HP Server Automation
Storage Visibility and Automation

for the HP-UX, IBM AIX, Red Hat Enterprise Linux, Solaris, SUSE Linux Enterprise Server, VMware, and Windows® operating systems

Software Version: 7.80

Installation & Administration Guide

Document Release Date: June 2009
Software Release Date: June 2009

Legal Notices

Warranty

The only warranties for HP 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. HP 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 HP 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 Notices

Trademark Notices

Intel® Itanium® is a trademarks of Intel Corporation in the U.S. and other countries.

Java™ is a US trademark of Sun Microsystems, Inc.

Microsoft®, Windows®, Windows® XP are U.S. registered trademarks of Microsoft Corporation.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

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:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

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

Support

Visit the HP Software Support Online web site at:

www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP 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 web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP 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 HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Contents

1 Introduction

Storage Essentials (SE) version 6.1.1 or later is required to view, report, or perform any Service Automation Visualizer (SAV) and Service Automation Reporter (SAR) operation on SAN objects, such as arrays, switches, volumes, and so on. SAN objects are discovered in Storage Essentials. To enable discovered SAN objects in the SA, SAV, and SAR products, the Server Automation SE Connector component must be installed and configured.

The following storage components for Storage Visibility and Automation must be installed and deployed:

- Storage Host Agent Extension (SHA)
- Database Scanner for Oracle
- SE Connector

Host storage supply chain information is discovered and collected by a Storage Host Agent Extension (SHA) in Storage Visibility and Automation. Storage asset information is discovered in Storage Essentials (SE) and then collected by Storage Scanners in Storage Visibility and Automation. This document explains how to install, configure, deploy, and manage Storage Host Agent Extensions and Storage Scanners in Storage Visibility and Automation.

- Information about a host storage supply chain is provided by a Storage Host Agent Extension (SHA). See Storage Host Agent Extension (SHA) on page 19 for more information about this component.
- Information about Oracle storage configurations in a SAN or Network Attached Storage (NAS) is collected by a component in Storage Visibility and Automation called the *Database Scanner for Oracle*. This Storage Scanner retrieves data about Oracle instance, tablespaces, and datafiles. See Database Scanner for Oracle on page 27 or Storage Scanner Configuration and Operation on page 34 for more information about this component.
- Information about storage arrays, switches, fabrics, and NetApp filers in your environment is collected by a component in SA called *SE Connector.* SE Connector retrieves data about the SAN infrastructure from SE. This storage data is transferred to the SA core and stored in the Model Repository. See SE Connector on page 21 or Storage Scanner Configuration and Operation on page 34 for more information about this component.

This guide is intended for system administrators and server administrators who are responsible for installing and configuring Storage Visibility and Automation. This documentation assumes that you are familiar with the operating systems on which this feature will be installed. It is also assumed that you have the required permissions to install this software on managed servers.

See the *SA Planning and Installation Guide* for information about how to install and configure Server Automation. See the *SA User Guide: Application Automation* for information about Service Automation Visualizer. See the *SAR User Guide* for information about Service Automation Reporter. See the *Storage Essentials Installation Guide* for information about how to install and configure Storage Essentials.

2 Installation & Deployment

The following table identifies the storage components for Storage Visibility and Automation that must be installed and deployed. This table also identifies the source required to install each storage component.

Table 1 Required Storage Components

Storage Component	Installation Source
Storage Host Agent Extension (SHA)	Agent and Utilities DVD
Database Scanner for Oracle	Agent and Utilities DVD
SE Connector	BSA Essentials Network

The SHA and Database Scanner for Oracle storage components are part of the Agent and Utilities DVD, which is commonly known as the *upload media*. These storage components are part of the `Software Repository - Content` in the upload media. The upload media contains the agents and utilities, such as the OS Provisioning Boot Agent, Agents for various operating systems, and so on. After the Server Automation (SA) core has been installed, these agents and utilities must be uploaded to the Software Repository.

For this release, SE Connector must be installed using the BSA Essentials Network. SE Connector is *not* part of the Agent and Utilities DVD. To access the BSA Essentials Network and download SE Connector installation instructions, go to www.hp.com/go/bsaenetwork.

When the Storage Visibility and Automation installation process is completed, you will have the following storage components in your SA core:

- Storage Host Agent Extension (SHA)
- Database Scanner for Oracle
- SE Connector

See Storage Host Agent Extension (SHA) on page 19, Database Scanner for Oracle on page 27, and SE Connector on page 21 for more information about these storage components.

Installation Transcript Example

The following is an example of the BSA Installer transcript that shows the sequence of user actions required to install the SHA and Database Scanner for Oracle storage components.

```
Welcome to the Opsware Installer.
Please select the components to upgrade.
1 ( ) Software Repository - Content (install once per mesh) [UP TO DATE]
2 ( ) OS Provisioning Linux Media Verification
Enter a component number to toggle ('a' for all, 'n' for none).
When ready, press 'c' to continue, or 'q' to quit.
```

`Selection:`

The SHA and Database Scanner for Oracle storage components are explicitly not shown in this example because they are included in the `Software Repository - Content`. These storage components are installed, upgraded, or uninstalled along with other Software Repository components.

During the installation process, the BSA Installer saves all transcript answers in a *response file* and provides the name and location of the response file.

For future use, specify the name of this response file to upgrade the Software Repository. When you specify the name of the response file, you do not need to repeatedly answer the same transcript questions.

When the `Software Repository - Content` is installed, you will have the following storage components in your SA core:

- Storage Host Agent Extension (SHA)
- Database Scanner for Oracle

See Storage Host Agent Extension (SHA) on page 19 and Database Scanner for Oracle on page 27 for more information about these storage components.

Storage Host Agent Extension (SHA)

For SHA, the installation process creates a server module named `com.opsware.storage.storex` in the `/Opsware/Tools/Server Modules/` folder. Typically, you will not have permission to access this server module.

You can access SHA (which is internally known as *storex*) by creating a snapshot specification for storex. This process is standard for any server module snapshot.

