Pulse Secure Virtual Traffic Manager: Release Notes

Supporting Pulse Secure Virtual Traffic Manager 20.3

Product Release	**20.3**
Published	**8 February, 2021**
Document Version	**1.0**

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

www.pulsesecure.net

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 20.3 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-43841, RFE-1492	Public availability of Analytics Export	The Analytics Export feature previously released in 17.2, but available via Services Director licensing only, is now available with all licenses. This feature allows Pulse Secure Virtual Traffic Manager to export data about the individual transactions processed by services running on the Traffic Manager cluster, as well as entries from log files stored on the each of the cluster members. Typically, the data would be exported to an analytics platform, such as Splunk, for offline analysis through aggregate searches and visualization tools. Cluster-wide configuration for export of transaction metadata and log files is available from the **System > Analytics Export** settings page. Additional per-service settings for export of transaction metadata can be configured from the **Virtual Server > Connection Analytics** settings page.

Report Number	Features	Description
VTM-43291, RFE-1442	Support for TLS Extended Master Secret	Added support for the extended_master_secret extension when a connection using TLS protocol 1.0, 1.1 or 1.2 is made to or from the Traffic Manager. This provides improved protection against "man-in-the-middle" attacks such as the Triple Handshake Attack. The TLS 1.3 protocol does not suffer from this class of attacks.
VTM-43461, RFE-1498	Acceleration for HMAC-SHA256 in TrafficScript	Added a TrafficScript function `string.hmacSHA256()` that calculates the keyed-hash message authentication code (HMAC) for a given input and key, as described in NIST FIPS 198-1 / RFC 2104.
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 6.5, 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. 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 8).

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 has been removed from the software installation package and appliance images 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. The database present in existing appliances or installations that are upgraded to this version will copied into the new traffic manager installation and will continue to be used until an update package with a newer database is applied.

Support for software running on RHEL/CentOS 6

VTM-43879 Release 20.3 will be the last release to support 2.6.32-based kernels or glibc 2.12. Future releases will require kernel version 3.10 or later, and glibc 2.17 or later.

In particular, software running on RHEL 6 or CentOS 6 will no longer be supported.

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
Authentication	
VTM-43708	Updated the MIT kerberos library to version 1.18.3, addressing CVE-2020-28196. This library is used when virtual servers have the setting 'kerberos_protocol_transition!enabled' configured to 'Yes'.
Administration Server	

Report Number	Description
VTM-43643, RFE-1468	The "Load Balance a Pulse Connect Secure" configuration wizard now sets the timeout on the HTTPS virtual server configured to 0. This setting is recommended for all customers using the ESP mode of PCS.
VTM-43560	Fixed an issue where the self-signed certificate created for the Administration Server during configuration of a new appliance or software installation did not specify its extended key usage, causing certain browser/operating system combinations to refuse to allow the certificate to be trusted.
VTM-42831	Fixed an issue where the **Diagnose** and **Activity** tabs in the Admin UI took excessive time to open when the Traffic Manager has many (for example, greater than 100) service discovery pools.
Connection Processing	
VTM-43887	Fixed an issue whereby the traffic manager would incorrectly handle an excessive number of outstanding HTTP/2 frames, resulting in connections being dropped or denied.
VTM-43882	Periodically logged diagnostics have been enhanced to include information of the size of internal queues for HTTP requests and TCP connections.
Fault Tolerance	
VTM-43258	Fixed an issue where 'machinetimeout' messages could be logged spuriously or fail to be logged when a Traffic Manager joined or left a cluster that used autoscaling with a pool.
Session Persistence	
VTM-43245	Fixed a race condition in the session persistence that multiple pool nodes could be chosen for the session data which should go to the same pool node if a client established its first session through multiple layer-4 connections to Traffic Manager near the same time. The issue mainly affected IP-based session persistence and could cause the traffic with the same source IP but different TCP/UDP source ports to go to different pool nodes.
Service Protection	
VTM-43551	Fixed an issue where it was possible to provide malformed arguments to the "BuiltIn-PCS_PPS" script.
VTM-43313, VTM-43314	Fixed an issue that a protection class could spuriously ban an IP address permanently until either the Traffic Manager is restarted or the protection class is changed if the corresponding client sends 'max_1_connections' number of HTTPS requests while the IP address is temporarily being banned due to high request rate.
VTM-43273	Fixed an issue that child processes could stall for excessive time if the service protection class configuration is changed while many banned HTTP connections have been responded to with error codes but the corresponding clients have not closed those TCP connections.
Global Load Balancing	
VTM-43636	Fixed an issue where the Admin UI presented outdated names for some countries in the Locations catalog.
VTM-43570	Fixed an issue where the "process_geoip.pl" script provided to convert MaxMind databases into the format needed by the Traffic Manager did not correctly parse location information in newer versions of the GeoIP2 databases.

