Server Automation

Software Version: 10.60

Release Notes

Document Release Date: October 23, 2017
Software Release Date: October 23, 2017

Hewlett Packard Enterprise

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to: https://softwaresupport.hpe.com/.

This site requires that you register for an HPE Passport and to sign in. To register for an HPE Passport ID, click **Register** on the HPE Software Support site or click **Create an Account** on the HPE Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HPE sales representative for details.

Support

Visit the HPE Software Support site at: https://softwaresupport.hpe.com.

This website provides contact information and details about the products, services, and support that HPE Software offers.

HPE Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support website to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HPE Support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HPE Passport user and to sign in. Many also require a support contract. To register for an HPE Passport ID, click **Register** on the HPE Support site or click **Create an Account** on the HPE Passport login page.

To find more information about access levels, go to: https://softwaresupport.hpe.com/web/softwaresupport/access-levels.

HPE Software Solutions Now accesses the HPESW Solution and Integration Portal website. This site enables you to explore HPE Product Solutions to meet your business needs, includes a full list of Integrations between HPE Products, as well as a listing of ITIL Processes. The URL for this website is https://softwaresupport.hpe.com/.

Contents

Release notes

This document provides an overview of the HPE Server Automation 10.60 release. It contains the following important information not included in the manuals or in the online Help.

What's new in Server Automation 10.60

Server Automation 10.60 includes the following new features, enhancements, and support changes:

Added features

Feature	Description
Autopass Integration	SA is now enabled with HPE AutoPass licensing, allowing you to track the capacity utilization of the current SA license model with respect to the number of SA Agent managed servers. For more information, see **AutoPass licesing** section in the Adminstration Guide. **Important:** Since SA is enabled with HPE AutoPass licensing, ensure that you have enough licenses available for the number of SA Agent managed servers in your business environment.
Support for importing content from SUSE network using SMT	You can now import the content from SUSE network using Subscriptions Management Tool (SMT). For more information on how to set up and use the new HPE SA SMT Import tool, see **Patch Management for SLES** in the SA 10.60 User Guide.
Support for external Public Key Infrastructure (PKI)	You can now use certificates issued by an external Certification Authority (CA) for encrypting the communication between the SA Core components and the SA Agents. This offers a high-security alternative to the existing workflow of using self-created certificates signed by SA's internal CAs. To switch to the new external PKI mode, upgrade your SA core and Agents to 10.60, then run a Core recertification job. This will replace the self-signed certificates with third-party ones. For more information, see the **Use SA in third-party certificate mode** section in the SA 10.60 Administration Guide.
Additional parameters for SA Core installation	When installing an SA Core, the installation interview now also asks you to specify a certificate mode for SA. You can choose to install the SA core either in **self-signed** certificate mode or in the new **third-party** certificate mode. In third-party certificate mode, SA generates Certificate Signing Requests (CSRs) for all SA core components. Submit these CSRs to your CA for signing and resume the core installation when all signed

Feature	Description
	certificates are available at your specified location. For more information, see the **Core Installation** section in the SA 10.60 Installation Guide.
Migration to WildFly 10.1.0	The JBoss community has recently stopped support for WildFly 8.2.1, the WildFly version used in SA 10.50 and 10.51. To avoid any possible security vulnerabilities, the SA Application Server has been upgraded to use WildFly 10.1, the latest version of WildFly.
Updated Service OS	SA 10.6 updates Linux 6 and Linux 7 Service OS for network and CD boot.
New for APX Framework	Starting with SA 10.60, PHP version bundled in SA is 5.6.30. This version is backwards compatible with previous version 4.4.8. Nevertheless, if you find issues when running existing APX-es, written in php 4.4.8, verify the PHP documentation at http://php.net/manual/en/migration5.incompatible.php
Configuration parameter	Starting with SA 10.60, Configuration Parameter `swprov.ui.default_supress_reboot` has been replaced with `remediate.default_reboot_behavior`, which can be used to control the reboot process more accurately. This parameter is also available for remediate and install patch jobs in addition to install software jobs. For more information, see **Set reboot options for remediation** in the SA 10.60 User Guide.

DCA COSO Reporting for Server Automation

DCA COSO Reporting for Server Automation provides reporting capabilities using COSO and Business Value Dashboard (BVD). DCA COSO Reporting can be used as an alternative to OBR for reporting Server Automation operational and historical data. You can use the metrics that are present in COSO to create custom reports and view them using BVD or any other business intelligence tool. The DCA COSO Reporting solution is available with the Independent and Mixed mode deployment.
For more information, see DCA COSO Reporting for Server Automation documentation.

Added support

The SA 10.60 provides support for:

- Windows Server 2016
- RHEL 6 HPC
- RHEL 7 HPC
- RHEL 7 Power(BE)
- SLES 12 s390X
- ESXi 6.5
- AIX 7.2
- Ubuntu 16.04 LTS

For more information, see the SA 10.60 Support and Compatibility Matrix.

Enhancements

SA 10.60 includes the following enhancement requests, implemented after the release of SA 10.51.

ID	Component	Summary	Added in version
QCCR1D119311	OCC Client Framework	Support for HPSA clients under Citrix	10.60

Fixed defects

The following table includes all the defects fixed after the release of SA 10.51.

ID	Component	Description
QCCR1D236198	Global Filesystem/Shell Backend	**FIX**: SA install fails on RHEL 7.3 during adapter build at file_remove_suid function.
QCCR1D218368	Gateway	**FIX**: Egress ephemeral port reuse can cause a slice to become registered in a non-TRANSITIONAL realm.
QCCR1D226680	Patch Management Backend	**FIX**: rhn_import fails "urlopen error [Errno 8] _ssl.c:504: EOF" occurred in violation of protocol.
QCCR1D229896	Patch Management Backend	**FIX**: rhn_import converts RedHat packages containing "++" characters in filename to spaces during import.
QCCR1D227516	Software Management Tools	**FIX**: Import from RHN fails with "Package download error: Cannot get package download link for..."
QCCR1D230853	Twist (Web Services Data Access Engine)	**FIX**: Twist hang randomly because of JBOSS deadlock.
QCCR1D231477	Software Management Backend	**FIX**: Rollback points not working "The RPM rollback point object cannot be found".
QCCR1D232532	Twist (Web Services Data Access Engine)	**FIX**: ComplianceTestDevices ejbs are loaded excessively during findAuditTaskRefs calls.
QCCR1D233530	Way (Command Engine)	**FIX**: Automate Communication Test aborts due to KeyError.
QCCR1D234328	Software Management Backend	**FIX**: Device counts in opsware.swprov.chunker results <global_phase_dict> are not calculated correctly.
QCCR1D234335	Jobs Backend	**FIX**: Range disagreement for "long" and "int" datatypes between lcxmlrpclib (python) and redstone (java) XMLRPC implementations.

