Pulse Secure Virtual Traffic Manager: Release Notes

Supporting Pulse Secure Virtual Traffic Manager 20.1r1

Product Release	20.1r1
Published	September 15, 2020
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

This chapter contains the following topics:

Overview

Pulse Secure Virtual Traffic Manager 20.1r1 is a maintenance release of the Pulse Secure Virtual Traffic Manager product family, containing a number of performance and functionality enhancements and bug fixes. Customers are recommended to upgrade to this version to take advantage of the changes.

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 20.1r1 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
Administration Server	
VTM-42831	Fixed an issue where the **Diagnose** and **Activity** tabs in the Traffic Manager Admin UI took excessive time to open when the Traffic Manager has many (for example, more than 100) service discovery pools.
VTM-43084	Fixed an issue where the permission check needed for the addition of a rule to a virtual server or GLB service could be bypassed.
TrafficScript	
VTM-43180	The Perl Compatible Regular Expression library (PCRE) has been updated to version 10.35, addressing CVE-2019-20454.
Connection Processing	
VTM-43204	Fixed an issue where HTTP/2 requests with a single Cookie header made to a virtual server with `http2!merge_cookie_headers` enabled could result in the omission of another header field and the addition of its value to the Cookie header when a request was sent to the pool node.
VTM-43004	Fixed an issue where the Traffic Manager could fail a lookup of a DNS name if exactly one of IPv4 or IPv6 lookup succeeds. When a negative lookup for one was cached and not expired, but a cached positive result was expired, the negative result was returned.
VTM-43038, VTM-25308, SR34763	Improved HTTP/1.1 header parsing to ensure RFC 7230 section 3.2.6 is correctly followed.

Report Number	Description
VTM-43002	Fixed an issue which caused DNS responses in the dataplane processes to be cached only for the `dns!min_ttl` value, even when the TTL of the response is longer. This affected DNS resolution in TrafficScript rules, as well as OCSP URLs.
Global Load Balancing	
VTM-42979	Fixed an issue where using the `glb.service.ignoreLocation()` TrafficScript function in a GLB service rule would terminate rule processing, preventing any following TrafficScript statements from being executed.
Service Protection	
VTM-43313	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.
VTM-43028	Updated the behavior of the Traffic Manager when receiving an HTTP/1(.1) request with invalid whitespace between an HTTP header name and the colon, to reject the request. This behavioral change is mandated by RFC 7230.
VTM-43008	Fixed an issue where a malformed chunked HTTP request could cause a further request to be smuggled.
SSL/TLS and Cryptography	
VTM-20811, VTM-38785, VTM-38781, VTM-25080, SR26757, SR34433	When acting as a TLS client, for example when connecting to a node in a pool that has `ssl_encrypt` enabled, connections now succeed in the presence of re-ordered or extraneous certificates in the server's certificate message, as described in RFC 8446.

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-38742	Support for `vmguestlib` has been added to the appliance image.

