# PULSE SECURE PRODUCT RELEASE NOTES

**PRODUCT:** BROCADE VIRTUAL TRAFFIC MANAGER

**RELEASE DATE:** 30TH APRIL, 2018

**VERSION:** 17.2R2

## CONTENTS

## 1) ABOUT THIS RELEASE

The Brocade Virtual Traffic Manager 17.2r2 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 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://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 cores. An additional 1GB of RAM is needed for each additional core for application data processing.

# 4) CHANGES IN 17.2R2

## Configuration

- **VTM-37488** Fixed an issue that prevented the successful regeneration of a Traffic Manager's UUID on Solaris/SmartOS platforms.

## Administration Server

- **VTM-34425**, **VTM-37772** Fixed an issue where using the restart button on the Admin UI (e.g. after an upgrade of the traffic manager software) would not restart the web server hosting the Admin UI.
- **VTM-37278** Fixed an issue where descriptions of custom event types were not HTML-encoded when displayed in the Admin UI. Only suitably privileged administrators are able to specify or edit the description of event types.

- **VTM-37432** Fixed an issue where virtual servers could display an error state during an upgrade in a cluster of three or more traffic managers if that upgrade includes a new virtual server configuration key.

### REST API

- **VTM-35443** Fixed an issue where changing the traffic manager name would sometimes cause the REST API to unexpectedly shutdown.
- **VTM-35452** A change has been made that allows the REST API process to be restarted if it exits after failing to reload the traffic manager configuration.

### SOAP API

- **VTM-38137** Fixed an issue where zcli and SOAP couldn't delete a user whose name contained the string "admin". Instead we prevent the current user from deleting their account.

### TrafficScript

- **VTM-37044** Updated libxml2, which the traffic manager is linked against, to version 2.9.7, which fixes various bugs.
- **VTM-37338** The TrafficScript function connection.data.set() now releases the memory used by an entry when it is overwritten, rather than at the time the connection is closed. This change prevents memory usage continuously increasing when connection.data.set() is used in rules that run every time data is received on long-lived connections.

### Connection Processing

- **VTM-37689** An HTTP client that issued a PUT or POST request eliciting a '100 Continue' response from the server might have received an extraneous 100 Continue response before receiving the server's final response headers. The traffic manager now responds with only one 100 Continue response, issued to the client as soon as it is received from the server.
- **VTM-36698**, **VTM-36701** Fixed an issue where the traffic manager's DNS resolver would leak memory when it received a DNS response with a TTL of 0.
- **VTM-37606** Fixed an issue where a pool managed by DNS-Derived Autoscaling would not contain the full set of expected nodes if a DNS reply was truncated. DNS-Derived Autoscaling now uses an EDNS0 query to increase the DNS packet size and allow a full reply to be received. The system falls back to using the truncated DNS results if the EDNS0 query does not complete successfully.
- **VTM-37155** Fixed an issue where DNSSEC NSEC3 resource records returned by a back-end server were corrupted when processed by a DNS virtual server.

## Connection Debugging and Tracing

- **VTM-37538** Corrected a request tracing message that reported an HTTP/2 connection as being closed when the stream was closed.

## SSL/TLS and Cryptography

- **VTM-37885** The library modified from OpenSSL that is used by the traffic manager has been upgraded to version 1.0.2o, addressing CVE-2017-3736, CVE-2017-3738 and CVE-2018-0739. This library is used to provide cryptographic primitives such as RSA or AES.
- **VTM-37419** The libcurl library that is used by the traffic manager's Azure Key Vault client has been upgraded to version 7.58.0, addressing CVE-2018-1000005 and CVE-2018-1000007.

## Internals

- **VTM-37322** Fixed an issue that could have caused the traffic manager to constantly poll a file descriptor for a closed connection, causing excessive CPU usage. The issue could have occurred when a client terminated a connection that had been paused by the traffic manager because the server had stopped reading data.
- **VTM-37207** Fixed an issue where the traffic manager's SNMP counters for network interface statistics were updated for only one interface. As a result, the Current Activity graph in the Admin UI would show information for only one interface when viewing any values in the 'Network interfaces' category.

