



Best Practices For Server Automation (SA) Upgrades

Software version: All supported SA versions

Document release date: May 2015

Software release date: May 2015

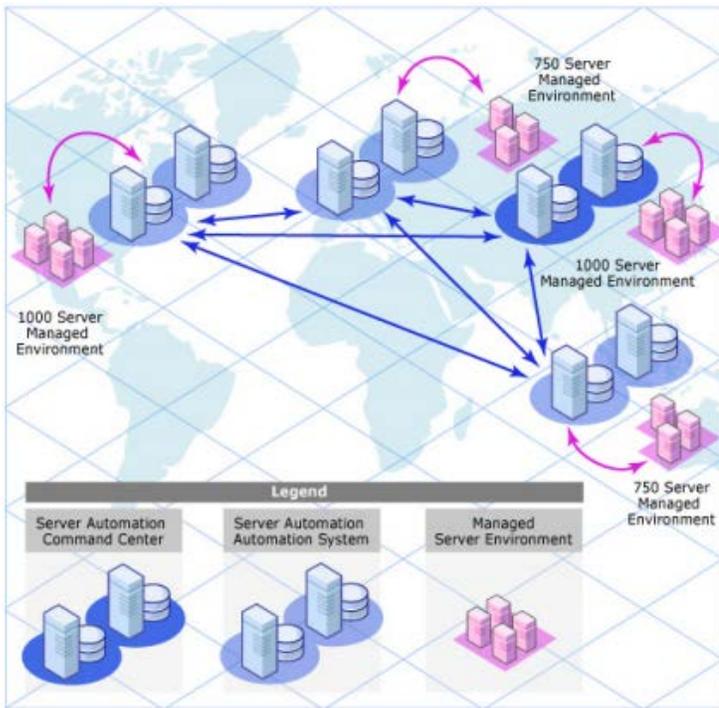
Contents

- Introduction 3**
- SA upgrade steps 3**
 - Step 1: Complete the prerequisites 4
 - 1-A Review your environment's requirements 4
 - Determine your version numbers 4
 - Identify your SA Core and SA Node: 4
 - Identify your deployment configuration: 5
 - 1-B Prepare your environment 5
 - Configure port requirements (upgrading from SA 9.1x only) 5
 - Grant permissions (upgrading from SA 9.1x only) 6
 - SUSE Linux host only 6
 - Step 2: Upgrade cores 7
 - Best practices: Use the screen utility for SA upgrades 7
 - Root access requirements 7
 - 2-A: Uninstall SA patches 7
 - 2-B: Shutdown and restart services 7
 - 2-C: Upgrade the primary core 8
 - 2-D: Upgrade the secondary core(s) for a mesh with multiple cores 9
 - Step 3: Upgrade satellites 9
 - Uninstall SA patches on SA satellites 9
 - Upgrade the satellites 9
 - Step 4: Perform the post-upgrade tasks 10
 - Upgrade the SA Agents 10

Related documentation..... 10
 SA documentation library 10
Send documentation feedback 11
Legal notices 11
 Warranty..... 11
 Restricted rights legend..... 11
 Copyright notice 11
 Trademark notices..... 11
 Documentation updates..... 11
 Support..... 11

Introduction

SA deployments usually span multiple machines and can be quite complex. Depending on the scalability requirements, a set up like the one depicted below is not uncommon.



Starting with SA 10.0, a more simplified and flexible SA upgrade installation script provides an easier upgrade experience than previous versions. Follow the simplified steps in this guide to get ready to upgrade your SA deployment.