Report Number	Description
DNS Server	
VTM-43675	Fixed an issue that virtual servers using the DNS protocol could wrongly append a byte to DNS responses with client subnet option. This applies both to responses generated by the built-in DNS server and to responses generated by DNS backend nodes.
Service Discovery	
VTM-43292	Improved the text displayed in the Admin UI's **Pools > Create a new Pool** section when the Pool Autoscaling license feature is not available.
SSL/TLS and Cryptography	
VTM-43561	Self-signed certificates made with the 'Create Self-Signed Certificate' option in the SSL Client/ Server Certificates catalogs now include the extended key usage extension with the appropriate usage signaled.
VTM-43306, RFE-1442	As a mitigation for the Triple Handshake Attack, TLS connections made to or from the Traffic Manager at protocol versions 1.0 - 1.2 will not permit re-negotiation following the resumption of a session that was created without the extended master secret. The Global Setting 'ssl!allow_rehandshake' can be used to disable this protection if it is set to 'Always Allow'.
VTM-39677	Fixed an issue where a virtual server with the TLS 1.3 protocol version enabled could resume a TLS session it had created earlier, while the virtual server's configuration did not allow TLS 1.3. The virtual server will now carry out a full handshake negotiating TLS 1.3 and creating a new session in this situation.
Technical Support Report (TSR)	
VTM-43883, RFE-1519	Periodically logged diagnostics have been enhanced to provided memory heap statistics.
VTM-43744, RFE-1493, RFE-1491, RFE-1480	Updated top command to run twice and show full command in periodic-log, procmon and technical support report. Added the following additional information to Technical Support Report: 1 GeoIP version to new file `support/geoip_version.txt`. 2 `/proc/<PID>/smaps` to new file `/proc/<PID>/smaps`. 3 NIC rx-flow-hash for TCP4, UDP4, TCP6 and UDP6 to existing file `support/networking.txt`. 4 Current CPU frequency settings to new file `support/cpufreq.txt`.
Pulse Connect Secure Integration	
VTM-43644, RFE-1468	The "Load Balance a Pulse Connect Secure" configuration wizard now sets the udp_rbuff_size and udp_wbuff_size on the UDP virtual server configured to 10MiB. This setting is recommended for all customers using the ESP mode of PCS.
VTM-43626, RFE-1468	Fixed a bug where the "Load Balance a Pulse Connect Secure" configuration wizard only recommended deploying the Traffic Manager with IP Transparency enabled when running on systems where IP Transparency was not available. Use of IP Transparency is recommended for all customers using the traffic manager to load balance a Pulse Connect Secure.

