Hewlett Packard
Enterprise

Server Automation

Release Notes

Software version: 10.22

Document release date: December 2015

Software release date: December 2015

Contents

Introduction

This document provides an overview of the Server Automation 10.22 release. It contains important information not included in the manuals or in the online help.

Up-to-date documentation

All the documentation is available from the new Server Automation 10.x Documentation Library. See the Documentation Information section for instructions on how to use the Documentation Library to access the guides and white papers relevant to this release.

For the most updated release notes, see the Server Automation Release Notes on the HPE Support website.

For information about what was new in previous releases, use your HPE Passport Credentials to log in to the HPSW Support Portal and use the Search button to search for a specific release-note document.

Support and compatibility information

For complete SA support and compatibility information for this release, see the Server Automation Support and Compatibility Matrix.

For a list of supported operating systems and platforms for Storage Visibility and Automation Managed Servers, SE Connector, SAN Arrays, Fibre Channel Adapters, SAN Switches, File System Software, Database Support, and Storage Essentials Compatibility, see the Storage Visibility and Automation Support and Compatibility Matrix.

For more information about supported configurations, see the Server Automation Installation Guide, chapter 2: “SA Core Configurations Supported for Customer Installation”.

Audience

These release notes contain information for users who are familiar with the installation and maintenance of Server Automation, Application Deployment Manager, and DMA integration.

New in this release

This section describes new functionality and other relevant release-specific information.

New SA Client support for Windows operating systems

This section lists the operating systems supported on the SA Client.

- Windows Server 2008
- Windows 7
- Windows 8
- Windows 8.1
- Windows Server 2012
- Windows Server 2012, R2

New for SA Agent

Configured debugging

Now you can configure debugging for ptymonitor via the ptymonitor.debug_name parameter in the agent's configuration file, agent.args.

Disabled RC4

In this release, RC4 has been disabled for SSL encryption.

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.

Uninstalling the Agent

For agents installed on a non-system drive (a feature 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 previously successfully run APXs.

Included in this release are three PAPXs for the following functionality:

- Assign Server to Customer
- Attach Server to Device Group
- Attach Server to Software Policies

Important: See Deprecation and End-of-Support Announcements for important SA Agent version deprecations and end-of-support announcements.

New for audit and compliance

A new optional element, preserveExceptions, is available in Audit Policy Filters. The element can be set to Yes or No.

New for certificates

Added CRL (Certificate Revocation List) support for access to SA using SA Client desktop client with smart card authentication.

New for localization

SA 10.22 will be localized to Simplified Chinese and Japanese.

New for 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.

New for Oracle database and model repository

See the Server Automation Oracle Setup for the Model Repository Stand-Alone document for changes to the Oracle Database and Model Repository.

New for patching

HPSA SUSE Manager Importer

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. For more information refer to White Paper: SUSE Manager SLES Importer and the Server Automation Support and Compatibility Matrix.

New for OS provisioning

New features:

- 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.

Upgrades:

- ProLiant content upgraded to Insight Control Server Provisioning 7.5.0
- 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

Python upgraded from Python 2.7.3 to Phython 2.7.10.

New for usability

Updates to the CAC/PKI SmartCard feature.

New for software management

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.

Deprecation and end-of-support announcements

This section lists deprecated platforms, features, and agents for this release as well as previously deprecated items that have now reached the end of their support lifecycle.

Deprecations

When a platform/agent/feature is identified as deprecated for a release, it means that you (the SA customer) are considered notified of its future removal. Deprecated features are still fully supported in the release they are deprecated in, unless specified otherwise. The intent is that deprecated features or platforms will have support removed in the next major or minor SA release; however, eventual removal is at the discretion of HPE.

Deprecated products or platforms

SE Connector

The SE Connector was deprecated in 10.21.

Managed platforms

The following platforms are deprecated as of SA 10.0:

- Windows Server 2003
- Windows Server 2003 R2
- Windows XP

Deprecated components

SA Agent deprecation and upgrade requirement

SA 10.2X no longer supports SA Agents associated with SA 9.10 or earlier versions. Therefore, at a minimum, any SA Agents with version 9.10 or earlier must be upgraded to an SA Agent that is version 9.11 or later.

See the Server Automation Upgrade Guide for instructions on upgrading your SA Agents.

Agent Upgrade Tool

The Agent Upgrade Tool that is run from the OPSH shell and allows upgrading the agents on managed servers was deprecated. As of SA 10.0, a replacement APX was introduced that has several improvements and can be run from the SA Client.

SA Web Client

The SA Web Client is being deprecated. The majority of retained features have been ported to the SA Client (NGUI).