ID	Component	Description
QCCR1D236745	Jobs UI	**FIX**: Ability to select policies for a group of servers.
QCCR1D233263	OCC Client Framework	**FIX**: occ.server startup times out with the message: "WARN OCC start-up exceeded wait limit".
QCCR1D230028	Library Framework	**FIX**: Scalability chokepoint around LibraryTableCacleEventHandler's use of "contains" method against ColumnTableModel's List.
QCCR1D229027	Virtualization Backend	**FIX**: vCenter data reload fails if a virtual machine has network interfaces with VLANs.
QCCR1D195041	Agent	**FIX**: Unicode characters outside the ASCII codeset from server scripts are replaced with "?" (question marks).
QCCR1D229028	Agent	**FIX**: bs_hardware fails to obtain CPU cache information for VMs hosted on XenServer.
QCCR1D227112	Way (Command Engine)	**FIX**: Way-to-way commands do not adhere to the new soft maximum timeout semantics.
QCCR1D230804	Twist (Web Services Data Access Engine)	**FIX**: Audits are failing to start after running a large number of SMO based audit jobs.
QCCR1D232077	AAA	**FIX**: twistclient logout audit event not recorded in the database.
QCCR1D233738	Twist (Web Services Data Access Engine)	**FIX**: CacheFullException or performance issues when running the attach_import_patches_to_policies.pyc.
QCCR1D236746	Jobs UI	**FIX**: Ability to select policies for a group of servers.
QCCR1D235440	Software Management Backend	**FIX**: Not able to create recommended patch policy for Solaris 11.3 server.
QCCR1D236704	Software Management User Interface	**FIX**: Importing RPM package library changes the file name displayed in the SA client.
QCCR1D236116	DCML Export Tool (DET)	**FIX**: Certain CBT functionalities stop working after 24 hours because of token expiration.
QCCR1D236272	OCC Web	**FIX**: OCC's SOAP/XML interface emits java.util.ConcurrentModificationException under high concurrent access.
QCCR1D230952	Spin (Data Access Engine)	**FIX**: Spin Python process takes up all RAM memory.

ID	Component	Description
QCCR1D236119	DCML Export Tool (DET)	**FIX**: CBT import nested audit policies fails when child policy already exists and import policy is set to "skip".
QCCR1D224584	Patch Management Backend	**FIX**: SLES remediation with Zypper may choose an older kernel to install.

Known issues, limitations, and workarounds

The 10.60 release of SA has the following known issues and limitations.

ID	Area	Description
QCCR1D240343	Certificate	Gateway recertification fails during core recertification from third party to legacy certificate mode.
QCCR1D240498	Certificate	In phase 13 of Core recertification, not all certificates and secret keys are removed. **Workaround**:Old certificates and secret keys should be removed.
QCCR1D240611	Certificate	Self-signed agent certificates are issued with 8 years of validity instead of 10 years of validity. **Workaround**:Manually update the validity period in the database by running the following command on the SA Core: `/opt/opsware/bin/python -m opsware_common.config_editors update spin --name "spin.cogbot.crypto_validity_period" --value 3650 .`
QCCR1D240649	Certificate	Recurring jobs are failing after recert phase 9.
QCCR1D240974	Installer (OI)	CA certificates in the components folder are not removed by upgrade process on satellites. **Workaround**: Remove the following files from the satellite servers once the upgrade is completed: • /var/opt/opsware/crypto/wordbot/admin-ca.crt • /var/opt/opsware/crypto/wordbot/agent-ca.crt • /var/opt/opsware/crypto/wordbot/opsware-ca.crt • /var/opt/opsware/crypto/wordcache/admin-ca.crt • /var/opt/opsware/crypto/wordcache/agent-ca.crt • /var/opt/opsware/crypto/wordcache/opsware-ca.crt

ID	Area	Description
CCR1D241194	Certificate	Agent certificate generator test from SysDiag fails after core recert with omit_self_signed_ certificates set.
QCCR1D241696	Installer (OI)	Resumed core installation updates **security.conf** to default values **Workaround**: Add the *fips.mode*, *crypto.hash_ algorithm* and the *crypto.key_length* parameters in the cdf.xml file used for the resumed install. You can find the correct values for these parameters in the `/etc/opt/opsware/crypto/security.conf` file.
QCCR1D242476	OO Integration	In SA-OO integration, an invalid OO URL exception is thrown when running the approval flow.
QCCR1D242342	Manage Platform	Multiple Vendor Recommended Patch Policy for the same Windows platform are available after SA is upgraded to the version 10.60.
QCCR1D242507	Patch Management Backend	Ubuntu 14.04 Dynamic Patch Policy remediation appears as failed.
QCCR1D239007	Patch Management	Package install does not work by default in Ubuntu 16.04. **Workaround**: Install **python** and **python-apt** packages on the target managed server to enable the install package functionality.
QCCR1D237482	Data migration	System Diagnostics jobs created prior to the SA10.60 upgrade fail with the following error message: "Invalid component buildmgr specified Valid components are :['truth', 'spin', 'word', 'way', 'vault', 'twist']" This is expected behavior, since the Build Manager component is no longer included in SA 10.60 and later. SA required this component only for executing OS Sequences, which have been completely replaced by OS Build Plans.
QCCR1D238059	Installer	Upgrading a Mesh to SA 10.60 after a CORD patch rollback fails if the *crypto.hash_algorithm*, *fips.mode* or *crypto.key_length* parameters do not have the default values.

ID	Area	Description
		Workaround: Add the *fips.mode*, *crypto.hash_algorithm* and the *crypto.key_length* parameters in the cdf.xml file used for the upgrade. You can find the correct values for these parameters in the `/etc/opt/opsware/crypto/security.conf` file.
QCCR1D239221	Installer (OI)	When adding slices to a core, the CSRs for the new slices are generated with default values for the *crypto.key_length*, *crypto.hash_algorithm* and *fips.mode* parameters **Workaround**: Add the *fips.mode*, *crypto.hash_algorithm* and the *crypto.key_length* parameters in the cdf.xml file used when adding the new slices. You can find the correct values for these parameters in the `/etc/opt/opsware/crypto/security.conf` file.
QCCR1D238186	Automation Platform Extensions (APX)	By default, when working in **third-party** certificate mode, you cannot use the BRDC HPSA agent sanitizer APX. This limitation is due to the recent changes introduced in the SA Agent Install flow which accommodate the new third-party certification mode. **Workaround**: When working in **third-party** certificate mode, set the *spin.agent.bootstrap_enabled* parameter to `1`. This allows SA Agents to register with the SA Core using the Bootstrap certificate. You can then replace this SA self-signed certificate with a third-party one. For more information see **Self-signed temporary SA Agent certificates** section in the SA 10.60 Administration guide.
QCCR1D239214	Product Functionality	Secondary Core installation fails when trying to connect to a primary Core that uses Oracle Database 11g. This error occurs if the secondary Core you are installing is using SA 10.50 and later. These versions install Oracle Database 12c for all the SA Cores. Ensure your secondary Core is using the same database version as the one on the primary Core.
QCCR1D238686	OS Provisioning	You cannot provision Windows operating systems using static UI.