SA upgrade steps

This upgrade consists of five basic steps:

SA Upgrade Steps

Step 1: Complete Prerequisites

- Get Ready—Review your environment’s requirements
 - determine version numbers, check upgrade paths and compatibility, identify your configuration
- Get Set—Prepare your environment
 - configure ports, verify your Multimaster Mesh is conflict-free, grant required permissions

Step 2: Upgrade the SA Cores

- Uninstall SA Patches on cores
- Shutdown/Restart Services
- Upgrade primary core
- Upgrade secondary cores

Step 3: Upgrade Satellites

- Uninstall SA Patches on satellites
- Upgrade the satellites

Step 4: Perform post-upgrade tasks

- Upgrade SA Agents

Step 1: Complete the prerequisites

This section describes prerequisite actions you must take before you upgrade SA.

Important: During the upgrade period, the SA service will not be available.

Documentation Note: This white paper references SA 10.2x guides in the core SA doc set for detailed instructions. These guides are also attached to this Best Practices PDF. To see attachments in the PDF, click the paper clip icon in the Acrobat navigation pane.

(For additional information, see [Related documentation](#) at the end of this document.)

1-A Review your environment's requirements

Determine your version numbers

This section describes how to determine the SA, OS, and database version numbers on your system.

Note: In this white paper, the words *node* and *host* are used interchangeably.

To determine your SA version:

1. In the SA Client, select **Help > About HPE Server Automation**.
2. Select HPE Server Automation Version.

This is an example of how version information is displayed:

```
HPE Server Automation 9.16 (build 45.0.47502.0)
```

In this example, the last digit of the SA version (9.16) is six (6), which is greater than zero, therefore this version of SA is a patch of the 9.10 SA GA release.

To determine your OS version:

1. Using a terminal, log on to one of the hosts on a core.
2. Enter the following command:

```
# cat /etc/issue
```

3. Repeat steps 1 and 2 for each core and satellite you are upgrading.

If your command is successful, you will see output similar to the following:

```
# cat /etc/issue
Red Hat Enterprise Linux Server release 6.5 (Santiago)
Kernel \r on an \m
```

To determine your database version:

1. Ask your Oracle database administrator.
2. Check Upgrade Paths and Compatibility.
3. Make sure that an upgrade from your present version of SA is supported. See the "*Upgrade Paths*" chapter in the [Server Automation Upgrade Guide](#) for more information.
4. Make sure that the SA version you are upgrading to is compatible with your OS and database versions. See the [Server Automation Support and Compatibility Matrix](#) to check if the new SA version is compliant with your OS version and Database Version.
5. Identify Your Deployment Configuration.

This section describes how to identify your deployment configuration, your SA Cores, and your SA nodes.

Note: Skip any steps related to components that you do not have in your configuration.

Identify your SA Core and SA Node:

For *every core* you must locate the hosts running the Infrastructure and Model Repository component bundles.

The following table describes how to identify the SA core and SA node on each core:

Table 1. Identify the SA core and SA node on each core

Component	Command	Run from	Comments
Infrastructure	<code>service opsware-sas list grep opswgw-mgw</code>	All hosts that are part of the SA core.	The host that gives an output is the Infrastructure node for your SA core. Each SA core has exactly one Infrastructure node.
Model Repository	<code>grep truth_marker /var/opt/opsware/install_opsware/inv/install.inv</code>	All hosts that are part of the SA core.	The host that gives an output is the Model Repository node of your SA core. Each SA core has exactly one Model Repository node. Note: The Model Repository and Infrastructure nodes may be collocated on the same host.

Identify your deployment configuration:

Identify your deployment configuration using the "Upgrading Supported SA Core Configuration" section in the Upgrading Procedure chapter, in the [Server Automation Upgrade Guide](#). This guide assumes the following SA core configuration:

First (Primary) Core with a Secondary Core (Multimaster Mesh)

1-B Prepare your environment

Configure port requirements (upgrading from SA 9.1x only)

Configure firewalls to allow the following:

- On the slice hosts: Open port 8061 for incoming connections from managed servers (used by the Software Repository Download Accelerator).
- On all slice and satellite hosts: Open ports 8084, 8086 and 8089 (required if you use Bandwidth Management of Remote Connections).