Deprecated API methods

The following API methods were removed following the move of application configurations into folder in SA 9.0:

- com.opsware.acm.CMLVO#setCustomers
- com.opsware.acm.CMLVO#getCustomers
- com.opsware.acm.ConfigurationVO#setCustomers
- com.opsware.acm.ConfigurationVO#getCustomers
- com.opsware.acm.Configurable#update
- com.opsware.acm.ConfigurationService# attachToConfigurable

OS provisioning OS Sequences

OS Sequences were replaced with OS Build Plans. See the Server Automation User Guide: Provisioning for instructions.

Embedded Reports

The Embedded Reports feature is deprecated as of SA 10.1.

Unsupported

Unsupported platforms

The following platforms are no longer supported as of SA 10.0:

- AIX 5.3
- Oracle Enterprise Linux 4
- Red Hat Enterprise Linux AS 3, AS 4, ES 3, ES 4, WS 3, WS 4
- SuSE Linux Enterprise Server 9
- SunOS 5.8, 5.9
- Windows Server 2000
- VMware ESX 3, 3.5
- VMware ESXi 3, 3.5

Unsupported products

BSAE reporting

Business Service Automation Essentials (BSAE) Reporting was removed in SA 10.1. It has been replaced by the Automation Insight (AI) product.

See Automation Insight (AI) documentation for details.

Unsupported features

Virtualization

- Unsupported Job Types

Legacy Job Types No Longer Supported	New Replacement Job Types
Clone Virtual Machine (VMware)	Clone Virtual Machine
Create Virtual Machine (Hyper-V) Create Virtual Machine (VMware)	Create Virtual Machine
Delete Virtual Machine (Hyper-V) Remove Virtual Machine	Delete Virtual Machine

Note: Any scheduled or blocked jobs of the legacy job types will be marked as Deleted during migration.

- Virtual Server Management Actions Individual hypervisor management for ESX, ESXi, and Hyper-V is no longer supported. You need to integrate with a VMware vCenter Server to manage ESX and ESXi hypervisors and VMs, or Microsoft's System Center Virtual Machine Manager (SCVMM) to manage Hyper-V hypervisors and VMs.
- All of the APIs, Reports, and SMOs that were previously deprecated have been removed. New APIs are available for the virtualization management through vCenter and SCVMM.

Unsupported scripts

As of SA 7.80, the following scripts are no longer supported:

- start_opsware.sh
- stop_opsware.sh

As of SA 9.0, you must use the unified start script:

/etc/init.d/opsware-sas

If you have any applications or scripts that depend on this script, you must rewrite them to use the unified start script.

Installation

New for installation

Install SA 10.22 Core Patch without Enabling root SSH Login for the root SSH User

New users

The following new users are supported with the SA installer:

User Name	Machine Type	Description
root user	Local	A root user
regular user	Local	A regular user who has permissions to invoke commands as root with sudo capabilities. **Note:** When you use a regular user for performing the installation or rollback of a core patch, make sure you invoke the command using sudo. For example: sudo <distro>/ opsware_installer/hpsa_patch.sh
root user	Remote	A root user, including root ssh access
regular user	Remote	A regular user with sudo capabilities (including user ssh access) **WARNING:** Password-less sudo is not supported for regular users with sudo capabilities.

Settings required for regular users with sudo capabilities

Make the following changes to the /etc/sudoers file on every machine where the user (in this case bob) installs SA:

- *Defaults   lecture=never*
- *bob   ALL=(ALL)   ALL*

General settings for user names

User names should:

- Be portable across systems conforming to POSIX.1-2008. The value is composed of characters from the portable filename character set.
- Not contain a hyphen (-) character as the first character of a portable user name.

Use the following set of characters if it is a portable filename:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z a b c d e f g h i j k l m n o p q r s t u v w x y z 0 1 2 3 4 5 6 7 8 9 . _

Standards

Respect the IEEE Std 1003.1, 2013 Edition. See: http://pubs.opengroup.org/onlinepubs/9699919799/basedefs/V1_chap03.html

See the Server Automation Installation Guide for installation instructions.

Renaming SA default folders

WARNING: Do not rename SA default folders, including the Package Repository folder.

New optional parameters for the enable_ipv6.sh script

There are two new optional parameters for the enable_ipv6.sh script:

- -i <IPV6 address>: use specified IPV6 address instead of autodiscovered based on hostname DNS AAAA resolution.
- -n : do not start/restart SA components when making configuration file changes.

Patch installation

Prerequisites

SA version requirements

SA 10.22 can only be installed on systems running the following:

- SA version 10.21 GA build (Build ID of opsware_60.0.59928.0)
- SA version 10.2 GA build (Build ID of 60.0.56699.0)

Patch installation updates the install.inv file to record the patch installation and the patch build ID.