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-43762	Updated the appliance kernel to version 4.15.0-128.131, and updated packages installed on the appliance. These updates include changes addressing: CVE-2018-7738 CVE-2018-10322 CVE-2018-11236 CVE-2018-11237 CVE-2018-19591 CVE-2018-20669 CVE-2018-1000035 CVE-2018-1000500 CVE-2019-0145 CVE-2019-0147 CVE-2019-0148 CVE-2019-1547 CVE-2019-1551 CVE-2019-1563 CVE-2019-8936 CVE-2019-9169 CVE-2019-9445 CVE-2019-9674 CVE-2019-12380 CVE-2019-13232 CVE-2019-14855 CVE-2019-16089 CVE-2019-17514 CVE-2019-18808 CVE-2019-19036 CVE-2019-19039 CVE-2019-19054 CVE-2019-19061 CVE-2019-19067 CVE-2019-19073 CVE-2019-19074 CVE-2019-19126 CVE-2019-19377 CVE-2019-19448 CVE-2019-19462 CVE-2019-19813 CVE-2019-19816 CVE-2019-19947 CVE-2019-20807 CVE-2019-20810 CVE-2019-20907 CVE-2019-20908 CVE-2020-1751 CVE-2020-1752 CVE-2020-1968 CVE-2020-1971 CVE-2020-4788 CVE-2020-6829 CVE-2020-8231 CVE-2020-8284 CVE-2020-8285 CVE-2020-8286 CVE-2020-8622 CVE-2020-8623 CVE-2020-8624 CVE-2020-8694 CVE-2020-10029 CVE-2020-10543 CVE-2020-10711 CVE-2020-10713 CVE-2020-10732 CVE-2020-10756 CVE-2020-10757 CVE-2020-10766 CVE-2020-10767 CVE-2020-10768 CVE-2020-10781 CVE-2020-10878 CVE-2020-11935 CVE-2020-12351 CVE-2020-12352 CVE-2020-12400 CVE-2020-12401 CVE-2020-12402 CVE-2020-12403 CVE-2020-12655 CVE-2020-12656 CVE-2020-12723 CVE-2020-12770 CVE-2020-12771 CVE-2020-12829 CVE-2020-12888 CVE-2020-13143 CVE-2020-13253 CVE-2020-13361 CVE-2020-13362 CVE-2020-13659 CVE-2020-13754 CVE-2020-13765 CVE-2020-13974 CVE-2020-14308 CVE-2020-14309 CVE-2020-14310 CVE-2020-14311 CVE-2020-14314 CVE-2020-14344 CVE-2020-14351 CVE-2020-14356 CVE-2020-14363 CVE-2020-14364 CVE-2020-14386 CVE-2020-14390 CVE-2020-14422 CVE-2020-14556 CVE-2020-14577 CVE-2020-14578 CVE-2020-14579 CVE-2020-14581 CVE-2020-14583 CVE-2020-14593 CVE-2020-14621 CVE-2020-14779 CVE-2020-14781 CVE-2020-14782 CVE-2020-14792 CVE-2020-14796 CVE-2020-14797 CVE-2020-14798 CVE-2020-14803 CVE-2020-15393 CVE-2020-15436 CVE-2020-15437 CVE-2020-15705 CVE-2020-15706 CVE-2020-15707 CVE-2020-15709 CVE-2020-15780 CVE-2020-15861 CVE-2020-15862 CVE-2020-15863 CVE-2020-15999 CVE-2020-16092 CVE-2020-16119 CVE-2020-16120 CVE-2020-16123 CVE-2020-16166 CVE-2020-17380 CVE-2020-24394 CVE-2020-25084 CVE-2020-25085 CVE-2020-25211 CVE-2020-25212 CVE-2020-25220 CVE-2020-25284 CVE-2020-25285 CVE-2020-25624 CVE-2020-25625 CVE-2020-25641 CVE-2020-25643 CVE-2020-25645 CVE-2020-25659 CVE-2020-25692 CVE-2020-25709 CVE-2020-25710 CVE-2020-25723 CVE-2020-26088 CVE-2020-26116 CVE-2020-26137 CVE-2020-27350 CVE-2020-27351 CVE-2020-27617 CVE-2020-28196 CVE-2020-28915 CVE-2020-29368 CVE-2020-29371
VTM-38742	Support for vmguestlib has been added to the appliance image.
Virtual Appliance	
VTM-43312	Fixed an issue where an IPv6 gateway address was incorrectly set when deploying a virtual appliance using VMWare Guest Customizations.
Cloud Platform	
VTM-43566	Fixed an issue in the SOAP API, zcli and Admin UI where changing a cluster member's "passive" state or adding or removing addresses to/from a Traffic IP Group containing EC2 VPC private IP addresses failed when a private IP was unchanged in the list.

Report Number	Description
VTM-43298, RFE-1483	Improved the way Private IPs from an EC2 Traffic IP Group are raised so that they are distributed evenly across all ENIs which have suitable subnets.
VTM-43101	The automatic installation of the GeoIP database when deploying new Google Compute Engine (GCE) Traffic Manager appliances can be achieved by specifying the custom metadata 'vtm-geoip-url' in the GCE settings. See the *Virtual Appliance Installation and Getting Started Guide* for more details.

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.
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 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 20.3 will be available for one year from the release date of 8 February, 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.