Pulse Secure Product Release Notes

Product: Pulse Secure Services Director

Release Date: 20 May 2019

Product Version: 19.1

Document Version: 1.0

Contents

1) About This Release

Pulse Secure Services Director v19.1 is a feature release of the management tool for the Pulse Secure Virtual Traffic Manager. In addition to a number of bug fixes, it introduces a number of new features.

2) Platform Availability

- Linux x86_64: Ubuntu 18.04 LTS, RHEL/CentOS 6
- Pulse Secure Services Director Virtual Appliance
- Amazon EC2 - as a virtual appliance or native software install

3) Resource Requirements

Software Environment - Pulse Secure Services Director

- Operating system:
  - Ubuntu 18.04 (x86_64)
  - RHEL/CentOS 6 (x86_64)
- Database: MySQL 5.5/5.6/5.7
- Other services: SMTP
- Recommended hardware (CPU): Intel Xeon / AMD Opteron
- Recommended hardware (Minimum memory): 2GB
- Recommended hardware (Minimum disk space): 10 GB (plus additional disk space for metering logs depending on number of instances metered)

Virtual Environment - Pulse Secure Services Director VA

- Hypervisor:
  - VMware vSphere ESXi 6.0/6.5/6.7
  - QEMU/KVM (RHEL/CentOS 6.x, 7.x; Ubuntu 18.04)
  - Amazon EC2
- Analytics engine (optional): Splunk 6.5/7.0
- Virtual Appliance resource requirements are listed in the table below:

Virtual Appliance	CPU	Memory	Disk
Services Director VA	4 vCPU	8 GB	46 GB
Amazon EC2 (t2.large)	2 vCPU	8 GB	46 GB

Software/Virtual Environment for Deployed vTMs

- Services Director deployed, software:
  - Ubuntu 14.04 (x86_64)
  - Ubuntu 16.04 (x86_64)
  - RHEL/CentOS 6 (x86_64)
- Externally deployed, software: Same as Pulse Secure Virtual Traffic Manager (17.2r2 or later)
- Externally deployed, VA: Same as Pulse Secure Virtual Traffic Manager (17.2r2 or later)

4) Upgrades

If a customer wishes to upgrade their Services Director Virtual Appliances on Amazon EC2, they should follow the same steps as for other supported hypervisors, but they should use the upgrade image for VMware.

If a customer wishes to run Ubuntu 18.04 package of Services Director combined with a Custom Instance Host, the recommendation is to choose Ubuntu 16.04 for the Instance Host. The reason is the incompatibility of Services Director with LXC v3.0 bundled with Ubuntu 18.04.

The following software packages also needs to be installed in the Ubuntu 16.04 Instance Host:

- OpenSSL 1.1 - At the time of writing this release notes, no packages for this available for Ubuntu 16.04. Users would need to build the libraries from source obtained from https://www.openssl.org/source/
- libpython2.7-dev (apt-get install libpython2.7-dev)

The *universal_v3* FLA license previously issued by Services Director was deprecated as of v2.5. Before upgrading to Services Director v18.3 from a version in which the *universal_v3* license is deprecated, ensure that your vTM instances have been relicensed to use the *universal_v4* FLA license. Failure to do this will result in the following message on upgrade:

Instance <instance_id> is using deprecated license 'universal_v3'

The controller (tmcm) REST API version has been revised to v2.8 to allow for various API changes. Throughout, backward compatibility has been maintained. New resources and additional properties introduced in this version do not invalidate or break existing scripts making calls to Services Director tmcm REST API v2.0.

5) Major New Features

Application Templates

Services Director now supports application templates that simplify and automate the configuration of vTMs for specific applications. Once a template has been installed, an instance of that template can be created with specific parameters (for example, certificates, node IPs) and applied to a vTM cluster. The template instance's parameters can also be edited afterwards. All the changes to the parameters are propagated automatically to the cluster when the changes are applied.

NOTE - Application templates are published and updated separately. Details are available in the Pulse Secure Knowledge Base at https://community.pulsesecure.net/.

vTM-SD Communications Channel

Services Director now supports a new vTM-initiated channel for communication between vTMs and Services Director. This allows Services Director to provide its full range of functionality for vTMs that cannot be routed to by Services Director (for example, because they are behind a NAT device). This feature will be used by default for self-registered vTMs where the vTM and Services Director versions are at least 19.1.