To determine the build ID for a core machine:

1. Open the file /var/opt/opsware/install_opsware/inv/install.inv.
2. Find the section beginning with %basics_.
3. Under this line, find the build_id parameter.

   Example:

   %basics_linux

   build_id: opsware_60.0.56699.0

   %opsware_patch

   build_id: opsware_60.0.59928.0

Note: Starting with release 10.02, the installed patch version can no longer be seen when you invoke rpm -qa. The version is still available in /var/opt/opsware/install_opsware/inv/install.inv under %opsware_patch.

Core and satellite services

Use the /etc/init.d/opsware-sas status command to verify that all core and satellite services are functioning correctly.

General recommendations

- Multi-host core/satellite: Patch each core and satellite separately, one at a time.
- Multi-master mesh: Patch the primary core first (to make sure that it has a higher version of SA), followed by secondary cores and satellites.
- Mixed-version core environments: These environments are only supported as transitory mixed-core versions during patch upgrades, when cores at different patch levels can temporarily coexist in a multi-master mesh.

Installing the patch

Follow the instructions in the patch readme and the install-script prompts to download and install the patch.

The *opsware_installer/hpsa_patch.sh* script is used both for installing and for uninstalling SA 10.22.

After a patch installation, all services on the core/satellite machine should be functional.

Troubleshooting the patchiInstallation

Error Text	Explanation and Workaround
Could not find spog.pkcs8 /var/opt/opsware/crypto/occ	In order to patch Wayscripts, the *spog.pkcs8* certificate must exist under */var/opt/opsware/crypto*. Copy the certificate from another core machine to your core server, then retry the operation.
ValueError: invalid certfile	Can occur after installing the Software Repository (Word). Make sure that spin.srv and opsware_ca.crt exist in the /var/opt/opsware/crypto/spin folder on the Software Repository machine, copy the certificate from another core machine to your core server, and retry the operation.
You don't have permission to update the patch meta database in HPE SA. Re-run this command with a proper hpsa_user and hpsa_pass. The hpsa_user needs permission to write the folder "/Opsware/Tools/Solaris Patching" and the Package Management Client Feature, "Manage Package" permission set "Read & Write". There was a problem with running update_supplements. Refer to section *Patch Management for Solaris* of the User Guide: Application Automation manual for details on how to set up Solaris patching on your core.	Solaris patching has not yet been set up. Disregard this error.

Rolling back the patch

This section contains patch roll-back information.

Prerequisites

- Versions: SA 10.22 can be rolled back, but only to the previous full release, SA 10.2.
- Wayscripts: The *spog.pkcs8* certificate must exist under */var/opt/opsware/crypto* (typically the certificate is installed with the Shell, SA Web Client, or Build Manager) to roll back wayscripts.
- Non-root (regular) user: To roll back as a non-root user, invoke this command:
  sudo <distro>/ opsware_rollback/hpsa_patch.sh

Rollback order for multimaster mesh

Roll back the patch in a multi-master mesh in the following order:

1. Secondary cores
2. Satellites
3. Primary core

Post-installation / upgrade tasks

This section lists the tasks that should be performed after you install or upgrade to SA 10.22. Some tasks might not be appropriate for your situation.

Upgrades

WARNING: Do not rename SA default folders, including the Package Repository folder.

This section lists the tasks that should be performed after you upgrade to SA 10.22.

Perform the required upgrade on all SA Agents

In order to be able to use the new functionality for SA 10.22, upgrade your SA Agents to 10.22.

This patch includes updated Server Agents that will be uploaded to the Software Repository. However, no agents will be upgraded on core machines (that is, in the Model Repository) or on managed servers without manual intervention.

Additionally, SA 10.22 no longer supports SA Agents associated with SA 9.10 or earlier versions. Therefore, at a minimum, any SA Agents with version 9.10 or earlier must be upgraded to an SA Agent that is version 9.11 or later.

Note: If you plan to install the SA Command-line Interface (OCLI) on a Windows Server after upgrading to SA 10.22, you must update the SA Agent on that server to the latest version. Errors occur during OCLI installation on Windows servers with earlier SA Agent versions.

See the Server Automation Upgrade Guide for instructions on upgrading your SA Agents.

Reapply your customized settings

If you have customized such settings as Java heap settings, you must reapply your customizations after you install SA 10.22, as the settings are set to the SA default during installation or upgrade.

Upgrade wayscript versions

If you install additional Slice Component bundle instances after patching the SA Core, wayscript versions are set to version 10.20, rather than to the patch version.

