Server Automation

Software Version: 10.51

Release Notes

Document Update Date: February, 2017
Software Release Date: November, 2016

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

Introduction

This document provides an overview of the HPE Server Automation (SA) 10.51 release. It contains the following important information not included in the manuals or in the online Help.

What's new in Server Automation 10.51

Server Automation 10.51 includes the following new features, enhancements, and support changes:

Features

Feature	Description
Migration to OpenJDK	Oracle JDK has been migrated to OpenJDK. Now, SA will run its Cores and Clients using OpenJDK.
Integration with Windows Server Update Services (WSUS)	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 10.51 User Guide Use section.
SELinux support for RHEL 6.8 and RHEL 7.x	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 from separate Start/Stop commands. For more information, see **Starting and stopping the SA Agent** in the SA 10.51 User Guide Use section.

Added support

Starting with the 10.51 release, Server Automation includes support for:

- Windows Server 2016
- vCenter Server Virtual Appliance

For more information, see the SA 10.51 Support and Compatibility Matrix.

New installation options for the SA Agent

Starting with the SA 10.51 release, you can use the following new options when installing the SA Agent installer on a managed server. For more information, see **Connecting to WSUS at Agent install/upgrade** in the SA 10.51 User Guide Use section.

Flag	Arguments
`--wsus_cfg_args`	`--setupConnection`. Mandatory argument. `--wsusURL` - specifies a WSUS URL that overrides any custom attributes already set for the selected managed servers. Optional argument. `--ignoreWSUSModeCheck` - ignores that **WSUS** patching mode is not enabled on the core. Optional argument.
`--wsus_cfg_skip`	Does not run the WSUS configuration script.

Enhancements

SA 10.51 includes the following enhancement requests, implemented after the release of SA 10.50.

ID	Component	Summary	Added in version
QCCR1D226280	Software Management	Suse_manager_import tool now supports SuSE Manager 3.0.	10.51

Fixed defects

The following table includes all the defects fixed after the release of SA 10.50.

ID	Component	Summary
QCCR1D202831	Patch Management	Multi-platform patch exceptions trigger *Incorrect Device Platform or Account* errors.
QCCR1D214689	Patch Management	HPELN requires reuploading some private patches.
QCCR1D222527	Patch Management	wsusscn2.cab is not added to Peer Content Caching for patch remediations and bs_software.
QCCR1D225847	Software Management	redhat_import fails when retrieving erratum for third-party repositories fedora-epel.
QCCR1D222259	Deployability	SA CORD patch uses certificate from crypto.0 directory. This makes the installer fail when patching Wayscripts on primary core.
QCCR1D220691	Deployability	Unsuccessful CORD patch installations are not resumed.
QCCR1D221766	OS Provisioning	OSBP Deploy Agent step picks a non-available gateway when two satellites are in the same realm.
QCCR1D230606	Product Functionality	rhn_import cannot validate redhat certificate.
QCCR1D232486	Patch Management	**populate-opsware-update-library** script fails when downloading patches that contain spaces in the URL.
QCCR1D227515	Software Management	Import from RHN fails with the following error message: *Package download error: Cannot get package download link for...*
QCCR1D230852	Product Functionality	Twist hangs randomly due to JBOSS deadlock.
QCCR1D231476	Product Functionality	Rollback points throw the following error message: *The RPM rollback point object cannot be found*.
QCCR1D230617	Product Functionality	SA user interface stops responding after upgrading to SA 10.50 from a version prior to SA 10.1.
QCCR1D144033	Product Functionality	SA does not integrate with WSUS. For details on the functionality implemented for this issue, see section "What's new in Server Automation 10.51" on page 5
QCCR1D227740	Software Management	The SA Client does not show failed script or failed script output until job completion.
QCCR1D225878	Patch Management	rhn_import fails with the following error message: *urlopen error [Errno 8] _ssl.c:504: EOF occurred in violation*.

Known issues, limitations, and workarounds

The 10.51 release of SA has the following known issues and limitations.

