Pulse Secure Virtual Traffic Manager: Release Notes

Supporting Pulse Secure Virtual Traffic Manager 19.1

Product Release	**19.1**
Published	**29 April, 2019**
Document Version	**1.0**

Pulse Secure, LLC
2700 Zanker Road,
Suite 200 San Jose
CA 95134

www.pulsesecure.net

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

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 7.0, 7.1, 7.6
- 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.

Support

Full support for version 19.1 will be available for one year from the release date of 29 April, 2019. See the following End of Support and End of Engineering Schedule for more information:

https://support.pulsesecure.net/product-service-policies/eol/software/vadc-virtual-traffic-manager/

Major Features in 19.1

TLS 1.3 client-side Support

- **VTM-39798, VTM-39422, VTM-39261, VTM-39260, VTM-38977** Connections from pools to back-end nodes made with SSL Encryption will negotiate the TLS 1.3 protocol where available. This behavior is configurable globally and per-pool, and is enabled by default, however on upgrade TLS 1.3 will be disabled either globally or for individual pools if the existing configuration for that context has TLS 1.2 disabled, or has other settings incompatible with TLS 1.3.

  Inter-cluster communication may now use TLS 1.3 connections, subject to configuration.

Enhance TLS certificate selection for a pool

- **VTM-23994, SR31942** Added a pool configuration key 'ssl_fixed_client_certificate' to force the usage of a specific client certificate regardless of the list of issuer CAs supplied by the back-end node when client certificate authentication is in use.

Enhanced RFC-5424 syslog output

- **VTM-30456** The format of remote syslog messages sent by the traffic manager's request logging and event log components has been updated to follow the specification defined in RFC 5424. Accordingly, syslog messages now contain hostname and timestamp information, and the default value for the maximum length of a remote syslog message has changed from 1024 bytes to 2048 bytes.

Maximum in-flight transactions per node setting

- **VTM-40379, VTM-38427** The traffic manager can now be configured to queue up incoming HTTP requests if all the nodes in the chosen pool are already busy handling ongoing transactions. The feature is introduced alongside the existing ability for the traffic manager to queue incoming requests when the number of connections established to each node reached a configured limit. Whereas the connection-based limit is useful for protecting servers running applications that consume resources on a per-connection basis, the new transaction-based limit can help protect servers from being overloaded when handling too many resource-intensive tasks simultaneously.

  The new feature can be enabled by configuring the 'max_transactions_per_node' setting on a pool to be the desired limit on the number of transactions each node in the pool should be handling simultaneously. The setting can be found in the 'Pool > Protocol Settings > TCP Connection Limits and Queueing' section of the Admin UI.

64bit webcache for objects greater than 2GiB in size

- **VTM-38745** The webcache has been enhanced to support caching objects that are greater than 2GB in size.

Traffic IP address groups in Google Compute Engine

- **VTM-40773** It is now possible to configure Traffic IP Groups on Google Compute Engine using GCE External IP Addresses as Traffic IP addresses. A maximum of one Traffic IP address is supported per Network Interface Card on a GCE instance. Traffic IP Groups are available in both active/active and active/passive mode, using single-hosted IP addresses. Refer to GCE documentation for how to create and configure GCE External IP Addresses.

Optimal Gateway Selection (OGS) Wizard

- **VTM-40351** Added the Optimal Gateway Selection Wizard to simplify configuration of vTM for global load-balancing of PCS clusters.

Services Director Support for vTMs behind NAT

- **VTM-40402** It is now possible to use a Services Director to license traffic managers which are only accessible via a NAT Gateway, e.g. a vTM Docker container. The traffic manager will create a long-running TCP websocket connection to the Services Director instance, through which all the required communications in both directions will be sent. This feature is only available when using self-registration, and is enabled by default when doing so.

Pulse Secure Virtual Web Application Firewall Features

- The traffic manager will install version 4.9-43361 of the Pulse Secure Virtual Web Application Firewall.