Report Number	Description
VTM-43237	Updated the appliance kernel to version 4.15.0-112.113, and updated packages installed on the appliance. These updates include changes addressing: CVE-2016-9840 CVE-2016-9841 CVE-2016-9842 CVE-2016-9843 CVE-2017-16808 CVE-2018-8945 CVE-2018-9138 CVE-2018-10103 CVE-2018-10105 CVE-2018-10372 CVE-2018-10373 CVE-2018-10534 CVE-2018-10535 CVE-2018-11236 CVE-2018-11237 CVE-2018-12641 CVE-2018-12697 CVE-2018-12698 CVE-2018-12699 CVE-2018-12700 CVE-2018-12934 CVE-2018-13033 CVE-2018-14461 CVE-2018-14462 CVE-2018-14463 CVE-2018-14464 CVE-2018-14465 CVE-2018-14466 CVE-2018-14467 CVE-2018-14468 CVE-2018-14469 CVE-2018-14470 CVE-2018-14879 CVE-2018-14880 CVE-2018-14881 CVE-2018-14882 CVE-2018-16227 CVE-2018-16228 CVE-2018-16229 CVE-2018-16230 CVE-2018-16300 CVE-2018-16451 CVE-2018-16452 CVE-2018-17358 CVE-2018-17359 CVE-2018-17360 CVE-2018-17794 CVE-2018-17985 CVE-2018-18309 CVE-2018-18483 CVE-2018-18484 CVE-2018-18605 CVE-2018-18606 CVE-2018-18607 CVE-2018-18700 CVE-2018-18701 CVE-2018-19519 CVE-2018-19591 CVE-2018-19931 CVE-2018-19932 CVE-2018-20002 CVE-2018-20623 CVE-2018-20651 CVE-2018-20671 CVE-2018-20786 CVE-2018-1000876 CVE-2019-1547 CVE-2019-1549 CVE-2019-1551 CVE-2019-1563 CVE-2019-2182 CVE-2019-2228 CVE-2019-3843 CVE-2019-3844 CVE-2019-5068 CVE-2019-5108 CVE-2019-9070 CVE-2019-9071 CVE-2019-9073 CVE-2019-9074 CVE-2019-9075 CVE-2019-9077 CVE-2019-9169 CVE-2019-9674 CVE-2019-10220 CVE-2019-12380 CVE-2019-12972 CVE-2019-13734 CVE-2019-13750 CVE-2019-13751 CVE-2019-13752 CVE-2019-13753 CVE-2019-14250 CVE-2019-14444 CVE-2019-14615 CVE-2019-15099 CVE-2019-15166 CVE-2019-15167 CVE-2019-15217 CVE-2019-15291 CVE-2019-16089 CVE-2019-16229 CVE-2019-16232 CVE-2019-16234 CVE-2019-17023 CVE-2019-17450 CVE-2019-17451 CVE-2019-17514 CVE-2019-18348 CVE-2019-18634 CVE-2019-18683 CVE-2019-18786 CVE-2019-18809 CVE-2019-18885 CVE-2019-19036 CVE-2019-19037 CVE-2019-19039 CVE-2019-19046 CVE-2019-19051 CVE-2019-19056 CVE-2019-19057 CVE-2019-19058 CVE-2019-19062 CVE-2019-19063 CVE-2019-19066 CVE-2019-19068 CVE-2019-19071 CVE-2019-19078 CVE-2019-19082 CVE-2019-19126 CVE-2019-19227 CVE-2019-19332 CVE-2019-19377 CVE-2019-19447 CVE-2019-19462 CVE-2019-19767 CVE-2019-19768 CVE-2019-19813 CVE-2019-19816 CVE-2019-19906 CVE-2019-19923 CVE-2019-19925 CVE-2019-19926 CVE-2019-19956 CVE-2019-19959 CVE-2019-19965 CVE-2019-20079 CVE-2019-20096 CVE-2019-20218 CVE-2019-20382 CVE-2019-20386 CVE-2019-20636 CVE-2019-20795 CVE-2019-20806 CVE-2019-20812 CVE-2019-20907 CVE-2019-20908 CVE-2019-1010220 CVE-2020-0009 CVE-2020-0067 CVE-2020-0255 CVE-2020-1711 CVE-2020-1712 CVE-2020-1749 CVE-2020-1751 CVE-2020-1752 CVE-2020-1983 CVE-2020-2583 CVE-2020-2590 CVE-2020-2593 CVE-2020-2601 CVE-2020-2604 CVE-2020-2654 CVE-2020-2659 CVE-2020-2732 CVE-2020-2754 CVE-2020-2755 CVE-2020-2756 CVE-2020-2757 CVE-2020-2773 CVE-2020-2781 CVE-2020-2800 CVE-2020-2803 CVE-2020-2805 CVE-2020-2830 CVE-2020-3810 CVE-2020-3898 CVE-2020-5208 CVE-2020-6829 CVE-2020-7039 CVE-2020-7053 CVE-2020-7595 CVE-2020-8177 CVE-2020-8231 CVE-2020-8428 CVE-2020-8492 CVE-2020-8608 CVE-2020-8616 CVE-2020-8617 CVE-2020-8622 CVE-2020-8623 CVE-2020-8624 CVE-2020-8647 CVE-2020-8648 CVE-2020-8649 CVE-2020-8832 CVE-2020-8834 CVE-2020-8903 CVE-2020-8907 CVE-2020-8933 CVE-2020-8992 CVE-2020-9327 CVE-2020-9383 CVE-2020-10029 CVE-2020-10531 CVE-2020-10690 CVE-2020-10711 CVE-2020-10713 CVE-2020-10751 CVE-2020-10756 CVE-2020-10757 CVE-2020-10942 CVE-2020-11494 CVE-2020-11565 CVE-2020-11608 CVE-2020-11609 CVE-2020-11668 CVE-2020-11669 CVE-2020-11884 CVE-2020-11931 CVE-2020-11935 CVE-2020-12049 CVE-2020-12114 CVE-2020-12243 CVE-2020-12399 CVE-2020-12400 CVE-2020-12401 CVE-2020-12402 CVE-2020-12464 CVE-2020-12652 CVE-2020-12653 CVE-2020-12654 CVE-2020-12657 CVE-2020-12762 CVE-2020-12769 CVE-2020-12770 CVE-2020-12826 CVE-2020-12829 CVE-2020-13143 CVE-2020-13253 CVE-2020-13361 CVE-2020-13362 CVE-2020-13434 CVE-2020-13630 CVE-2020-13632 CVE-2020-13659 CVE-2020-13754 CVE-2020-13765 CVE-2020-13790 CVE-2020-14308 CVE-2020-14309 CVE-2020-14310 CVE-2020-14311 CVE-2020-14416 CVE-2020-14422

Report Number	Description
	`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-2020-15705 CVE-2020-15706 CVE-2020-15707 CVE-2020-15709 CVE-2020-15780 CVE-2020-15861 CVE-2020-15862 CVE-2020-15863 CVE-2020-16092`
Virtual Appliance	
VTM-43312	Fixed an issue where an IPv6 gateway address was incorrectly set when deploying a virtual appliance using VMWare Guest Customizations

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 Admin UI **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

20.1r1 can be installed directly using any supported installation mechanism. Traffic Manager software installations can be upgraded directly to 20.1r1 using any supported upgrade mechanism, except those running Traffic Manager version 17.2 which must be upgraded to some other version (for example 17.2r3 or 19.2) before upgrading.

Traffic manager instances (appliance or cloud) running release 18.2 or later can be upgraded directly to 20.1r1 using any supported upgrade mechanism.

Traffic manager instances (appliance or cloud) running versions prior to 18.2 must first be upgraded to a non-r-release, such as 18.2 or 19.2.

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 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 July 15, 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.