PULSE SECURE PRODUCT RELEASE NOTES

PRODUCT: PULSE SECURE VIRTUAL TRAFFIC MANAGER

RELEASE DATE: 9TH OCTOBER, 2017

VERSION: 17.4

CONTENTS

1) ABOUT THIS RELEASE

Pulse Secure Virtual Traffic Manager 17.4 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 - 4.4, 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, 7.2
- Oracle VM for x86 3.2, 3.3, 3.4
- Microsoft Hyper-V Server 2012, 2012 R2, and 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.

Appliances intended for use with Data Plane Acceleration mode should be allocated a minimum of 3GB of RAM, and have a minimum of 2 CPU cores. An additional 1GB of RAM is needed for each additional CPU core for application data processing.

4) MAJOR FEATURES IN 17.4

SAML Service Provider, for Single-Sign-On

- **VTM-32291** The traffic manager now supports acting as a SAML Service Provider on HTTP virtual servers running either with or without SSL/TLS decryption.

  Supported SAML features:

  - SAML version 2.0
  - SP-initiated authentication
  - Web Browser SSO Profile
  - HTTP Redirect Binding for SAML requests
  - HTTP POST Binding for SAML responses
  - Signed SAML responses

vTM Docker Image

- **VTM-36489** Virtual Traffic Manager is available as a Docker Image.

Cluster-wide Upgrades

- **VTM-34266** For upgrades from vTM 17.4 onwards it is possible to upgrade multiple remote traffic managers in a cluster. Multiple traffic managers being upgraded in a single operation must be running on the same platform or hypervisor in order to use the same upgrade package.

  After uploading the upgrade package via the Admin UI you will be able to see which traffic managers the upgrade package is valid for, and select one or more traffic managers to upgrade. Traffic managers will be upgraded sequentially to avoid cluster downtime.

  This operation is also possible via a new "upgrade-cluster" script provided with the traffic manager in "$ZEUSHOME/zxtm/bin/". For full customization options, refer to the product documentation and the upgrade-cluster help output.

Support for Elastic Network Adapter in Amazon EC2 Virtual Appliance Images

- **VTM-33359** Enabled enhanced networking on Amazon EC2 using Elastic Network Adaptor (ENA) when launching an instance from a Pulse Secure vTM AMI into a VPC on an instance type that supports ENA-based enhanced networking.

Virtual Traffic Manager is now a Pulse Secure product

- **VTM-35082** All uses of "Brocade" in the vTM User Interface and APIs have been replaced with "Pulse Secure". This should have little impact on most customers, with the following exceptions:
  - The SMTP HELLO message now reads: 220 Pulse Secure Virtual Traffic Manager STMP Service
  - The program name for Remote Syslog is now set to "pulsevtm" instead of "Brocade". See issue VTM-36260 for more details

  Note: the version of Virtual Web Application Firewall included in this release presently retains the "Brocade" name.

5) PULSE SECURE VIRTUAL WEB APPLICATION FIREWALL FEATURES

- The traffic manager will install version 4.9-43001 of the Pulse Secure Virtual Web Application Firewall.

6) OTHER CHANGES IN 17.4

Installation and Upgrading

- **VTM-34988** Fixed a problem where the application firewall was not restarted after upgrading the traffic manager until the traffic manager itself was restarted.
- **VTM-33739** Fixed an issue where an upgrade package for a different hypervisor would overwrite a previously uploaded package if the two upgrade packages were for the same version. The list of previously uploaded packages on the upgrade page now lists packages by both version and hypervisor.

Configuration

- **VTM-36214** Fixed an issue where the Admin UI and the SOAP API would not accept URLs with IPv6 literal addresses in configuration settings that specify a URL. The REST API was not affected.
- **VTM-35670** Fixed an issue where an incorrect list of changes was displayed when previewing the import and merge of a partial configuration backup.
- **VTM-34447** The zconf program now supports using its exit code to indicate the presence of a config difference, when the --exit-code command line flag is supplied. This is intended to allow scripts to use zconf to determine whether a config difference exists, without needing to parse the output text.

Administration Server

- **VTM-35507** The expat XML parser library included in the administration server has been updated to version 2.2.3 to fix the security vulnerabilities CVE-2017-9233 and CVE-2016-9063.
- **VTM-35397** Fixed an issue in the traffic manager rc scripts that could cause restart-zeus to fail if the environment contained an invalid LANG value.
- **VTM-23992, SR31939** Fixed an issue where restarting any process from the Admin UI would cause the process being restarted to inherit the nice level of the Admin UI.
- **VTM-19083, SR23836** Added X-Frame-Options, X-Content-Type-Options and X-XSS-Protection HTTP headers in responses from the Admin UI to enable the additional security protection measures in user agents where they are supported.

