



Pulse Secure Virtual Traffic Manager: Release Notes

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: 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	1
OVERVIEW	1
NEW FEATURES.....	1
PRODUCT COMPATIBILITY.....	2
SOFTWARE	2
CONTAINERS	2
CLOUD PLATFORMS.....	2
HARDWARE PLATFORMS	2
VIRTUAL APPLIANCE EDITIONS.....	2
LARGE OBJECTS IN THE WEBCACHE.....	2
FIXED ISSUES AND OTHER CHANGES.....	3
PULSE SECURE VIRTUAL TRAFFIC MANAGER APPLIANCE.....	5
KNOWN ISSUES.....	5
UPGRADE INSTRUCTIONS.....	6
DOCUMENTATION	6
TECHNICAL SUPPORT	6

Release Notes

This chapter contains the following topics:

• Overview	1
• New Features	1
• Product Compatibility	2
• Large Objects in the Webcache	2
• Fixed Issues and Other Changes	3
• Known Issues	5
• Upgrade Instructions	6
• Documentation	6
• Technical Support	6

Overview

Pulse Secure Virtual Traffic Manager 20.1 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-11412, VTM-13029, SR15162, SR16855	Encrypted LDAP (LDAPS and STARTTLS) administration authentication added	<p>The user and password needed to login to the Traffic Manager's administration interfaces can now be protected while being sent to an LDAP server configured in a LDAP authenticator, for example, through the Admin UI System > Users > Authenticators page.</p> <p>The new ldap!ssl configuration key can be used to require that connections to a remote LDAP server are SSL-encrypted using either the STARTTLS or LDAPS mechanism. The Certificate Authority used to issue the certificate presented by the LDAP server must be entered into the new SSL > Administration Certificate Authorities and Certificate Revocation Lists catalog in order for the required server identity checks to succeed.</p>

Pulse Secure Virtual Web Application Firewall Features

The Traffic Manager will install version 4.9-43423 of the Pulse Secure Virtual Web Application Firewall.

Product Compatibility

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

Software

- Linux x86_64: Kernel 2.6.32 - 5.2, glibc 2.12+
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 6.0, 6.5, 6.7
- XenServer 7.1, 8.0, 8.1
- 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.

Large Objects in the Webcache

A Traffic Manager running 20.1 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 6](#)).

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
Installation and Upgrading	
VTM-42672	Fixed a bug where the configure script would still loop if --nolooop was provided but clustering failed.
VTM-42476	The script used to list installed Traffic Manager versions on appliances now uses the read-only option to mount, reducing the amount of time that operation takes.
VTM-42371	The Traffic Manager software installer no longer depends on the presence of the libnsl.so system library so that the Traffic Manager can be installed on systems whose base package set does not include libnsl.
Authentication	
VTM-18659, VTM-36053, VTM-28340, VTM-23999, VTM-17657, SR23353, SR31954, SR22049	Fixed an issue where the System > Users > Authenticators > Edit page wasn't formatted correctly, and looked ugly in the browser. All the page elements are now aligned within the background box.
Administration Server	
VTM-42705	Fixed an issue where ec2!query_server was not always honored and requests were sometimes made to ec2.amazonaws.com regardless of this setting.
VTM-42592	Fixed an issue where the cert utility would always set the serial number of certificates it created from certificate requests to zero. The serial number will now be set to a randomly-generated number.
VTM-42403	Fixed an issue in the Admin UI where the Status Applet would not display, nor the event log auto-update, when Internet Explorer 11 was being used to view the UI.
VTM-42432	Fixed an issue where displaying the Pools summary page in the Admin UI was slow when using Service Discovery with many pools.
REST API	
VTM-42178	<p>The REST API has increased its major version to 8.0. This is a backwards incompatible change, and whilst 6.x and 7.x continue to be supported, they are deprecated and you are strongly encouraged to update your scripts to the latest version of the API.</p> <p>See the <i>REST API Guide</i> for a comprehensive set of changes and help with updating.</p> <p>Following the earlier deprecation announcement API versions 5.x have been removed.</p>
TrafficScript	

