Pulse Secure®

Pulse Secure Virtual Traffic Manager: Release Notes

Supporting Pulse Secure Virtual Traffic Manager 19.2r1

Product Release	19.2r1
Published	September 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 19.2r1 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.

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.

Upgrading to 19.2r1

19.2r1 can be installed directly using any supported installation mechanism. Traffic manager software installations can be upgraded directly to 19.2r1 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 19.2r1 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.

Changes in 19.2r1

Administration Server

- **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.
- **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.

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.

Global Load Balancing

- **VTM-41943** Updated GeoIP database to 2019-08-06.

Licensing

- **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.

Virtual Traffic Manager Appliance

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-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.
- **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

Cloud Platforms

- **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 in 19.2r1

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