Other Changes in 19.1

Installation and Upgrading

- **VTM-40471** Fixed an issue where installing a hotfix via the command line did not record it in the list of applied hotfixes.
- **VTM-40155** Re-phrased event log messages for the Community Edition related to cluster size limits and license acceptance to be more consistent with other Community Edition logs.
- **VTM-38544**, **VTM-37767** Fixed an issue where applying a hotfix with the upgrade-cluster tool would not restart the remote traffic managers automatically to apply the hotfix changes.
- **VTM-37935**, **VTM-38535** Fixed an issue when applying a hotfix to a cluster which caused it to be recorded on the traffic manager where the upgrade was initiated rather than the cluster members where it was applied.

Configuration

- **VTM-41232** Fixed an issue that prevented TLS certificate mappings for a virtual server from being imported by the configuration importer tool.
- **VTM-41221** Fixed an issue that caused configuration documents containing Unicode strings and object names to be incorrectly imported by the configuration importer tool.
- **VTM-40874** Fixed an issue that prevented the configuration importer tool from importing table keys with list, set or boolean values.
- **VTM-40820** Fixed an issue that prevented user permission groups from being correctly imported by the configuration importer tool. Previously, it was possible to configure only top-level permissions.
- **VTM-40227** The 'traffic_managers' section in configuration documents now supports a 'local_tm' field in which machine-specific configuration can be specified that will be applied to the traffic manager on which the Configuration Importer is run.
- **VTM-39812**, **VTM-39284** The Configuration Importer now supports importing configuration using historic API versions. The set of supported API versions is the same as for the REST API. The existing "version" field at the top level of a configuration document specifies the API version of configuration within that document.
- **VTM-39282** The configuration of the traffic manager can now be exported as a single JSON or YAML configuration document. Configuration documents can be used to replace the running configuration of a traffic manager, or to deploy a fully configured traffic manager Docker container or Kubernetes pod. The configuration export feature can be accessed through the Administration GUI on the 'Services > Config Summary' and 'System > Backups' pages, or through the 'config-export' utility on the command-line. For further details, see the Configuration Importer Guide.

Administration Server

- **VTM-41387** Fixed a value encoding issue on the Current Activity page in the Admin UI.
- **VTM-41375** Fixed a value encoding issue for dropdown boxes in the Admin UI.
- **VTM-40220** The upstream fix for CVE-2018-18311 was applied to the version of Perl included in the product.
- **VTM-15293, SR19322** Fixed an issue where restarting the Admin server could cause high CPU usage when multiple browsers were connected to the Admin UI.
- **VTM-8701, SR12285** Added a new option to the historical activity graph that allows you to view an aggregate for all of the plotted lines.

REST API

- The current REST API version is 6.2.
- **VTM-41159** Fixed an issue where requesting metadata for SSL certificates caused the REST API to crash
- **VTM-39944** Added a setting 'rest!maxfds' to global settings to specify a limit for open file descriptors in the REST daemon.
- **VTM-37412** REST API schemas have been modified to indicate whether a resource is a Single, Collection, Certificate, File or Dynamic resource in the "resourceType" element.

- **VTM-37368** The REST API has been modified to correctly generate the schemas for dynamic type resources.

Zeusbench

- **VTM-40082** Fixed an issue in the "zeusbench" tool where attempting to use the --linger and --keepalive options together would cause the tool to abort.

SNMP

- **VTM-41030** The following SNMP counters are now obsolete: hourlyPeakBytesInPerSecond, hourlyPeakBytesOutPerSecond, hourlyPeakRequestsPerSecond and hourlyPeakSSLConnectionsPerSecond. For equivalent functionality, an SNMP client can monitor totalBytesIn, totalBytesOut, totalRequests and sslConnections and calculate peak values.