To update the wayscript versions:

1. Identify the SA core server:
    a. Log in to the SA Client as administrator (opsware admin user).
    b. Navigate to Administration > Customers.
    c. Select the Opsware Customer.
    d. View the Custom Attributes.
    e. Check the value field of the custom attribute CORD_OPSWwayscripts.
2. Log in to the SA Core server you identified in step 1 and execute the following two commands:

    Command #1:

    ```
    cd /var/opt/opsware/OPSWpatch/OPSWwayscripts/scripts
    ```

    Command #2:

    ```
    ./post_after_startup.sh
    ```

3. Apply any required hotfixes to the wayscripts.

Troubleshoot the upgrade

Red Hat EL 5.9

If SA 10.22 is installed on Red Hat EL 5.9, sporadic org.omg.CORBA.COMM_FAILURE exceptions are displayed in the SA Client console.

To eliminate the exceptions:

1. In order for the kernel parameters to persist across restarts, set the sysctl parameters in the /etc/sysctl.conf file:

   ```
   net.ipv4.tcp_tw_recycle=1
   net.ipv4.tcp_tw_reuse=1
   ```

2. Load the sysctl.conf settings you edited in Step 1:

   ```
   # sysctl -p
   ```

3. Set the property to not use the socket option SO_REUSEADDR on all gateways:

   ```
   # edit /etc/opt/opsware/opswgw-agw*/opswgw.custom
   # edit /etc/opt/opsware/opswgw-cgw*/opswgw.custom
   # edit /etc/opt/opsware/opswgw-mgw*/opswgw.custom
   ```

   Directive:

   ```
   opswgw.SoReuseAddr=false
   ```

4. Restart all gateways:

   ```
   service opsware-sas restart
   ```

See also https://access.redhat.com/site/solutions/357683.

Patch deduplication steps for Windows patching

Duplicate patches (which cause conflicts during remediation and compliance checks) can occur in the SA database if you import the Microsoft Patch Supplement (MPS) and then run the SA Patch Import process using the Microsoft Offline Patch Catalog (wsusscn2.cab).

Finding duplicates

In the SA Client, navigate to **Administration > Patch Settings > Patch Database** to view the Last Import Summary field. If it displays a warning message after performing a patch import, then there are duplicates in your database.

Resolving duplicates with deduplication

Access the white paper Resolving Conflicts between SA Patching and the MS Patch Supplement that is specific for this release.

IMPORTANT: Perform de-duplication:

- Only once.
- For SA upgrades only (not fresh installs).
- If the procedure was not previously performed during an SA 10.0 upgrade.

Known issues

This section describes known issues for SA. The tables list issues first alphabetically by Subsystem, then numerically within each subsystem.

QCCR1D	Symptom/Description	Platform	Workaround
AGENT			
192728	When using the ADT Scan feature, an error message appears in the SA Client when scanning ranges using * or /24 (CIDR) notations.	Independent	An nmap (the tool used to make the network map) error will be displayed, but it doesn't have any negative impact on the scan itself. It is an issue with nmap (bug raised to nmap).
193587	In some scenarios and network topologies, when scanning for an IPv6 enabled server the SSH port it is shown as unavailable and the agent cannot be deployed.	Independent	From the SA Client, modify the ADT scanning parameters based on the network topology, proy and firewall rules.
APX CONTENT			
111925	A deployment which includes a Configuration File component fails without any warning or error when attempting to place a file in a directory which has not been created in advance.	Independent	Ensure that a code (or other type of ADM component) creates the destination directory in preparation for placement by the Configuration File component.
AUDIT AND COMPLIANCE			
151552	If you cancel a running audit job, and a target server shows a "SKIPPED" job status in the audit results, until an audit has successfully run, the server's compliance view shows the following incorrect status for the policy: “Policy has changed since the last scan”.	Independent	Rerun the Audit.
183967	Running a "Users and Group" remediation job with multiple uses and user groups will fail with error message: "No Group found".	Independent	Run a "Users and Group" remediation job with user groups followed by a remediation job to remediate users that belong to the remediated user group.
CERTIFICATE			
184908	Occasionally, core recert status will show core recert session not in progress, even though core recert has been executed. May be most applicable to FIPS-enabled customers.	Linux	Generally waiting 10 minutes or so seems to resolve the problem.
189893	After core recert infrastructure-only (non-slice) boxes will not have the proper certificates for the word_upload component and work_upload may not work properly on that box.	Linux	May be resolved manually by copying certificates in /var/opt/opsware/crypto/word_uploads on box with slice to the corresponding directory on the infrastructure-only box.
191875	During core recert the security.conf file (in the directory /etc/opt/opsware/crypto) is created or updated on all cores, slices and satellites. The core recert process has no obvious way to reach an oracle-only box that is part of the mesh, so the file is not propagated.	Linux	Customers should not experience any problems because of this. If desired, a copy of security.conf can be copied from one of the mesh's cores to the oracle-only box.
GATEWAY			
193091	After upgrading core from 10.0 to 10.20 and up, the 10.0 satellite is unreachable.	Independent	See https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01365141
HPUX-VIRTUALIZATION			