## Appliance OS

- **VTM-38113** Updated the appliance kernel to 4.4.0-119.143, and updated packages installed on the appliance. These updates include changes addressing:

  CVE-2015-8952 CVE-2016-2774 CVE-2016-3186 CVE-2016-5102 CVE-2016-5318 CVE-2016-6185 CVE-2016-10009 CVE-2016-10010 CVE-2016-10011 CVE-2016-10012 CVE-2016-10266 CVE-2016-10267 CVE-2016-10268 CVE-2016-10269 CVE-2016-10371 CVE-2017-0861 CVE-2017-3144 CVE-2017-3145 CVE-2017-3737 CVE-2017-3738 CVE-2017-5563 CVE-2017-5715 CVE-2017-5753 CVE-2017-5754 CVE-2017-6312 CVE-2017-6313 CVE-2017-6314 CVE-2017-6512 CVE-2017-7518 CVE-2017-7592 CVE-2017-7593 CVE-2017-7594 CVE-2017-7595 CVE-2017-7596 CVE-2017-7597 CVE-2017-7598 CVE-2017-7599 CVE-2017-7600 CVE-2017-7601 CVE-2017-7602 CVE-2017-8816 CVE-2017-8817 CVE-2017-8824 CVE-2017-9117 CVE-2017-9147 CVE-2017-9403 CVE-2017-9404 CVE-2017-9815 CVE-2017-9935 CVE-2017-9936

CVE-2017-10688 CVE-2017-10790 CVE-2017-11335 CVE-2017-11472 CVE-2017-11613
CVE-2017-12190 CVE-2017-12193 CVE-2017-12944 CVE-2017-13726 CVE-2017-13727
CVE-2017-14632 CVE-2017-14633 CVE-2017-15115 CVE-2017-15129 CVE-2017-15412
CVE-2017-15422 CVE-2017-15670 CVE-2017-15804 CVE-2017-15906 CVE-2017-15908
CVE-2017-16528 CVE-2017-16532 CVE-2017-16536 CVE-2017-16537 CVE-2017-16548
CVE-2017-16612 CVE-2017-16643 CVE-2017-16645 CVE-2017-16646 CVE-2017-16649
CVE-2017-16650 CVE-2017-16911 CVE-2017-16912 CVE-2017-16913 CVE-2017-16914
CVE-2017-16932 CVE-2017-16939 CVE-2017-16994 CVE-2017-16997 CVE-2017-17095
CVE-2017-17433 CVE-2017-17434 CVE-2017-17448 CVE-2017-17449 CVE-2017-17450
CVE-2017-17512 CVE-2017-17558 CVE-2017-17712 CVE-2017-17741 CVE-2017-17805
CVE-2017-17806 CVE-2017-17807 CVE-2017-17862 CVE-2017-18013 CVE-2017-18075
CVE-2017-18190 CVE-2017-18203 CVE-2017-18204 CVE-2017-18208
CVE-2017-1000405 CVE-2017-1000407 CVE-2017-1000408 CVE-2017-1000409
CVE-2017-1000422 CVE-2018-0739 CVE-2018-1049 CVE-2018-2579 CVE-2018-2582
CVE-2018-2588 CVE-2018-2599 CVE-2018-2602 CVE-2018-2603 CVE-2018-2618
CVE-2018-2629 CVE-2018-2633 CVE-2018-2634 CVE-2018-2637 CVE-2018-2641
CVE-2018-2663 CVE-2018-2677 CVE-2018-2678 CVE-2018-5146 CVE-2018-5332
CVE-2018-5333 CVE-2018-5344 CVE-2018-5732 CVE-2018-5733 CVE-2018-5764
CVE-2018-5784 CVE-2018-6003 CVE-2018-6797 CVE-2018-6798 CVE-2018-6913
CVE-2018-6927 CVE-2018-7492 CVE-2018-8043 CVE-2018-1000001
CVE-2018-1000005 CVE-2018-1000007 CVE-2018-1000026 CVE-2018-1000120
CVE-2018-1000121 CVE-2018-1000122

### Cloud Platforms

- **VTM-37854** Fixed an issue where Virtual Traffic Manager AMIs regenerated their Admin UI SSL certificates on AWS on each reboot.
- **VTM-37502** Updated the version of the EC2 Query Server API used by the traffic manager to version "2016-11-15".
- **VTM-31990** Pulse Secure Virtual Traffic Manager appliances on Google Compute Engine now support multiple network interfaces. See Google's documentation for details on how to create instances with multiple NICs.
- **VTM-37056** The "GCE Firewall Rules" section of the Networking page has been removed as a change to the underlying tool it used rendered it inoperative. GCE firewall rules can be managed via the Google Cloud Console.

## 5) WEB APPLICATION FIREWALL

The traffic manager will install version 4.9-43062 of the Pulse Secure Virtual Web Application Firewall.

## 6) KNOWN ISSUES IN 17.2R2

There are no additional known issues in 17.2r2. 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/