ID	Area	Description
QCCR1D237353	Installer	You cannot upgrade to SA 10.60 if the SA Core's existing certificate is MD5 base. **Workaround**: Recertify the SA Core to use a different signature algorithm.
QCCR1D238614	Product Functionality	Core Recertification fails in mesh environments when any of the Satellites connected to a 10.60 Core use a previous SA version.
QCCR1D233169	Patch Management Backend	Some failed patch installations may show up as successful although they have been rolled back during server reboot. **Workaround**: Always check the **Patch Compliance** page of the **Job Status** window to make sure you are getting the correct result for your remediation job.
QCCR1D159841	Software Management Backend	When upgrading a Core, SA may show UNITS and REALM_UNITS tables conflicts. **Workaround**: Resolve conflicts manually or use the Force Resolver script then continue with the upgrade. To minimize the number of model repository conflicts, run all operations on units through the master spin.
QCCR1D151092	Patch Management	Duplicated patches exist between HPLN Patches and WSUSSCN2.CAB Patches. **Workaround**: A hotfix is available on the HPE support site.
QCCR1D161961	Patch Management Backed	The uninstallation of SP1 on Windows 2008 R2 fails with timeout. **Workaround**: No workaround; the issue corrects itself with the next scan.
QCCR1D162337	Patch Management	The W2k12 software policy remediation fails with the error, "`AGENT_ERROR_PATCH_DATABASE_CERTIFICATE_ERROR`". **Workaround**: Import and run the latest Microsoft patch CAB file.
QCCR1D147304	Patch Management	The second recommended binaries for KB979309 and KB2416400 are not shown as recommended binaries in SA, but are available in scanpatchoutput.

ID	Area	Description
QCCR1D223544	Patch Management	The *com.hp.sa.patching.ubuntu.importer.deb.pre_approval_path* parameter is not used during the package import.
QCCR1D131674	Patch Management Backend	The services of Create Solaris Patch Policy exposed through the API do not validate the Platforms added.
QCCR1D163518	Software Management UI	Server remediation is completed but the job is still in progress.
QCCR1D193587	Agent Deployment/Upgrade Backend	Cannot deploy IPV6 enabled servers with ADT; the scan shows SSH port is not available.
QCCR1D92244	Search Backend	Searching on extended ASCII (that is European) characters returns no matching results.
QCCR1D192728	Agent Deployment/Upgrade UI	Error message appears in NGUI when scanning ranges using * or /24 (CIDR) notations.
QCCR1D192013	Server Module (SMO) Backend	Windows Local Security Settings SMO reports incorrect Security Settings for Not Applicable entries.
QCCR1D183967	Audit & Compliance Backend	User and Group Snapshot Remediation Error (in both Windows and Unix systems).
QCCR1D193063	Server Module (SMO) Backend	SMTool upload fails when /var/tmp folder is not present on the twist box where the command is run.
QCCR1D151552	Audit & Compliance UI	Server Compliance View: Skipped server displays "Policy has changed since the last scan" when there has been no change in policy.
QCCR1D166350	Work Load Manager	Job stuck in Active status while its task is Successful.
QCCR1D203515	Installer (OI)	Word can complain about tens of missing files in case of multislice environment on top of a custom LVM partitioning.
QCCR1D224267	Installer (OI)	Giving custom realm_name to a satellite [different from facility name] breaks functionality.
QCCR1D227522	Installer (OI)	Slices do not show the right SA version in the NGUI client.
QCCR1D227998	Installer (OI)	Additional slice installation fails if there are recurring jobs configured.

ID	Area	Description
QCCR1D232581	Installer (OI)	Variables in kickstart file on Satellite (ks-linux6SERVER-X86_64-ogfs.cfg) are not replaced.
QCCR1D188553	Truth (Model Repository)	SA installed Oracle RDBMS modifies file `/etc/sysconfig/selinux` and inserts entry for SELINUX regardless of whether a previous entry exists.
QCCR1D232666	Agent	Rolling back an SA patch causes cert.pem from OPSWopenssl to be deleted.
QCCR1D193091	Gateway	After upgrading core from 10.0 to IMR2, the 10.0 satellite is unreachable.
QCCR1D184455	Certificate	Core Recert on FIPS enabled core will cause buildmgr to fail starting after phase 9.
QCCR1D184908	Certificate	In multiple slices mesh environment without satellite, run corerecert -s after run core recert -phase, shows Core recert session not in progress.
QCCR1D189612	Certificate	`cleanup_old_opsware_ca` should include remove old certifcate files from crypto.0
QCCR1D189893	Certificate	For Primary Core Infrac only non slice box, certficate in word_upload directory are not recerted.
QCCR1D194366	UCMDB	SA - UCMDB integration does not load SA data correctly when UCMDB server is configured in multi-tenancy mode.
QCCR1D191478	Manage Platform	CentOS 7 Build Plan fails with TypeError after migration from SA 10.02 with platform installed to SA 10.2.
QCCR1D232004	Manage Platform	The Deploy VM job fails on Windows Server 2016 x64.
QCCR1D131725	Patch Management Backend	The services of Create Solaris Patch Policy exposed through API do not validate the platforms added.
QCCR1D181473	SAV (Server Automation Visualizer)	SAV does not show IPv6 Inet addresses or IP address for loopback
QCCR1D111925	APX	Copy Configs APX does not give a user understandable message when target directory does not exist.

ID	Area	Description
QCCR1D160891	Virtualization UI	Cannot delete VMs in a life-cycle state "Build Failed".
QCCR1D142522	DCML Export Tool (DET)	CBT full export hangs.
QCCR1D160408	HPUX Virtualization-HPVM Frontend	Search with IP Address or Hostnames on Add Virtual Server screen does not list HP-UX machines.
QCCR1D183608	Virtualization Backend	Floating IP for OpenStack servers is not present in the list of IP interfaces.
QCCR1D209175	Patch Management Backend	MS Patch DB import status in SA Client may not reflect the actual status.
QCCR1D229895	Patch Management	When importing RedHat 6 rpms using redhat_ import, any "++" characters available in the package title are converted to spaces. This leads to the following error when trying to apply patches: "An error occurred while installing or removing this package. The package may not be applicable to the selected server. Parameters: results: {0} package: {1} command: {2} Action: Ensure that the package is correctly defined and applicable to the selected server. If the problem persists, please contact technical support".
QCCR1D179480	Software Management Backend	The tokens used by recurring application configuration compliance jobs have a limited lifetime of one year. This causes the recurring jobs to stop working without a warning.
QCCR1D219299	Product Functionality	Cannot install/update HP-UX operating environments through SA patching mechanism.
QCCR1D220924	Patch Management Backend	MemoryError exception raised when remediating HP-UX managed servers.
QCCR1D93690	Storage DB Scanner	For Application (Database) created on Virtual Machine, SAN relationship (SAN Fabrics, Switches) information is displayed, but for Virtual Machine, SAN relationship (SAN Fabrics, Switches) is blank.
QCCR1D105953	Storage Host Agent (storex)	On RHEL 5.4 x64 (8 GB/s HBA Card), Filesystem and Manager Software panels are blank and in OGFS FileSystem and Services Folders are NOT present.