ID	Area	Issue
QCCR1D203515	Product Functionality	Word reports missing packages when working in a multislice environment deployed on top of a Logical Volume Manager (LVM) custom partitioning. **Workaround**: Do not mount Word on the core servers where you are planning to install SA slices. Mount `/var/opt/opsware/word` on a local partition only for the core server where infrastructure/wordstore will be installed. Packages are stored in the `/var/opt/opsware/word` on the infrastructure/wordstore server. Slices only mount the NFS export, therefore no actual space is required on the slice server for this folder. Therefore, before installing the core make sure that `/var/opt/opsware/word` is not mounted and does not exist under `/etc/fstab`. After installation, only the wordstore NFS mount should be available.
QCCR1D213724	Product Functionality	Installing a secondary core fails with the following error message: *Failed to determine data pump dir*.
QCCR1D227522	Deployability	Slices may not always show the right product version in the SA client.
QCCR1D227998	Deployability	Installing additional slices fails if recurring jobs are scheduled to run. **Workaround**: Cancel any pending recurring scheduled jobs, and restart the slice installation.
QCCR1D202377	Product Functionality	CORD installation on a secondary core fails if the installer runs `word_uploads` before `patch_opsware`.
QCCR1D209907	Interface/Usability	Using kill -9 or CTRL-\ on the installer script causes `/var/tmp/oitmp` to hang. When trying to restart the installer, the following error message is displayed: `Cannot mkdir /var/tmp/oitmp`.
QCCR1D222141	Product Functionality	Tsunami is not enabled for satellites upgraded from SA 9.1x.
QCCR1D191511	Product Functionality	Oracle RAC Connection Failover is not transparent.
QCCR1D172654	Interface/Usability	SA 10.0 installer does not validate `/etc/hosts` against multiple 'localhost' definitions.

ID	Area	Issue
QCCR1D112384	Product Functionality	It is not possible to activate debug logging in apx.c.
QCCR1D209175	Product Functionality	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	The tokens used by recurring app config 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.
QCCR1D142522	DCML Export Tool (DET)	Exporting a full CBT with all.rdf and `cbt.numthreads=10` hangs. **Workaround**: Run the export with a single CBT thread by setting `cbt.numthreads=1` in the CBT configuration file. By default, the configuration file is available on the HPE Server Automation core at `/opt/opsware/cbt/cfg/default.properties`
QCCR1D220924	Product Functionality	MemoryError exception raised when remediating HP-UX managed servers.
QCCR1D156389	Product Functionality	Users and Groups SMO do not report all the groups created on Windows 2012 Essentials. The SMO does not record any changes made to the user properties. This means that audits with U&G rules are not accurate for Windows 2012 Essentials.
QCCR1D237353	Installer	You cannot upgrade to version 10.60 if the SA Core's existing certificate is MD5 base. **Workaround**: Recertify the SA Core to use a different signature algorithm.
QCCR1D233038	SA-OO integration	After upgrading SA 10.50 to SA 10.51, the certificates from keystore are deleted, which results in the failure of SA-OO Integration. **Workaround**: Perform the following steps to reimport the certificates: 1. Stop the Web Services Data Access Engine (Twist): `/etc/init.d/opsware-sas stop twist`

ID	Area	Issue

		2. Transfer the OO Central Certificate to SA:
		
		Note: When you are prompted for a password, provide the password as **changeit**.
		
		a. Export the OO Central Certificate.
		
		The procedure to export the certificate may differ depending on the OS version you have on your OO server. For more details, see the OO documentation.
		
		Note: The client certificate is not bundled with SA, therefore, you must run the certificate export command on the OO server.
		
		For example; run the following command to certificate from an OO 10.x instance installed on a Windows server:
		
		`<OO_INSTALL_DIR>\java\bin\keytool.exe -exportcert -alias tomcat -file`
		
		`C:\oocentral.crt -keystore <OO_INSTALL_DIR>\central\var\security\key.store`
		
		b. Import the OO Central Certificate to the SA Java Runtime Environment (JRE) Keystore:
		
		`/opt/opsware/openjdk/jre/bin/keytool -importcert -alias oocert -file`
		
		`/tmp/oocentral.crt -keystore /opt/opsware/openjdk/jre/lib/security/cacerts`
		
		Note: The example above uses the alias, `oocert`. However, you can use any alias when importing the certificate, provided the alias is not already used in that keystore.
		
		3. Verify whether OO Central Certificate was imported successfully:
		
		`/opt/opsware/openjdk/jre/bin/keytool –list –alias oocert –keystore`
		
		`/opt/opsware/openjdk/jre/lib/security/cacerts`
		
		4. Restart the Web Services Data Access Engine (Twist):
		
		`/etc/init.d/opsware-sas restart twist`

QCCR1D232666	Agent	If a custom certificate is added to the cert.pem file, this certificate is not available when rolling back the SA 10.51 cert pem patch. **Workaround**: Back up `/opt/opsware/openssl/cert.pem` to a secure location and restore it after upgrading.
QCCR1D233169	Patching	Some failed patch installations may show up as successful although they have been rolled back during server reboot.

