresponding release.

Report Number	Features	Description
VTM-43928, RFE-1501	Support for HTTP Strict Transport Security in Admin UI	Added support for adding HTTP Strict Transport Security (HSTS) headers when accessing the Admin UI. HSTS is a web security policy mechanism (defined in RFC 6797) that helps to protect the Admin Server against man-in-the-middle attacks such as protocol downgrade attacks and cookie hijacking. When enabled, HSTS headers declare that web browsers (or other user agents) should only interact with it using HTTPS connections.

Pulse Secure Virtual Web Application Firewall Features

The Traffic Manager will install version 4.10-0 of Pulse Secure Virtual Web Application Firewall (vWAF). This new version includes a number of important internal updates, including migrating the codebase to Python 3.

Before upgrading, users must ensure that any Python scripts they have included in script libraries are compatible with Python 3.

Note: "Resource Requirements" on page 2 now includes a recommendation that virtual appliances running vWAF should have a RAM allocation of at least 4GB. Version 4.10 of vWAF should be expected to consume approximately 500MB more system RAM than previous versions.

Product Compatibility

You can install and use this product version on the following platforms:

Software

- Linux x86_64: Kernel 3.10 - 5.2, glibc 2.17+

  For Route Health Injection: ncurses 5 (libncurses.so.5, libtinfo.so.5)

Containers

- Docker: 1.13.0 or later recommended

Cloud Platforms

- Amazon EC2 - as a virtual appliance or native software install
- Microsoft Azure - as a virtual appliance
- Google Compute Engine - as a virtual appliance or native software install

Hardware Platforms

- Bare Metal Server - for information on qualified servers, see the Pulse Secure Virtual Traffic Manager Hardware Compatibility List at https://www.pulsesecure.net/techpubs

Virtual Appliance Editions

- VMware vSphere 6.5, 6.7, 7.0
- XenServer 7.1, 8.1, 8.2
- Microsoft Hyper-V Server 2016
- Microsoft Hyper-V under Windows Server 2016 and 2019
- QEMU/KVM (RHEL/CentOS 6.x, 7.x; Ubuntu 16.04, 18.04)

Resource Requirements

Virtual appliances should be allocated a minimum of 2GB of RAM. Virtual appliances running Pulse Secure Virtual Web Application Firewall should be allocated a minimum of 4GB of RAM.

For a virtual appliance upgrade to succeed, a minimum of 2.7GB must be available on the `/logs` partition. To confirm the available free disk space, use the **System > Traffic Managers** page of the Admin UI.

Large Objects in the Webcache

A Traffic Manager running version 20.1 or later will be unable to store objects greater than 2GB in the web cache, even if the web cache is enabled and all cacheability conditions are met. If you rely upon this feature, please contact Pulse Secure Technical Support through the usual support mechanism (see "Technical Support" on page 7).

GeoIP database

VTM-43072, RFE-1472 The database used by the Traffic Manager to look up the geographic location of incoming requests based on their IP address was removed from the software installation package and appliance images in version 20.3 in order to better comply with various privacy protection laws. This database is used when performing Global Load Balancing, when displaying the Activity Map or using the geo.* TrafficScript functions.

Update packages containing the most recent version of this database can be obtained from the Pulse Secure customer portal.

Note: The GeoIP database already present in Traffic Manager instances that are upgraded to this version is retained, and continues to be used until an update package with a newer database is applied.

Support for software running on RHEL/CentOS 6

VTM-43879 Version 20.3 is the last release to support 2.6.32-based kernels or glibc 2.12. Versions from 21.1 onwards require kernel version 3.10 or later, and glibc 2.17 or later, as described in "Product Compatibility" on page 2.

In particular, this means that it is not possible to install version 21.1 on a RHEL/CentOS 6 system or to upgrade an existing Traffic Manager instance on RHEL/CentOS 6 to version 21.1 or beyond.

Fixed Issues and Other Changes

The following table lists issues that have been fixed and are resolved by upgrading to this release.