ID	Area	Description
QCCR1D219299	Software Management Backend	Unable to install/update HP-UX operating environments through SA patching mechanism.
QCCR1D112384	APX	It is not possible to turn on debug logging in apx.c.
QCCR1D191511	Truth (Model Repository)	Oracle RAC Connection Failover is not transparent.
QCCR1D172654	OCC Web	SA 10.0 installer should validate `/etc/hosts` against multiple 'localhost' definitions.
QCCR1D202377	Installer (OI)	CORD installer does word_uploads before patch_opsware.
QCCR1D209907	Installer (OI)	The installer should be more idempotent to restarts and failures.
QCCR1D222141	Installer (OI)	Tsunami not enabled for Satellites upgraded from SA 9.1x.
QCCR1D157372	Patch Management	SA displays incorrect message when it tries to remediate HP-UX server (without custom attribute).
QCCR1D213724	Installer (OI)	Secondary Core installation error - Failed to determine data pump dir.
QCCR1D156389	Server Module (SMO) Backend	Windows Users and Groups SMO do not work on Windows 2012 Essentials.
QCCR1D157228	Patch Management Backend	Install of Q2416400 failed with exit code 4 when reboot was suppressed in the remediation job although the patch was actually installed.

Server Automation version history

This table lists the new features, enhancements, and fixed defects introduced in previous SA 10.x releases.

Feature	Area	Description	Introduced in version
Migration to OpenJDK		Oracle JDK has been migrated to OpenJDK. Now, SA will run its Cores and Clients using OpenJDK.	10.51
Integration with Windows Server Update Services (WSUS)	Patch management	SA can now connect to a WSUS server on your network to retrieve Microsoft patches from a central Windows patching repository. This adds an alternative workflow to the standard way of importing Windows patches from HPELN and Microsoft's offline catalog of updates. For tightly secured environments that cannot access the internet, switch SA to the new WSUS patching mode to pull in Windows updates from a custom WSUS repository in your network. The new WSUS patching option is available under **Patch Administration** > **Patch settings** and it connects SA to a Web service that you deploy on the WSUS machine. The SA-WSUS Web service connection supports both HTTP and HTTPS requests. Your selected patching mode applies to all the managed servers in the SA mesh. This means that you cannot target only specific servers for WSUS patching and keep others under Offline Catalog patching. **Note:** The populate-opsware-update-library and the live-network-connector scripts are still specific to Microsoft Offline Catalog patching and do not run in WSUS patching mode. For more information on the WSUS patching mode, see Importing the Windows patch database from WSUS in the SA User Guide.	10.51
SELinux support for RHEL 6.8 and RHEL	Managed Platform Support/OS	SA Agents running on RHEL 7.x managed servers now integrate with Systemd service. To use SA SELinux policies on RHEL 6.8 and RHEL 7.x managed servers, update the SA Agent to the 10.51 version. SA Agents using Systemd benefit	10.51

Feature	Area	Description	Introduced in version
7.x	Systems Support	from separate Start/Stop commands. For more information, see Starting and stopping the SA Agent in the SA User Guide.	
Windows operating systems supported on the SA Client	Managed Platform Support/OS Systems Support	Following operating systems are supported on the SA Client. • Windows Server 2008 R2 • Windows 7 • Windows 8 • Windows 8.1 • Windows 10 • Windows Server 2012 • Windows Server 2012, R2	10.50
New Linux Service operating system		The new Linux Service OSs provided with SA 10.50 is based on CentOS. Service OS (SOS) bits are not available for the PPC and IA processor architectures in the current distribution. In case of an upgrade, the existing RHEL IA and PPC Service OS bits will not be removed. The existing RHEL x86/x64 bits will be renamed, adding 'rpmsave' to the original name. If you want to reuse these bits, restoration can be performed by replacing the **linux50/linux60/linux60x64** folder with **rhel50rpmsave/rhel60rpmsave/rhel60x64rpmsave**, at this path: **/opt/opsware/boot/tftpboot/** and **/opt/opsware/boot/kickstart/**. If you are performing a new installation, there will be no Linux Service OS for these two processor architectures. SE Linux is supported in Permissive or Enforcing modes for RHEL 6.6. F	10.50
Configured debugging	Agent	You can configure debugging for ptymonitor through the ptymonitor.debug_name parameter in the agent's configuration file, agent.args.	10.50
Disabled RC4		RC4 has been disabled for SSL encryption.	10.50
Importing users		The new custom attribute **hpsa_preserve_solaris_user_home_path** allows you to import users using your user-home path in **/home/…**. In previous SA versions, the import tool added **/export** to the path.	10.50

Feature	Area	Description	Introduced in version
		To exclude the **/export** addition to the path, set the custom attribute to managed server.	
Changes made to the Agents installed on a non-system drive		For agents installed on a non-system drive (a feature available from SA 10.21 for Windows platforms), the agent uninstaller removes symbolic links on the system drive and all agent files, except the target directory.	10.50
Selecting PAPXs after Agent installation		Using ADT (Agent Deployment Tool) you can select a maximum of 10 PAPXs to be run sequentially after the agent is successfully installed. If one of the APX scripts fails, the system stops at that step, and does not run the remaining APXs, and reports the job as FAILED. Three PAPXs are included for the following functionality: • Assign Server to Customer • Attach Server to Device Group • Attach Server to Software Policies	10.50
New features	OS provisioning	• New Run OS Build Plan UI. • Support for deploying platforms on UEFI with secure boot enabled on HPE ProLiant. ◦ New Linux 7 service OS with network and CD boot support for Legacy BIOS, UEFI and UEFI with secure boot. ◦ New WinPE4 service OS with network and CD boot support for Legacy BIOS, UEFI and UEFI with secure boot. • New UAPI to allow the creation of customized pre-unprovisioned servers. See ServerService.create (ServerVO vo, ServerHardwareVO hwVO). • Content SDK to help customers with the development and deployment of Build Plans. For more details see the documentation under /Opsware/Tools/Content SDK/ContentSDK-<version>.zip.	10.50
Updates		• ProLiant content upgraded to Insight Control Server Provisioning 7.5.1. • WinPE 3 and 4 based service OS drivers updated.	10.50

Feature	Area	Description	Introduced in version
New platforms supported by build plans		• Solaris 10 SPARC • Solaris 11 SPARC • Windows 10 • SLES 12 • Ubuntu 14.04 • Novel OES 11 For all platforms, OS Sequences are deprecated in SA 10.50 and later. The migration of any existing OS sequences to OS Build Plans for these platforms is strongly recommended.	10.50
RPM Rollback	Software Management	SA 10.50 introduces RPM rollback functionality based on yum history, available for yum versions 3.2.25 or later. In previous releases the RPM rollback functionality was only available on Linux servers where the installation was done using RPM versions 4.2 to 4.6, but the upstream feature was discontinued	10.50
Unit history		Starting with SA 10.50, all changes made to the units in the SA Library can be tracked using the new History element. The logged information includes name, description, platforms, location, install path, scripts, and flags	10.50
Timeout handling for remediation and installation jobs		Server Automation now offers improved timeout handling for remediation and installation jobs. After a timeout occurs and until the job execution stops, the status of the server is changed to Stopping. While in the Stopping state, the agent does not take on any additional jobs and completes any job that is currently in progress. Moreover, if the timeout occurs during an agent reboot, then after restarting, the agent will not resume the job. After the job execution stops, the server will be marked as Timed Out. This fixes the discrepancy of the core showing the job as Failed because of a timeout, while the agent is performing the job.	10.50
Job enhancements		Software remediation jobs now support a secondary expansion mode **At runtime** for device groups, software policies, and patch policies. This way, when a remediation job is scheduled to run in the future, the device groups, software policies, or patch policies are expanded when the job is started, compared to previagents installed on a non-systemous releases where the expansion was done at the	10.50