157368/160408	Search with IP Address or Hostnames on Add Virtual Server screen does not list HP-UX machines.	HP-UX	None.
MANAGED PLATFORMS			
191478	CentOS 7 Build Plan fails with TypeError after migration from SA 10.02 with platform installed to SA 10.2.	Independent	None.
OCC			
135460	Not able to select servers in Run Custom Extensions submenus.	Independent	None.
172654	Unable to start httpsProxy. SA installer should validate /etc/hosts against multiple 'localhost' definitions.	Linux	In the /etc/hosts file, remove 'localhost' and 'localhost.localdomain' from the definition line that begins with:1. Save the file, and retry the installer. **Note:** This installer issue is only valid for Major release not CORD release.
191941/192463	The SA Client progress bars are reduced at a line and doesn't indicate progress for Windows 8/8.1/2012/2012 R2.	Independent	None.
213050	Launcher cannot log in to SA Core using its IPv6 address.	Independent	This is a Java Web Start issue, not an SA issue. No workaround.
OS PROVISIONING			
114523	OS Sequences can fail with persistence error when sequence includes a device group and is run repeatedly	Independent	Use Build Plans to implement the equivalent use-case.
175069/213698	Cannot use an OS Build Plan to provision Windows Server 2012 to a UEFI ProLiant server's second hard disk unless both of the server's hard disks are empty.	Windows 2012	Ensure that all data has been removed from both hard disks then retry the provisioning.
213391	Running default BP "Add Migrated Linux Server" fails at "Set One Time PXE Boot"	Independent	These build plans are specific to RDP to ICsp migration, so are not applicable to SA. This issue is caused by incorrect usage of the product.
PATCH MANAGEMENT			
100566	When the last patch in job has reboot-normal setting, the job status shows incorrect "Reboot later" information for this patch. Although the reboot is performed correctly, when previewing remediating a patch policy on a server, or view the job status for a patch policy that is already remediated, the reboot setting might incorrectly display "Install and Reboot Later" when it should display "Install and Reboot".	Solaris	A workaround is not required because the reboot is performed correctly, even though the display may be incorrect.
102713	Number of Rules of patch policy compliance is not correct after remediation or installation of patches.	Independent	From an overall compliance perspective, SA is reporting the correct color. It just doesn't report the same number of patches before and after the scan. This is controlled by how Microsoft reports applicable/installed patches.
146902/157891	Solaris 11 Patch policies must prevent the user from changing the reboot option from the default option 'hold all server reboots until all actions are complete'.	Solaris	None.
148400	After MBSA import completes, it takes a long time to update patches in library and database info in admin page	Windows	None.

151092	Customers see duplicates between HPLN Patches and WSUSSCN2.CAB Patches. They have to run scripts that delete one of the conflicting patches from the SA database.	Independent	Version agnostic scripts have been provided in a hotfix which can be used to remove patches from the SA database. https://patch-central.corp.hp.com/crypt-web/protected/viewContent.do?patchId=QCCR1D151092
161961	The windows 2008 R2 SP1 consists of 2 binaries. When the user selects binary with file name windows6.1-KB976932-X64.exe and clicks uninstall in actuality the file gets uninstall and the server reboots and is now on Windows 2008 R2 RTM but the job times out and fails.	Windows 2008 R2	No workaround. Problem corrects itself with next scan.
162337	Windows 2k12 software policy remediation fails with the following type of error: 'AGENT_ERROR_PATCH_DATABASE_CERTIFICATE_ERROR'	Windows 2012;Windows 2012 R2	Import and run the latest (later than October 2012) Microsoft patch CAB file once. You should only have to do this one time.
SAV (SERVER AUTOMATION VISUALIZER)			
181473	SAV does not show IPv6 inet addresses or IP address for loopback.	Independent	None.
SEARCH			
92244	Searching on extended ASCII (words contains the "ß") characters returns no matching results.	Independent	None.
SERVER			
156389	Users and Groups SMO will not report all the groups that are created on a Windows 2012 Essentials. If user properties are edited, these changes will not be reported by the SMO. This means that audits with U&G rules will not be relevant on a Windows 2012 Essentials.	Windows 2012	None.
192013	Windows Local Security Settings SMO reports incorrect Security Settings for Not Applicable entries.	Independent	None.
193063	SMTool upload fails when /var/tmp folder is not present on the twist box where the command is run.	Independent	None.
SOFTWARE MANAGEMENT			
159841	When performing a core upgrade, you might experience conflicts originating from the UNITS and REALM_UNITS tables.	Independent	In order to continue with the upgrade process, the user needs to either manually resolve the conflicts or to clear them using the force resolver script.
163518	"End Job" button is still enabled after the job has completed.	Independent	None.
179479/179480	Recurring app config compliance jobs uses tokens with a one year lifetime.	Independent	None.
SPIN (DATA ACCESS ENGINE)			
193285	All gateways in a satellite facility should have the same weights defined for primary and backup tunnels.	Independent	None.
TRUTH (MODEL REPOSITORY)			
166334/188553	SA installed Oracle RDBMS modifies file /etc/sysconfig/selinux and inserts entry for SELINUX regardless of whether a previous entry exists.	Linux	None.

