PULSE SECURE PRODUCT RELEASE NOTES

PRODUCT: PULSE SECURE VIRTUAL TRAFFIC MANAGER

RELEASE DATE: 1ST AUGUST, 2018

VERSION: 18.2

CONTENTS

1) ABOUT THIS RELEASE

Pulse Secure Virtual Traffic Manager 18.2 is a feature release of the Pulse Secure Virtual Traffic Manager product family, containing a number of performance and functionality enhancements and bug fixes.

2) 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)
- SmartOS x86_64: Kernel 20141030T164802Z and newer

Virtual Traffic Manager containers

- Docker: 1.13.0 or later recommended

Virtual Traffic Manager virtual appliances

- VMware vSphere 5.5, 6.0, 6.5
- XenServer 7.0, 7.1, 7.4
- Microsoft Hyper-V Server 2016
- Microsoft Hyper-V under Windows Server 2012, 2012 R2, and 2016
- QEMU/KVM (RHEL/CentOS 6.x, 7.x; Ubuntu 14.04, 16.04)

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

3) RESOURCE REQUIREMENTS

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

4) MAJOR FEATURES IN 18.2

Long Term Support

- Pulse Secure Virtual Traffic Manager 18.2 is designated a Long Term Support (LTS) release. This means that full software support for Pulse Secure vTM 18.2 will be available for three years.

Configuration Wizard for load-balancing PCS servers

- **VTM-38288** Easily set up load-balancing for Pulse Connect Secure (PCS) with the new Pulse Connect Secure Configuration Wizard. The wizard walks through the process of configuring the services necessary to load-balance VPN connections to Pulse Connect Secure servers.

PROXY Protocol version 2 support

- **VTM-38289** Support for virtual servers to receive connections that are prefixed with a PROXY Protocol header has now been extended to include both version 1 and version 2 of the protocol. For a connection with a PROXY Protocol version 2 header, any information included in TLV (Type-Length-Value) data items can be accessed from TrafficScript. As with PROXY Protocol version 1, the client connection protocol type and client and server addresses are also accessible from TrafficScript for connections prefixed with a version 2 header.

Appliance OS upgrade to Ubuntu 18.04

- **VTM-38272** The underlying operating system on appliances has been updated to Ubuntu 18.04 in this release, and corresponding updates have been applied to installed packages. The bootloader has been updated to GRUB 2 and the SysV init scripts have been replaced with systemd equivalents.

Data Plane Acceleration Mode Not Available in this Release

- Data Plane Acceleration mode (DPA mode) is not available in this release. If you are using DPA mode, and require more information, please contact technical support.

REST API Major Version Update

- **VTM-38404**, **VTM-35555** The REST API has increased its major version to 6.0. This is a backwards incompatible change, and whilst 5.X will continue to be supported you are strongly encouraged to update your scripts to the latest version of the API.

  Version 5.2 is deprecated though it remains supported.

  Following the earlier deprecation announcement REST API Version 4.0 will be removed in a subsequent release.

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

5) PULSE SECURE VIRTUAL WEB APPLICATION FIREWALL FEATURES

- The traffic manager will install version 4.9-43269 of the Pulse Secure Virtual Web Application Firewall.

6) OTHER CHANGES IN 18.2

Authentication

- **VTM-36477** The MIT Kerberos libraries used by the traffic manager have been updated to version 1.14.6. This includes a fix for the security issue reported in CVE-2014-9423.

Administration Server

- **VTM-38803** Fixed an issue where files in the Admin Server docroot were unnecessarily visible via directory listings to users who had logged into the Admin UI.
- **VTM-38801**, **VTM-29994** Fixed an issue where a 500 Internal Server error response would be returned if an unknown wizard section was visited; now a 404 response will be produced.
- **VTM-38800** All Admin UI cookies are now marked as "secure" as they are only used by resources served over HTTPS connections.
- **VTM-36342** Added Content-Security-Policy HTTP headers in responses from the traffic manager's Admin UI. This improves security for administrators using user agents that support this standard. Note that the vWAF UI pages do not currently provide Content-Security-Policy headers.
- **VTM-27677** Fixed an issue where location names containing HTML tags were rendered incorrectly on the Backup Comparisons page of the Admin UI.
- **VTM-23453**, **VTM-19065 SR30839**, **SR23813** Auto-completion of the password field on the login page of the Admin UI has been disabled to improve security.

REST API

- **VTM-38428** Fixed an issue where the REST API returned invalid JSON, omitting the leading quote for section names in the metadata response.
- **VTM-38405** Added missing config key 'autoscaling!extraargs' to the REST API's pool config as 'auto_scaling/extraargs'.
- **VTM-38055** Fixed an issue where if the REST API encountered a connection error to another proxied REST API it would not report or log the address and port.