TrafficScript

- **VTM-40987** The Perl Compatible Regular Expression library (PCRE) has been updated to version 10.32, addressing CVE-2017-8399.
- **VTM-40554** Fixed an issue that, when the traffic manager is receiving a POST request with a large body and a TrafficScript rule aborts due to a usage error, results in connections being dropped or denied.

Java

- **VTM-40183**, **VTM-40522** To reduce initial resource usage, Java support is now disabled by default for new installations and the Java process will not be started. To use Java Extensions from TrafficScript, Java support must be enabled from the 'Global Settings > Java Extension Settings' page in the Admin UI. Existing installations are unaffected on upgrade.

Connection Queueing

- **VTM-41170** Fixed an issue that could have prevented an error page being sent to a client if their request was timed out when waiting in a queue.
- **VTM-40425** Fixed an issue that allowed a pool's maximum configured queue size to be exceeded by up to 1 connection per traffic manager child process.
- **VTM-40392** Fixed an issue that could cause the pool connection queuing counters to become incorrect after a traffic manager child process was unexpectedly restarted. The incorrect counters could cause the limits configured by 'max_queued' and 'max_connections_pernode' to be enforced incorrectly.

Connection Processing

- **VTM-40135** Fixed incorrect text in HTTP/2 request tracing, where previously the traffic manager closing the stream to the client was logged as "Client closed HTTP/2 stream" it is now correctly logged as "Traffic Manager closed HTTP/2 stream".

- **VTM-36376**, **VTM-37302** A new TrafficScript function - http.connection.sendOrigin() - has been added that issues an HTTP/2 ORIGIN frame to the client, informing it for which other origins it can re-use the current HTTP/2 connection. Web browsers can, but are not required to, use this information to reduce the number of secure TCP connections that must be established to fetch all the resources on a web page, potentially reducing the time it takes for the page to load.
- **VTM-36335** Fixed an issue where a SIP UDP virtual server with 'udp_endpoint_persistence' disabled could abandon a SIP transaction if it overlapped with another transaction that was part of the same session and the two transactions were routed to different destinations. Transactions can now be independently routed when 'udp_endpoint_persistence' is disabled. For newly created SIP UDP virtual servers, the 'udp_endpoint_persistence' setting is now disabled by default.

Connection Debugging and Tracing

- **VTM-40166** Fixed an issue where the request tracing event "First byte written to back-end server" could be logged after the "Wrote TCP data to back-end server" event.

Analytics Export

- **VTM-40393** Log export metadata can now be configured to contain nested objects. In addition, a set of macros have been provided that can be used as metadata values - these include the traffic manager's instance identifier and cluster identifier.

Fault Tolerance

- **VTM-40457**, **VTM-40946** Fixed an issue where the cluster communication test conducted after joining a cluster could fail if the traffic manager joining the cluster had a Traffic IP group configured.

IP Transparency

- **VTM-40280** Fixed an issue that prevented the virtual server transparent proxying feature settings from being displayed in the Admin UI.

Health Monitoring

- **VTM-39584** Fixed an issue where the 'Pool > Monitors' page in the Admin UI could not be displayed if any of the configured monitors for that pool did not exist in the catalog. Now the names of non-existent monitors are shown, and they can be removed from the configuration of the pool.

Licensing

- **VTM-40207** The URL for purchasing licenses has been added to the vTM title bar when using the Community Edition.

SSL/TLS and Cryptography

- **VTM-41377** An SSL decrypting virtual server now permits the client to omit the 'Certificate' message, as an alternative to an empty 'Certificate' message, in TLS versions prior to 1.3, where a TLS client certificate is requested by not required.