Feature	Area	Description	Introduced in version
		time the job was created.	
SPARC provisioning		SPARC servers can be provisioned now using OS Build Plans and not just OS Sequences. However, both the methods cannot be used at the same time. The default configuration is the OS Build Plans provisioning mode. To ease the switch between modes and the dhcpd.conf configuration, use the following script: `/opt/opsware/boot/jumpstart-sparc-ogfs/tools/switch_OSS-OSBP.sh` When run, it will print the current provisioning mode for SPARC servers and request for your confirmation before switching the mode. If you continue, the script will backup the **dhcpd.conf** file, perform the required changes and restart the dhcpd service.	10.50
Security features	Security	SA Client Session Inactivity is enabled and set by default to 30 minutes. This will lock the SA Java Client if you are idle for the specified period. You need to re-enter the password to unlock the SA Java Client. This setting will not be enforced when upgrading installations that have any custom settings applied under **Administration > Users and Groups > Security Settings > Password Policy Settings**.	10.50
RHEL7 Core Platform	Support	SA can be installed on servers that are running Red Hat Enterprise Linux 7 (x86_64).	10.50
New for SA Web Client	SA Web Client	The SA Web Client is only used for downloading the SA Client launcher. The Web Client can be accessed as before, by navigating to a slice IP address or hostname and it features a completely re-designed home page that contains a **Download Server Automation Launcher** button, information about SA version and build and a link to the HPE Support site. The functionalities that were previously available in SA Web Client can be accessed from the SA Client as follows: • Service Levels can now be found in the SA Client under **Administration > System Configuration**. • OS Installation Profiles are now created through a script on an SA Core.	10.23
New for SA	SA Client	Authentication to the SA Core is done in the SA Client, after	10.23

Feature	Area	Description	Introduced in version
Client Launcher	Launcher	the Launcher has downloaded the required files. The SA Client Launcher now accepts only one input from the user: the SA Core hostname/IP address. A new window appears, where the user must enter the SA username and password.	
Overview	TLS compliance	According to PCI DSS v3.1 standard, TLS v1.1 and v1.2 are required to be used. Also, SSL and early TLS are no longer considered strong from the cryptography point of view.	10.23
Patch installation interview		During the interview, an additional step appears asking for "Cryptographic Protocol Selection for the Server Automation Components". The options are (with the option to select each of the protocols listed): • TLSv1 • TLSv1.1 • TLSv1.2	10.23
Protocol switch tool		This is a script that automates and eases the change between TLS protocol versions. It can be called automatically from the patch installer or can be run manually by invoking it from command line as follows: `# /opt/opsware/oi_util/protocol_switch_tool/protocol_switch_tool.sh --backup` (to backup the current configuration that can be later restored) `# /opt/opsware/oi_util/protocol_switch_tool/protocol_switch_tool.sh --protocol <TLSvX>` It is recommended to run the script with `--help` option first.	10.23
Supportability		To use TLS v1.1 or TLS v1.2 protocols, all Cores and satellites must be running an SA version that supports these protocols (SA 10.23 or later). Mixed protocol environment is not officially supported.	10.23
New satellite media for 10.23		• The satellite media for SA 10.20 currently supports protocol up to TLS v1.0. • In case of an already hardened infrastructure with TLSv1.1 or TLSv1.2, if a new satellite is required to be added, you must use the newly released SA 10.23 satellite media that supports all protocols (TLS v1.0, TLS v1.1, and TLS v1.2). • SA 10.23 satellite media can be installed by using the same installation procedure as for SA 10.20.	10.23

Feature	Area	Description	Introduced in version
Patch rollback with hardened infrastructure		On hardened infrastructures, the rollback mechanism must be called from SA 10.23 media (or greater). **Note:** When a patch rollback is done on satellites and the cores to which they are connected to do not support TLS v1.0, the services on the satellite will not be started until a new CORD patch/upgrade is done. The services should not be started manually.	10.23
FIPS and TLS v1.0		Due to a third-party software limitation, only support for TLS v1.0 exists on FIPS-enabled environments. As a consequence, the only option listed by the patch installer will be TLS v1.0.	10.23
Red Hat Satellite 6.x support	Support	Modifications have been made to the HPE Server Automation (SA) RHN import tool to support content download from Red Hat content delivery network (CDN) using Red Hat subscription management (RHSM). This allows you to download content for Red Hat Enterprise Linux 7 (RHEL).	10.23
Latest version of HPE Live Network Connector	HPE Live Network Connector	The Live Network Connector (LNc) that is installed on the SA core at: **/opt/opsware/hpln/lnc/bin** is outdated and can no longer be used to download content. Download the latest version of LNc and install it on the core. 1. From HPELN, download the latest version of the HPE Live Network Connector. 2. Copy the new version to the SA core at /opt/opsware/hpln/lnc and install it: `#./install`	10.23
Configured debugging	Agent	Now you can configure debugging for ptymonitor via the ptymonitor.debug_name parameter in the agent's configuration file, agent.args.	10.22
Disabled RC4		In this release, RC4 has been disabled for SSL encryption.	10.22
Importing users		A new custom attribute, **hpsa_preserve_solaris_user_home_path**, allows you to import users using your user-home path in /home/…. In previous SA versions, the import tool added /export to the path. To exclude the /export addition to the path, set the custom attribute to managed server.	10.22
Uninstalling the Agent		For agents installed on a non-system drive (a feature	10.22

Feature	Area	Description	Introduced in version
		available from 10.21 onwards for Windows platforms), the agent uninstaller removes symbolic links on the system drive and all agent files, except the target directory.	
Agent install customization		Using ADT (Agent Deployment Tool) you can select a maximum of 10 PAPXs to be run sequentially after the agent is successfully installed. If one of the APX scripts fails, the system stops at that step, does not run the remaining APXs, and reports the job as FAILED. **Note:** In case of an error during the APX script run, the system will not roll back the currently successfully run APXs, nor the previouslysuccessfully run APXs Three PAPXs are included for the following functionality: • Assign Server to Customer • Attach Server to Device Group • Attach Server to Software Policies	10.22
Optional element	Audit and compliance	A new optional element, **preserveExceptions**, is available in Audit Policy Filters. The element can be set to Yes or No.	10.22
New for certificates	Certificates	Added CRL (Certificate Revocation List) support for access to SA using SA Client desktop client with smart card authentication.	10.22
HPSA SUSE Manager Importer	Patching	SA now offers a SUSE Manager Importer tool based on the HPSA RedHat Importer. The tool is capable of importing packages and errata from the SUSE Manager 2.1 Server and creating HPSA Software Policies for errata and packages hosted by SUSE Manager.	10.22
New features	OS provisioning	• Build Plan filtering: You can now associate a platform with an OS Build Plan and use this to improve filtering servers before running the OS Build Plan. • Improved customer assignment: ◦ The **Assign Customer** step is now part of the OOTB build plans. ◦ The UI is improved to be able to assign the server to a customer.	10.22
Upgrades		• ProLiant content upgraded to Insight Control Server Provisioning 7.5.0	10.22

