Pulse Secure Services Director: Release Notes

21.1

Copyright Notice

Contents

About this Release

Pulse Secure Services Director 21.1 is a feature release of the management tool for Pulse Secure Virtual Traffic Manager, which includes fixes for security vulnerabilities.

This release has been designated a Long Term Support (LTS) release. Full support for version 21.1 will be available for three years from the release date of 12 October, 2021. See the following End of Support and End of Engineering Schedule for more information: https://support.pulsesecure.net/product-service-policies/eol/software/vadc-services-director/.

Platform Availability

Services Director is supported on the following platforms:

- *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.

Resource Requirements

This section describes the resource requirements Services Director and the vTMs in its estate.

Software Environment - Pulse Secure Services Director

The required software environment for Services Director is described below:

- *Operating system:* Ubuntu 18.04 (x86_64), RHEL/CentOS 6 (x86_64)
- *Database:* MySQL 5.6, MySQL 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 Virtual Appliance

The required virtual environment for the Services Director VA is described below:

- *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:

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

Software/Virtual Environments for Deployed vTMs

The required software/virtual environment for deployed vTMs is described below:

- *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 above).
- *Externally deployed, VA:* Same as Pulse Secure Virtual Traffic Manager (17.2r2 or above)

Upgrades

Customers upgrading Pulse Secure Services Director Virtual Appliance on Amazon EC2 should follow the same steps as the other supported hypervisors but should use the upgrade image for VMware.

If a customer wishes to run the 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 need to be installed in the Ubuntu 16.04 Instance Host:

- *OpenSSL 1.1*: At the time of writing, no packages for this are available for Ubuntu 16.04. Libraries can be built with source code obtained from https://www.openssl.org/source/
- *libpython2.7-dev:* (apt-get install libpython2.7-dev)

The *universal_v4* FLA license previously issued by Services Director is deprecated, but will continue to work after upgrade. Customers are advised to relicense their vTMs with the newer *universal_v5* FLA license at a convenient time after upgrade.

REST API versions in this release remain the same as for release 20.1:

- tmcm API: v2.9
- sd API: v1.1

Major New Features

Services Director now restricts access to TCP ports which are meant to be used for internal use, by using a firewall. These ports are accessible by peers in a High Availability configuration, but are blocked for external access.

The ports blocked using the firewall are:

- 9070/9090: Internal vTM.
- 3306: MySQL server.

More information on this feature can be found in the *Pulse Secure Services Director Getting Started Guide*.

Security Vulnerabilities

Notable fixed vulnerabilties include:

Report Number	Description
SD-14184	Fixed an issue to address vulnerabilities due to not setting "secure" attribute for cookies.
SD-14192	Fixed an issue where one of the VA's API endpoints was vulnerable to path traversal attacks by logged in locally authenticated users. Note that the endpoint was not vulnerable to attacks from unauthenticated users and remotely authenticated users.
SD-14193	Fixed an issue where one of the VA's API endpoints was vulnerable to shell injection attack by logged in users. Note that the endpoint was not vulnerable to attacks from unauthenticated users.
SD-14202	Fixed security vulnerabilities due to outdated internal components telnet and IPMItool.

Known Issues

Known issues at this release are:

Report Num	Description
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-12558	Upgrading a HA pair of Services Directors may require the use of the **ssc database validation-err ignore** command 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 the 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 the **ssc database validation-err ignore** command 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 a 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-13085	Creating HA primary node after 'ssc high-avail reset' leaves Services Director service stopped. Restarting the Services Director service through "System->Service Status" or the CLI command "pm process ssc restart" will restore the services.
SD-13108	Disabling NTP and setting time manually causes Services Director service to terminate. To workaround this issue, reboot the Services Director VA after changing the time.

Report Num	Description
SD-13881	The following validation error can erroneously be seen when upgrading a Secondary Services Director from version 2.4r1: "% 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." It is safe to follow the indicated instructions to override the validation.
SD-13913	Executing the **ssc high-avail force-failover** CLI command on AWS can result in the following error: "% Failed to fetch operation status: Service endpoint IP address <IP> not raised on interface primary". Force failover can be successfully executed via the Services > Manage HA page of the GUI when logged in to your secondary Services Director."
SD-14000	Setting the SSL cipher list to contain only unsupported ciphers disables parts of the CLI and breaks Instances page. To workaround this issue, manually modify the file */opt/riverbed-ssc/conf/ssc_config.ini* to use the following default ciphers: ECDH+AESGCM:ECDH+CHACHA20:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:!aNULL:!MD5:!DSS:DH+AES256 Then, restart Services Director using the command: **pm process ssc restart**.
SD-14071	Services Director comms channel links to individual vTM instances can in rare circumstances become blocked. This is recognisable by repeated occurrences of "Error: Second connection attempt from <uid>" in the Services Director Log and a corresponding monitoring failure. The workaround for this problem is to restart the Services Director API (**System > Service Status > Restart** on the VA, see the *Services Director Advanced User Guide* for Ubuntu and CentOS).

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.

Updated Functionality

No updates to functionality are introduced in this release.

Fixed Functionality

This release contains the following fixed functionality:

Report Number	Description
SD-12094	Fixed an issue where universal FLA CA certificate was set to expire on 2025. This has been extended to 2031.
SD-14055	Fixed an issue where installation was broken on Ubuntu 18.04, due to mismatched configuration options.
SD-14167	Fixed an issue where the Comms Channel fails when master password is not saved to disk. Now the VA retries waiting for master password to be provided by the user, and correctly enables the Comms Channel.
SD-14183	Fixed an issue where poor time synchronization between Services Director and vTM instances could cause a FLA license server certificate validation error. Now the FLA license server certificate will be generated to have more lenient validity restrictions. The **Not Before** field is set to 1 day before the certificate is generated.
SD-14215	On AWS only, Services Director's built-in firewall (disabled by default in previous releases) is disabled on upgrade. AWS provides more suitable tools (for example, security groups) for blocking access to the Services Director VA's ports.
SD-14216	Fixed an issue where a message from "mysqldump" about needing the PROCESS privilege to dump tablespaces could appear during various operations, for MySQL version 5.7 or later. This message should now no longer appear.

Documentation

Ivanti documentation is available at https://www.ivanti.com/support/product-documentation.

For policy reasons, security issues are not normally mentioned in release notes. To find more information about our security advisories, see the security advisory page on the website.

Technical Support

For additional information or assistance, contact Global Support Center (PSGSC):

- https://support.pulsesecure.net
- support@pulsesecure.net
- Call 1-844-751-7629 (toll-free USA)

For technical support resources, browse the Pulse Secure Technical Support website https://support.pulsesecure.net.

Revision History

The following table lists the revision history for this document.

Revision	Revision Date	Description
1.0	12 April 2020	First release.