- **VTM-41220** Fixed an issue where the per-pool configuration settings for the policy around caching SSL client sessions or session tickets for pool nodes were not correctly respected until the traffic manager was restarted.
- **VTM-40888**, **VTM-40897** Fixed an issue where certain TLS message sequences from an SSL-encrypting pool node could have caused the pool connection to disconnect.
- **VTM-40798** Fixed an issue where the elliptic curve used for ECDHE key exchanges was not reported for TLS 1.3 connections in the export of analytics data.
- **VTM-40614** Fixed an issue where under certain conditions a large amount of data sent through a TLS 1.3 connection could result in an unexpected termination of the connection.
- **VTM-40586** Fixed an issue where 'Certificate' messages from a TLS 1.3 client containing extensions (which are rarely used) would not be parsed, causing the connection to be closed.
- **VTM-40510** Fixed an issue where an SSL/TLS decrypting virtual server would incorrectly permit the selection of an RSASSA-PSS certificate following the negotiation of two classes of TLS protocol parameters; selection of either, versions of TLS that do not support RSA-PSS signatures (1.1 and earlier), or cipher suites that use RSA encryption (non-PFS), rather than signatures, for the key exchange.
- **VTM-40427** Fixed an issue where a TLS client sending a RSASSA-PSS client certificate but using a RSASSA-PKCS1-v1_5 signature could be successfully, but incorrectly, authenticated by virtual servers using TLS 1.2 or lower. The signature was verified correctly, meaning that a client would need the correct private key to authenticate, but was not checked against the algorithm parameters in the certificate.
- **VTM-40366** Added support for PSS-based RSA signature algorithms (RSA-PSS_SHA256, RSA-PSS_SHA384, RSA-PSS_SHA512, RSAPSS-PSS_SHA256, RSAPSS-PSS_SHA384 or RSAPSS-PSS_SHA512) in TLS 1.2 ServerKeyExchange messages and server certificate chains used for TLS 1.2, in both virtual servers and pools.
- **VTM-40312** Fixed an issue where spaces in SSL client and server key catalog object names caused data corruption when written via the REST API.
- **VTM-40302** Added a global and per-pool configuration to control whether TLS 1.3 is used in "middlebox compatibility" mode. See Appendix D.4 of RFC 8446 for more details on where this might be required. By default, middlebox compatibility mode will be used for all TLS 1.3 connections initiated by the traffic manager.
- **VTM-40276** Updated the OpenSSL library used when connecting to the Azure Key Vault addressing CVE-2018-0732.
- **VTM-40182** Fixed an issue where an upgrade to, or restoring a backup from, 18.3 or 18.3r1 would fail if the configuration included an invalid virtual server configuration that referenced a SSL server certificate/key pair that did not exist in the SSL Server Certificates catalog.
- **VTM-40161** The library modified from OpenSSL that is used by the traffic manager has been upgraded to version 1.1.1a, addressing CVE-2018-0734 and CVE-2018-0735. This library is used to provide cryptographic primitives such as RSA or AES.
- **VTM-39799** Added support for TLS 1.3 for control and management plane connections initiated by the traffic manager, if configuration permits it. Since support for accepting TLS 1.3 connections in the control plane and management plane was added in 18.3, this will result in TLS 1.3 being used for internal cluster communications once the entire cluster is upgraded.

- **VTM-39219** The cipher suites SSL_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 and SSL_ECDHE_RSA_WITH_AES_256_CBC_SHA384 are now disabled by default in the traffic manager as they may be vulnerable to timing attacks. They can still be enabled globally, per virtual server or per pool via the appropriate configuration settings if required. No change to explicitly configured cipher suites settings will be made when upgrading.
- **VTM-38096** The global configuration keys 'ssl!prevent_timing_side_channels' and 'admin!ssl_prevent_timing_side_channels' have been obsoleted. These allowed mitigations for the Lucky-13 attack to be disabled, but their performance impact has been measured to be negligible, and they are now always enabled. The configuration keys currently remain configurable via the SOAP and REST APIs, which now have no effect; these will be removed in a future version when the REST API major version is incremented.
- **VTM-30863** In line with best practice following the publication of the SWEET32 vulnerability, the cipher suites SSL_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA and SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA are now disabled by default in the traffic manager. They can still be enabled globally, per virtual server or per pool via the appropriate configuration settings if required. No change to explicitly configured cipher suites settings will be made when upgrading. Refer to CVE-2016-2183 for discussion of this vulnerability as it applies to SSL/TLS connections.

