Pulse Secure Virtual Traffic Manager: Release Notes

Supporting Pulse Secure Virtual Traffic Manager 19.3

Product Release	**19.3**
Published	**15 October, 2019**
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

The Pulse Secure Virtual Traffic Manager 19.3 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-41736	Session persistence using RADIUS calling-station-id	Added explicit support for session persistence based on RADIUS calling-station-id via universal session persistence.
VTM-41706	License-based load balancing of PCS/PPS	Added support for adjusting the node weights used for load balancing PCS/PPS backends based upon the number of available unused license seats. Support for this is via the BuiltIn-PCS_PPS service discovery plugin, and requires PCS/PPS version 9.1R3.
Pulse Secure Virtual Web Application Firewall Features		
The traffic manager will install version 4.9-43361 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, 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)

Resource Requirements

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

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-42261	Fixed an issue where warnings appeared in the admin error log about uninitialized values during the Initial Config Wizard.
Administration Server	
VTM-42284	Fixes for CVE-2018-6913 and CVE-2018-18313 were applied to the version of Perl included in the product.
VTM-42283	The version of the expat XML parser library used in the Administration Server has been increased to 2.2.8, addressing CVE-2019-15903.

Report Number	Description
VTM-41769	Fixed an issue where the Traffic Manager's SSL-related "admin!" configuration keys were not propagated to the Administration Server unless set from Administration Server's UI. This caused a failure to access the GUI after upgrading to 19.1 or later, if a non-default cipher list had been configured for the Administration Server. The settings are now propagated when the Administration Server starts or restarts.
REST API	
VTM-41709	The REST API has increased its minor version to 7.1. This is a backwards compatible change with 7.0. Version 7.0 was a backwards incompatible change with versions 5.x and 6.x. 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.
TrafficScript	
VTM-41764	The libxslt library incorporated in the traffic manager has been updated to version 1.1.33 and had fixes for CVE-2019-13117 and CVE-2019-13118 applied.
Connection Processing	
VTM-42306	Limited the number of HTTP/2 frames queued per connection to 10,000 when the TCP buffers for that connection are full. This is significantly more than is expected that an RFC 7540 protocol-following HTTP/2 client would generate. This mitigates against excessive memory increases caused by superfluous HTTP/2 frame floods, and protects against the following denial-of-service attacks: CVE-2019-9511, CVE-2019-9512, CVE-2019-9514 and CVE-2019-9515.
VTM-42289	The special-case treatment of 503 responses from HTTP back-end nodes that applied to idempotent requests made with passive monitoring and no session persistence has been removed. Such responses will now behave in the same way as for other 5xx responses.
VTM-42147	A new TrafficScript function has been added, 'radius.getCallingStationId()', which extracts and returns the 'Calling-Station-Id' attribute from a RADIUS Access-Request message. In particular, when used in conjunction with a universal session persistence class, this allows session persistence based upon RADIUS 'Calling-Station-Id'.
Health Monitoring	
VTM-42285	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 which had failed was now available, if the frequency that the service discovery plugin was run was the same as the monitor used for checking node health, and they both ran at the same time.
Global Load Balancing	
VTM-41830	Updated GeoIP database to 2019-09-17.
Licensing	

Report Number	Description
VTM-40304	Fixed an issue where an error condition for a FLA license key would continue to be reported if a child zeus.zxtm process exited and was restarted even after the error condition had been cleared.

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-42334	Updated the appliance kernel to 4.15.0-64.73, and updated packages installed on the appliance. These updates include changes addressing: CVE-2016-3977 CVE-2018-5383 CVE-2018-11490 CVE-2018-13053 CVE-2018-13093 CVE-2018-13096 CVE-2018-13097 CVE-2018-13098 CVE-2018-13099 CVE-2018-13100 CVE-2018-14609 CVE-2018-14610 CVE-2018-14611 CVE-2018-14612 CVE-2018-14613 CVE-2018-14614 CVE-2018-14615 CVE-2018-14616 CVE-2018-14617 CVE-2018-16862 CVE-2018-19985 CVE-2018-20169 CVE-2018-20511 CVE-2018-20784 CVE-2018-20852 CVE-2018-20856 CVE-2019-0136 CVE-2019-1125 CVE-2019-2024 CVE-2019-2101 CVE-2019-2745 CVE-2019-2762 CVE-2019-2769 CVE-2019-2786 CVE-2019-2816 CVE-2019-2842 CVE-2019-3701 CVE-2019-3819 CVE-2019-3846 CVE-2019-3900 CVE-2019-5010 CVE-2019-5481 CVE-2019-5482 CVE-2019-7317 CVE-2019-8675 CVE-2019-8696 CVE-2019-9506 CVE-2019-9636 CVE-2019-9740 CVE-2019-9947 CVE-2019-9948 CVE-2019-10126 CVE-2019-10160 CVE-2019-10207 CVE-2019-10638 CVE-2019-10639 CVE-2019-11085 CVE-2019-11487 CVE-2019-11599 CVE-2019-11719 CVE-2019-11729 CVE-2019-11810 CVE-2019-11815 CVE-2019-11833 CVE-2019-11884 CVE-2019-11922 CVE-2019-12614 CVE-2019-12818 CVE-2019-12819 CVE-2019-12984 CVE-2019-13012 CVE-2019-13057 CVE-2019-13233 CVE-2019-13272 CVE-2019-13565 CVE-2019-13631 CVE-2019-13648 CVE-2019-14283 CVE-2019-14284 CVE-2019-14763 CVE-2019-14835 CVE-2019-15030 CVE-2019-15031 CVE-2019-15090 CVE-2019-15133 CVE-2019-15211 CVE-2019-15212 CVE-2019-15214 CVE-2019-15215 CVE-2019-15216 CVE-2019-15218 CVE-2019-15220 CVE-2019-15221 CVE-2019-15292 CVE-2019-15718 CVE-2019-15903 CVE-2019-1010305
VTM-41786	Wizards displayed by the Administration UI now apply their validation of user-supplied data more consistently
VTM-41745	Fixed an issue in the timezone field of UI wizards so that invalid timezones are no longer accepted
VTM-37057, VTM-38971	Fixed an issue where importing a configuration backup made on a pre-17.2 traffic manager would not have restored traffic manager-specific settings. When such a configuration backup import is carried out the interface names will not be changed, and configuration may need to be adjusted manually.
Cloud Platforms	

Report Number	Description
VTM-42167	Traffic managers running on Amazon EC2 will no longer accept the Access Key and Secret Access Key method of authentication with AWS services. In order to use Traffic IP Groups or Pool Node Autoscaling an IAM Role must be assigned to the EC2 instance. This change applies to vTM AMIs deployed through the AWS Marketplace and vTM software installed on Linux EC2 instances. Refer to the vTM Cloud Getting Started Guide for the policies an IAM Role requires.
VTM-42109	Fixed an issue that caused traffic managers to fail to authenticate with the Azure Key Vault service, following a change to its behavior in August 2019.

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 '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 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 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 19.3 will be available for one year from the release date of 15 October, 2019. 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.