NOTE - Updates to the Services Director server certificate must be managed carefully when using the vTM-SD Communications Channel to avoid breaking connectivity with the vTM estate. A script to assist with this process will be available in the Pulse Secure Knowledge Base at https://community.pulsesecure.net/.

Automatic Removal of Inactive vTM Instances

Services Director can now automatically remove vTMs that have repeatedly failed monitoring from its records, complementing its ability to automatically accept new vTM registration requests. This feature is disabled by default.

Improved MySQL Replication Log Management

Services Director HA pairs now proactively remove database replication logs that have already been processed, reducing the likelihood of disk space running out for customers with large estates. The setting for the number of days to keep replication logs now only has an effect on non-HA Services Directors or when database replication has failed.

6) Security Vulnerabilities

Notable fixed vulnerabilities include:

- **SD-12325**: Upgraded *openssl* to 1.0.2r to address multiple CVEs.
- **SD-12960**: Both *curl* and *curlib* used by the Virtual Appliance have been upgraded to version 7.64.1, to fix CVEs associated with the previously used version 7.60.0.
- **SD-13292**: Fixed an internal API used by Services Director HA pairs for backup so that it no longer supports protocols affected by multiple CVEs.
- **SD-13593**: Upgraded *polkit* to version 0.96-11.el6_10.1 to address *CVE-2019-6133*, and upgraded *nss* to version 3.36.0-9.el6_10 to address *CVE-2018-12384*.
- **SD-13607**: Upgraded the Linux kernel to version 2.6.32-754.11.1 to address *CVE-2018-10902*.

7) Known Issues

- **SD-4023**: Poorly configured passwordless SSH may result in an error message containing 'Agent admitted failure to sign using the key' during some Instance Host operations. The passwordless SSH connection should be configured as described in the *Services Director Advanced User Guide*.
- **SD-4079**: Updating an FLA license for an Instance resource may fail due to FLA health checks but the resource status will remain 'Active' or 'Idle'. You should check the status of the 'pending_action' property (if one exists) instead of waiting for the Instance status to change to a failed state.
- **SD-4151**: Deployment of a managed instance in a cluster will fail if not all existing vTM instances are set to status 'Active'. Before creating a managed instance resource which uses a cluster resource, please ensure that all existing instance resources using that cluster resource are set to status 'Active'.
- **SD-5111**: In the Setup Wizard for a Secondary node, if authentication details are entered for one Primary node and then the user decides to join to a different Primary node, the join will fail. To work around this problem, run the CLI command **ssc high-avail token remove** before choosing a different Primary node.
- **SD-5321**: Non-printable and extended ASCII characters in resource names and resource property values may cause CLI command issues. Only use printable standard ASCII characters for resource names and resource property values.

- **SD-5382**: Deploying an instance using a legacy FLA license fails due to FLA health checks. On a software install, use the query parameter 'override_fla_check=true' to disable FLA health checks for that deployment. You can also disable FLA health checks globally for all deployments by settings the 'fla_check_enabled' property of the settings/fla_check resource to *false*.
- **SD-7090**: Restoring an instance backup from a cluster using a different FLA licence to the target cluster can result in multiple FLA licences being installed. If this situation is encountered, the user should use the **vTM System > Licences** page to remove any FLA licenses other than the one recorded for that vTM in the Services Director GUI. Note that this will only be a problem where the Services Director estate uses more than one FLA licence type. Users are advised to use the latest universal FLA licence.
- **SD-10434**: Sometimes a pool called "None" and a node called "None" may be displayed when exploring analytics data. These "None" entries represent traffic for which there was no pool or node. This can happen for a variety of reasons, such as a cached response being returned or the traffic being handled entirely by *TrafficScript*.
- **SD-10676**: Analytics searches cannot be performed for date ranges over 1000 days in length. The results of such searches will be truncated to 1000 days in length.
- **SD-10800**: Services Director software installs may require a MySQL configuration change. When a Services Director software installation is used in conjunction with a default MySQL installation of 5.6 or greater, the query cache must be activated in the MySQL configuration. If not already activated, this can be achieved by amending */etc/my.cnf* to include the following stanza, then restarting MySQL.

