PULSE SECURE PRODUCT RELEASE NOTES

PRODUCT: BROCADE VIRTUAL TRAFFIC MANAGER

RELEASE DATE: 13TH DECEMBER, 2017

VERSION: 17.2R1

CONTENTS

1) ABOUT THIS RELEASE

The Brocade Virtual Traffic Manager 17.2r1 is a maintenance release of the Brocade 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.

2) PLATFORM AVAILABILITY

- Linux x86_64: Kernel 2.6.32 - 4.4, glibc 2.12+
- SmartOS x86_64: Kernel 20141030T164802Z and newer

- Virtual Appliances:
  - VMware vSphere 5.5, 6.0, 6.5;
  - XenServer 7.0;
  - 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);
- 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
- Bare Metal Server - for information on qualified servers, please see the Pulse Secure vTM Hardware Compatibility List at:

  https://community.pulsesecure.net/t5/Pulse-vADC-Updates/Pulse-Secure-vTM-Hardware-Compatibility-List/ba-p/34012

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 cores. An additional 1GB of RAM is needed for each additional core for application data processing.

4) CHANGES IN 17.2R1

Installation and Upgrading

- **VTM-36991** Fixed a value encoding issue on the 'System > Traffic Managers' page of the Admin UI.
- **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-35503** Fixed an issue which prevented the geoip update package from being installed on an appliance.

Analytics Export

- **VTM-36782** Added documentation for the 'protocol' field in the analytics export transaction metadata schema.

- **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.
- **VTM-35266**, **VTM-35337** When exporting log entries, the traffic manager now includes the time of the event in the 'time' field of exported entries for additional log export categories. The additional categories for which this information is exported include the traffic manager's audit, access and Data Plane Acceleration mode log files, application firewall log files, and the system's authentication log and syslog files. The time is parsed from timestamp information in the log entries, and is expressed as seconds since the UNIX epoch. Log entries that do not contain timezone information will use the system's timezone.
- **VTM-35407** Fixed an issue where exported log entries had an incorrect epoch time associated with them if the timestamp of the log entry had a timezone with a 30- or 45-minute offset.

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.

Authentication

- **VTM-36924** Added a warning to the user permission groups page that some permission settings give the ability to run scripts with the same UNIX user permissions as the traffic manager, and should be treated with caution. For more details see the 'Permission Groups' section of the User's Guide.
- **VTM-36271** Passwordless login for local ZCLI command execution now uses a dedicated transient secret protected by filesystem ACLs.

Administration Server

- **VTM-36984** Fixed a value encoding issue in the Sysctl page of the Admin UI on appliances.
- **VTM-34076** Explicit upgrade of group permissions for new features has been added to the traffic manager, and is applied retroactively back to version 7.2. In most cases a safe default of 'No Access' is set for new permissions added by a feature. Note that as a result of this change, features to which non-admin users previously had 'Read-Only' access might no longer be accessible. A suitably privileged administrator can update group permissions to restore access for affected users.
- **VTM-23643**, **SR31188** Added the 'HttpOnly' property to the session cookie that provides authenticated access to the Admin UI.
- **VTM-36864** Fixed an issue where any authenticated user logged into the Admin UI could access images of historical activity graphs.

- **VTM-36292** Improved the security of internal communication channels used between the traffic manager and the applet of the administrative 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-35328** The version of Perl bundled with the traffic manager has been patched to address CVE-2017-6512.

REST API

- **VTM-37048** Fixed an issue where a REST request for a resource protected by a group sub permission could be incorrectly granted PUT / GET access even though the permission was set to "none". For example, if SSL!Client_Keys was "none" and SSL was "ro" then REST would incorrectly permit and respond to GET requests for /config/active/ssl/client_keys.
- **VTM-36999** Fixed a bug where on Data Plane Acceleration mode capable appliances and SmartOS, REST PUT requests containing config key values that could contain IPv4 addresses or hostnames would not check the hostnames resolved to only IPv4 addresses. Fixed a bug on Linux software installs where 32-bit only counters in the REST statistics API could not be correctly filtered out, even when setting the query string.
- **VTM-36607** Fixed an issue where the href property in a REST API backup resource incorrectly had a trailing slash appended to it.
- **VTM-35096** A change has been made to check whether a load has succeeded before reporting a failure if a load has taken longer than the load timeout.
- **VTM-36291** Improved the security of internal communication channels used between the REST API and traffic manager processes.
- **VTM-36296** Improved the security of REST API proxied statistics requests. As a result of this change, traffic managers running versions from 17.4, 17.2r1, 10.4r2 or 9.9r3 onwards will be unable to proxy REST API requests to traffic managers without this improvement.
- **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-34882** Fixed an issue where the REST daemon leaked memory when a management IP address was configured, on each request to the stats API and more slowly in the background.

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.

TrafficScript

- **VTM-31604** Fixed an issue where client requests might stall after running an asynchronous response rule.
- **VTM-35385** The libxml2 XML parser library has been patched to fix CVE-2017-9047, CVE-2017-9048, CVE-2017-9049 and CVE-2017-9050.