See Storage Host Agent Extension (SHA) on page 19 for more information about this storage component.

Database Scanner for Oracle

For the Database Scanner for Oracle, the installation process creates the following:

- An APX module named `APX Oracle database scanner` in the `/Opsware/Storage/Tools/DbScanner` folder.
- A server module named `com.opsware.server.module.storage.dbscanner.oracle` in the `/Opsware/Tools/Server Modules/` folder.
- An ASAS Agent named `OracleDBScanner` that provides a user interface for viewing and managing the login credentials.
- A secured namespace named `OPSW_SCANNER_ORACLE_INSTANCE` for login credentials.

This installation process also configures metadata that is used for the login credentials. To support different locales, this metadata is stored as a UTF-8 string.

SE Connector

SE Connector must be installed from the BSA Essentials Network at www.hp.com/go/bsaenetwork.

The following processes are required to get the SE Connector executable to a managed server:

- The *installation process* prepares packages and software policies in the core.
- The *deployment process* copies the binaries to a managed server and then configures them.

Prerequisites

Server Automation 7.80 or later and Storage Essentials 6.1.1.x and are required to install, configure, and deploy SE Connector.

Installation Process

The installation process creates the following:

- An `/Opsware/Storage/Agents/SE` folder that contains all required packages for SE Connector and software policies for all versions of SE Client Library. Based on the operating system, the following two types of packages are uploaded to the SE folder:

  `OPSWsa-se-<OS>-xx.x.x.x.xx.zip`

  This file contains the SE Connector code (binaries) for a certain operating system (<OS>).

  Examples:

  `OPSWsa-se-linux-37.0.0.4.20.zip`

  `OPSWsa-se-solaris-37.0.0.4.20.zip`

  `OPSWsa-se-win-37.0.0.4.20.zip`

  `OPSWsa-seclient-x.x.x.x-<OS>.zip`

  This file contains the default SE Client Library for a certain operating system (<OS>).

  Examples:

  `OPSWsa-seclient-6.1.1.9-linux.zip`

  `OPSWsa-seclient-6.1.1.9-solaris.zip`

  `OPSWsa-seclient-6.1.1.9-win.zip`

For each supported operating system, the installation process prepares two packages in the SE folder. The examples above show packages for Linux, Solaris, and Windows operating systems.

- A software policy named `SE Storage Scanner` in the `/Opsware/Storage/SE` folder.
- Several common packages in the `/Opsware/Storage/Agents` folder.

See SE Connector on page 21 for more information about this storage component.

Deployment Process

In the deployment process, the administrator selects the software policy for SE Connector and assigns managed servers to it. During deployment, all relevant packages are copied to a managed server and all pre- and post-install scripts are executed. To complete the deployment process, SE Connector must be configured and then (automatically) started.

To deploy SE Connector on a managed server, perform the following steps:

1. In the Navigation pane, select **Library ➤ By Folder**.
2. Select **Opsware ➤ Storage ➤ Agents ➤ SE** to open the SE folder.
3. Open the "SE Storage Scanner" software policy.
4. (Optional) Modify the post-install script. See Modifying a Post-install Script on page 12.
5. In the Views pane, select Server Usage.
6. Select **Actions ➤ Attach Server**.
7. In the Attach Server dialog, select **All Managed Servers** to view a list of servers that meet the qualifications for an SE Scanner.
8. In the Attach Server content pane, select a managed server and then click **Attach**.
9. Complete the Attach Server wizard. When remediation is finished, SE Connector is configured and running on the specified managed server.

Modifying a Post-install Script

If port 7050 or port 7034 (the default) are not available on the managed server, you must modify the post-install script of the main package of SE Connector (for the corresponding operating system). Post-install scripts are executed after the package is copied and unpacked on the managed server. To modify a post-install script, perform the following steps:

1. Open the "SE Storage Scanner" software policy.
2. In the Views pane, select Policy Items.
3. Select a package with a name similar to "OPSWsa-se-linux-37.0.0.4.0.zip". This name must match the operating system name of the managed server.
4. Right-click and then select Open to display the package Properties.
5. Expand "Install Scripts" and then select the "Post-Install Script" tab.
6. In the script, find the USER PARAMETERS section, such as

```
################## USER PARAMETERS ################
SRQST_JNP_PORT=7050
HTTP_PORT_VALUE=7034
################## USER PARAMETERS ################
```

7. Change the value(s) and then save the package.

Deployed Components

The following filesystem layouts identify deployed storage components, by operating system.

Unix-like Operating System

```
/etc/opt/opsware/pam-se .. config files
/etc/opt/opsware/startup/pam-se start|stop|status
```

```
/opt/opsware/pam-se
   bin ............... start/stop scripts
   lib ............... jar-files, third party libraries
   jboss .............
   clientlib ......... common folder for all supported SE Client libs

/opt/opsware/pam-common/
   lib   ............. common libraries (netmux.pyc)
   jdk   ............

/var/log/opsware/pam-se/ ... log-files

/var/opt/opsware/pam-se
   data  ............. Full sync
   security .......... DeviceAccessControls
   requests .......... ServiceRequests   OPTIONAL
```

Windows Operating System

```
%ProgramFiles%\Opsware\pam-se
   bin ............... start/stop scripts
   lib ............... jar-files, third party libraries
   jboss .............
   clientlib ......... common folder for all supported SE Client libs

%ProgramFiles%\Common Files\Opsware\etc\pam-se ... config
%ProgramFiles%\Common Files\Opsware\log\pam-se ... log-files OPTIONAL
%ProgramFiles%\Common Files\Opsware\pam-se
   data  ............. Full/sync
   security .......... DeviceAccessControls
   requests .......... ServiceRequests    OPTIONAL
%ProgramFiles%\Common Files\Opsware\pam-common ...
   lib    ............ common libraries (netmux.pyc)
   jdk    ............
```

3 Uninstallation & Undeployment

You can uninstall or undeploy storage components as follows:

- Uninstalling Components from a Core
- Uninstalling SE Connector from a Managed Server
- Removing SE Connector from the Model Repository
- Uninstalling the Database Scanner for Oracle

Uninstalling Components from a Core

SHA and Database Scanner for Oracle Components

To uninstall the SHA and Database Scanner for Oracle storage components, run the BSA Installer `uninstall_opsware.sh` script from the upload media. You cannot individually uninstall these storage components because they are part of the upload media. This action uninstalls the SHA and Database Scanner for Oracle storage components, including *all* Software Repository components. This script does *not* uninstall SE Connector from a core because SE Connector is not part of the upload media.