  [mysqld]
  query_cache_type = 1
- **SD-10829**: Adding a self-registered v17.3 vTM to a cluster will result in a vTM error and Services Director not knowing the new credentials for that vTM. To recover from this issue, correct the credentials for the affected vTM(s) on Services Director **vTM Instances** page.

- **SD-10843**: The Analytics Application component filter entries can be truncated for very large estates. The options shown in the component filter category dropdowns will be truncated where there are more than 50,000 combinations of country / cluster / vTM / vServer / pool / node to be found in the selected period of the transaction dataset. It is still possible to filter even on a category value missing from the component filter by either clicking on the equivalent category value in (for example) the tree view, or in a split line chart, or by using the advanced filter function and manually entering the desired value.
- **SD-11910**: Analytics Application Geo filter will show an empty entry when sampling excludes a previously filtered value from the dataset. When using a Geo filter in the component filters and then choosing a sampling ratio, the selected filter may no longer be available in the sampled dataset - this will show 'No data available' in all the charts. Please select an available value from the dropdown in this case.
- **SD-11964**: Spurious email warning when restoring a Services Director backup. Under certain circumstances, when restoring a backup of the Services Director the admin can receive an email warning of 'Crash of process x86_64'. This does not represent a problem and can be safely ignored. .
- **SD-11966**: Top 5 TIPs and Top 5 Pools charts mix connection and request avg. durations. Users may use the filter to limit the search to request-based vServers to see only average request durations, or to connection-based vServers to see only average connection durations. Alternatively, the line chart view allows users to select request or connection specific duration metrics.
- **SD-12553**: Analytics application guided tour does not work well in Internet Explorer 11. For the best experience of the Analytics Application guided tour users should open the application in another browser such as Chrome, Safari or Edge and re-select the guided tour.
- **SD-12558**: Upgrading a HA pair of Services Directors may require use of the **ssc database validation-err ignore** directive on the secondary node. When performing an upgrade of a Services Director HA pair, the user may be presented with an error message "Cannot validate service configuration or database. Please check log for details. Use command 'ssc database validation-err ignore' to override validation result and redo image install/upgrade.". If appearing on the second node to be upgraded, the warning can safely be disregarded and **ssc database validation-err ignore** used to allow the upgrade to progress. If appearing on the first node to be upgraded, it may indicate a problem with Services Director's inventory; users should consult Pulse Secure support in this case.

- **SD-12564**: The "Connection duration" metric in analytics application is called "Transaction duration" in the extended filter panel. Users of the analytics application Explore view wishing to perform filtering on the basis of connection durations should use the "Transaction Duration" field in the extended filter panel. The "Transaction Duration" field is equivalent to connection duration for connection-based vServers.
- **SD-12652**: Upgrading an HA pair directly from versions earlier than 17.1 to version 18.1 (or later) can fail to update internal passwords. Customers following affected upgrade paths should run the CLI command **ssc high-avail refresh-state** after the upgrade on the Primary node, and (once that is complete) also on the Secondary node. Note that standalone Primary nodes are unaffected by this issue.
- **SD-13043**: On first boot, admin password is sometimes not shown in AWS EC2 System Logs due to buffering of the logging by AWS. If the password is not shown in system logs, it can be obtained using CLI. SSH to the instance using the private key and type:

  enable
  configure terminal
  support show default-password
- **SD-13085**: Creating HA primary node after **ssc high-avail reset** leaves the Services Director service stopped. Restarting the Services Director service through **System > Service Status** or the **pm process ssc restart** CLI command will restore the services.
- **SD-13104**: Updated email settings do not get synchronised with peer node in the cluster. Updating email settings through **Email Alerts** page does not propagate those changes to peer node in the cluster. To work around this issue, update the email settings on the peer node as well.
- **SD-13108**: Disabling NTP and setting time manually causes Services Director service to terminate. To work around this issue, reboot the Services Director VA after changing the time.
- **SD-13109**: Correcting the incorrect AWS credentials entered using Setup Wizard still cause it to fail. If incorrect AWS credentials are entered into the setup wizard and setup fails, going back to the relevant step and correcting those credentials does not result in setup succeeding. To work around this issue, go back to the "Service Endpoint Address" step, enter a new IP address, and continue through the steps.

