Pulse Secure®

Pulse Secure Virtual Traffic Manager: Release Notes

Supporting Pulse Secure Virtual Traffic Manager 19.2

Product Release	19.2
Published	15 July, 2019
Document Version	1.0

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

About this Release

Pulse Secure Virtual Traffic Manager 19.2 is a feature release of the Pulse Secure Virtual Traffic Manager product family, containing a number of performance and functionality enhancements and bug fixes.

Platform Availability

Virtual Traffic Manager software

- Linux x86_64: Kernel 2.6.32 - 4.15, glibc 2.12+
  For Route Health Injection: ncurses 5 (libncurses.so.5, libtinfo.so.5)

Virtual Traffic Manager containers

- Docker: 1.13.0 or later recommended

Virtual Traffic Manager virtual appliances

- VMware vSphere 6.0, 6.5, 6.7
- XenServer 7.1, 7.6, 8.0
- 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)

Virtual Traffic Manager 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

Virtual Traffic Manager physical appliances

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

Resource Requirements

Virtual appliances should be allocated a minimum of 2 GB of RAM.

Support

Pulse Secure Virtual Traffic Manager 19.2 is designated a Long Term Support (LTS) release.

Full support for version 19.2 will be available for three years from the release date of 15 July, 2019. See the following End of Support and End of Engineering Schedule for more information:
https://support.pulsesecure.net/product-service-policies/eol/software/vadc-virtual-traffic-manager/

Major Features in 19.2

Timeouts on cache-based session persistence types

- **VTM-41501** It is now possible to set an expiry timeout on the Universal, J2EE and Source IP address-based session persistence types, with a separate global configuration key per type.

Load balancing based upon PCS/PPS License headroom (via service discovery plugin)

- **VTM-41411** Added a new Service Discovery Plugin for Pulse Connect Secure or Pulse Policy Secure products. This plugin, when configured with the hostnames of servers which are running PCS/PPS, will check the number of licensed sessions used and balance new sessions to servers which are least used.

Support for weights in service discovery plugins

- **VTM-41525** Added a new JSON field in the API for service discovery plugins to provide weights for each node in a pool which they discover. See the 'Custom User Plug-ins' section under 'Service Discovery' in the user guide for more details.

Pulse Secure Virtual Web Application Firewall Features

- The traffic manager will install version 4.9-43361 of Pulse Secure Virtual Web Application Firewall.

Other Changes in 19.2

Configuration

- **VTM-41447** Fixed a value encoding issue in the "Backup my configuration" Wizard.

Authentication

- **VTM-41451** Updated the OpenLDAP library used by the traffic manager to version 2.4.47, addressing CVE-2015-6908.

Administration Server

- **VTM-41675** The version of the expat XML parser library used in the Administration Server has been increased to 2.2.7, addressing CVE-2018-20843.
- **VTM-41577** Fixed a value encoding issue on the Historical Activity page in the Admin UI.
- **VTM-12631**, **VTM-41647**, **VTM-35880**, **SR16452** The Administration Server no longer returns a "Server" header in its HTTP responses.

REST API

- **VTM-40224** The REST API has increased its major version to 7.0. This is a backwards incompatible change, and whilst 5.x and 6.x continue to be supported, they are deprecated and you are strongly encouraged to update your scripts to the latest version of the API.

  See the REST API Guide for a comprehensive set of changes and help with updating.

  Following the earlier deprecation announcement API version 4.0 has been removed.

ZCLI

- **VTM-41460** Fixed an issue where names containing the ampersand (&) character could result in invalid responses to several SOAP API requests. This would also cause zcli commands accessing those APIs to fail.

Connection Processing

- **VTM-41249** A new virtual server config key, sip_udp_associate_by_source, has been added that specifies whether it is required that all datagrams sent by the client in a SIP UDP transaction must be sent from the same IP address and port. The setting is enabled by default. If disabled, the address from which a datagram has been sent is not taken into account when identifying the transaction to which a datagram belongs. Note that the client address to which response datagrams are sent will remain unchanged, even if datagrams are received from an address which is different to that from which the first datagram in a transaction was received.

Pools

- **VTM-41643** Fixed an issue where a sequence of requests would sometimes be sent to the same node if a pool was configured using the weighted round robin algorithm and the weights were high.

Fault Tolerance

- **VTM-41613** Fixed a value encoding issue in the "Join a cluster" Wizard.
- **VTM-40281** The error message has been changed to clarify that the inability to show the hosting cluster member could be caused by a communications failure, rather than that the TIP group actually not being hosted on any machine.

Global Load Balancing

- **VTM-41662** The GeoIP data included in the traffic manager has been updated to version 20190625.

- **VTM-41530** Fixed an issue in GLB clustered setups where the recovery of a service would not cause its Service IP address to be returned to clients for which it was the closest. The clients would instead keep getting the IP address of the service that was the closest working before the optimal one recovered.
- **VTM-40267** Fixed an issue where the round robin algorithm of the GLB service is not truly round robin if the domain to be balanced is specified with wildcards in it and multiple DNS records are matched by it in responses from the DNS backend.