- **VTM-38046** A property, 'html_description', has been added to the property metadata. This is to indicate that the property description should be treated as if it contained HTML.
- **VTM-23428**, **VTM-35819 SR30802** Obsolete 32bit Hi and Lo split SNMP counters for 64bit values are no-longer available in the 6.0 REST status API.

Zeusbench

- **VTM-35444** Fixed an issue where running Zeusbench when specifying both -c 0 and --http2 caused an assertion failure.
- **VTM-35441** Updated the Zeusbench performance benchmarking tool to support TCP connection concurrency step-up with HTTP/2 requests.
- **VTM-35437**, **VTM-36151** Fixed an issue where running zeusbench with --http2 and -v incorrectly showed the number of HTTP/2 streams in the "Sockets" and "Connecting" columns. It now correctly shows the number of TCP connections.

Connection Processing

- **VTM-38859** Fixed an issue where a traffic manager child process could stop processing traffic after receiving an HTTP/2 SETTINGS frame, with the corresponding child process automatically being restarted after a short period to recover from the error state.
- **VTM-38729** Fixed an issue that could occur when an HTTP/2 stream is closed.
- **VTM-38699** Fixed an issue where IPv6 addresses from a PROXY Protocol version 1 header were not normalized before being returned by the connection.getProxyClientIP() and connection.getProxyServerIP() TrafficScript functions.

Analytics Export

- **VTM-38649** The transaction metadata export schema now contains a version in the value of the 'id' field. Events exported from the traffic manager now report the schema version, and the traffic manager software version. These fields are documented in the schema.

Pools

- **VTM-38796** Fixed an issue where the Admin UI would incorrectly state that non-autoscaled pools contained no nodes when Multi-Site Manager mode was enabled.
- **VTM-38666** Fixed an issue where, when using the Admin UI, a node could not be removed from a pool that shares a persistence class with another pool.

- **VTM-38429** Fixed an issue that prevented removing, disabling or draining nodes from a pool when using the Admin UI if the node was specified as a hostname that resolved to a single IP address. The issue also resulted in nodes that were marked as 'disabled' not being shown in the Admin UI and the Current Activity graph displaying information for nodes that were not selected.

Health Monitoring

- **VTM-38377** The built-in "DNS" monitor now supports monitoring of DNS nodes running on ports other than the default of 53.

Service Discovery

- **VTM-38476** Fixed an issue where multiple pools using the built-in Caching DNS Resolver Service Discovery plugin with the same hostname but using different IP versions or name servers could display the same nodes.

SSL/TLS and Cryptography

- **VTM-38298** Updated the Diffie-Hellman parameters used for key agreements in DHE TLS cipher suites as per best practice.

Internals

- **VTM-38764** Added new SNMP counters to monitor HTTP response codes returned by virtual servers. virtualserverHTTPServerxxxResponses counters log response codes for responses received from back-end servers, after undergoing any modifications applied by the traffic manager virtualserverHTTPGeneratedxxxResponses counters log response codes for responses generated by the traffic manager virtualserverHTTPCachexxxResponses counters log response codes returned by the traffic manager's content cache virtualserverHTTPxxxResponses counters count all of the above, representing all responses returned to clients The new SNMP counters can be monitored through the Current Activity page of the Admin UI and can be fetched through the REST API.
- **VTM-38388** Added new SNMP counters to monitor HTTP response codes returned by a pool: poolHTTP1xxResponses, poolHTTP2xxResponses, poolHTTP3xxResponses, poolHTTP4xxResponses, poolHTTP5xxResponses. In addition, a counter tracking the number of 503 responses that were automatically retried by the pool 'poolHTTP503Retries' has been added. The new SNMP counters can be monitored through the Current Activity page of the Admin UI and can be fetched through the REST API.
- **VTM-38351** Fixed an issue where the JSON parser used by the traffic manager in, for example, TrafficScript or the Service Discovery feature, could exhaust the stack while parsing a deeply nested JSON data structure leading to a crash. The traffic manager will now reject such JSON data structures with an error message.