SE Connector Component

To uninstall the SE Connector storage component from a core, you must use the BSA Essentials Network. To access the BSA Essentials Network and download SE Connector uninstallation instructions, go to www.hp.com/go/bsaenetwork.

Before you uninstall the SE Connector component from a core, make sure the SE Storage Scanner has been undeployed from all managed servers.

Uninstalling SE Connector from a Managed Server

When you uninstall SE Connector from a managed server, the access controls and discovered data are deleted from the managed server. *Uninstalling SE Connector from a managed server* is also known as *undeploying SE Connector from a managed server.* You would typically undeploy SE Connector from a managed server when you need to repurpose that server. Because SE Connector implements common Server Automation features (such as software policy and remediation) that are independently controlled by the user interface, you can selectively uninstall this storage component without affecting any other storage component.

If you need the existing configured access controls for future use, be sure and save them before detaching the managed server from SE Connector. When you detach the server from the software policy, all SE Connector binaries and data will be removed from the managed server.

To uninstall (undeploy) SE Connector from a managed server, perform the following steps:

1. In the Navigation pane, select **All Managed Servers**.
2. Select the server that you want to undeploy SE Connector from.
3. From the View drop-down, select Software Policies.
4. In the lower Software Policies pane, select the SE Storage Scanner software policy.
5. Right-click and then select Detach.
6. In the Detach Software Policy dialog, click **Detach**.
7. In the Remediate dialog, confirm your selection and then run or schedule the job.
8. Wait until the job completes.

Or

1. In the Navigation pane, select **Library ➤ By Folder**.
2. Select **Opsware ➤ Storage ➤ Agents ➤ SE** to open the SE folder.
3. Open the "SE Storage Scanner" software policy.
4. In the Views pane, select Server Usage.
5. In the Server Usage content pane, select a managed server, right-click, and then select Detach Server.
6. Click **Detach** to start the job and then wait until the job completes.

Removing SE Connector from the Model Repository

When you remove SE Connector, its entry is removed from the Model Repository.

This operation applies only to SE Connector. It does not apply to the Database Scanner for Oracle.

To remove SE Connector, perform the following steps:

1. In the Navigation pane, select **Administration ➤ Storage Scanners**.
2. In the content pane, select a Storage Scanner.
3. Right-click and then select Remove.

Uninstalling the Database Scanner for Oracle

The Database Scanner for Oracle component is uninstalled by running the BSA Installer `uninstall_opsware.sh` script.

During the uninstall process, you will be asked whether configured login credentials should be preserved. If you are planning to install the Software Repository again and repeat discovery for the same databases, it is recommended that you preserve these login credentials. When you confirm that you want to keep these credentials, the uninstall process continues without removing them.

To uninstall the Database Scanner for Oracle, perform the following steps:

1. Insert the upload media.
2. Run the BSA Installer `opsware_installer/uninstall_opsware.sh` script.
3. Select `Software Repository - Content` and start the uninstall process. This process removes the Database Scanner for Oracle component.

4 Storage Host Agent Extension (SHA)

Storage Host Agent Extension (SHA) is a Server Automation (SA) server module that manages host storage. SHA provides the Web Services Data Access Engine with information about a host storage supply chain. This information includes, but is not limited to, the following artifacts:

- Fabric channel HBA assets—adapters and ports
- Fabric channel HBA devices—targets and logical units
- Disk devices—block, raw, and partitions
- Multipath I/O (MPIO) assets, configuration, and devices
- Volume manager (VM) assets, configuration, and devices
- Filesystems

This storage information is collected by a snapshot specification that you create.

See the *Storage Visibility and Automation Release Notes* for a list of operating systems SHA supports.

Prerequisites

The Server Automation (SA) core must be running when you install the SHA distribution. See the *SA Planning and Installation Guide* for information about installing and configuring an SA core.

Before installing a Storage Host Agent Extension (SHA) on an HP-UX system, verify that the operating system has all available updates and patches installed.

Upgrading a Storage Host Agent Extension

SHA is upgraded when an administrator needs to install SHA on an SA core that already contains an SHA module.

Before starting the upgrade process, verify that there are no storage inventory snapshot jobs running.

During the upgrade process, the HP BSA Installer removes all previous versions of the SHA module from the SA core before installing the new version. All existing snapshot specifications remain unchanged and are ready for execution with the upgraded SHA module.

To upgrade SHA on an SA core, use the `upgrade_opsware.sh` command.

To upgrade SHA on a managed server, use the SA Web Client or run a snapshot.

Creating a Storage Inventory Snapshot for Host & VMware Servers

You can create storage inventory snapshots for host (SHA) servers and VMware ESX and ESXi servers. SHA is a server module that you run on a managed server (or group of servers) by creating a snapshot specification that includes storage inventory information. VMware is part of the storage inventory snapshot for Unix operating systems, where the target is an ESX or ESXi server.

In addition to creating storage inventory snapshots of an ESX server, you also need to create snapshots for all associated virtual machines defined on that ESX server in order to collect complete storage supply chain information for the machines. File system data for ESX and ESXi servers is not collected.

