ivanti

Pulse Secure Services Director Virtual Appliance: Release Notes

21.1r1

Contents

About this Release

Pulse Secure Services Director Virtual Appliance 21.1r1 is a maintenance release of the management tool for Pulse Secure Virtual Traffic Manager, which includes fixes for security vulnerabilities.

This is a Virtual Appliance (VA) only release, with no changes to Services Director Ubuntu/CentOS software editions.

Platform Availability

Services Director VA is supported on the following platforms:

- *VMware ESX / KVM:* as a virtual appliance.
- *Amazon EC2:* as a virtual appliance or native software install.

Resource Requirements

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

Virtual Environment - Pulse Secure Services Director Virtual Appliance

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

- *Hypervisor:* VMware vSphere ESXi 6.0/6.5/6.7/7.0, 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:

- *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.

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 21.1:

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

Major New Features

No major features are introduced in this release.

Security Vulnerabilities

Notable fixed vulnerabilities include:

Report Number	Description
SD-14230	Upgraded apache httpd to 2.4.51 to address CVE-2021-40438

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-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.
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.

Report Num	Description
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 VA.

Updated Functionality

No updates to functionality are introduced in this release.

Fixed Functionality

No fixes are included in this release.

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	5 November, 2021	First release.