Data Connections

- **VTM-32057** Fixed an issue where the Networking page of the Admin UI reported uncabled network ports as 'running' in Data Plane Acceleration mode.

Connection Processing

- **VTM-36513** Fixed an issue in Data Plane Acceleration mode that caused IPv6 packets to be dropped when the traffic manager did not already know the MAC address of the next hop for the packet. The error 'Csync KNI: IPv6 raw socket sendto failed' was reported in the event log when this happened.
- **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-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.
- **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-35116** Fixed an issue where the SNMP counter 'virtualserverCurrentConn' failed to decrement if a TLS session was closed after the handshake was completed but before the request was received.

Connection Debugging and Tracing

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

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.
- **VTM-36751** Fixed an issue where the elapsed times returned by the zcli command Pool.getNodesLastUsed could disregard data sent to or received from a node after the time at which a connection to that node had been created.

Bandwidth Management

- **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.

Webcache

- **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.
- **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.

Fault Tolerance

- **VTM-36331** Removed the ability to upgrade directly from software versions prior to 7.0. It remains possible to upgrade via an intermediary release version (7.0 or onward) without this restriction.

DNS Server

- **VTM-36693** Fixed a value encoding issue in the DNS Zones Files catalog page of the Admin UI.

SSL/TLS and Cryptography

- **VTM-36744** The library modified from OpenSSL that is used by the traffic manager has been upgraded to version 1.0.2m, addressing CVE-2017-3736. This library is used to provide cryptographic primitives such as RSA or AES.
- **VTM-36247** Improved the security of internal communication channels used between traffic manager processes.

- **VTM-35553**, **VTM-18863**, **VTM-7378**, **SR23577**, **SR10791** Integrated support for the Thales nShield product family has been removed from traffic manager appliances. The capability to install, configure and use nShield Connect products remains an option through the use of the generic PKCS#11 SSL Hardware capability and the Open Access VA policy. Warning: Upgrading to this release will remove all security worlds that were managed by the traffic manager in appliances created using previous releases. As a result all keys protected by those security worlds will no longer be usable, meaning SSL decrypting virtual servers using SSL/TLS certificates based upon those keys will no longer be able to create new connections. There is a similar impact for client certificates used to authenticate the traffic manager to pool nodes. Administrators using the integrated support for Thales nShield products, wanting to upgrade a traffic manager cluster to this release, should do so with a plan that includes the deployment of support software for their HSM hardware, along with the creation of new SSL/TLS certificates where hardware protected keys are required.
- **VTM-35483** Improvements have been made to enable parsing more DER structures for X.509 objects.
- **VTM-31971**, **VTM-32021**, **VTM-31970** Fixed an issue where the SSL Server Certificate catalog of the Admin UI would report an unexpected error when an SSL certificate without Subject Alternative Name extension was present.

Logging

- **VTM-23984**, **VTM-23985**, **SR31922**, **SR31923** When changing a secret via the REST API the value of the secret will be audit logged as a row of asterisks.

Technical Support Report (TSR)

- **VTM-34975** Fixed an issue where the periodic logs could omit some information if the traffic manager was restarted from the command line with a non-English locale selected.
- **VTM-35274** Fixed an issue where the generation of a Technical Support Report would fail if the Application Firewall Support Pack included in it took longer than 30 seconds to create.

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.

- **VTM-35201** Fixed an issue when using DNS-derived autoscaling that caused an error to be logged to the event log when a DNS server returned a SERVFAIL (rcode 2) error. SERVFAIL errors are now treated as a type of DNS unavailable response, for which a warning is emitted once when entering and leaving the failure state. SERVFAIL response codes continue to be ignored when considering whether to change membership of the pool.

Java

- **VTM-36014** Improved the security of internal communication channels used between the traffic manager and subordinate Java extensions.

Internals

- **VTM-36761**, **VTM-36710** Fixed an issue where a connection to a virtual server configured to have close_with_RST enabled could be terminated by the traffic manager with a normal FIN-ACK handshake instead of a connection reset.
- **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-35536** Updated the Periodic Logging system to collect internal traffic manager diagnostic information.

Appliance OS

- **VTM-36913** Fixed an issue where traffic manager appliances failed to disable SSH properly, causing it to be temporarily enabled on reboot.
- **VTM-36812** Updated the appliance kernel to version 4.4.0-101.124, and updated packages installed on the appliance. These updates include changes addressing: CVE-2010-4664 CVE-2014-9900 CVE-2015-7837 CVE-2015-8944 CVE-2016-0634 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-2016-7098 CVE-2016-7426 CVE-2016-7427 CVE-2016-7428 CVE-2016-7429 CVE-2016-7433 CVE-2016-7434 CVE-2016-7543 CVE-2016-7913 CVE-2016-7917 CVE-2016-8632 CVE-2016-9083 CVE-2016-9084 CVE-2016-9310 CVE-2016-9311 CVE-2016-9401 CVE-2016-9586 CVE-2016-9604 CVE-2017-0605 CVE-2017-0663 CVE-2017-0750 CVE-2017-2596 CVE-2017-2671 CVE-2017-2862 CVE-2017-2870

