ivanti

Pulse Secure Virtual Traffic Manager: Release Notes

21.4

Contents

New Features

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

Report Number	Features	Description
Pulse Secure Virtual Web Application Firewall Features		
The Traffic Manager will install version 4.10-6 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 from version 4.9-x to version 4.10-x, users must ensure that any Python scripts they have included in script libraries are compatible with Python 3. Resource Requirements now includes a recommendation that virtual appliances running vWAF should have a RAM allocation of at least 4GB. Version 4.10-x 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 - 5.13, 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.ivanti.com/support/product-documentation

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 7.x; Ubuntu 18.04, 20.04)

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).

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 Ivanti customer portal.

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 was 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.

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

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-45019	Fixed an issue which could lead to rejection of self-signed admin SSL certificate by prospective clients because of absence of subject alternative name extension in the certificate.
Administrative Server	
VTM-45124	Fixed an issue where the 'adminport' setting could not be changed using the Admin UI.
VTM-41382	Added X-Content-Type-Options: nosniff header in all responses for the admin server UI to enable the additional security protection measures in user agent where they are supported.
SOAP API	
VTM-45015	The version of the expat XML parser library used in the Administration Server has been increased to 2.4.1.
Connection Processing	
VTM-45092	Fixed an issue where the 'max_connections_pernode' setting could cause some requests to wait for longer than needed to restrict the number of connections to nodes.
Pools	
VTM-45234	Fixed an issue when setting max_connections_per_node, could cause a child process crash when a request is made to a pool with no working nodes.
VTM-45113	Fixed an issue where the connection/transaction counters for a draining pool node could fail to decrease when a connection/transaction to a pool node is closed/completed. If the node was then reactivated the discrepancy in the counters could cause the traffic manager to cap the number of connections/transactions to the pool node to be much less than the configuration max_connections_pernode or max_transactions_per_node.

Report Number	Description
Fault Tolerance	
VTM-19838, SR-25020	Fixed an issue where vTM doesn't honor the flipper!use_bindip setting for binding the flipper port to a single IP Address following a software restart.
Service Protection	
VTM-45147	Fixed an issue that a client can establish more than max_1_connections connections to the vTM once some HTTP/1.x connections from the same client have been rejected due to being capped by max_1_connection.
Global Load Balancing	
VTM-45011	Fixed an issue where a request rule that used the TrafficScript function request.setRemoteIP() on a virtual server configured with GLB could cause the zeus.zxtm child process to restart.
VTM-44973	Fixed an issue where a zeus.zxtm child process could restart if the GLB feature was used without a GeoIP database loaded. Where a GLB algorithm with geographic effect is used and no location can be discovered for a DNS query, for example if the source IP address is in a private range, the nearest datacentre calculation will no longer select the datacentre nearest to 0"N 0"E. In this situation DNS answers for any of the datacentres can be returned at random according to their weighting in response to a DNS request made to a GLB virtual server. The locations.cfg configuration file can be used to give geographic locations to private IP ranges.
DNS Server	
VTM-44992	Fixed an issue where a virtual server using the built-in DNS server could fail to find the most specific case-insensitive match, if a wildcard was present in zone file.
VTM-37162	Fixed an issue which prevented the Traffic Manager's built-in DNS server from using DNSSEC NSEC/NSEC3 with resource record types greater than 255.
VTM-36262	The Traffic Manager's built-in DNS server now supports CAA records.
SSL/TLS and Cryptography	

Report Number	Description
VTM-45042	Fixed an issue where a virtual server receiving an invalid TLS client hello could emit log messages referring to an 'IP Prefix' even when the 'ssl_trust_magic' configuration setting was disabled.
VTM-41781	Fixed an issue where a virtual server with 'log!ssl_failures' enabled displayed wrong timings in the event log when a connection timed out during the TLS handshake - the "Client idle since" field now contains the time at which the connection was closed, having failed to complete the TLS handshake.
Logging	
VTM-44118	Fixed an issue that could lead to increase in log buffer size with no limit in case of any failed communication with eventd process.

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-45172	Updated the appliance kernel to version 4.15.0-166.174, and updated packages installed on the appliance. These updates include changes addressing:

Report Number	Description
	CVE-2019-19449 CVE-2020-3702 CVE-2020-16592 CVE-2020-21913 CVE-2020-36322 CVE-2020-36385 CVE-2021-0920 CVE-2021-2341 CVE-2021-2369 CVE-2021-2388 CVE-2021-3487 CVE-2021-3655 CVE-2021-3679 CVE-2021-3732 CVE-2021-3733 CVE-2021-3737 CVE-2021-3743 CVE-2021-3744 CVE-2021-3753 CVE-2021-3759 CVE-2021-3760 CVE-2021-3764 CVE-2021-3778 CVE-2021-3796 CVE-2021-3800 CVE-2021-3903 CVE-2021-3927 CVE-2021-3928 CVE-2021-4002 CVE-2021-20317 CVE-2021-20321 CVE-2021-22543 CVE-2021-25219 CVE-2021-28831 CVE-2021-35550 CVE-2021-35556 CVE-2021-35559 CVE-2021-35561 CVE-2021-35564 CVE-2021-35565 CVE-2021-35567 CVE-2021-35578 CVE-2021-35586 CVE-2021-35588 CVE-2021-35603 CVE-2021-37159 CVE-2021-37576 CVE-2021-38198 CVE-2021-38199 CVE-2021-38204 CVE-2021-38205 CVE-2021-40490 CVE-2021-41864 CVE-2021-42008 CVE-2021-42252 CVE-2021-42374 CVE-2021-42378 CVE-2021-42379 CVE-2021-42380 CVE-2021-42381 CVE-2021-43527
Cloud Platforms	
VTM-45058	Fixed an issue that appliance upgrade could fail if the appliance's grub2 configuration did not match the disk device that the system booted from.
VTM-43524	Fixed an issue where a software installation of the Traffic Manageron the EC2 platform could log failures regarding 'awstool', if the OS-supplied netcat program did not support Unix domain sockets.

Pulse Secure Virtual Web Application Firewall

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

Report Number	Description
WAF-1111	Fixed an issue preventing the application log details page from loading.
WAF-1112	Fixed an issue preventing the download of application logs.
WAF-1113	Improved logging when parsing body data.

Report Number	Description
WAF-1106, VTM-45107	Reverted back to using cx_Freeze now that it supports python 3.9 for improved memory and disk space usage.

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.

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

Ivanti documentation is available at https://www.ivanti.com/support/product-documentation.

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 Ivanti website.

Technical Support

Full support for version 21.4 will be available for one year from the release date of 18 January, 2022. 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 Ivanti 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	18 January, 2022	21.4 Release Notes created.