Verify your multimaster-mesh state is conflict free

To verify the state of your mesh:

- SA 9.1x mesh:
In the SA Web Client, select **Administration > Multimaster Tools > State View / Conflict View**.
- SA 10.0x mesh or later:
In the SA Client, select **Administration > Multimaster Tools > State View / Conflict View**.
- Resolve any conflicted transaction states (Not Sent, Not Received, or Conflict), and, for outstanding transactions (Not Sent or Not Received), allow time for replication.

See the [Server Automation Administration Guide](#) for more information on resolving mesh conflicts. If you cannot resolve the conflicts, contact HPE Support. You must resolve all conflicts before you upgrade.

Copy response files or core-definition files (CDF) (optional)

Response files and Core Definition Files (CDF) store the SA parameters used to configure your SA installation. Prior to SA 10.0, SA "response files" were used; after SA 10.0, "CDF files" were used.

This section pertains only to environments where the response or CDF files were saved to a secure location after the initial SA installation.

- If you retained the response and CDF files in their default location after the SA installation, you can skip to the next section.
- If, for security reasons, your response or CDF file was saved to a location other than the default location, you can copy it back to the respective directory on the core's Infrastructure host that you are upgrading, as described below:
 - For response files: `/var/opt/opsware/install_opsware/resp`
 - For CDF files: `/var/opt/opsware/install_opsware/CDF`

Instructions vary depending on the version of SA you are upgrading from, as described in this section.

Note: For an explanation of the use case for saving a copy of these files to a non-default location, see "The SA Interview and the Core Definition File (CDF)" topic in the [Server Automation Upgrade Guide](#).

If you are upgrading from SA 9.1x:

1. For each SA core:
 - a. Find the response file that was used during the initial SA installation on the core's Infrastructure node.
 - b. Copy this file to the following directory on the core's Infrastructure host:

```
/var/opt/opsware/install_opsware/resp
```

Tip: Note the filename as you will need it later when you are performing the SA upgrade.

2. For each SA satellite:
 - a. Find the response file that was used during the initial SA installation on the satellite's host.
 - b. Copy this file to the following directory on the satellite's host:

```
/var/opt/opsware/install_opsware/resp
```

Tip: Note the filename as you will need it later when you are performing the SA upgrade.

If you are upgrading from SA 10.0 or later:

1. For each SA core:
 - a. Find the CDF file that was used during the initial SA installation on the core's Infrastructure node.
 - b. Copy this file to the following directory on the core's Infrastructure host:

```
/var/opt/opsware/install_opsware/cdf
```

Tip: Note the filename as you will need it later when you are performing the SA upgrade.

2. For each SA satellite:
 - a. Find the CDF file that was used during the initial SA installation on the satellite's host.
 - b. Copy this file to the following directory on the satellite's host:

```
/var/opt/opsware/install_opsware/cdf
```

Tip: Note the filename as you will need it later when you are performing the SA upgrade.

Grant permissions (upgrading from SA 9.1x only)

To grant the required "create job" permission to the `opsware_admin` database user, ask your database administrator to run the following command on the database node:

```
# su - oracle
# sqlplus "/" as sysdba
grant create job to opsware_admin with admin option;
```

SUSE Linux host only

Note: These instructions pertain only to core hosts running on a SUSE Linux operating system.

Before upgrading, run the following command on the all of the SUSE Linux core and satellite hosts:

Server Automation

Best Practices For Server Automation (SA) Upgrades

```
# rpm -e rsync
```

Important: If you do not run this command now, the prerequisite check will render a failure message during the upgrade.

Step 2: Upgrade cores

This section explains how to upgrade your cores.

Important: During the upgrade period, the SA service will not be available.

Note: For topics pertaining to upgrade disk space requirements, search for "space" in the [SA Upgrade Guide](#).

Best practices: Use the screen utility for SA upgrades

HPE recommends that you invoke the SA upgrade scripts from the root (/) directory using the *screen* utility.