- **SD-13115**: Upgrading from versions older than 2.1r1 leaves Services Director service in a stopped state. After the upgrade, users need to create an SSC primary node using the **Create Primary** dialog box from the **Manage HA** page. Check the Services Director service status using the **Service Status** page. If the service is not running, start the service by clicking on the **Start** button.
- **SD-13729**: Attempting to relicense an uncontactable vTM using the Comms Channel gives a misleading message in logs: "Unable to access REST API at 127.0.0.1:9070". The IP address in this warning should be ignored.
- **SD-13802**: Days to keep replication logs and replication logs purge interval do not get synchronised with peer node in the cluster. Updating the "days to keep replication logs" and "replication logs purge interval" does not propagate those changes to peer node in the cluster. To work around this, update the replication logs settings on the peer node as well.

8) Deprecation Notices

Please note that the Services Director Instance Host Virtual Appliance has been deprecated. Affected customers should switch to using externally deployed vTM instances or custom instance hosts before upgrading to this version of Services Director.

9) Updated Functionality

- **SD-4163**: The SSL cipher list used by Services Director is now configurable via the CLI (on the VA) or via **configure_ssc** (for non-VA installations).
- **SD-13447**: The default MySQL replication log expiry time has now been changed from previous 3 days to 1 day. As before the value can be modified by a user **Diagnose > Data Storage Status**.
- **SD-13736**: Tools included for support have been improved to gather more useful filesystem information.

10) Fixed Functionality

- **SD-12552**: Fixed an issue where the comparative analysis chart allows a metric incompatible with percentiles to be selected while percentiles are enabled. A warning is now displayed when percentiles are enabled and the mouse is moved over an incompatible metric. If an incompatible metric is selected, the chart ignores the enabled percentiles.
- **SD-12581**: Fixed an issue where the downward-pointing triangle icons to indicate drop-down menus were missing from the analytics app. These icons now appear in the appropriate locations.
- **SD-12583**: Fixed an issue where, when showing two metrics, one of the line colours on the comparative analysis chart did not match the colour of the corresponding axis. The colour of each line now always matches the colour of the corresponding axis when two metrics are being shown.
- **SD-13057**: Fixed an issue where the **show ssc settings security** CLI command would show some incorrect field names and no corresponding values. Corrected field names are now shown, along with the corresponding values.
- **SD-13101**: Fixed an issue where the **ssc high-avail force-failover** CLI command always exited with the message "An internal error occurred".
- **SD-13220**: Fixed an issue where, in rare circumstances, emails about monitoring events were no longer sent and the list of vTM and Services Director instances being monitored would stop updating.
- **SD-13232**: Fixed an issue where a High Availability force-failover operation could appear to become stuck at "waiting for services to be operational" after failover, despite the services actually being operational. Force-failover operations will now no longer become stuck at this point if the services are operational.
- **SD-13289**: Fixed a defect where, for a Services Director with a large vTM estate, the Services Director service process could run out of available file handles. The number of file handles available to Services Director has been significantly increased.
- **SD-13578**: Fixed an issue where an upgrade from Services Director v2.6 or v2.6r1 could result in an incorrect set of features being enabled for pre-existing Feature Packs. For systems with *ENT-Enterprise* bandwidth packs, Services Director core software service could fail to start. Now the correct features will be enabled and the core software will not fail to start for this reason.

- **SD-13580**: Fixed an issue where multiple registration requests from the same vTM sent in a short period of time could cause a race condition in the Services Director resulting in excessive logging and registration entries. Now only the first registration request is logged and results in a registration entry.

11) Contacting Pulse Secure Support

Visit the Pulse Secure website to download software updates and documentation, browse our library of Knowledge Base articles and manage your account.

Go to https://support.pulsesecure.net/ to submit a support case online and for the latest telephone contact information.

Copyright © 2019 Pulse Secure, LLC. All rights reserved.