Service Discovery

- **VTM-41645** Fixed an issue where pool health monitors when used in combination with a service discovery plugin to dynamically generate a pool configuration would not always reliably detect if a node in a pool had failed, if the frequency the service discovery plugin was run was more often that the monitor checked node health.

Services Director Communications

- **VTM-41446** Fixed an issue where a traffic manager would report "SD Communication Channel" error messages following an upgrade to version 19.1 if it was being licensed by a Service Director with version earlier than 19.1. The 'remote_licensing!comm_channel_enabled' configuration introduced in vTM 19.1 will now be set to 'No' when upgrading from a traffic manager version earlier than 19.1.

SSL/TLS and Cryptography

- **VTM-41344** Fixed an issue where malformed date and time values presented in SSL/TLS certificates, both by clients and servers, could be accepted by the traffic manager.
- **VTM-41321** Fixed a specification compliance issue in TLS handshake message validation.
- **VTM-41305** If SSL 3.0 is enabled for outgoing connections, it will always be included in the 'supported_versions' ClientHello extension, whereas previously it was included only if SNI was not in use.
- **VTM-39567** Fixed an issue where the Traffic Manager would not take into account the contents of the 'supported_versions' TLS extension when receiving connections, unless TLS 1.3 was enabled for the Virtual Server.

Container-based Deployment

- **VTM-41346** Added the package ca-certificates to the vTM docker image.
- **VTM-41345** Added the editors "vim" and "nano" to the vTM docker container image.
- **VTM-41250** The vTM Docker container now includes the files /etc/protocols and /etc/services.
- **VTM-39762** Updated Docker base image to Ubuntu 18.04.

Virtual Traffic Manager Appliance

Appliance OS

- **VTM-41687** Updated the appliance kernel to version 4.15.0-54.58, and updated packages installed on the appliance. These updates include changes addressing:
  CVE-2017-14245 CVE-2017-14246 CVE-2017-14634 CVE-2017-17456 CVE-2017-17457
  CVE-2018-5743 CVE-2018-10844 CVE-2018-10845 CVE-2018-10846 CVE-2018-12126
  CVE-2018-12127 CVE-2018-12130 CVE-2018-13139 CVE-2018-16062 CVE-2018-16402
  CVE-2018-16403 CVE-2018-16884 CVE-2018-18310 CVE-2018-18520 CVE-2018-18521
  CVE-2018-19432 CVE-2018-19661 CVE-2018-19662 CVE-2018-19758 CVE-2018-20060
  CVE-2018-20346 CVE-2018-20505 CVE-2018-20506 CVE-2018-20815 CVE-2018-20843
  CVE-2019-2602 CVE-2019-2684 CVE-2019-2697 CVE-2019-2698 CVE-2019-3829
  CVE-2019-3832 CVE-2019-3874 CVE-2019-3882 CVE-2019-5436 CVE-2019-6470
  CVE-2019-6471 CVE-2019-7149 CVE-2019-7150 CVE-2019-7317 CVE-2019-7665
  CVE-2019-8457 CVE-2019-9500 CVE-2019-9503 CVE-2019-9824 CVE-2019-9893
  CVE-2019-9936 CVE-2019-9937 CVE-2019-10906 CVE-2019-11091 CVE-2019-11191
  CVE-2019-11236 CVE-2019-11324 CVE-2019-11477 CVE-2019-11478 CVE-2019-11479
  CVE-2019-12450 CVE-2019-12735 CVE-2019-12749 CVE-2019-12900

  This kernel update includes support for a new sysctl net.ipv4.tcp_min_snd_mss to control the minimal MSS used by the TCP stack. This can be set via the System > Sysctl page in the Admin UI.

Cloud Platforms

- **VTM-41698** Fixed an issue where after installation the traffic manager log would contain SERIOUS errors with messages saying 'Error: argument "vtm1" is wrong: invalid table ID'.

Known Issues in 19.2

Software in Ubuntu 16.04 on GCE

- **VTM-41385** 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.

KVM Network Interface Card renaming

- **VTM-34654** 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 'Networking' page and re-adding it to the correct card.

Obsolete counters are missing from old REST API versions

- **VTM-38881** 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.

The format of encrypted bootloader passwords has changed in version 18.2

- **VTM-38948** 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 Global Settings page of the Admin UI.

Pre-18.2 Admin UI rollback tools will not offer roll-forward to 18.2 or later

- **VTM-38962** After rolling back from 19.2 to a vTM version earlier than 18.2 the rollback version selector on the 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.

Contacting Support

Visit the Pulse Secure Web site to download software updates and documentation, browse our library of Knowledge Center articles and manage your account.

To request support, go to https://support.pulsesecure.net