Root access requirements

To perform the SA Upgrade installation, you must have the following access:

- Root SSH access to all hosts used by the SA core, and
- Read/write root access to any mounted directories used during the upgrade of SA components, including any NFS-mounted network volumes.

2-A: Uninstall SA patches

If you have any SA patches installed on the servers you want to upgrade, remove them all before upgrading.

Important Notes:

- **Requirement:** You must remove all the patches from all the servers being upgraded prior to performing the upgrade.
- **Warning:** Follow all the steps in this section consecutively to ensure that you completely uninstall the patches. You can skip any steps related to components you do not have in your configuration.
- **Note:** The `--force_run` option, which is used in many of the commands in this section, is required since SA 10.0 and allows the script to run on standalone hosts.
- **Best Practice—sequence matters:** In a multimaster-mesh environment, HPE recommends that you rollback the secondary cores first, then the primary core, to make sure that the primary core is at a higher version than the secondary cores.

To uninstall SA patches, perform the following steps on each SA core:

1. Run the following command on all hosts that are part of the core, starting with the Infrastructure node:

```
<distro>/*-primary/disk001/opsware_installer/uninstall_patch.sh --force_run
```

(where `<distro>` is the root mount of the new SA version distribution).

Warning: Run this step only on hosts that are part of the SA core. Do NOT run this step on SA satellites or on the remote database host.

2. Run the following command to uninstall the database patches on the Model Repository:

```
<distro>/*-primary/disk001/opsware_installer/uninstall_patch_db.sh -r  
/var/opt/opsware/install_opsware/resp/resp.<Timestamp> --force_run
```

(where `<distro>` is the root mount of the new SA version distribution and the response file specified using the "-r" option is the one that was used during the core installation).

2-B: Shutdown and restart services

1. On each secondary core host, use the following command to shut down all SA services in the Multimaster Mesh:

```
/etc/init.d/opsware-sas stop
```

2. On each secondary core host, use the following command to start the management and core gateways:

```
/etc/init.d/opsware-sas start opswgw-mgw opswgw-cgws
```

2-C: Upgrade the primary core

Important: Upgrade the primary core only after completing steps 2-A and 2-B.

Upgrade the primary core, first. Instructions for upgrading the primary core vary depending on the version from which you are upgrading.

If upgrading from SA 9.1x:

1. On the primary Infrastructure node, make sure that the response file that was used during SA installation is located in the following directory:

```
/var/opt/opsware/install_opsware/resp/
```

2. Run the following command on the Infrastructure node:

```
<distro>/*-primary/disk001/opsware_installer/hpsa_upgrade.sh
```

(where <distro> is the root mount of the new SA version distribution)

Note: If you copied in a saved response file in [step 1-B](#), run this command to specify that response file, where "resp.<copiedFileName>" is the name of your copied response file:

```
<distro>/*-primary/disk001/opsware_installer/hpsa_upgrade.sh -r  
/var/opt/opsware/install_opsware/resp/resp.<copiedFileName>
```

3. When prompted, specify all the hosts that are part of the SA core you are upgrading.

If upgrading from SA 10.0 or later:

1. On the primary Infrastructure node, make sure the Core Definition File (CDF) used during SA installation is located in the following directory:

```
/var/opt/opsware/install_opsware/cdf/
```

2. Run the following command on the Infrastructure node:

```
<distro>/*-primary/disk001/opsware_installer/hpsa_upgrade.sh -c  
/var/opt/opsware/install_opsware/cdf/cdf.xml
```

(where <distro> is the root mount of the new SA version distribution)

Note: If you copied in a saved CDF file in [step 1-B](#), run this command to specify that CDF file, where "cdf.<copiedFileName>" is the name of your copied CDF file:

```
<distro>/*-primary/disk001/opsware_installer/hpsa_upgrade.sh -c  
/var/opt/opsware/install_opsware/cdf/cdf.<copiedFileName>
```

3. When prompted, specify all the hosts that are part of the SA core you are upgrading.

2-D: Upgrade the secondary core(s) for a mesh with multiple cores

Important: Only proceed with upgrading the secondary core(s) after completing the primary core upgrade process.