7) PULSE SECURE VIRTUAL WEB APPLICATION FIREWALL CHANGES

- Fixed an issue where vTM banner_accept setting caused vWAF REST API to fail

8) VIRTUAL TRAFFIC MANAGER APPLIANCE

Appliance OS

- **VTM-39030** Updated the appliance kernel to version 4.15.0-29.31, and updated packages installed on the appliance. These updates include changes addressing:
  CVE-2009-5080 CVE-2011-5325 CVE-2012-0039 CVE-2012-1093 CVE-2012-2663
  CVE-2013-4235 CVE-2014-9913 CVE-2015-1336 CVE-2015-1350 CVE-2015-3239
  CVE-2015-5180 CVE-2015-5191 CVE-2015-8629 CVE-2015-8630 CVE-2015-8631
  CVE-2016-2147 CVE-2016-2148 CVE-2016-2226 CVE-2016-2775 CVE-2016-2779
  CVE-2016-2853 CVE-2016-3119 CVE-2016-3120 CVE-2016-3189 CVE-2016-4484
  CVE-2016-5011 CVE-2016-5319 CVE-2016-5863 CVE-2016-6153 CVE-2016-6170
  CVE-2016-7076 CVE-2016-7942 CVE-2016-7943 CVE-2016-7944 CVE-2016-7945
  CVE-2016-7946 CVE-2016-7947 CVE-2016-7948 CVE-2016-7949 CVE-2016-7950
  CVE-2016-7951 CVE-2016-7952 CVE-2016-8660 CVE-2016-9082 CVE-2016-9318
  CVE-2016-9840 CVE-2016-9841 CVE-2016-9842 CVE-2016-9843 CVE-2016-9844
  CVE-2016-10087 CVE-2016-10165 CVE-2016-10254 CVE-2016-10255
  CVE-2016-10708 CVE-2017-0537 CVE-2017-1000 CVE-2017-2518 CVE-2017-2519
  CVE-2017-2520 CVE-2017-2625 CVE-2017-5550 CVE-2017-5953 CVE-2017-5967
  CVE-2017-6004 CVE-2017-6349 CVE-2017-6350 CVE-2017-6594 CVE-2017-6892
  CVE-2017-6965 CVE-2017-6966 CVE-2017-6969 CVE-2017-7186 CVE-2017-7209
  CVE-2017-7210 CVE-2017-7223 CVE-2017-7224 CVE-2017-7225 CVE-2017-7226
  CVE-2017-7227 CVE-2017-7244 CVE-2017-7245 CVE-2017-7246 CVE-2017-7299
  CVE-2017-7300 CVE-2017-7301 CVE-2017-7302 CVE-2017-7475 CVE-2017-7607
  CVE-2017-7608 CVE-2017-7609 CVE-2017-7610 CVE-2017-7611 CVE-2017-7612
  CVE-2017-7613 CVE-2017-7614 CVE-2017-8283 CVE-2017-8797 CVE-2017-8804
  CVE-2017-9038 CVE-2017-9039 CVE-2017-9040 CVE-2017-9041 CVE-2017-9043
  CVE-2017-9044 CVE-2017-9059 CVE-2017-9525 CVE-2017-9742 CVE-2017-9744
  CVE-2017-9745 CVE-2017-9746 CVE-2017-9747 CVE-2017-9748 CVE-2017-9749
  CVE-2017-9750 CVE-2017-9751 CVE-2017-9752 CVE-2017-9753 CVE-2017-9754
  CVE-2017-9755 CVE-2017-9756 CVE-2017-9778 CVE-2017-9814 CVE-2017-9955
  CVE-2017-9986 CVE-2017-10684 CVE-2017-10685 CVE-2017-10989 CVE-2017-11109