Feature	Area	Description	Introduced in version
		• WinPE 3 and 4 based service OS drivers updated • RHEL 6 service OS drivers updated • RHEL 6 service OSs were upgraded to 6.7	
New upgraded Third-Party products	Third-Party products	Python upgraded from Python 2.7.3 to Phython 2.7.10.	10.22
New for usability	Usability	Updates to the CAC/PKI SmartCard feature.	10.22
Timeout handling for remediation and installation jobs	Software Management	Server Automation now offers improved timeout handling for remediation and installation jobs. After a timeout occurs and until the job execution stops, the status of the server is changed to Stopping. While in the Stopping state, the agent does not take on any additional jobs and completes any job that is currently in progress. Moreover, if the timeout occurs during an agent reboot, then after restarting, the agent will not resume the job. After the job execution stops, the server will be marked as Timed Out. This fixes the discrepancy of the core showing the job as Failed because of a timeout, while the agent is performing the job.	10.22
SA Agent Installation to a Non-System Drive	Agents	You can now install the SA Agent to another location in Windows Vista, or a newer Windows version, as long you have an NTFS system drive. Additionally, an SA agent previously installed in the default location can be moved to a new location. The implementation is based on symlinking the default-system drive location to the new install location.	10.21
Installing the Agent to a New Folder		To designate the new folder, in the Agent Deployment Tool (ADT) Install SA Agent window choose **Options** > **Advanced** > **Windows** installation path field. **Note:** The installation path field only supports ASCII characters. If the directory path contains spaces, do not enclose them in double quotes.	10.21
Moving a Previously Installed SA Agent To a New		Agents installed in the default location can be moved to a different location. The following prerequisites must be met: • The SA user needs Allow Install Agent permission	10.21

Feature	Area	Description	Introduced in version
Folder		• The SA user needs permissions to run an APX on target servers • The Windows user used by ADT on the managed server must have the Create symbolic links permission (this permission is granted to Administrators by default) To move the agent, run the APX Move Agent to Custom Location on the relevant servers. This APX is located in the SA Library in folder /Opsware/Tools/Administrative Extensions. **Note:** You can also move pre-10.2 SA Agents.	
Uninstalling the Agent		The agent uninstaller will remove the symbolic links on the system drive and all the agent files, except the target directory structure. However, for pre-10.2 agents, the uninstaller is unable to remove the symbolic links.	10.21
Integration with OS Provisioning		OSBPs can use the custom attribute AgentInstallDir to a custom value for Windows agent installation location. If the custom attribute is not present, the agent will be installed to the default location. This custom attribute is ignored for non-applicable platforms. **Note:** The SA Virtualization feature does not support the use of agents located on a non-system drive.	10.21
Agent Install Customization		Using ADT (Agent Deployment Tool) you can select a maximum of 10 PAPXs to be run sequentially after the agent is successfully installed. If one of the APX scripts fails, the system will stop at that step and will not run the remaining APXs. In this case the job is reported as FAILED. **Note:** In case of an error during the APX script run, the system will not rollback the currently successfully run, nor the previously successfully run, APXs. Included in this release are three PAPXs for the following functionality: • Assign Server to Customer • Attach Server to Device Group	10.21

Feature	Area	Description	Introduced in version
		• Attach Server to Software Policies	
New Samba Version	Provisioning	New version of Samba (3.6.25).	10.21
Build Plans Changes		• Non-C drive agent installation supported in Windows build plans. • Instead of OS Sequences, use Build Plans for new provisioning jobs. • OS build plans are now supported for SLES 12.	10.21
Proliant Content Changes		• New OS build plans for: ESXi 5.1 U3, RHEL 5.11, RHEL 6.6, RHEL 7.1, SLES 12, Windows 8.1 Pro • New drivers: 2015.03.0	10.21
Linux Service OS Upgrade		Upgraded Linux service OS to RHEL 6.6.	10.21
Disk-Space Management During Compliance Scanning and Software Registration	Patching	SA now checks the amount of free space available on managed servers before downloading Windows utility files (such as the Microsoft Offline Catalog) during compliance scanning and software registration.	10.21
Custom Attributes Changes Viewable in the History Panel	Software Management	SA now offers the ability to see custom attributes changes in the History Panel for servers, device groups, OS installation profiles, and software policies.	10.21
Server Scripts Execution		Ability to execute server scripts in parallel. You can also limit the maximum number of scripts executed by an agent at one time.	10.21
Installing Zip Packages		Added support for installing zip packages with the same filename but different contents by adding file size and checksum verification. This feature works with agent version 10.21 or higher.	10.21

Feature	Area	Description	Introduced in version
RHEL 7 Import Available		Import of RHEL 7 content is now possible using the new redhat_import tool through Red Hat Subscription Management.	10.21
SA Client Support for Windows	Managed Platform Support/OS Systems Support	Windows 8.1	10.20
SA Managed Platform Support for Additional Operating Systems		• RHEL 7 • OEL 7 • CentOS 7	
SA Agent Installation	Agents	SA 10.20 supports SA Agent installation on IPv6.	
SA Agent for FIPS Enablement		This SA version continues support for enabling FIPS at installation, and also supports enabling FIPS status through the Core Recertification process. In order to support FIPS enablement, your SA Agent version must be SA 10.1 or higher.	
SA Agent and IPv6 Support		This SA version supports the following for the SA Agent: • Dual Stack(IPv4 and IPv6) • IPv6-only environments	
Software Policy Ordering	APIs	The following methods of com.opsware.swmgmt.PolicyAttachable now return the software policies ordered by name: • getPolicyAttachableStates • getSoftwarePolicyAssociations • getSoftwarePolicies The policies naming scheme becomes a basic mechanism to control the order in which software policies are remediated within a job. As a consequence the following API methods now remediate the software policies ordered alphanumerically: • com.opsware.swmgmt.PolicyAttachable#startFullRemediateNow	

Feature	Area	Description	Introduced in version
		• com.opsware.swmgmt.SoftwarePolicyService#startFullRemediateNow (com.opsware.swmgmt.PolicyAttachableReference)	
OS build plan flow control		The following methods have update input parameters: • com.opsware.osprov.OSBuildPlanService# startOSBuildPlan(OSBuildPlanRef, OSBuildableReference, OSBuildPlanJobParams,String,JobNotification,JobSchedule) • com.opsware.osprov.OSBuildPlanService# startOSBuildPlan(OSBuildPlanRef, OSBuildableReferenc[],OSBuildPlanJobParams,String,JobNotification,JobSchedule) The com.opsware.osprov.OSBuildPlanJobParams was updated so OS build plan flow control configuration can be checked/set: • getInitialFlowControlDirective() • setInitialFlowControlDirective() • isFlowControlDisabled() • setFlowControlDisabled()	
Core Recert Service		The method startCoreRecertSetup takes the argument CoreRecertSetupJobArgument. This object has changed to include the following methods: • getCustomCertPath. Gets the path of a custom certificate on recert core. • getKeysize. Gets the keysize to be used to generate SA certificates. • getSignatureAlgorithm. Get the signature algorithm to be used to generate SA certificates. • isFipsEnabled. Returns true if fips enablement parameter is set, else false. • setCustomCertPath. Set the customer certificate path on recert core. • setFipsEnabled. Sets Fips enablement on or off. • setKeysize. Sets the keysize to be used to generate SA certificates.	