REST API

- The current REST API version is 5.1. Versions 4.0 and 5.0 are supported but deprecated.
- **VTM-35749** Fixed an issue where configuration backups from an earlier traffic manager version were not updated to the current version when uploaded via REST. This could generate multiple configuration errors if the backups were restored.
- **VTM-35351** Fixed an issue where GET of a REST resource in the status tree (/api/tm/VERSION/status/) could fail when the traffic manager configuration was very large.

ZCLI

- **VTM-36021** Fixed an issue where the zcli command would fail to connect when the combined length of the username and password exceeded 56 characters.

SNMP

- **VTM-31957** Fixed an issue where the counters "Bandwidth", "Bandwidth per Node", "Bandwidth per Pool", and "Bandwidth per Virtual Server" were not available to select from the values to monitor when changing the data to plot on 'Current Activity' page on the Admin UI.

TrafficScript

- **VTM-31604** Fixed an issue where client requests might stall after running an asynchronous response rule.

Connection Processing

- **VTM-36176** Fixed an issue where HTTP/2 requests containing a proxy-connection header with the value 'Keep-Alive' caused the stream on which the request was handled to remain active. Streams in this state would be visible on the 'Activity > Connections' page in the state 'Keep-alive'. The proxy-connection header is now correctly ignored by the traffic manager.
- **VTM-36156** Fixed an issue where the traffic manager would incorrectly retain a copy of an HTTP/2 request if its headers decompressed to be greater in size than http2!headers_size_limit. Requests that were incorrectly retained would show up on the 'Activity > Connections' page in the state 'Client Read' and could have led to increasing memory consumption until the virtual server was restarted.
- **VTM-35864**, **VTM-35975** Fixed an issue where a 'DNS (UDP)' or 'DNS (TCP)' virtual server would incorrectly respond to queries for new DNS Resource Record types such as CAA (Certification Authority Authorization) with a 'REFUSED' error rather than allowing the request through to a back-end node.
- **VTM-35681** Fixed an issue where a server returning a chunked HTTP response with incomplete body data could have resulted in the corresponding client connection remaining open until the virtual server's timeout limit was reached.

Connection Debugging and Tracing

- **VTM-36405** Added descriptions to the Admin UI for request tracing events that were added in the 17.2 release.

Analytics Export

- **VTM-35576** Fixed a problem where analytics export would continue to use the previous UUID of the traffic manager after a new UUID had been generated.

Pools

- **VTM-11904**, **VTM-35634, SR15694** The documentation for the connect_timeout setting has been updated to more accurately describe how the setting behaves for HTTP, SIP and RTSP services.

Webcache

- **VTM-35848** Fixed an issue where an HTTP request referencing a resource with an absolute URI and no path would have been incorrectly stored in the web cache. The request was previously stored against the host specified by the Host header field in the original request, now it is correctly stored against the host specified in the request URI.

- **VTM-24078, SR32078** Fixed an issue that could have caused partial HTTP responses to be stored in the content cache if the response had no Content-Length header, did not use chunked encoding, and the connection to the back-end server was terminated with an error. Such responses are now treated as server failures, and are not cached.

SSL/TLS and Cryptography

- **VTM-36327** Fixed an issue where self registration of a traffic manager with Services Director would fail with an SSL/TLS decode error.
- **VTM-35987** Updated the Diffie-Hellman parameters used for key agreements in DHE TLS cipher suites as per best practice.

Logging

- **VTM-36260** Fixed an issue where syslog entries were prefixed with "Virtual Traffic Manager" and the syslog program name was "Brocade". The syslog program name is now "pulsevtm".

Pool Autoscaling

- **VTM-35649**, **VTM-36290** Fixed an issue that caused DNS-derived autoscaling to not add a node back into a pool if that node had previously been removed from the pool and was marked as having failed by a health monitor at the time it was removed.

Internals

- **VTM-36135**, **VTM-36372** Fixed an issue that caused the traffic manager to buffer more data than configured by the max_client_buffer setting if the client sent data faster than it could be written to the server, for example if a pool-based bandwidth class limited the rate at which data could be written to the server. This issue could have led to increasing memory consumption if a service was handling long-lived high bandwidth connections.
- **VTM-21912**, **VTM-36372**, **VTM-23011, SR28529**, **SR30135** Fixed an issue where a traffic manager child process that had been restarted after unexpectedly terminating could have failed to process new connections, resulting in them stalling indefinitely.

7) PULSE SECURE VIRTUAL WEB APPLICATION FIREWALL CHANGES

- Enhanced ValidHTTPMethodHandler to allow CalDAV methods.