Logging

- **VTM-40238** Fixed a value encoding issue in the alerting Event Types edit page in the Admin UI.

Web Accelerator

- **VTM-40739** Web Accelerator has been updated to use libjpeg version 9c
- **VTM-40454** Fixed an issue that caused Web Accelerator to return pages with HTTP Date and Expires headers that had incorrect timestamps, reducing the effectiveness of downstream caching.

Pool Autoscaling

- **VTM-40804** Fixed an issue which could cause the autoscaler process to restart if a pool was configured to use both autoscaling and DNS-derived autoscaling.

Telemetry

- **VTM-17840, SR22270** The traffic manager's telemetry system has been updated to report anonymized data in the event of certain traffic manager processes failing.

Internals

- **VTM-40771** Changes to the mtrace utility address the following vulnerabilities: CVE-2016-10254 and CVE-2016-10255
- **VTM-40528** Fixed an issue where TrafficScript code that accesses array elements by the direct use of a function call could, in some specific circumstances, cause an ASSERT failure.

- **VTM-37355** The internal implementation of TrafficScript hashes has changed, and as a result the ordering of keys returned by hash.keys() and the ordering of content within lang.dump() output has changed. If you have a rule that depends on this ordering, you may need to rewrite it, either by making it independent of the order or by using array.sort() on the result of hash.keys() to ensure a repeatable order.
- **VTM-35318** The watchdog process (procmon), which monitors data-plane processes, now has a configurable timeout that determines how long a process must be unresponsive before the watchdog raises an alert. The timeout setting can be configured from 'Global Settings > Watchdog'. The 'watchdog' alert that is generated can now also be included in an event type to use in the alerting system.

Pulse Connect Secure Integration

- **VTM-40525** Fixed an issue that caused the "Load-balance Pulse Connect Secure" Wizard to fail when given a service name containing spaces and the HTTP redirect option was enabled.

Virtual Traffic Manager Appliance

Appliance OS

- **VTM-41270** Updated the appliance kernel to version 4.15.0-47.50, and updated packages installed on the appliance. These updates include changes addressing:

  CVE-2017-6519 CVE-2018-0495 CVE-2018-0734 CVE-2018-0735 CVE-2018-3136 CVE-2018-3139
  CVE-2018-3149 CVE-2018-3169 CVE-2018-3180 CVE-2018-3183 CVE-2018-3214 CVE-2018-4700
  CVE-2018-5407 CVE-2018-5729 CVE-2018-5730 CVE-2018-5744 CVE-2018-5745 CVE-2018-6559
  CVE-2018-6954 CVE-2018-8905 CVE-2018-9516 CVE-2018-10779 CVE-2018-10839 CVE-2018-10876
  CVE-2018-10877 CVE-2018-10878 CVE-2018-10879 CVE-2018-10880 CVE-2018-10882
  CVE-2018-10883 CVE-2018-10902 CVE-2018-10963 CVE-2018-11806 CVE-2018-12384
  CVE-2018-12404 CVE-2018-12617 CVE-2018-12896 CVE-2018-12900 CVE-2018-14625
  CVE-2018-14647 CVE-2018-14678 CVE-2018-14734 CVE-2018-16276 CVE-2018-16847
  CVE-2018-16864 CVE-2018-16865 CVE-2018-16866 CVE-2018-16872 CVE-2018-16882
  CVE-2018-16890 CVE-2018-17000 CVE-2018-17100 CVE-2018-17101 CVE-2018-17958
  CVE-2018-17962 CVE-2018-17963 CVE-2018-17972 CVE-2018-18021 CVE-2018-18281
  CVE-2018-18311 CVE-2018-18312 CVE-2018-18313 CVE-2018-18314 CVE-2018-18397
  CVE-2018-18445 CVE-2018-18508 CVE-2018-18557 CVE-2018-18661 CVE-2018-18690
  CVE-2018-18710 CVE-2018-18849 CVE-2018-18954 CVE-2018-18955 CVE-2018-19210
  CVE-2018-19364 CVE-2018-19407 CVE-2018-19489 CVE-2018-19824 CVE-2018-19854
  CVE-2018-20406 CVE-2018-20483 CVE-2018-20679 CVE-2018-20685 CVE-2018-1000517
  CVE-2018-1000845 CVE-2018-1000858 CVE-2019-0804 CVE-2019-0816 CVE-2019-1559
  CVE-2019-2422 CVE-2019-3459 CVE-2019-3460 CVE-2019-3462 CVE-2019-3812 CVE-2019-3822
  CVE-2019-3823 CVE-2019-3842 CVE-2019-5747 CVE-2019-5953 CVE-2019-6109 CVE-2019-6111
  CVE-2019-6128 CVE-2019-6133 CVE-2019-6454 CVE-2019-6465 CVE-2019-6778 CVE-2019-6974
  CVE-2019-7221 CVE-2019-7222 CVE-2019-7308 CVE-2019-7663 CVE-2019-8905 CVE-2019-8906
  CVE-2019-8907 CVE-2019-8912 CVE-2019-8980 CVE-2019-9213 CVE-2019-11068