191511	There is a connectivity issue from MM infra slice to the secondary core DB when secondary core's database is in a RAC configuration and that secondary RAC fails over to a second node. Currently, a manual change to the MGW properties file and the tnsnames.ora files are needed to achieve a failover.	Independent	None.
UCMDB			
194366	The data from SA is not loaded correctly and completely when UCMDB server is configured in multi-tenancy mode.	Independent	None.
VIRTUALIZATION			
141907	If you configured the number of cores per socket using the native vSphere client, and modify the number of virtual processors with a Modify VM job in SA, the CPUs might end up in an invalid configuration. When you edit the CPU settings in the native vSphere client, this error, “Number of cores per socket cannot be greater than number of virtual CPUs” occurs when the configuration is invalid.	VMware	If the number of cores per socket for a VM is greater than 1, and you want to modify the CPUs: From SA, set the number of Virtual Processors as a strong multiple of the number of cores per socket. Or, use the native vSphere client to modify the CPUs.
160891	If a Create VM, Clone VM, or Deploy VM from VM Template job fails running the OSBP, and the VM ends up in Build Server Failed state, the VM cannot be deleted from SA Client.	Independent	Delete the VM from native vendor tool and reload in SA.
183608	The Openstack VM server is reachable externally only through its public floating IP, not through its internal private IP. The SA Agent is installed on the server using its floating IP, so eventually the management IP of the server is set to its floating IP. The server’s operating system is not aware of the floating IP, so the SA Agent is unable to gather this information. As a result, the server's floating IP is not present in the interface list for this server nor in the Management IP drop-down list on the server's Network view.	Independent	Do not try to change the IP from its “Default” setting to the internal OpenStack IP.
WORKLOAD MANAGER			
166350	Jobs remain with a status of Active, even though their associated tasks show a status of Success.	Independent	This issue occurs only in multi-core mesh installations where the SA Jobs are being approved using Operations Orchestration on all the cores of the mesh. To work around this issue, setup OO workflow only on the primary core of the mesh.

Fixed issues

The Fixed Issues table includes issues that:

- Were found during SA 10.22 release period.
- Were in the Known Issues table, but are now fixed.

The table lists issues first by subsystem, then numerically within each subsystem.

Feature Area/ QCCR1D	Symptom/Description	Platform
AGENT		

193194	SA does not support importing users with /home path directory.	Solaris
194086/194087	Windows watchdog value should be parameterized.	Windows
195034/195038	Unicode characters outside the ASCII codeset from server scripts are replaced with "?" (question marks)	AIX
201693/203269	ADT becomes root does not properly set the sudo algorithm	Linux
205450/205455	Agent startup failure on Windows Domain Controllers	Windows
209632/209636	ptymonitor's debug_name should be configurable in agent.args and ptymonitor.debug_name, and ptymonitor.nopam should be exposed to users via agent.args.	Independent
210057/210133	Attempt to upgrade to latest agent (ex 60.0.62417.1) fails and agent.err log reports below error. Run bs_hardware on the managed server also fails with the same error. -----Unexpected Error----- Traceback (most recent call last): File ".\bs_hardware.py", line 978, in blockingmainThread File ".\bs_hardware.py", line 872, in blockingmain SSLError: disabled for fips The issue only occurs on upgraded SA environment. Upgrade agent completes successfully on fresh install SA 10.20 and SA 10.21 environment.	
210421/210425	Solaris 10 'unable to extract installed package list: 32512' error during software registration.	Solaris
210428/210709	Agent installation takes a long time when /etc/hosts has many lines.	Independent
210440/210443	package.dbg is increasing in size uncontrollably.	HP-UX
APX CONTENT		
209759/210208	"Change user passwords for selected servers" fails to change the password when the UNIX server has a locale with chars outside the ASCII set.	Linux
AUDIT AND COMPLIANCE		
194053/194273	Exceptions are deleted from the Audit when promote changes on the Audit Policy.	Linux
202175/202177	Failed to take registry snapshot on Chinese Windows. UnicodeEncodeError: 'cp950'	Linux
214650/214651	Audit & Compliance reports are not saved correctly in Unicode format.	Independent
CHEF		
202047/202213	Downloading an updated existing cookbook does not get the latest one if tsunami is used.	Independent
DCML EXPORT TOOL (DET)		
203364	CBT message should be clear when certain Windows patches are not uploaded.	Linux
GATEWAY		
209890/209892	spin:1004 load balancing rule should be not be set to STICKY.	