- Added support for customizable subject and filename for report emails.
- Added null byte detection to baseline protection handler.
- Added support for custom client IP HTTP header.
- Fixed syntax error in start script for SmartOS.
- Fixed an issue that could occasionally cause an error while loading the event log.
- Updated zlib to zlib-1.2.11.
- **VTM-30486** Fixed an issue where the Application Firewall Enforcer rule was not updated when importing a configuration backup from a traffic manager version that used a different Enforcer rule. The old rule would then be used if that backup was restored.

8) VIRTUAL TRAFFIC MANAGER APPLIANCE

Appliance OS

- **VTM-36180** Fixed an issue where 'lstopo' processes were consuming 100% CPU time on traffic manager appliances after generating support reports.
- **VTM-35923** Updated the appliance kernel to version 4.4.0-96.119, and updated packages installed on the appliance. These updates include changes addressing:

  CVE-2014-9900 CVE-2015-7837 CVE-2015-8944 CVE-2016-2226 CVE-2016-2519 CVE-2016-4487 CVE-2016-4488 CVE-2016-4489 CVE-2016-4490 CVE-2016-4491 CVE-2016-4492 CVE-2016-4493 CVE-2016-6131 CVE-2016-7426 CVE-2016-7427 CVE-2016-7428 CVE-2016-7429 CVE-2016-7433 CVE-2016-7434 CVE-2016-9310 CVE-2016-9311 CVE-2017-0663 CVE-2017-2862 CVE-2017-2870 CVE-2017-3142 CVE-2017-3143 CVE-2017-6311 CVE-2017-6419 CVE-2017-6458 CVE-2017-6460 CVE-2017-6462 CVE-2017-6463 CVE-2017-6464 CVE-2017-7346 CVE-2017-7375 CVE-2017-7376 CVE-2017-7482 CVE-2017-7487 CVE-2017-7495 CVE-2017-7502 CVE-2017-7526 CVE-2017-7533 CVE-2017-7541 CVE-2017-7771 CVE-2017-7772 CVE-2017-7773 CVE-2017-7774 CVE-2017-7775 CVE-2017-7776 CVE-2017-7777 CVE-2017-7778 CVE-2017-8831 CVE-2017-8890 CVE-2017-9047 CVE-2017-9048 CVE-2017-9049 CVE-2017-9050 CVE-2017-9074 CVE-2017-9075 CVE-2017-9076 CVE-2017-9077 CVE-2017-9150 CVE-2017-9217 CVE-2017-9233 CVE-2017-9242 CVE-2017-9445 CVE-2017-9526 CVE-2017-9605

CVE-2017-10053 CVE-2017-10067 CVE-2017-10074 CVE-2017-10078
CVE-2017-10081 CVE-2017-10087 CVE-2017-10089 CVE-2017-10090
CVE-2017-10096 CVE-2017-10101 CVE-2017-10102 CVE-2017-10107
CVE-2017-10108 CVE-2017-10109 CVE-2017-10110 CVE-2017-10111
CVE-2017-10115 CVE-2017-10116 CVE-2017-10118 CVE-2017-10135
CVE-2017-10176 CVE-2017-10193 CVE-2017-10198 CVE-2017-10243
CVE-2017-10662 CVE-2017-10663 CVE-2017-10810 CVE-2017-11103
CVE-2017-11108 CVE-2017-11176 CVE-2017-11423 CVE-2017-11424
CVE-2017-11473 CVE-2017-11541 CVE-2017-11542 CVE-2017-11543
CVE-2017-12146 CVE-2017-12762 CVE-2017-12893 CVE-2017-12894
CVE-2017-12895 CVE-2017-12896 CVE-2017-12897 CVE-2017-12898
CVE-2017-12899 CVE-2017-12900 CVE-2017-12901 CVE-2017-12902
CVE-2017-12985 CVE-2017-12986 CVE-2017-12987 CVE-2017-12988
CVE-2017-12989 CVE-2017-12990 CVE-2017-12991 CVE-2017-12992
CVE-2017-12993 CVE-2017-12994 CVE-2017-12995 CVE-2017-12996
CVE-2017-12997 CVE-2017-12998 CVE-2017-12999 CVE-2017-13000
CVE-2017-13001 CVE-2017-13002 CVE-2017-13003 CVE-2017-13004
CVE-2017-13005 CVE-2017-13006 CVE-2017-13007 CVE-2017-13008
CVE-2017-13009 CVE-2017-13010 CVE-2017-13011 CVE-2017-13012
CVE-2017-13013 CVE-2017-13014 CVE-2017-13015 CVE-2017-13016
CVE-2017-13017 CVE-2017-13018 CVE-2017-13019 CVE-2017-13020
CVE-2017-13021 CVE-2017-13022 CVE-2017-13023 CVE-2017-13024
CVE-2017-13025 CVE-2017-13026 CVE-2017-13027 CVE-2017-13028
CVE-2017-13029 CVE-2017-13030 CVE-2017-13031 CVE-2017-13032
CVE-2017-13033 CVE-2017-13034 CVE-2017-13035 CVE-2017-13036
CVE-2017-13037 CVE-2017-13038 CVE-2017-13039 CVE-2017-13040
CVE-2017-13041 CVE-2017-13042 CVE-2017-13043 CVE-2017-13044
CVE-2017-13045 CVE-2017-13046 CVE-2017-13047 CVE-2017-13048
CVE-2017-13049 CVE-2017-13050 CVE-2017-13051 CVE-2017-13052
CVE-2017-13053 CVE-2017-13054 CVE-2017-13055 CVE-2017-13687
CVE-2017-13688 CVE-2017-13689 CVE-2017-13690 CVE-2017-13725

