Pulse Secure Services Director Release Notes

Supporting Pulse Secure Services Director 20.1

Product Release	**20.1**
Published	**15 April 2020**
Document Version	**1.0**

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

www.pulsesecure.net

Pulse Secure Services Director 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 Services Director v20.1 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.

This release has been designated a Long Term Support (LTS) release. Full support for version 20.1 will be available for three years from the release date of 15th of April 2020. 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 VA

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)4) Upgrades Customers upgrading their Services Director Virtual Appliances on Amazon EC2 should follow the same steps as the other supported hypervisors but should use the upgrade image for VMware.

Upgrades

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 need to be installed in the Ubuntu 16.04 Instance Host:

- *OpenSSL 1.1*: At the time of writing, no packages for this available for Ubuntu 16.04. Libraries can be built with 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 19.1r1, ensure that any universal FLA licensed vTM instances using *universal_v3* or earlier have been relicensed to use the *universal_v4* license. Services Director version v2.5 supported both *universal_v3* and *universal_v4* and may be used to perform this relicensing if upgrading from an earlier version Failing 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 v2.9 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.

The Services Director ("sd") REST API version has been revised to v1.1 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 "sd" REST API v1.0.

New Major Features

There is a single new feature in this release. (see below)

Encrypted LDAP (LDAPS and STARTTLS) Administration Authentication

The user and password needed to login to Services Director's administrative interfaces can now be protected while being sent to an LDAP server configured in a LDAP authenticator. A new option ("ssl" in the REST API and CLI, "Secure connection method" in the GUI) can be used require that connections to a remote LDAP server are SSL-encrypted using either the STARTTLS or LDAPS mechanism. The Certificate Authority used to issue the certificate presented by the LDAP server must be added as a new "Certificate Authority" resource in order for the required server identify checks to succeed.

Services Director also supports configuring the same setting for vTM authenticators and adding vTM certificate authorities, to be applied to vTMs as part of access profiles. Only vTM version 20.1 onwards supports encrypted LDAP.

Security Vulnerabilities

Notable fixed vulnerabilties include:

Report Number	Description
SD-14087	The **sudo** and **freetype** packages on the Services Director VA have been upgraded to fix *CVE-2015-9382*, *CVE-2015-9381*, *CVE-2019-18634* and *CVE-2019-14287*.
SD-14089	The Services Director VA's kernel has been upgraded to *kernel-2.6.32-754.27.1.el6* to fix multiple CVEs.

Known Issues

Known issues at this release are:

Report Number	Description
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 unless 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 workaround 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; wherever possible, users are advised to use the latest universal FLA licence.

Report Number	Description
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 version 17.3 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's **vTM Instances** page.
SD-10843	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 avgerage 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.

Report Number	Description
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-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 run the **enable configure terminal support show default-password** command.
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-13104	Updated email settings do not get synchronised with peer node in the cluster. Updating email settings through the **Email Alerts** page does not propogate those changes to peer node in the cluster. To workaround this, 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 workaround this issue, reboot the Services Director VA after changing the time.
SD-13115	Upgrading from versions older than 2.1r1 leaves Services Director service in 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-13496	Application Templates can only be applied to vTMs of version 18.3 or later. To workaround this issue, use vTM version 18.3 or later.
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	The 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 propogate those changes to peer node in the cluster. To workaround this, update the replication logs settings on the peer node as well.

Report Number	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 */opt/riverbed-ssc/conf/ssc_config.ini* file to use the default ciphers (ECDH+AESGCM:ECDH+CHACHA20:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:!aNULL:!MD5:!DSS:DH+AES256), and restart Services Director using **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

Fixed functions at this release are:

Report Number	Description
SD-12905	Fixed an issue where LDAP-based authentication would fail when the LDAP server returned a referral. Services Director now ignores referrals, matching the behaviour of vTM.
SD-13217	Fixed an issue where, when deploying the Services Director OVA, the following warning message appeared: "No manifest entry found for: 'image-file1.nvram'." This message should no longer appear.
SD-13739	Fixed an issue where manually deleted Services Director deployed ("managed") vTM instances do not get removed by auto-purging mechanism. Now such vTM instances are automatically purged as expected.
SD-13865	Fixed an issue where Services Director would fail to store vTM backups over approximately 4MB in size. Such backups are now successfully stored.
SD-14019	Fixed an issue where the bandwidth allocation chart on the **Home** page of the Services Director UI could show incorrect data due to inconsistent capitalisation of feature pack names. This issue has now been fixed so that the correct data will be shown even when there is inconsistent capitalisation.
SD-14065	Fixed an issue where the Services Director RPM package (for CentOS) did not declare its dependency on OpenLDAP. This package now correctly declares its dependency.
SD-14108	Fixed an issue where Services Director authenticators created via the GUI were enabled by default. Now, they are only enabled if the **Enabled** checkbox is checked.
SD-14109	Fixed an issue with Services Director authenticators where the "Test and Save" functionality in the GUI would always enable the authenticator after a successful test. Now authenticators are only enabled upon "Test and Save" if the **Enabled** checkbox is checked.

Documentation

Pulse Secure documentation is available at https://www.pulsesecure.net/techpubs.

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 Pulse Secure website.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@pulsesecure.net.

Technical Support

For additional information or assistance, contact Pulse Secure 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	15 April 2020	First release.