Feature	Area	Description	Introduced in version
		• setSignatureAlgorithm. Sets the algorithm parameter to be used to generate SA certificates.	
Other changes		• A new method com.opsware.server.ServerService#decommission (com.opsware.server.ServerRef, boolean) allows servers of customer Opsware to be decommissioned too. • The DNS domain of a facility is now public, see: ◦ com.opsware.locality.FacilityVO#getDnsSubdomain ◦ com.opsware.locality.FacilityVO#setDnsSubdomain • New fields for the CoreRecertJobArgument: signature algorithm, keysize, fips enablement, and custom certificate path. • Additional job parameters for start build plans (initialFlowControl and disableFlowControl) • New APIs to get PatchUnits information for multiple servers.	
Removed or Deprecated APIs		Class com.opsware.system.integration.OOMessageSpec (deprecated in 10.0) was removed from the API.	10.20
	Audit	You can now perform the following audit-related actions for ESXi servers: • Create audits. • Create snapshots and snapshots specifications. • Create and manage audit policies. Your ESXi servers must be managed by a vCenter that has PowerShell and PowerCLI installed.	10.1
	Localization	SA 10.20 has been localized to Simplified Chinese, Japanese, German, Russian, French, and Spanish.	10.1
Oracle Database and Model Repository	Support	SA 10.2 supports Oracle 12c RAC.	10.1
New Features	Provisioning	• Support for deployments over IPV6. • Refer to the OS support matrix for details.	10.1

Feature	Area	Description	Introduced in version
		• ProLiant content from ICsp 7.4.0 (with support for ProLiant Gen9 SNAP1). • Provisioning support for RedHat Enterprise Linux 7 and 5.11, Solaris 11.2, Windows 7 and 8.1, ESXi 5.5 U1 and U2, CentOS 7, Oracle Linux 7, Ubuntu 12.04.5 • Build Plan Flow Control: ◦ Initial flow control (from UAPI) ◦ Restart from last point of failure ◦ Checkpoint/Restart ◦ Completed the SA Provisioning rewrite	
Legacy syntax for hpsa_ netconfig custom attribute deprecated		Use the new JSON-based syntax to specify configuration values for the hpsa_netconfig custom attribute.	10.1
Support for provisioning of Windows 2003 deprecated		Support for provisioning of Windows 2003 with build plans has been removed.	10.1
OS Sequences Deprecated		The following types of OS Sequences are deprecated: • OS Sequences that have build plans. • OS Sequences that are related to platforms that either are presently designated as 'end-of-life', or will be designated 'end-of-life' soon and no Build Plan support is planned. Instead of OS Sequences, use Build Plans for new provisioning jobs.	10.1
Performance Improvements	Patching	Windows Patch Compliance Export Performance The Windows “Patch Compliance Export” feature's performance was enhanced. This feature allows you to export compliance information for all Windows patches, and with this release, can scale to a large number of servers more effectively	10.1
Minor Enhanceme		• Exposure Time	10.1

Feature	Area	Description	Introduced in version
nts		The new Exposure Time column was added to the installed windows patch view. Exposure Time is calculated with the following formula: *Exposure Time (in Days) = [Date When a Patch Was Installed] - [Date When a Patch Was Released By The Vendor]* . • Improved Windows Patch Install Date Reporting Starting with this release, SA reports installation dates for all patches, regardless of whether they were installed by SA. If the Windows OS reports that a patch does not have available install dates, the installation date field will be empty. SLES Patching is now performed using the SLES native package manager Zypper on SLES 11 GA or later, replacing yum.	
Support native tool for remediation on SLES 11	Software Management	SA now supports Zypper as the package manager used by remediation jobs on SLES 11 GA or later.	10.1
Viewing package contents for DEB packages		It is now possible to view the package contents for Ubuntu (DEB) packages, similarly to the functionality already available for RPM and ZIP packages.	10.1
New features	Virtualization Management	• Genealogy, which offers complete visibility over the hierarchy of VMs and VM templates that have the same parent. • IPV6 support: ◦ Discovery and use of IPv6 network addresses of the V12N infrastructure, such as virtualization services and hypervisors. ◦ Create/edit Solaris zones with IPv6 network address. ◦ Leverage OS provisioning with IPv6.	10.1
SA Client Support for Windows Operating Systems	Managed Platform Support/OS Systems Support	The following operating-systems are supported on the SA Client. • Windows Server 2003 • Windows Server 2008	10.1

Feature	Area	Description	Introduced in version
		• Windows XP • Windows Vista • Windows 7 • Windows 8 • Windows Server 2012 • Windows Server 2012, R2	
SA Managed Platform Support for Additional Operating Systems		• Ubuntu 12.04 LTS • ESXi 5.5	10.1
SA Platforms		• Python 2.7 • Java 7 • Weblogic 11	10.1
Faster SA Agent Installation	Agents	For information on the Agent Upgrade tool, on installing the agent, and on bringing servers under SA management, see the SA User Guide.	10.1
SA Agent Installer		The SA Agent Installer was added as a Web Services Data Access Engine (Twist) service.	10.1
Authentication	Support	SA now supports two-factor authentication using Department of Defense personal identity verification (PIV) smart cards.	10.1
CPU Interface		Central processing unit (CPU) properties are now displayed in the SA Client in the **Inventory** > **Hardware** window.	10.1
Interactive Installation Configurator (iDoc)	Installation	The Interactive Installation Configurator (iDoc) allows you generate and view (PDF) an SA Core installation procedure document that is confined to only the SA Core configuration and the SA Core Host operating system you have selected. This allows you to view (PDF) or print an installation procedure document that does not contain information intended for SA Core configurations or core host operating systems that are not relevant to the installation you intend to perform. Simply run **SA_10.10_core_install_config.zip** in a browser, select your preferred SA Core Layout and core host operating	10.1