To create a snapshot specification, perform the following steps:

1. From the Navigation pane, select **Library ➤ By Type ➤Audit and Remediation ➤ Snapshot Specifications**.
2. From the expanded Snapshot Specifications folder, select the operating system that you are creating the snapshot specification for—Windows or Unix. For ESX hypervisors, select Unix.
3. From the Actions menu, select **New** to display the Snapshot Specification Properties window.
4. Enter a name for the storage inventory snapshot.
5. (Optional) Enter a description for the inventory snapshot.
6. Verify that the Perform Inventory option is checked. The default is unchecked.
7. From the Views pane, expand Targets to display the Snapshot Specification Targets window.
8. Click **Add** to add the hosts or host groups that are to be included in the storage inventory snapshot.
9. From the Views pane, select **Rules ➤ Storage** to display the Snapshot Specification Rules Storage window.
10. To request an Inventory snapshot, select Inventory in the Available for Snapshot Specification section.
11. Click the + >> button to move Inventory to the Selected for Snapshot Specification section.
12. From the File menu, select **Save** or press **Ctrl-S**.
13. From the Actions menu, select **Run Snapshot Specification**.
14. Continue advancing through the Run Snapshot Specification steps until the job completes.
15. Click **Close** to close the Job Status window.

See the *Storage Visibilty and Automation User Guide* for more information about Storage Host Agent Extension (SHA) and VMware ESX and ESXi support.

5 SE Connector

SE Connector is the Storage Scanner that collects data from Storage Essentials (SE) about SAN elements and inventory, and their connectivity. These SAN elements include storage arrays, fabrics, switches, and NAS filers.

The frequency of collecting this storage data is configured by the user. By default, SE Connector collects SAN information from SE once every 24 hours. This action is commonly known as *a scheduled full synchronization*. You can adjust the collection frequency by modifying a setting in SE. In SE Connector, you can specify the maximum wait time (in minutes) for a scheduled full synchronization when the Get All Elements Detail (GAED) process in SE is in progress. The following property specifies the maximum wait time for a scheduled full synchronization task when GAED is in progress:

```
com.creekpath.agent.common.devices.scheduled.full.sync.max.wait.minutes=60
```

SE Connector can communicate with multiple Storage Essentials instances. For scalability and performance reasons, it is recommended that you have *multiple* SE Connectors communicating to *one* instance of Storage Essentials; however, each Access Control must be configured to collect a unique set of devices from the same Storage Essentials instance. You can also have *multiple* SE Connectors communicating with *multiple* instances Storage Essentials.

Since, by default, storage information is collected from SE once every 24 hours, you might need updated data more frequently than once a day. You can modify this data collection frequency by modifying a setting in SE. See the *Storage Essentials SRM Software User Guide* for information about configuring the schedule for data collection. You can also request an update of SAN information from SE at the storage device level, such as arrays and NetApp filers. See Update from Storage Essentials on page 25 for more information.

When you are viewing storage information about a SAN array or NetApp filer in Storage Visibility and Automation and would also like to view storage information for the same SAN array or NetApp filer in Storage Essentials, you can launch Storage Essentials to display the data that was discovered. See Authorizing a Storage Scanner on page 35 for more information. See the *Storage Essentials SRM Software User Guide* for information about the discovery process in SE.

See Storage Scanner Configuration and Operation on page 34 for information about managing the SE Connector.

See the *Storage Visibility and Automation Release Notes* for a list of operating systems SE Connector supports.

Prerequisites

Server Automation 7.80 or later and Storage Essentials 6.1.1.x and are required to install, configure, and deploy SE Connector.

For this release, SE Connector must be installed using the BSA Essentials Network. SE Connector is *not* part of the Agent and Utilities DVD. To access the BSA Essentials Network and download SE Connector installation instructions, go to www.hp.com/go/bsaenetwork.

You must also authorize SE Connector before using it. Authorization enables SE Connector to accept different requests, such as start and stop. See Authorizing a Storage Scanner on page 35.

The identity of this Storage Scanner is defined by Server Automation Agent properties. This identity is not changed until the Storage Scanner is restarted. This means that you must always stop the Storage Scanner *before* an SA Agent is reinstalled on a server. See Starting a Storage Scanner on page 35, Stopping a Storage Scanner on page 36, and Reassigning a Deployed SE Connector on page 24.

Access Controls

The SE Connector Storage Scanner uses access controls to communicate with an instance of Storage Essentials for collecting information about SAN array, switch, fabric, and NetApp filer inventory.

To create an access control for SE Connector, the following information is required:

- IP address of the host where Storage Essentials is running
- Username of an existing user in Storage Essentials
- Password for the existing user in Storage Essentials

Do not collect the same set of devices from the same instance of Storage Essentials from different access controls.

Viewing Access Controls for SE Connector

To view access controls for SE Connector, perform the following steps:

1. From the Navigation pane, select **Administration ➤ Storage Scanners**.
2. In the content pane, select a Storage Scanner and then select **Actions ➤ Open**.
3. In the Views pane, select **Management Console**.
4. Expand **SE** and then expand **Access Controls**.
   - Select **List** to display the access controls for SE Connector.

Creating Access Controls for SE Connector

To create access controls for SE Connector, perform the following steps:

1. From the Navigation pane, select **Administration ➤ Storage Scanners**.
2. In the content pane, select a Storage Scanner and then select **Actions ➤ Open**.
3. In the Views pane, select **Management Console**.
4. Expand **SE** and then expand **Access Controls**.
5. Select **Create New** to open the Create Access Control dialog for the SE Connector.
6. Enter values for the access control in the following fields:

   Caption: A unique name that identifies the access control.

The Caption name must be unique. If an existing (duplicate) name is used to create an access control, the new access control properties will replace (overwrite) the existing access control properties.

Host Address: IP or DNS hostname of the SE Central Management Server (CMS)

User Name: The user name required to access the devices in SE

Password: Corresponding password

Or, for an HP Storage Essentials server that is integrated with HP Systems Insight Manager (SIM), enter values for the access control in the following fields:

Host Address: IP or DNS hostname of the HP Systems Insight Manager server

User Name: The user name required to access the devices in SIM and SE.

Syntax: domain-name\username

Where "domain-name" is the name of the server where the user is created or the domain of the user "username" is the name of the user who has access to the devices to collect with this Scanner.