ID	Area	Issue
		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.
QCCR1D193587	Interface/Usability	When scanning hosts with ipv4 and ipv6 enabled, results show both ipv6 and ipv4 IPs. However, the SSH port is not available for IPv6. **Workaround**: Modify the ADT scanning parameters based on the network topology, proxy and firewall rules. If you cannot scan unmanaged servers via ADT on IPv6, go to the **SA Client** > **Tools** > **Options** > **SA Agent Installation** > **Advanced** and remove `-S %GATEWAY_IP% --exclude %GATEWAY_IP%` from the scan parameters.
QCCR1D183967	Product Functionality	**Users and Group** remediation jobs with multiple uses and user groups fail with the following error message: *No Group found*. **Workaround**: Run a **Users and Group** remediation job with user groups followed by a remediation job. This remediates users that belong to the remediated user group.
QCCR1D175236	Product Functionality	Content import from HPE Live Network for SAVA fails in a air-gapped environments. **Workaround**: Make sure you have network connectivity before you import content from HPELN.
QCCR1D191478	Data Migration	CentOS 7 Build Plan fails with TypeError after migrating to SA 10.2 from SA 10.02 with platform installed.
QCCR1D232004	Product Functionality	Deploying a VM fails on Windows Server 2016 x64 fails with the following error message: *An error occured while running the following OS build Plan.Run 'Windows 2016 x64 Guest Customization' build plan...*
QCCR1D159841	Data Migration	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.
QCCR1D160891	Product Functionality	Cannot delete VMs from the SA Client after 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. **Workaround**: Delete the VM from the native vendor tool and reload it into SA.
QCCR1D224267	Deployability	When installing a satellite, using a realm_name different than the facility name, breaks SA functionality.
QCCR1D232753	Core Recertification	The SA web interface is not accessible from Windows browsers if your SA certificates are using an **SHA-224** signature algorithm.

ID	Area	Issue
		This is not an SA issue, but a limitation of browsers when running on Windows. **Workaround**: Access the SA web interface via a Linux browser.
QCCR1D232753	Core Recertification	The SA Java RMI Client, opswclient.jar, might not work on Windows platforms if your SA certificates are using an SHA-224 signature algorithm. This is caused by the following JDK change: Remove SHA224 from the default support list if SunMSCAPI enabled. **Workaround**: Disable the SunMSCAPI security provider. This restores support for SHA-224 in the JDK. To disable the SunMSCAPI provider either: • edit `<JRE_HOME>/lib/security/java.security` and comment out the line that defines the SunMSCAPI provider OR • disable the SunMSCAPI provider programatically by using the `java.security.Security.removeProvider()` method.
QCCR1D232581	Deployability	When upgrading to a newer SA version, variables such as BOOTSERVER, AGW and AGWPORT are not replaced in the cfg files under `/opt/opsware/boot/kickstart/opsware`.

Installation

This section describes information about installing the SA 10.51 patch:

Prerequisites for installing the patch

Before installing the SA 10.51 patch:

- Make sure your Core is using SA version 10.50 (build ID of 65.0.70496.0). See "Determining the build ID of a core server" on the next page.
- Run the `/etc/init.d/opsware-sas status` command to verify that all Core and Satellite services are functioning correctly.
- Check the certificate signing algorithm on your SA Core. If your Core is using MD5 certificates, run a full Core recertification with a signature algorithm of at least SHA1.

General recommendations

- If you are working in a multi-master mesh environment, patch the primary Core first. You can then continue with patching the secondary Cores and satellites. Do not install the patch on the secondary cores until the primary core patching has completed successfully.
- Patch each Core and satellite separately, one at a time.

- Do not work in mixed-version Core environments. These environments are supported only as transitory mixed-Core versions during patch upgrades. This is the only situation when Cores at different patch levels can temporarily coexist in a multi-master mesh.

Determining the build ID of a core server

When you install an SA patch, SA updates the **install.inv** file to record the patch installation and the patch build ID.

To determine the build ID of a core server:

1. Go to `/var/opt/opsware/install_opsware/inv`.
2. Open the **install.inv** file and search for `%basics_`.
3. Check the `build_id` parameter under the `basics_linux` line to see which base version of SA is installed on your system. For SA 10.51, this should be `build_id: opsware_65.0.72322.0`.
4. Search for `opsware_patch` in the **install.inv** file. This shows which SA patch is installed on top of the major SA release. If the `opsware_patch` entry does not exist in the **install.inv** file, no patches have been applied to your SA core.

Installing SA 10.51

To install the 10.51 SA patch follow the steps below and the instructions provided in the install script prompts.

The `opsware_installer/hpsa_patch.sh` script is used both for installing and for uninstalling SA patches. The `hpsa_patch.sh` script patches all the servers that are part of the specified SA core, as defined by the CDF file.

> HPE recommends that you install the patch on the server where the Infrastructure component is available. This is because the Infrastructure component already contains the CDF file.

1. Check the patch readme file for information on how to download the SA 10.51 patch.
2. Copy (or NFS mount) the patch installation media on the machine where you want to install the patch. The **patch_upload** folder in the installation media is only required when patching the primary core.
3. Enter one of the following commands. Add `sudo` in front of the commands to install the patch as a

non-root user.