Feature	Area	Description	Introduced in version
		system and select View or Print.	
FIPS Compliance Options		SA complies with the Federal Information Processing Standards publication 140-2, a security standard that enables government entities to procure equipment that uses validated cryptographic modules. During installation you can choose to enable FIPS by setting the fips.mode parameter to enabled. When FIPS is enabled, you will be restricted to SHA1 as the hash algorithm. You will be prompted during the installation to specify whether FIPS should be enabled or not. Under normal security conditions, HP recommends using SHA1 with a key length of 2048. Higher security requirements could require FIPS with a key length of 4096 or SHA256. Note that use of FIPS or SHA256 can impact core performance. Contact your Security Administrator for more information.	10.1
Reserved Ports		SA 10.10 requires that the following ports be open: 8084/8086 - For bandwidth management, if enabled These, and other ports, are configurable at install/upgrade time through installer parameters. Note: In addition, other ports are required to be open for previous releases of SA.	10.1
Upgrade		If your SA Core matches one of the SA Core configurations supported for customer upgrade and described in the SA Install Guide, you can upgrade from a previous SA version to SA 10.0 yourself. However, if your core does not match any of these SA Core configurations, your first SA Core upgrade to SA 10.0 from a previous version must be performed by HP Professional Services or an HP certified consultant. After the core has been upgraded to SA 10.0, HP supports customer-performed upgrades to SA 10.x or later as long as your core configuration is one of the supported configurations. All other core configurations will continue to require the services of HP Professional Services. If you are uncertain whether you can upgrade an existing SA Core yourself, contact HP Technical Support.	10.1
Localization	Localization	In addition to Simplified Chinese and Japanese, the SA 10.10 interface has now been localized to German, Russian, French, and Spanish.	10.1

Feature	Area	Description	Introduced in version
OO-SA Integration		Updates pertaining specifically to the OO-SA integration (Server Automation operations performed within Operations Orchestration) are delivered via the HPE Live Network at https://hpln.hpe.com	10.1
Oracle 12.1.0.1	Oracle Database and Model Repository	The SA distributions Media includes preinstalled customized Oracle 12.1.0.1 RDBMS software and the truth database that can be installed during the SA core installation. You can also use the Oracle Universal Installer to manually install an Oracle 11g or 12c database, however, you will need to perform certain tasks that the HP-supplied database performs automatically on installation.	10.1
	Provisioning	The following new features have been added to Provisioning for this release: • Support for Windows Server 2012, Red Hat 6, ESXi5, SLES11 • Update ILO support in MBC to support ILO 2, 3 and 4 • New public ILO UAPI • Build plan support in MBC SA Client UI updates for: ◦ Register ILO device ◦ Set static IP configuration ◦ Multipath configuration support • New 64 bit Linux service OS • Windows PE 64-bit updated to 3.1 • Bare metal PXE boot support (SmartBoot) • Improved network booting - new pxe_boot_arguments custom attribute	10.1
New Build-Plan Features		The following new build-plan features have been added: • New platform support ◦ CentOS 5 and 6 ◦ OEL 5 and 6 ◦ Ubuntu Server 12.04 LTS ◦ Solaris 11 and 10 on X86 hardware • UEFI support for HP ProLiant hardware: ◦ OS Provisioning for RHEL 6.5, SLES 11 SP3, ESXi	10.1

Feature	Area	Description	Introduced in version
		5.1 ◦ OS Provisioning for Windows 2012 R2, 2012, 2008 R2, 2008 x64 SP2 ◦ iLO UAPI updates • New Post-Install Network Personalization build plan step (formerly provided by Post-Install Network Configuration APX) • Updated ProLiant content • Improved network booting ◦ w PXE menu ◦ pxe_boot_arguments custom attribute ◦ New Hardware Detection Tool ◦ New WinPE 4 based maintenance OS ◦ Updated RHEL 6.5 based Linux maintenance OS • Improved history for tracking operations on Build Plans	
OS Sequences Deprecated		The following types of OS Sequences are deprecated: • OS Sequences that have build plans • OS Sequences that are related to platforms that either are presently designated as 'end-of-life', or will be designated 'end-of-life' soon and no Build Plan support is planned. Instead of OS Sequences, use Build Plans for new provisioning jobs.	10.1
New for Patching	Patching	Server Automation (SA) now supports patch management for Ubuntu, enabling you to identify, install, and remove Ubuntu Debian package updates, and maintain a high level of security across managed servers in your organization.	10.1
OCLI	Software Management	OCLI can now be installed using a software policy on the managed servers.	10.1
Support for Handling Native Chef Cookbooks in SA		Server Automation (SA) can be used to view and manage Chef Cookbooks and run Chef Recipes. You can upload native Chef Cookbooks to SA, manage them in SA, and run Chef Recipes from SA without having to deploy parallel Chef infrastructure.	10.1

Feature	Area	Description	Introduced in version
		Features include: • Integration with the SA Package Repository (yum based OS-es) • A new 'Chef Group' User Group for seamless extension of the SA security framework • Multi-tenancy support for Chef Cookbooks • OOTB mechanism to easily upgrade and configure the used Chef client • Support for migrating Chef content between meshes (cbt) • Chef Cookbook management in SA, which enables you to: ◦ download Chef Cookbooks from the Chef community and upload them straight into SA ◦ view Chef Cookbook properties, metadata and recipes in SA ◦ run Chef Recipes on managed servers and device groups ◦ customize a Run Chef Recipe job using SA custom attributes ◦ view job history and detailed output logs for Run Chef Recipes jobs	
Vertical Scalability: Redesign Job Results		In order to improve the performance and scalability of remediation jobs, both the job backend and the UI responsible for displaying the job progress and job results were redesigned. Redundant or verbose data was dropped from the job results, reducing the load on the SA components. The user experience is now enhanced by having only relevant data displayed to the user, thus making the user interface much more usable, especially for large remediation jobs.	10.1
Detach and remediate without uninstall		Software policies can now be detached without remediation.	10.1
New attribute	UCMDB	There is a new attribute implemented in mapping.xml: <Attribute source='Node/Vendor' target-attr='vendor' enable='false'/>	10.1

Feature	Area	Description	Introduced in version
		When enabled (TRUE), the data is flowing in UCMDB.	
	Usability	Two non-supported features (Code Deployment and Rollback (CDR), and Configuration Tracking) were removed from the SA Client interface. CDR was replaced by ADM. Configuration Tracking was replaced by A&R.	10.1
OpenStack as a Virtualization Service	Virtualization Management	SA's OpenStack as a Virtualization Service provides the ability to add your in-house deployment of OpenStack as a Virtualization Service to discover Projects and VMs (OpenStack Instances).	10.1
FIPS		SA complies with the Federal Information Processing Standards (FIPS) publication 140-2, a security standard that enables government entities to procure equipment that uses validated cryptographic modules. If FIPS is enabled, you need to upload CA certificates for each virtualization service.	10.1
Virtualization Secure Mode		**Secure Mode** in SA Virtualization is enabled (or True) by default in a new SA 10.10 installation and disabled (or False) on an upgrade to SA 10.1. See also the deprecated and unsupported sections of these release notes for deprecated and unsupported virtualization components.	10.1

Send documentation feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Release Notes (Server Automation 10.60)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to hpe_sa_docs@hpe.com.

We appreciate your feedback!