Report Number	Description
VTM-42422	<p>Entries in the Authenticators Catalog with ldap!ssl enabled and ldap!ssl!cert specified now include a Server Identity Check as well as verifying that the LDAP server certificate is signed by the specified certificate authority.</p> <p>Attempts by a TrafficScript rule to use such an authenticator via auth.query(), and that connect to a server that does not have a certificate matching its identity will fail and log a message in the event log.</p>
VTM-42419	Updated libxslt, which the Traffic Manager is linked against, to version 1.1.34, which fixes the following security vulnerabilities: CVE-2019-18197
VTM-37997	Updated libxml2, which the Traffic Manager is linked against, to version 2.9.9, which addresses CVE-2018-14404.
Connection Processing	
VTM-42829	Fixed an issue where a virtual server using the DNS protocol could read from heap memory after it had been freed.
VTM-42444	Fixed an issue where the traffic manager would incorrectly handle an irregular packet received by a virtual server configured to support HTTP/2, resulting in connections being dropped or denied.
Webcache	
VTM-41602	Fixed an issue where the Traffic Manager's content cache would occasionally contain invalid data, resulting in responses containing incorrect content, or connections being dropped or denied.
Global Load Balancing	
VTM-42827	Updated GeolIP database to 2020-02-25.
VTM-42732	Added a TrafficScript function glb.service.getLocationLoad() to access the load of particular locations assigned to a Global Load Balancing service.
Service Discovery	
VTM-42500	Fixed an issue where deleting pools using service discovery caused persistent error log entries of "Internal Service Discovery pool data unexpectedly missing"
vTM Self Registration	
VTM-42837	Fixed an issue where licensing settings (including Services Director self-registration settings) entered during the Initial Configuration Wizard were not saved.
Container-based Deployment	
VTM-42446	Fixed an issue whereby an outdated version of the Ubuntu base layer was used to build the docker image.

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-42613	Updated the appliance kernel to 4.15.0-74.84, and updated packages installed on the appliance. These updates include changes addressing: CVE-2018-12207 CVE-2018-14498 CVE-2018-20976 CVE-2018-21008 CVE-2019-0154 CVE-2019-0155 CVE-2019-2201 CVE-2019-2894 CVE-2019-2945 CVE-2019-2949 CVE-2019-2962 CVE-2019-2964 CVE-2019-2973 CVE-2019-2975 CVE-2019-2978 CVE-2019-2981 CVE-2019-2983 CVE-2019-2987 CVE-2019-2988 CVE-2019-2989 CVE-2019-2992 CVE-2019-2999 CVE-2019-5094 CVE-2019-5188 CVE-2019-5827 CVE-2019-6477 CVE-2019-11135 CVE-2019-11745 CVE-2019-12068 CVE-2019-12155 CVE-2019-12290 CVE-2019-13117 CVE-2019-13118 CVE-2019-13164 CVE-2019-13627 CVE-2019-14287 CVE-2019-14378 CVE-2019-14814 CVE-2019-14815 CVE-2019-14816 CVE-2019-14821 CVE-2019-14866 CVE-2019-14895 CVE-2019-14896 CVE-2019-14897 CVE-2019-14901 CVE-2019-14973 CVE-2019-15098 CVE-2019-15117 CVE-2019-15118 CVE-2019-15165 CVE-2019-15505 CVE-2019-15538 CVE-2019-15795 CVE-2019-15796 CVE-2019-15890 CVE-2019-15902 CVE-2019-15918 CVE-2019-16056 CVE-2019-16168 CVE-2019-16231 CVE-2019-16233 CVE-2019-16746 CVE-2019-16935 CVE-2019-17006 CVE-2019-17007 CVE-2019-17052 CVE-2019-17053 CVE-2019-17054 CVE-2019-17055 CVE-2019-17056 CVE-2019-17075 CVE-2019-17133 CVE-2019-17546 CVE-2019-17666 CVE-2019-18197 CVE-2019-18218 CVE-2019-18224 CVE-2019-18660 CVE-2019-18806 CVE-2019-19045 CVE-2019-19052 CVE-2019-19060 CVE-2019-19065 CVE-2019-19075 CVE-2019-19083 CVE-2019-19523 CVE-2019-19524 CVE-2019-19525 CVE-2019-19526 CVE-2019-19527 CVE-2019-19528 CVE-2019-19529 CVE-2019-19530 CVE-2019-19531 CVE-2019-19532 CVE-2019-19533 CVE-2019-19534 CVE-2019-19535 CVE-2019-19536 CVE-2019-19537 CVE-2019-19725 CVE-2019-19807 CVE-2019-20367
VTM-42461	Fixed an issue where sometimes a systemd-timesyncd process would be running instead of the correctly configured ntpd.
VTM-42506	Fixed an issue where sysconfig took excessive time to complete when a large number of service discovery pools were configured.
Cloud Platforms	
VTM-39229	Fixed an issue where NTP would not be correctly configured on appliances running in Azure.

Known Issues

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

Report Number	Report	Description
VTM-41385	Software in Ubuntu 16.04 on GCE	A Traffic Manager software install on a GCE instance running Ubuntu 16.04 can report a serious error "sysconfig_error GCE IP routes error: Didn't find nic label for <MAC address>". This does not occur for Ubuntu 18.04.

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.
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 vTM 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

Pulse Secure Virtual Traffic Manager 20.1 is designated a Long Term Support (LTS) release.

Full support for version 20.1 will be available for three years from the release date of 16 March, 2020. 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>.