Password: Corresponding password

7 Click **Create Access Control**.

Creating Multiple Access Controls to One Instance of Storage Essentials

You can configure multiple SE Connectors communicating to one instance of Storage Essentials; however, each access control must be configured to collect a unique set of devices from the Storage Essentials instance. This is done by first configuring users in Storage Essentials, each with restricted access to a unique set of storage devices. Then create each access control with a different user. The access control will collect only those devices that the individual user can access.

Configure users in Storage Essentials, each with restricted access to unique sets of storage devices. See the *Storage Essentials SRM Software User Guide* for information about adding users and adding them to roles and organizations.

To create access controls for SE Connector, perform the following steps:

1 From the Navigation pane, select **Administration ➤ Storage Scanners**.

2 In the content pane, select a Storage Scanner and then select **Actions ➤ Open**.

3 In the Views pane, select **Management Console**.

4 Expand **SE** and then expand **Access Controls**.

5 Select **Create New** to open the Create Access Control dialog for the SE Connector.

6 Enter values for the access control in the following fields:

Caption: A unique name that identifies the access control.

The Caption name must be unique. If an existing (duplicate) name is used to create an access control, the new access control properties will replace (overwrite) the existing access control properties.

Host Address: IP or DNS hostname of the SE Central Management Server (CMS)

User Name: User name required to access the unique set of devices in SE

Password: Corresponding password

7 Click **Create Access Control**.

Viewing Storage Essentials Servers for SE Connector

To view the access controls and information about all Storage Essentials servers that an SE Connector communicates with, perform the following steps:

1. From the Navigation pane, select **Administration ➤ Storage Scanners**.
2. In the content pane, open a Storage Scanner.
3. From the Views pane, select **Storage Essentials**.

Viewing Storage Essentials Servers Managed Elements for SE Connector

To view a list of managed elements discovered by each access control for the SE Connector, perform the following steps:

1. From the Navigation pane, select **Administration ➤ Storage Scanners**.
2. In the content pane, open a Storage Scanner.
3. From the Views pane, select **Storage Essentials**.
4. Select an access control in the right pane. The list of managed elements discovered by that access control displays in the bottom pane.

Reassigning a Deployed SE Connector

To reassign a managed server that has a deployed SE Connector (Storage Scanner) running on it to another core, perform the following steps:

1. Save all access controls on the managed server to a temporary folder. Access controls are stored on the managed server where SE Connector is running. Based on the operating system running on the managed server, these access controls are located in the following directories:

   On Unix: `/var/opt/opsware/pam-se/security`

   On Windows: `%ProgramFiles%\Common Files\Opsware\pam-se\security`
2. Undeploy SE Connector from the managed server in Core A. See Uninstalling SE Connector from a Managed Server on page 15.
3. Deploy SE Connector on the managed server in Core B. See Deployment Process on page 12.
4. Authorize the Storage Scanner in Core B. See Authorizing a Storage Scanner on page 35.
5. Stop the Storage Scanner. See Stopping a Storage Scanner on page 36.
6. Copy the access controls that you saved in Step 1.
7. Start the Storage Scanner. See Starting a Storage Scanner on page 35.

Update from Storage Essentials

You must have the required SA user permissions to request an “Update from Storage Essentials”. See the Server Automation (SA) Permissions on page 31 for more information.

“Update from Storage Essentials” is an option in the Actions menu that requests an update of storage information about an individual storage device, such as a SAN array or NetApp filer. SE Connector provides this synchronization of data for a storage system when you request an update at the device level.

SE Connector does not directly communicate with a storage device to collect data about it. SE Connector collects data about an individual storage device from Storage Essentials. This request copies data from the SE repository into the Model Repository.

You can specify the maximum wait time (in minutes) for the “Update from Storage Essentials” action in SE Connector while SE performs GAED for certain storage elements. The following property specifies the maximum wait time for the "Update From Storage Essentials" action when GAED is in progress:

```
com.creekpath.agent.common.devices.manual.full.sync.max.wait.minutes=60
```

The Jobs and Sessions user interface displays the status of the update request. A “Success” status indicates that the Model Repository has been updated. The timestamp for the job also provides the following information about the “Update from Storage Essentials” request:

- When the request was made
- When SE discovered the data
- What the status of the update job is, such as:
  - **OK**—Request was submitted successfully. SE Connector will collect the data for the requested device and send it to the Web Services Data Access Engine.
  - **Error**—Request could not be submitted. Check the SE Connector logs on the managed server to troubleshoot this error. Begin with the `pam-0-0.trace` log file and then check other trace files.

See the *SA User Guide: Server Automation* for more information about Jobs and Sessions.

-

Open with Storage Essentials (Click & Launch)

“Open with Storage Essentials” is an option in the Actions menu that launches Storage Visibility and Automation for an individual storage device, such as a SAN array or NetApp filer. You can also launch Storage Essentials for a device by selecting it and then by right-clicking—this is commonly referred to as the *Click & Launch* user interface.

SE Connector supports Click & Launch for storage devices that are managed by Storage Essentials. This functionality requires an SE account login. When you select other storage objects and then Click & Launch from them (while in the same session), the initial SE login will persist. There is no single sign-on capability for Storage Visibility and Automation and SE.

You can launch SE only from a storage device. You cannot launch SE from a host.

6 Database Scanner for Oracle

The Database Scanner for Oracle collects data about Oracle storage configurations in a SAN or Network Attached Storage (NAS), such as the Oracle instance, tablespaces, and datafiles.

Storage elements configured for an Oracle instance can be classified as *physical database storage* and *logical database storage*:

- **Physical database storage** includes datafiles and redo logs that directly consume system storage resources (filesystems or partitions) or are built on top of ASM Files.
- **Logical database storage** includes entities such as tablespaces that are created inside the instance consuming different physical and logical storage entities.

This Storage Scanner identifies relationships between the database elements and other storage assets as described in Table 1.