CVE-2017-1000111 CVE-2017-1000112 CVE-2017-1000251 CVE-2017-1000363
CVE-2017-1000365 CVE-2017-1000370 CVE-2017-1000371 CVE-2017-1000380

- **VTM-35841** Virtual Appliance default ntp servers are now set to:
  0.zeus.pool.ntp.org
  1.zeus.pool.ntp.org
  2.zeus.pool.ntp.org
  3.zeus.pool.ntp.org
- **VTM-35273**, **VTM-36074**, **VTM-35662** Fixed an issue where a cloud-init warning would be reported on the terminal when logging in via SSH.

Appliance Hardware

- **VTM-35562** Fixed an issue on baremetal appliances where the speed of network cards faster than 10G may be displayed incorrectly on the 'System > Networking' page of the Admin UI.
- **VTM-25800, SR35665** Fixed an issue where the Networking page of the Admin UI did not offer the correct speeds to be selected for a network interface with auto-negotiation turned off.

Virtual Appliance

- **VTM-35704** The z-expand-logs-partition tool was not functioning on appliances running traffic manager version 17.2 or 17.3. The tool now operates as expected.
- **VTM-34955** Fixed an issue where the z-expand-logs-partition tool would not work if SSH Intrusion Prevention was enabled. The SSH Intrusion Prevention tool will now be temporarily deactivated for the duration of the disk expansion.

Cloud Platforms

- **VTM-35687** Fixed an issue where traffic manager instances launched in Azure could fail to set the user password and hostname.
- **VTM-34990** Fixed an issue where it was not possible to detach network interfaces from the traffic manager instance on EC2 when enhanced networking drivers were in use (ixgbevf and ENA).

9) KNOWN ISSUES IN 17.4

Roll forward to 17.4 from Admin UI

- **VTM-36398** After upgrading to 17.4, if the traffic manager is rolled back to a version earlier than 17.4 it will not be possible to use the version selector on the Traffic Managers page of the Admin UI to switch back to 17.4 again. The rollback script can still be used to switch between these versions via the command line interface.

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.

Limitations in Data Plane Acceleration Mode

- **VTM-35990** An appliance with Data Plane Acceleration mode enabled will not boot if it has insufficient memory. To recover from this situation shut down the appliance, assign additional memory, and restart.
- **VTM-29462** In Data Plane Acceleration mode the MTU of an interface cannot exceed 1518 bytes.
- **VTM-33786** In Data Plane Acceleration mode, the traffic manager may experience packet loss on a VLAN interface configured on an SR-IOV NIC.
- **VTM-33768** In Data Plane Acceleration mode, the traffic manager may experience packet loss on an SR-IOV NIC when it is part of an IEEE 802.3ad ethernet bond. This issue can be worked around by using PCIe passthrough instead of SR-IOV.
- **VTM-31747** When the traffic manager has more than 10 interfaces and is running in Data Plane Acceleration mode, it may generate the error "SERIOUS DPAError Out of memory, <count> times". This indicates a momentary shortage of packet buffers. This does not affect the functionality of the traffic manager. This issue can be resolved by setting "iop!num_hugepages 1024" in $ZEUSHOME/zxtm/global.cfg if this key doesn't exist, or doubling the existing value if this key is already present.

Unsupported Features in Data Plane Acceleration Mode:

- Kerberos Constrained Delegation (KCD)
- Multi-hosted Traffic IP addresses
- Clusters containing more than 2 traffic managers
- Clusters in which the traffic managers have differing numbers of child processes
- Clusters in which the traffic managers are running on different operating systems
- Clusters in which only 1 traffic manager is running in Data Plane Acceleration Mode
- Multi-Site Manager (MSM)
- Loopback virtual servers
- Node drain to delete
- Transparent Proxying
- Return Path Routing (RPR)
- Network Address Translation (NAT)

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/