- **VTM-40628** Fixed an issue which made the Traffic IP Groups page of the Admin UI inaccessible if Multi-Site Manager was enabled.
- **VTM-40336** The SSH Intrusion Prevention feature for appliances is now enabled by default for new deployments.
- **VTM-38760** The VMware appliance now contains the VMware balloon kernel module.
- **VTM-37197** The appliance kernel now contains more congestion control and packet scheduling modules which can be selected using sysctls.
- **VTM-35587, VTM-35586, VTM-34358** Fixed an issue where an appliance upgrade would not delete the files related to the kernel being replaced from the boot partition. After a number of upgrades, this could leave insufficient space in the boot partition, causing subsequent upgrade attempts to fail.
- **VTM-18677, SR23373** It is now possible to set the interface MTU on a traffic manager appliance on Hyper-V.

Virtual Appliance

- **VTM-38761** Fixed an issue which prevented configuration of the VMware appliance using Guest OS Customizations.

Cloud Platforms

- **VTM-40863** Fixed an issue which caused EC2 VPC instances to generate a warning if they had no external IP address.
- **VTM-40815** Fixed an issue which made Google Compute Platform instances with more than 6 interfaces uncontactable.
- **VTM-40222** Fixed an issue which caused the status applet to incorrectly report an error when the only public IP address on an instance of our AWS Marketplace AMI was an Elastic IP TIP.

Other changes supplied in previous minor revisions of 18.3

- **VTM-40373** Fixed an issue where TLS client connections made by the traffic manager would advertise support for RSA-PSS signature schemes when it is not supported. Previously this issue meant that connections to TLS servers that preferred the use of RSA certificates, supported RSA-PSS and preferred the use of RSA-PSS over PKCS#1 v1.5, would fail with the traffic manager emitting an invalid key exchange error.
- **VTM-40372** Fixed an issue where the traffic manager would stall when sending data on an SSL connection, if the socket buffer became full while writing out the last bytes of a response. In particular, this impacted control plane status messages when the traffic manager configuration was large (more than ~50 configuration objects).
- **VTM-40417** Fixed an issue where RSASSA-PSS signatures in TLS 1.3 handshakes were handled incorrectly in some circumstances, resulting in connections being dropped or denied.
- **VTM-40363** Fixed an issue where the traffic manager would incorrectly handle an irregular packet when received by a virtual server configured with support for TLS 1.3, resulting in connections being dropped or denied.

- **VTM-40368** Fixed an issue where traffic manager appliances deployed on EC2 could not use AWS CloudFormation.

Known Issues in 19.1

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 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** 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 19.1 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://www.pulsesecure.net/support