You can upgrade the secondary cores in a mesh one at a time, or you can upgrade multiple secondary cores at the same time.

To upgrade the secondary cores:

1. On the secondary infrastructure node, follow the steps described under [Upgrade the Primary Core](#) in this document.
2. After each secondary core has been upgraded, its services are automatically restarted.

The upgraded core will remain running while you upgrade the other secondary cores.

Step 3: Upgrade satellites

Important: You are not *required* to upgrade your satellites immediately after a Core upgrade, but it is *highly recommended*.

Note: When upgrading from SA 10.0 or SA 10.01 to SA 10.2, the SA 10.0/10.01 satellites become unreachable. To resolve this [known issue](#), upgrade all SA satellites to version 10.2 after upgrading the SA core.

To upgrade the satellites:

1. Uninstall SA Patches for the SA Satellites
2. Perform the upgrade on each satellite

Uninstall SA patches on SA satellites

To uninstall SA patches on satellites:

1. On each of the core's satellites run the following command to determine if an SA patch has been applied:

```
grep opsware_patch /var/opt/opsware/install_opsware/inv/install.inv
```

If the command returns output, a patch has been applied to the satellite.

2. On the same host, run the following command to uninstall the patch:

```
<distro>/*-primary/disk001/opsware_installer/uninstall_patch.sh --force_run
```

(where <distro> is the root mount of the new SA version distribution)

Upgrade the satellites

If upgrading from SA 9.1x:

1. Run the following command on the satellite:

```
<distro>/*-sat_osprov/disk001/opsware_installer/hpsa_upgrade_satellite.sh
```

(where <distro> is the root mount of the new SA version distribution)

2. When prompted, add all the satellite hosts (for satellites with distributed components).

If upgrading from SA 10.0 or later:

1. Run the following command on each satellite:

```
<distro>/*-sat_osprov/disk001/opsware_installer/hpsa_upgrade_satellite.sh
```

(where <distro> is the root mount of the new SA version distribution)

2. When prompted, add all the hosts that the satellite runs on (for satellites with distributed components).

Step 4: Perform the post-upgrade tasks

This section describes the post-upgrade tasks you should perform on your system.

Upgrade the SA Agents

You are not required to upgrade the agents, but in order to take advantage of the latest functionality that may have been added in the new release, agents must be upgraded. If you continue using an older agent, certain new functionality may not be available on the server managed by that agent.

To upgrade SA agents:

1. In the SA Client, select **Devices > All Managed Servers**.
2. Select one or more servers from the list of available servers.
3. Select **Actions > Run > Agent Upgrade**.

Note: See the "Agent Installation and Upgrade Utilities" chapter in the *SA User Guide: Server Automation* for more information.

Related documentation

This white paper references relevant guides in the core SA 10.2 doc set for detailed instructions:

- [Server Automation 10.2 Upgrade Guide](#)
- [Server Automation 10.2 Administration Guide](#)
- [Server Automation 10.2x Support and Compatibility Matrix](#)

These guides are attached to this Best Practices PDF for your convenience. To see attachments in the PDF, click the paper clip icon in the Acrobat navigation pane. Click the bookmark icon to return to the navigation view.

SA documentation library

You can use the *SA Documentation Library* to find the latest version of the guides for your version of SA on the [HPE Software Support Online](#) (HPE Passport required):

- [Server Automation 9.1x Documentation Library](#)
- [Server Automation 10.x Documentation Library](#)

Note: The landing page on the SA 10.x Client Help also links to the SA Documentation Library.

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

© Copyright 2015 Hewlett Packard Enterprise Development LP

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.hpe.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.hpe.com/>