Report Number	Description
Configuration	
VTM-44158	Removed a rare race condition that had allowed corruption of replicated configs which subsequently caused cluster members to be expunged from their cluster.
VTM-44005	Fixed an issue where logging in to the UI of a Traffic Manager cluster member triggered spurious config modification ("confmod") events.
VTM-43976	Fixed a race in config-importer which resulted in transient "No such file or directory" errors for parts of the config while being read by the Traffic Manager.
VTM-43955	Two virtual server settings **http2_client_buffer_multiplier** and **http2_server_buffer_multiplier** have been added to limit the amount of in-process memory allocated by the Traffic Manager to buffer data for a HTTP/2 connection. **http2_client_buffer_multiplier** limits HTTP/2 data received from clients not yet sent to pool nodes and **http2_server_buffer_multiplier** limits the HTTP/2 data received from pool nodes not yet sent to clients.
VTM-15765 SR19864	Fixed an intermittent failure during configuration replication caused by transient temporary configuration files.
Administration Server	
VTM-34131	Fixed a repeated crash if $ZEUSHOME/log/statd directory is removed accidentally by a user; this directory is now recreated automatically.

Report Number	Description
REST API	
VTM-44011	Fixed an issue where an invalid value written into the Locations catalog configuration could stop the REST API from working.
SNMP	
VTM-16220 SR20354	Fixed an issue where SNMPv2 TRAPs emitted by the traffic manager didn't confirm to RFC 2578 because they had a superfluous ".0" (zero) appended to the OID.
Connection Processing	
VTM-44178	Fixed an issue where, when HTTP/2 was enabled, memory could be gradually leaked if a malicious client caused a very large number frames to be queued, as a previous update in 17.2r2 to mitigate CVE-2019-9517 was ineffective.
VTM-44147	Fixed an issue that the memory used to buffer TCP data for a HTTP/2 request could be uncapped. Such uncapped TCP buffer could cause excessive memory usage.
VTM-44133	Fixed an issue that some buffered data for closed TCP connections might not be deallocated promptly.
VTM-44110	Periodically logged diagnostics have been enhanced to include information of memory usages for different purposes.
VTM-44088	Fixed an issue that the memory used by HTTP/2 streams which are blocked by protection class could be held by the Traffic Manager until either the Traffic Manager is restarted or the corresponding virtual server's configuration is changed.
VTM-42577	When receiving a request from an HTTP/2 client with no request body, the Traffic Manager no longer sends a "Content-Length: 0" header to an HTTP/1.1 backend node. Whilst the previous behaviour was valid in RFE 7241, some servers were confused by the additional header.
Fault Tolerance	
VTM-44221	Fixed an issue in persistence classes that Traffic Manager processes could be stalled, killed and restarted once persistence classes start evicting oldest cached entry when the corresponding cache table is full. For IP persistence class, the cached entry eviction starts after **ip_cache_size** (default 32768) different client IP addresses have been cached.
IP Transparency	
VTM-43961	The ztrans module, previously available for use with older Linux kernel versions, is no longer required as all supported kernel versions have the necessary built-in support for IP_TRANSPARENT when using the "**transparent**" pool setting.
SSL/TLS and Cryptography	
VTM-43999	Fixed an issue where only the client certificate itself was sent to a pool node when the pool setting **ssl_fixed_client_certificate** was used to specify a chain of certificates to be sent in response to any certificate request from a node.
VTM-43993	The library modified from OpenSSL that is used by the Traffic Manager has been upgraded to version 1.1.1j, addressing CVE-2021-23840. This library is used to provide cryptographic primitives such as RSA or AES.
Telemetry	

Report Number	Description
VTM-44019	Fixed an issue that the telemetry script zxtm-crash could consume too much memory if the event log file size is large.
Internals	
VTM-43989	The $ZEUSHOME/zxtm/bin/mtrace utility has been removed as better tools are now available to profile memory usage.

Pulse Secure Virtual Traffic Manager Appliance

The following table lists issues that have been fixed and are resolved by upgrading to this release.