Table 1 Database Assets & SAN Relationships

Database Asset	External Storage Asset	Dependency	Description
SAN-based physical database storage	Server assets SAN array assets Fabric assets Switch assets	Block storage dependency	Provides the dependency chain between the database storage elements and SAN arrays through system (server) resources and fabrics.
NAS-based physical database storage	Server assets NetApp assets	NAS storage dependency	Provides the dependency chain between the database storage elements, server resources, and NetApp.

See Storage Scanner Configuration and Operation on page 34 for information about managing the Database Scanner for Oracle.

This section describes the following prerequisites for setting up the Database Scanner for Oracle:

- Storage Host Agent Extension
- Hardware Registration for the Model Repository
- Login Credentials

Storage Host Agent Extension

Before running database discovery, a snapshot of the Storage Host Agent Extension (SHA) must be created for the managed server where the Oracle instance or database is.

Hardware Registration for the Model Repository

You must perform a hardware registration with the Model Repository so that the Storage Scanner (Database Scanner for Oracle) is able to collect information about Oracle databases. For more information about hardware registration, see *SA User's Guide: Server Automation*.

Login Credentials

This section describes the login credentials for each database instance that the Database Scanner for Oracle will manage. A login credential contains values that direct the Database Scanner for Oracle to where a specific instance resides. Table 2 describes the login credentials you must create before running the Database Scanner for Oracle for the first time.

Table 2 Database Scanner for Oracle Login Credentials

Login Credential	Description
Caption	An arbitrary name that identifies the login credential. The default is Oracle LoginCredential.
User Name	The Oracle user name that is authorized to access the Oracle database. The default is oraclepam.
User Password	The Oracle password that is authorized to access the Oracle database.The default is pam.
Oracle System ID	A unique name that identifies an Oracle instance on a managed server. This ID is provided by the database administrator.
Port	The TCP port that the Oracle listener uses. The Storage Scanner communicates with the Oracle instance through this port. The default is 1521.

Viewing & Creating Login Credentials

Login credentials are parameters that allow the Database Scanner for Oracle to connect to databases and run queries that discover software application storage. To view or modify information about the login credentials for the Database Scanner for Oracle, or to add or delete credentials, perform the following steps:

1. From the Navigation pane, select **Administration ➤ Storage Scanners**.
2. In the content pane, open a Database Storage Scanner for Oracle.
3. From the Views pane, select **Login Credentials**.
4. In the content pane, select a server.
5. (Optional) Select a credential and then right-click and select one of the following options:
   - Add Credential
   - Edit
   - Delete

Viewing Login Credentials on a Server

To view the login credentials on a managed server, perform the following steps:

1. From the Navigation pane, select **Administration ➤ Storage Scanners**.
2. In the content pane, open a Database Storage Scanner for Oracle.
3. From the Views pane, select **Login Credentials**. The content pane lists the managed servers that have at least one or more login credentials created. This list will be empty if there are no login credentials configured for any of the managed servers. An empty list is typical and expected when Storage Visibility and Automation has just been installed or upgraded in a datacenter.

Creating a Database Scanner Storage Inventory Snapshot

A Database Scanner for Oracle storage inventory snapshot can be scheduled or manually started. During the snapshot process, login credentials for every managed server specified in the snapshot are retrieved. The snapshot executes discovery for all of these login credentials.

An SHA storage inventory snapshot is required before you create a database storage inventory snapshot. See Creating a Storage Inventory Snapshot for Host & VMware Servers on page 20 for more information.

To create a snapshot specification, perform the following steps:

1. From the Navigation pane, select **Library ➤ By Type ➤Audit and Remediation ➤ Snapshot Specifications**.
2. From the expanded Snapshot Specifications folder, select the operating system that you are creating the snapshot specification for—Windows or Unix.
3. From the Actions menu, select **New** to display the Snapshot Specification Properties window.
4. Enter a name for the inventory snapshot.
5. (Optional) Enter a description for the inventory snapshot.
6. Verify that the Perform Inventory option is checked. The default is unchecked.

7 From the Views pane, expand Targets and then specify one or more targets.

8 Click **Add** to add the hosts or host groups that are to be included in the inventory snapshot.

9 From the Views pane, select **Rules ➤ Database Scanner for Oracle** to display the Snapshot Specification Rules Storage window.

10 To request an Inventory snapshot, select Inventory in the Available for Snapshot Specification section.

11 Click the + >> button to move Inventory to the Selected for Snapshot Specification section.

12 From the File menu, select **Save** or press Ctrl-S.

13 From the Actions menu, select **Run Snapshot Specification**.

14 Continue advancing through the Run Snapshot Specification steps until the job completes.

A successful snapshot job is one where all discoveries are successfully completed (Succeeded). If any discovery fails, the snapshot job status will indicate a failure. If there are no login credentials created for a managed server, the snapshot job status will be reported as Failed.

15 Click **Close** to close the Job Status window.

7 Administration

This section explains the user permissions required to view storage devices and related information, and how to manage the Storage Scanners.

Server Automation (SA) Permissions

SA permissions allow users to view storage devices and related data. Table 3 specifies the permissions required by users to perform specific actions in the Storage Visibility and Automation feature. For storage administrators, this table answers the question: To perform a particular action, what permissions does a user need?

In Table 3, most of the entries in the User Action column correspond to menu items in the SA Client. In addition to feature permissions, server permissions are required on the managed servers affected by the storage discovery operation.