INSTALLER		
209202	The SA uninstaller script: "hpsa_uninstall.sh" has been removed and replaced with the script: "uninstall_opsware.sh". Use the "uninstall_opsware.sh" script for SA installation procedures.	Independent
JOBS		
203674/203677	"User doesn't have install software permissions" on scheduled jobs if one of the server is decommissioned and the server id does not exist.	Independent
MANAGED PLATFORM SIMPLIFICATION		
204565/204797	Unknown OS showing up for RHEL 7.1 bs_hardware and in SA UI.	Independent
OGFS/OGSH (HUB)		
194543/202417	Input/output error when accessing a server filesystem in OGFS.	Linux
208193	Error messages for OGFS UAPI are missing.	Independent
OS PROVISIONING		
93006	Ability to create/modify network boot ISO was added.	Windows, Linux
194888	When saving the configuration file for a Build Plan in the SA Client, an exception will be raised when adding a "." (dot).	Independent
207208	Previous use of OS Sequences to build out a RHEL 5 server allowed the use of Permissive SELinux settings, which in turn provided valuable logging information of any suspect actions SELinux detected on the system. OSBPs on 10.20 appear to disable SELinux entirely, removing these logs. You can now set SELinux permissive mode in OS Build Plans.	Linux
207496/207497	Server boots into unprovisioned servers pool with incorrect NIC info.	Windows
208369/212185	MBC hostname being changed to default after hardware registration	Independent
208875	During RHEL 7 OS Provisioning, SA makes changes to custom ks.cfg file causing to fail due to incorrect placement of %end tag.	RHEL
212650	Mount hangs prompting for password at 5SERVER_X86_64 platform, finally failing the overall build.	Linux
PATCH MANAGEMENT		
188279/204811	PatchBundle unittype adding changed unit_file_name and unit_loc format. This caused CBT import/exports to fail leaving customers with unusable data.	Linux
189989/203289	Intermittently no patches being recommended in Win Patch Remediate	Windows
193736/202830	Multi-platform patch exceptions trigger "Incorrect Device Platform or Account" sys diag errors.	Independent
201369/202388	Previously installed common multi binary can then cause false "Installed Patch"	Windows
202022/203298	Unable to import Solaris 10 01/13 (Update 11) Patch Bundle into SA.	Solaris

203190/203201	HP-UX depots might be downloaded multiple times, wasting disk space and potentially causing timeouts	HP-UX
203191/203206	HP-UX bundles are not reported in compliance	HP-UX
204068/214323	Provide option to skip importing superseded MBSA patches	Windows
204623/204763	Could not uninstall windows patch KB3018238 via SA.	Windows
207414	When using old version of unzip, below error is reported during solpatch_import: # echo "Recommended OS Patchset Solaris 10 x86" | /opt/opsware/solpatch_import/bin/solpatch_import -a import Importing patch cluster Recommended OS Patchset Solaris 10 x86 ... Unexpected error: Traceback (most recent call last): File "./bin/solpatch_import_versioned.py", line 3827, in main ... NameError: global name 'srcpath' is not defined	Solaris
210407/210937	Upgrade rpm gives conflict error while deploying package	Independent
SCRIPTS		
156243/213633	Server scripts failing with the following Error Code: wayscripts.lockFailed	Linux
207396	Email from a remediation job contains a stack trace regardless of the job status.	Independent
SERVER MODULE (SMO)		
132960/203672	Last Logoff Time not set when users log out of Windows	Windows
SOFTWARE MANAGEMENT		
203847/203905	uln_import is not able to register user/servers in SA versions higher than 10.02. "AttributeError: sendall" error	OEL
211056	Remediation fails with following error on SA client: The remediate operation cannot be performed because an error occurred during preview. Non-zero exit code (None) from dependency solver.	Linux
SPIN (DATA ACCESS ENGINE)		
208105/208107	Spin software registration logging is too verbose, causes performance bottleneck	Independent
SPOKE (GLOBAL FILE SYSTEM MODULE)		
210203	The logging configuration should be read from /etc/opt/opsware/spoke/spoke.conf to maintain consistency with the main configuration file.	Independent
213522/213527	Spoke spawned subprocesses can escape termination on timeout	Linux
TWIST (WEB SERVICES DATA ACCESS ENGINE)		
192429/192718	SoftwarePolicyService.startRemediate does not scale well	Independent
210531	Add CRL (Certificate Revocation List) support for access to SA using SA Client desktop client with smart card authentication.	Independent
212522	Modify CAC / PIV Smartcard certificate validation to allow multiple CA root certificates.	Linux
UCMDB		