CVE-2017-3142 CVE-2017-3143 CVE-2017-3735 CVE-2017-3736 CVE-2017-6001
CVE-2017-6311 CVE-2017-6419 CVE-2017-6458 CVE-2017-6460 CVE-2017-6462
CVE-2017-6463 CVE-2017-6464 CVE-2017-6508 CVE-2017-6891 CVE-2017-7187
CVE-2017-7261 CVE-2017-7294 CVE-2017-7346 CVE-2017-7375 CVE-2017-7376
CVE-2017-7407 CVE-2017-7472 CVE-2017-7482 CVE-2017-7487 CVE-2017-7495
CVE-2017-7502 CVE-2017-7507 CVE-2017-7526 CVE-2017-7533 CVE-2017-7541
CVE-2017-7542 CVE-2017-7585 CVE-2017-7586 CVE-2017-7616 CVE-2017-7618
CVE-2017-7645 CVE-2017-7741 CVE-2017-7742 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-2017-7805 CVE-2017-7869 CVE-2017-7889 CVE-2017-7895
CVE-2017-8361 CVE-2017-8362 CVE-2017-8363 CVE-2017-8365 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-2017-9287 CVE-2017-9445
CVE-2017-9526 CVE-2017-9605 CVE-2017-9984 CVE-2017-9985 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-2017-10140
CVE-2017-10176 CVE-2017-10193 CVE-2017-10198 CVE-2017-10243
CVE-2017-10274 CVE-2017-10281 CVE-2017-10285 CVE-2017-10295
CVE-2017-10345 CVE-2017-10346 CVE-2017-10347 CVE-2017-10348
CVE-2017-10349 CVE-2017-10350 CVE-2017-10355 CVE-2017-10356
CVE-2017-10357 CVE-2017-10388 CVE-2017-10661 CVE-2017-10662
CVE-2017-10663 CVE-2017-10810 CVE-2017-10911 CVE-2017-11089
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-2017-12134 CVE-2017-12146 CVE-2017-12153
CVE-2017-12154 CVE-2017-12192 CVE-2017-12762 CVE-2017-12837
CVE-2017-12883 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-2017-13089 CVE-2017-13090
CVE-2017-13687 CVE-2017-13688 CVE-2017-13689 CVE-2017-13690
CVE-2017-13725 CVE-2017-14051 CVE-2017-14062 CVE-2017-14106
CVE-2017-14140 CVE-2017-14156 CVE-2017-14340 CVE-2017-14489
CVE-2017-14952 CVE-2017-14991 CVE-2017-15265 CVE-2017-15274
CVE-2017-15299 CVE-2017-15537 CVE-2017-15649 CVE-2017-15951
CVE-2017-16525 CVE-2017-16526 CVE-2017-16527 CVE-2017-16529
CVE-2017-16530 CVE-2017-16531 CVE-2017-16533 CVE-2017-16534
CVE-2017-16535 CVE-2017-1000100 CVE-2017-1000101 CVE-2017-1000111
CVE-2017-1000112 CVE-2017-1000158 CVE-2017-1000251 CVE-2017-1000252
CVE-2017-1000254 CVE-2017-1000257 CVE-2017-1000363 CVE-2017-1000364
CVE-2017-1000365 CVE-2017-1000366 CVE-2017-1000367 CVE-2017-1000370
CVE-2017-1000371 CVE-2017-1000379 CVE-2017-1000380

- **VTM-36180** Fixed an issue where 'lstopo' processes were consuming 100% CPU time on traffic manager appliances after generating support reports.
- **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.
- **VTM-28579**, **VTM-35611** Appliances will now set the 'net.ipv4.ip_local_reserved_ports' sysctl in order to avoid other processes using ports required for normal traffic manager and application firewall operation. If this sysctl has been set already using the 'System > Sysctl' page then the current value will be replaced on upgrade.

Appliance Hardware

- **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.

- **VTM-35363** Fixed an issue where IP addresses on a VLAN configured bond could become unreachable if IP addresses were added to or removed from the underlying bond interface.
- **VTM-33584** Fixed an issue where the Networking page of the Admin UI did not allow an IP address of a bond interface to be deleted if the interface had a VLAN child and the IP address was the first one to be added to the interface.

Cloud Platforms

- **VTM-36760** Fixed an issue where the "gcloud" tool included with virtual appliances on the GCE platform would not be updated during an upgrade to a maintenance release.
- **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).

5) WEB APPLICATION FIREWALL

- The traffic manager will install version 4.9-43062 of the Pulse Secure Virtual Web Application Firewall.
- Fixed an Updater UI issue where it was reporting an upgrade failure even after successful upgrade
- 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.

6) KNOWN ISSUES IN 17.2R1

There are no additional known issues in 17.2r1. For known issues in 17.2, see the release notes provided with the Brocade Virtual Traffic Manager 17.2 release.

7) 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/