Table 3 Storage Visibility and Automation Permissions Required for User Actions

User Action	Required Feature	Required Permissions
Storage Systems		
Manage Storage Systems	Manage SE Storage Scanner	Read & Write
View Initiator Dependencies for Storage Systems	Manage SE Storage Scanner	Yes
View Target Dependencies for Storage Systems	Manage SE Storage Scanner	Yes
View Fabric Dependencies for Storage Systems	Manage SE Storage Scanner	Yes
Manage Public Device Group	Manage SE Storage Scanner	Yes
Start Inventory Scan	Manage SE Storage Scanner	Yes
View information for a storage array/NAS Filer	Manage SE Storage Scanner	Read
View inventory for a storage array/NAS Filer	Manage SE Storage Scanner	Read
Modify properties of a storage array/NAS Filer, such as updating a caption for a storage array/NAS Filer	Manage SE Storage Scanner	Read & Write
Delete (remove) a storage array/NAS Filer	Manage SE Storage Scanner	Read & Write
Fabrics		

Table 3 Storage Visibility and Automation Permissions Required for User Actions (cont'd)

User Action	Required Feature	Required Permissions
Manage Fabrics	Manage SE Storage Scanner	Read & Write
View Server Dependencies for Fabrics	Manage SE Storage Scanner	Yes
View Storage Dependencies for Fabrics	Manage SE Storage Scanner	Yes
Manage Public Device Group	Manage SE Storage Scanner	Yes
Start Inventory Scan	Manage SE Storage Scanner	Yes
Application Storage Automation System		
Manage DB Scanner	Manage SE Storage Scanner	Yes
Manage Fabric Agent	Manage SE Storage Scanner	Yes
Manage Storage Agent	Manage SE Storage Scanner	Yes
Authorize SE Connector	Manage SE Storage Scanner	Yes
Start SE Connector	Manage SE Storage Scanner	Yes
Stop SE Connector	Manage SE Storage Scanner	Yes
Create access controls for SE Connector	Manage SE Storage Scanner	Read & Write
Modify login credentials for the Database Scanner for Oracle	Manage Database Agent	Read & Write
Issue a synchronization request	Manage SE Storage Scanner	Yes
Remove (unauthorize) SE Connector	Manage SE Storage Scanner	Yes
Checking the current state of SE Connector	Manage SE Storage Scanner	Yes
Modifying the settings for SE Connector	Manage SE Storage Scanner	Yes
View information for a database	Manage Databases	Read
View inventory for a database	Manage Databases	Read
Modify properties of a database, such as updating a caption for a database	Manage Databases	Read & Write
Delete (remove) a database	Manage Databases	Read & Write
Add a storage array/NAS Filer to a Public Device Group	Manage Public Device Group (Storage Systems)	N/A
Add a storage array/NAS Filer to a Public Device Group	Manage Public Device Group (Storage Systems)	N/A
View relationships of servers consuming storage using the fabrics/storage switches in a storage data path	View Fabric Dependencies for Servers	Read

Table 3 Storage Visibility and Automation Permissions Required for User Actions (cont'd)

User Action	Required Feature	Required Permissions
View relationships for servers consuming storage from storage arrays/NAS Filers	View Storage Supply Chain for Servers	Read
View relationships between storage arrays/ NAS Filers and servers	View Server Dependencies for Storage Systems	N/A
View relationships for storage arrays/NAS Filers providing storage using the fabrics/ storage switches in a storage data path	View Fabric Dependencies for Storage Systems	N/A
View relationships between fabrics/storage switches in the storage data path for servers connected to them and consuming storage using them	View Server Dependencies for Fabric	N/A
View relationships between fabrics/storage switches in the storage data path for storage provided by storage arrays/NAS Filers	View Storage Dependencies for Fabric	N/A

In addition to the feature permissions listed in Table 3, every user action also requires the Managed Servers and Groups feature permission.

A user or user group must also have the "Manage Storage Systems" and "Manage Fabrics" permissions to enable corresponding "View..." storage permissions. The "View..." permissions are valid only if the user or user group has read permission for that resource type, such as you must have the "Manage Storage Systems" permission to enable the "View Server Dependencies for Storage Systems" permission.

To run database discovery, the administrator must have the following permissions:

- Permissions to create and execute a snapshot
- "Managed Servers and Groups" permission. This privilege is granted in the OCC Web client.
- Additional Read & Write privileges for "Customers" and "Facilities" containing the target server (the server that contains the Oracle database). This privilege is granted in the OCC Web client.
- "Execute" permission for the `Opsware/Storage/Tools/DbScanner` folder. This permission is granted from NGUI folder properties. The "Execute" permission must be granted through the same user group that has privileges for snapshot management.
- "Manage Database Scanner" permission

By default, the Advanced Users group does not have permissions for `/Opsware/Storage` and underlying folders. Members of this group will not be able to view or use any software policies in the folders. When permissions for this group are granted, they are based on the corresponding Storage Visibility and Automation features that are assigned to that group.

For more information about users, groups, and granting permissions, see the *SA User Guide: Application Automation*.

Viewing SA Permissions

To view SA permissions, perform the following steps:

1. Log in to the SAS Web Client as an Administrator.
2. In the Navigation pane, select **Administration ➤ Users and Groups**. The View Groups pane appears.
3. Click the Groups tab.
4. Select a group. The group is displayed in the View Groups pane.
5. Click the Client Features tab.

   If a user has no SA permissions, the SA Client will not display the SA Client item on the Tools menu.

Storage Scanner Configuration and Operation

Each Storage Scanner requires configuration and management tasks, such as creating access controls and login credentials, authorizing the Storage Scanner, starting and stopping the Storage Scanner, and modifying Storage Scanner settings.

To configure a Storage Scanner on a managed server, you must have read and write permission on that server.

See SE Connector on page 21 or Database Scanner for Oracle on page 27 for information that is specific to the type of Storage Scanner, such as access controls and login credentials.

Storage Scanner Settings

Storage Scanner settings (properties) manage SE Connector behavior. After you install and configure SE Connector (the Storage Scanner), you can adjust these settings.

You can modify the following Storage Scanner properties:

- DataManager.properties
- JmsMessenger.properties
- Logging.properties
- RequestManager.properties
- SEPlugin.properties
- StatusManager.properties

To conserve disk space, modify the maximum size of log files and the level of detail gathered for log messages. See Log File Settings on page 35. To tune system performance, adjust the intervals at which full synchronization runs.

If you need to modify thread pools, contact HP Support.