Report Number	Description
Appliance OS	
VTM-44184	Updated the appliance kernel to version 4.15.0-140.144, and updated packages installed on the appliance. These updates include changes addressing: CVE-2018-20482 CVE-2019-9923 CVE-2019-19770 CVE-2020-0423 CVE-2020-8625 CVE-2020-10135 CVE-2020-11947 CVE-2020-15859 CVE-2020-25656 CVE-2020-25668 CVE-2020-25669 CVE-2020-25704 CVE-2020-25705 CVE-2020-27170 CVE-2020-27171 CVE-2020-27619 CVE-2020-27673 CVE-2020-27675 CVE-2020-27777 CVE-2020-27815 CVE-2020-27830 CVE-2020-28374 CVE-2020-28916 CVE-2020-28941 CVE-2020-28974 CVE-2020-29361 CVE-2020-29362 CVE-2020-29363 CVE-2020-29374 CVE-2020-29443 CVE-2020-29568 CVE-2020-29569 CVE-2020-29660 CVE-2020-29661 CVE-2020-35508 CVE-2020-35523 CVE-2020-35524 CVE-2020-36158 CVE-2020-36221 CVE-2020-36222 CVE-2020-36223 CVE-2020-36224 CVE-2020-36225 CVE-2020-36226 CVE-2020-36227 CVE-2020-36228 CVE-2020-36229 CVE-2020-36230 CVE-2021-3156 CVE-2021-3177 CVE-2021-3178 CVE-2021-3449 CVE-2021-20181 CVE-2021-23239 CVE-2021-23840 CVE-2021-23841 CVE-2021-24031 CVE-2021-24032 CVE-2021-26937 CVE-2021-27212 CVE-2021-27218 CVE-2021-27219 CVE-2021-27363 CVE-2021-27364 CVE-2021-27365 CVE-2021-28153

Known Issues

The following table lists the Known issues in the current release..

Report Number	Report	Description
VTM-34654	KVM Network Interface Card renaming	In rare circumstances a KVM host may change the PCI addresses of a virtual appliance's network cards after a reboot, resulting in the network interface labels changing. This can be fixed by removing the configuration from the non-existent card on the Traffic Manager **System > Networking** page and re-adding it to the correct card.
VTM-38881	Obsolete counters are missing from old REST API versions	Obsolete counters removed from version 6.0 of the status API are missing in versions 5.X, despite the schemata published with the product claiming they are still present.

Report Number	Report	Description
VTM-38948	The format of encrypted bootloader passwords has changed in version 18.2	The format of encrypted bootloader passwords changed in version 18.2. When upgrading from a version earlier than 18.2 with a bootloader password set, the bootloader will be unprotected, and a configuration error will be reported until the password is re-entered. It can be set on the **System > Global Settings** page of the Admin UI.
VTM-38962	Pre-18.2 Admin UI rollback tools will not offer roll-forward to 18.2 or later	After rolling back from 19.2 to a Traffic Manager version earlier than 18.2 the rollback version selector on the **System > Traffic Managers** page of the Admin UI will not offer versions after 18.2 as an option. Use `$ZEUSHOME/zxtm/bin/rollback` from the command line to switch back instead.

Upgrade Instructions

To learn more about upgrading your Traffic Manager, see the *Pulse Secure Virtual Traffic Manager: Installation and Getting Started Guide* applicable to your product variant.

Documentation

Pulse Secure documentation is available at https://www.pulsesecure.net/techpubs.

For policy reasons, security issues are not normally mentioned in release notes. To find more information about our security advisories, see the security advisory page on the Pulse Secure website.

Technical Support

Full support for version 21.1 will be available for one year from the release date of 19 April, 2021. For more information, see the End of Support and End of Engineering Schedule notices at the following location: https://support.pulsesecure.net/product-service-policies/eol/software/vadc-virtual-traffic-manager/

For additional information or assistance, contact Pulse Secure Global Support Center (PSGSC):

- https://support.pulsesecure.net
- support@pulsesecure.net
- Call 1-844-751-7629 (toll-free USA)

For technical support resources, browse the Pulse Secure Technical Support website https://support.pulsesecure.net.

Revision History

The following table lists the revision history for this document:

Revision	Revision Date	Description
1.0	19 April 2021	21.1 Release Notes created.
1.1	26 April 2021	Updated the issue list in "Fixed Issues and Other Changes".