- To patch a core: `<distribution_path>/<prefix>-patch/disk001/opsware_installer/hpsa_patch.sh [-c <cdf_file>]`
- To patch a satellite: `<distribution_path>/<prefix>-patch/disk001/opsware_installer/hpsa_patch_satellite.sh [-c <cdf_file>]`.

You can optionally provide a CDF file. Otherwise, SA uses the latest CDF version saved by the installer. This is available under `/var/opt/opsware/install_opsware/cdf/cdf.xml`.

4. In the following confirmation prompt, check that the installer has identified all the servers that are part of the core:

```
patch will be performed on the following identified core host(s). If there is any inconsistency then try again with the correct CDF.

192.168.220.10 (slice, oracle_sas, infrastructure, truth_mm_slave)

192.168.220.11 (slice, osprov)

---------------------------------------

Do you want to continue (Y/N) [Y]:patch will be performed on the following identified core host(s). If there is any inconsistency then try again with the correct CDF.

192.168.220.10 (slice, oracle_sas, infrastructure, truth_mm_slave)

192.168.220.11 (slice, osprov)

---------------------------------------

Do you want to continue (Y/N) [Y]:
```

   - press **Y** to start the patch installation.
   - press **N** to cancel the installation. Provide the latest version of the CDF file which contains all the servers, then run the patch installation command again.

5. In the **Host Passwords** screen, enter the credentials for the listed core servers:

```
Host Passwords

==============

Parameter 1 of 2

192.168.220.11 user [user34]:

Validating user
```

```
Parameter 2 of 2

192.168.220.11 password []:
```

6. Select one of the listed cryptographic protocols and press **Enter**:

```
Cryptographic Protocol Selection for the Server Automation Components

[WARNING] Please make sure that all the cores and satellites from the mesh are
at the same TLS level.

=========================================================================

1. TLSv1

2. TLSv1.1

3. TLSv1.2

Enter the option number or one of the following directives

(<p>revious, <h>elp, <q>uit)[2]:
```

   The installer runs a component status check. If the check is successful, the installer starts the patching process. You can start using all services on the core/satellite machine as soon as the patch installation completes.

Rolling back the patch

To revert SA back to version 10.50:

- on an SA core: `<distro>/opsware_installer/hpsa_patch.sh --rollback`
- on an SA satellite: `<distro>/opsware_installer/hpsa_patch_satellite.sh --rollback`
- as a non-root user: `sudo <distro>/ opsware_installer/hpsa_patch.sh --rollback`

> After uninstalling the patch, the cryptographic protocol version (i.e. TLS version) is reverted to the one set before installing the patch.

> After the rollback, do not start the services on satellites if the core is at TLS 1.0. Start the services only if the core and the satellite use the same TLS version.

Rollback order for multimaster mesh

In a multi-master mesh, roll back the patch in the following order:

1. Secondary cores
2. Satellites
3. Primary core

Supported users for patching

You can install an SA patch as one of the following users:

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. When using a regular user for installing or rolling back 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). 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 installs SA. In the example below, the user is bob.

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

General settings for user names

Make sure user names:

- are portable across systems conforming to POSIX.1-2008. The value is composed of characters from the portable filename character set. Use the following set of characters for 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 . _
- do not contain a hyphen (-) character as the first character.

Optional parameters for enable_ipv6.sh

The enable_ipv6.sh script accepts the following optional parameters:

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

Troubleshooting the patch installation

Make sure not to rename any SA default folders. This includes the **Package Repository** folder.

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. **Fix**: 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).

	Fix: 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 do not 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 SA 10.51 User Guide Use section for details on how to set up Solaris patching on your core.	Solaris patching has not yet been set up. Disregard this error.

Post-upgrade tasks

After installing the SA 10.51 patch, upgrade the SA Agents and reapply any custom settings:

1. Upgrade all the SA Agents on the managed servers and on the core machines (Model Repository). The 10.51 patch uploads updated Server Agents to the Software Repository but does not upgrade these SA Agents automatically.
2. Upgrade any SA Agents version 9.10 or earlier to version 9.11 or later. SA 10.51 does not support SA Agents older than 9.11.
3. Upgrade the SA Agents on all Windows servers where you plan to install the SA Command-line Interface (OCLI) to version 10.51. OCLI throws errors if installed on Windows servers that use SA Agent 10.50 or earlier.
4. Reapply any custom SA settings. After installing or upgrading SA, custom setting such as those for Java heap are reverted to default.

For instructions on upgrading SA Agents, see the SA 10.51 Upgrade Guide Upgrade section.

SA version history

For information on the new features, enhancements, and fixed defects introduced in previous SA 10.x releases, see:

- SA 10.50 Release notes
- SA 10.23 Release notes
- SA Release notes 10.22
- SA Release notes 10.21
- SA Release notes 10.20
- SA Release notes 10.10
- SA Release notes 10.02
- SA Release notes 10.01
- SA Release notes 10.00

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 10.51)

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!