Log File Settings

To conserve disk space and control the types of log messages that Storage Visibility and Automation collects, you can adjust the maximum size of log files and the logging level. For troubleshooting, you can also adjust trace error messages.

- **File Level:**
  - Trace-messages: FINE, FINER, FINEST, INFO, SEVERE, WARNING
  - Log-messages: INFO, SEVERE, WARNING
  - Error messages: SEVERE, WARNING
- **File Count**: 10 (default)
- **File Limi**t: the size of one file before rolling it out to another file
  - The default for error and log files is 1MB.
  - The default for debug (trace error) messages is 10 MB.

Modify the following settings to completely switch off corresponding messages:

- **Error File Enables**: True | False
- **Tracing Enabled**: True | False

Authorizing a Storage Scanner

The purpose of authorization is to provide a matching pair of security tokens—one token in the core and the other token on the managed server where the Storage Scanner (SE Connector) is deployed. When SE Connector is initially deployed to a managed server, you must authorize it so that messages from the Storage Scanner are accepted by the core server.

To authorize a Storage Scanner, perform the following steps:

1. From the Navigation pane, select **Administration ➤ Storage Scanners**.
2. Open the Storage Scanner that needs to be authorized.
3. From the **Actions** menu, select **Authorize**.

Starting a Storage Scanner

When the Storage Scanner (SE Connector) starts for the first time, it begins collecting storage information and synchronizing device data. During this process, the Storage Scanner gathers information from various elements and reports that information to the Web Services Data Access Engine so that the device data is synchronized. Depending on the size of the element, device synchronization could require several hours.

For performance reasons, it is recommended that you start the Storage Scanner during off-peak hours.

To start a Storage Scanner on a managed server, perform the following steps:

1. In the Storage Scanners content pane, select a Storage Scanner and then select **Actions ➤ Open** to display its browser.
2. Select **Action ➤ Start**.
3. Click the “Check current state” link to verify that the Storage Scanner is Running.

The start action does not apply to the Database Scanner for Oracle.

Starting the Storage Scanner on a Remote Windows Server

To start the Storage Scanner (SE Connector) on a remote Windows managed server, perform the following steps:

1. From the Control Panel, select **Administrative Tools ➤ Services**.
2. In the Services window, select **OpswareSEStorageScanner** and then select **Action ➤ Start**.

Stopping a Storage Scanner

Before you modify any Storage Scanner (SE Connector) settings, you must stop the Storage Scanner. You should also stop and then restart the Storage Scanner after any storage element changes are made. This action does not interfere with any database changes that are in progress. You can stop the Storage Scanner by using the Storage Visibility and Automation Client on a managed server or by running a saved script on a remote managed server.

After the Storage Scanner is stopped or undeployed, the status does not change.

To stop a Storage Scanner (SE Connector) on a managed server by using the Storage Visibility and Automation Client, perform the following steps:

1. In the Storage Scanners content pane, select a Storage Scanner and then select **Actions ➤ Open** to display its browser.
2. Select **Actions ➤ Stop**.
3. Click the “Check current state” link to verify that the Storage Scanner is Not Running.

The stop action does not apply to the Database Scanner for Oracle.

Stopping the Scanner on a Remote Windows Server

To stop the Storage Scanner (SE Connector) on a remote Windows managed server, perform the following steps:

1. From the Control Panel, select **Administrative Tools ➤ Services**.
2. In the Services window, select **OpswareSEStorageScanner** and then select **Action ➤ Stop**.

Checking the Storage Scanner Status

When the Storage Scanner (SE Connector) starts, it begins the collection and synchronization process.To check the status of this process, perform the following steps:

1. From the Navigation pane, select **Administration ➤ Storage Scanners**.
2. Select a Storage Scanner.
3. From the View drop-down list, select Properties.
4. Click the “Check current state” link in the content pane to verify that the Storage Scanner is Running or Not Running.

The check status action does not apply to the Database Scanner for Oracle.

Viewing Storage Scanner Properties & Current State

To view the properties for a Storage Scanner or check the current state of a Storage Scanner, perform the following steps:

1. From the Navigation pane, select **Administration ➤ Storage Scanners**.
2. From the View drop-down list, select **Properties**.
3. In the content pane, open a Storage Scanner.
4. (Optional) Select the “Check current state” link to view the most recent status of the Storage Scanner, such as Running or Not Running.

Viewing Storage Scanner Managed Elements

This task applies to the SE Connector (Storage Scanner) and the Database Scanner for Oracle (Storage Scanner). You can view managed elements collected by a Storage Scanner and managed elements collected by an individual access control. The managed elements collected by an access control is a subset of the elements collected by the Storage Scanner.

To view the managed elements collected by the Storage Scanner, perform the following steps:

1. From the Navigation pane, select **Administration ➤ Storage Scanners**.
2. In the Content pane, open a Storage Scanner.
3. From the View drop-down list, select **Managed Elements**.

Customer and Facility are determined based on similar properties of the managed server where the Storage Scanner is running. This is the Storage Scanner that discovered the managed device, such as an array, NetApp filer, and so on. Fabrics are excluded from this list of managed elements. To view managed elements for fabrics, see the next task.

To view the managed elements (such as fabrics) collected by an individual access control, perform the following steps:

1. From the Navigation pane, select **Administration ➤ Storage Scanners**.
2. In the Content pane, open a Storage Scanner.
3. From the Views pane, select **Storage Essentials**.
4. In the Content pane, select an access control to view.

Viewing the Storage Scanner History Log

To view the history log for a Storage Scanner, perform the following steps:

1. From the Navigation pane, select **Administration ➤ Storage Scanners**.
2. In the content pane, open a Storage Scanner.
1. In the View drop-down list, select **History**.

2 In the content pane, select an event from the history log and then select the following option from the Actions menu:

- **View Event Details**—Displays detailed information about the event.

  Or

- Right-click on the event and select **View Event Details**.

Events in the history log are reported by the Storage Scanner while performing data synchronization.

Index

U

V

W