CVE-2017-11112 CVE-2017-11113 CVE-2017-11368 CVE-2017-11462 CVE-2017-12132 CVE-2017-12133 CVE-2017-12424 CVE-2017-12448 CVE-2017-12449 CVE-2017-12450 CVE-2017-12451 CVE-2017-12452 CVE-2017-12453 CVE-2017-12454 CVE-2017-12455 CVE-2017-12456 CVE-2017-12457 CVE-2017-12458 CVE-2017-12459 CVE-2017-12562 CVE-2017-12799 CVE-2017-12967 CVE-2017-13165 CVE-2017-13168 CVE-2017-13305 CVE-2017-13685 CVE-2017-13695 CVE-2017-13728 CVE-2017-13729 CVE-2017-13730 CVE-2017-13731 CVE-2017-13732 CVE-2017-13733 CVE-2017-13734 CVE-2017-14130 CVE-2017-14159 CVE-2017-14160 CVE-2017-14245 CVE-2017-14246 CVE-2017-14333 CVE-2017-14634 CVE-2017-15128 CVE-2017-15873 CVE-2017-16538 CVE-2017-16544 CVE-2017-16644 CVE-2017-16647 CVE-2017-16942 CVE-2017-17053 CVE-2017-17975 CVE-2017-18174 CVE-2017-18193 CVE-2017-18216 CVE-2017-18222 CVE-2017-18232 CVE-2017-18241 CVE-2017-18248 CVE-2017-18249 CVE-2017-18255 CVE-2017-18257 CVE-2017-18261 CVE-2017-1000382 CVE-2018-0494 CVE-2018-0495 CVE-2018-0732 CVE-2018-0737 CVE-2018-1065 CVE-2018-1068 CVE-2018-1087 CVE-2018-1092 CVE-2018-1093 CVE-2018-1094 CVE-2018-1120 CVE-2018-1122 CVE-2018-1123 CVE-2018-1124 CVE-2018-1125 CVE-2018-1126 CVE-2018-1130 CVE-2018-1152 CVE-2018-2783 CVE-2018-2790 CVE-2018-2794 CVE-2018-2795 CVE-2018-2796 CVE-2018-2797 CVE-2018-2798 CVE-2018-2799 CVE-2018-2800 CVE-2018-2814 CVE-2018-2815 CVE-2018-3639 CVE-2018-3665 CVE-2018-4180 CVE-2018-4181 CVE-2018-5750 CVE-2018-5803 CVE-2018-5814 CVE-2018-5873 CVE-2018-6323 CVE-2018-6485 CVE-2018-6553 CVE-2018-6759 CVE-2018-7169 CVE-2018-7170 CVE-2018-7183 CVE-2018-7185 CVE-2018-7273 CVE-2018-7409 CVE-2018-7456 CVE-2018-7480 CVE-2018-7566 CVE-2018-7740 CVE-2018-7755 CVE-2018-7757 CVE-2018-7995 CVE-2018-7999 CVE-2018-8087 CVE-2018-8740 CVE-2018-8781 CVE-2018-8822 CVE-2018-8897 CVE-2018-8905 CVE-2018-9415 CVE-2018-9422 CVE-2018-10021 CVE-2018-10087 CVE-2018-10124 CVE-2018-10322 CVE-2018-10323 CVE-2018-10360 CVE-2018-10392 CVE-2018-10393 CVE-2018-10779 CVE-2018-10801 CVE-2018-10853 CVE-2018-10876 CVE-2018-10877 CVE-2018-10878 CVE-2018-10879 CVE-2018-10880 CVE-2018-10881 CVE-2018-10882 CVE-2018-10883 CVE-2018-10940 CVE-2018-10963 CVE-2018-11489 CVE-2018-11490 CVE-2018-12015 CVE-2018-12020 CVE-2018-12233 CVE-2018-12327 CVE-2018-13093 CVE-2018-13094 CVE-2018-13095 CVE-2018-13405 CVE-2018-13406 CVE-2018-1000004 CVE-2018-1000030 CVE-2018-1000199 CVE-2018-1000204 CVE-2018-1000301

- **VTM-38883** The appliance OS, or "Stingray OS", version number has been increased to 4.3
- **VTM-38861** Fixed an issue where virtual Traffic Manager Hardware Appliances printed "Unable to get the health status of the hardware" for non-hardware cluster peers on the Traffic Managers admin UI page.
- **VTM-38620** The 3rd party package "vmguestlib" which provided the vmguest-stats tool has been removed from VMware virtual appliances due to an incompatibility with Ubuntu 18.04.

- **VTM-38615** Fixed a problem where the compaction of some IPv6 addresses did not conform to RFC 5952. As a result, some IPv6 addresses will have a different textual representation in the Admin UI, the REST API, and in the return value of TrafficScript functions such as string.normalizeIPAddress(). For example, the address that would have been displayed as 2001::157:0:0:0:0:6a will now be displayed as 2001:0:157::6a. The traffic manager can still recognize and parse IPv6 addresses that have been improperly compacted.

Virtual Appliance

- **VTM-38768** Fixed issues in appliance log partition monitoring, where the traffic manager failed to generate "logdiskoverload" and "logdiskfull" events when the "/logs" partition reached thresholds of 85% or 95% full, respectively. These events are now generated correctly as soon as a new threshold is reached, and are repeated daily while that condition persists. Recovery occurs the next day if use has dropped only slightly below the threshold, or immediately if use drops to at least 5% below the threshold. Upon recovery, the traffic manager reports the new condition: either "logdiskoverload" (if recovered to between 85% and 95%), or with a new event type "logdiskrecovered" (if recovered to below 85%).

9) KNOWN ISSUES IN 18.2

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 and 4.0, 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** When upgrading from an earlier version 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.

After VA rollback from 18.2 the rollback UI widget doesn't appear

- **VTM-38962** After rolling back from 18.2 to an earlier vTM version the rollback version selector on the Traffic Managers page of the Admin UI will not offer version 18.2 as an option. Use "$ZEUSHOME/zxtm/bin/rollback" from the command line to switch back to 18.2 instead.

VMware Guest OS Customization does not support Ubuntu 18.04

- **VTM-38761** The virtual Traffic Manager VMware appliances are based on Ubuntu 18.04, VMware Guest Customization for this operating system is not supported on ESX versions prior to 6.5 update 2.

Admin UI fails to upgrade remote traffic managers with restartable hotfixes

- **VTM-38544** Hotfix packages received from vADC Support which require a traffic manager restart should not be applied to remote traffic managers using the Cluster-wide upgrade mechanism. They must be installed on each traffic manager's Admin UI individually, by choosing "Upgrade specified traffic managers" and then selecting the current traffic manager.

10) 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://www.pulsesecure.net/support/