210696/210696	The SA-UCMDB connector periodically sends updates to uCMDB but it does not try to remove objects that don't exist in SA any more. That is, if an IP is changed on a managed server SA sends the new one to uCMDB but doesn't remove the old one. In uCMDB the server now will be associated with 2 IPs.	Linux
WAY (COMMAND ENGINE)		
205299/205302	opsware.agent_reach.check_reachability does not handle errors gracefully for remote commands	Linux
212106	The job load fails with the spin.invalidTransaction error, and then when a Way tries to reload the job it gets marked as STALE.	Independent

Documentation information

This section discusses documentation information for this release.

Access to SA documentation

All SA documentation is available as individual documents, or as a bundle in the SA 10.x Documentation Library on the HPE Software Support website. This site allows access to guides, release notes, support matrices, and white papers for all current and past SA releases. You can also access the current Documentation Library from the SA client online help: select **Help > Help Contents, Index and Search**.

Note: The HPE Software Support website requires an HPE Passport, which you can create once you access the site. After signing in, click the **Search** button and begin filtering documentation and knowledge documents using the filter panel. To download the documents, click the **go** link.

Once you download documents to your local drive:

1. Unzip the files.
2. Use docCatalog.html (which provides an indexed portal to the downloaded documents in your local directory) to find individual documents.
3. To search across all SA guides for a key word:
   a. Open all the PDFs.
   b. In one PDF, choose Edit > Advanced > All PDF Documents.
   c. Browse to the local directory containing your PDFs.
   d. Enter your key word and click Search.

Guides are updated for major releases only. White papers are uploaded as they are created. Changes that occur between major releases are in the Documentation errata section of release notes for the release that comes after the change.

Note: Some of guides and white papers, although released in earlier patches, are still relevant to this release. You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HPE sales representative for details. Note the Document Release Date on the title page of your guide and see the Documentation Change Notes on page 3 of most documents for a list of any revisions. The release-notes change table is at the bottom of this document.

Documentation errata

This section describes:

- Corrected information in the SA 10.20 guides.
- New information/features that will be added to the guides for the next major release.

Online Help	
SA Client	If you see a blank browser page when you try to get page-level help for your current feature window, click the Show Navigation button (upper left corner) to display the online-help table of contents.

SA Web Client	In the Summary of Server information page: "— Agent: This displays communication status, the time when the server was last registered, the number of applications and patches registered with SA" "And patches registered" should be removed.

New whitepapers

- SA Backup and Restore Best Practices - This white paper reviews the best practices you can use to backup and restore SA with minimal data loss in a situation where SA has been adversely affected by data or power failures.
- SUSE Manager SLES Importer - This whitepaper provides information about the HPSA SUSE Manager Importer, which is a tool based on HPSA RedHat Importer. The program imports packages and errata from the SUSE Manager 2.1 Server, and creates HPSA Software Policies for errata and packages hosted by SUSE Manager.
- SA Failover and High Availability - This white paper examines how to achieve failover, server load balancing, and high availability in the SA environment.
- Best Practices for using SA rhn_import to download Red Hat content for RHEL 7 - This whitepaper discusses best practices for importing RHEL 7 Content.

Send documentation feedback

If you have comments about this document, you can send them to hpe_sa_docs@hpe.com.

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.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

RED HAT READY™ Logo and RED HAT CERTIFIED PARTNER™ Logo are trademarks of Red Hat, Inc.

The OpenStack word mark and the Square O Design, together or apart, are trademarks or registered trademarks of OpenStack Foundation in the United States and other countries, and are used with the OpenStack Foundation's permission.

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 the following URL and sign-in or register: https://softwaresupport.hp.com/

Select Manuals from the Dashboard menu to view all available documentation. Use the search and filter functions to find documentation, whitepapers, and other information sources.

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

Support

Visit the Hewlett Packard Enterprise Software Support Online web site at https://softwaresupport.hp.com/