HP Application Storage Automation System

for the HP-UX, Solaris, Red Hat Enterprise Linux, AIX, and Windows operating systems

Software Version: 7.50

Installation & Administration Guide

Document Release Date: September, 2008

Software Release Date: September, 2008

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.

For information about third party license agreements, see the Third Party and Open Source Notices document in the product installation media directory.

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

Microsoft®, Windows®, Windows Vista®, and Windows® XP 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:

`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.

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.

For downloads, see:

```
https://h10078.www1.hp.com/cda/hpdc/display/main/
index.jsp?zn=bto&cp=54_4012_100__
```

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`

Table Of Contents

Preface 13

Chapter 1: Overview 17

Chapter 2: Storage Agent Installation 25

Chapter 3: Storage Host Agent Extension Installation 49

Chapter 4: Administration 61

Chapter 5: Brocade Storage Agent 71

Chapter 6: CLARiiON Storage Agent 89

Chapter 7: HiCommand Storage Agent 107

Chapter 8: McDATA Storage Agent 119

Chapter 10: Oracle Storage Agent 149

Chapter 11: Symmetrix Storage Agent 171

Preface

Overview of this Guide

This guide describes how to install and configure Application Storage Automation System (ASAS). For information on how to install and configure HP Server Automation (SA), see the *SA Planning and Installation Guide*.

Audience and Assumptions

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

Conventions in this Guide

This guide uses the following typographical and formatting conventions.

NOTATION	DESCRIPTION
Bold	Identifies field menu names, menu items, button names, and inline terms that begin with a bullet.
`Courier`	Identifies text that is entered or displayed at the command-line prompt, such as Unix commands, HP Server Automation commands, file names, paths, directories, environment variable names, contents of text files that are viewed or edited with a text editor, source code in a programming language, and SQL (database) commands.

NOTATION	DESCRIPTION
Italics	Identifies document titles, DVD titles, web site addresses. Used to introduce new terms when they are first defined in a document and for emphasis.

Icons in this Guide

This guide uses the following icons.

ICON	DESCRIPTION
📄	This icon represents a note. It identifies especially important concepts that warrant added emphasis.
☑	This icon represents a requirement. It identifies a task that must be performed before an action under discussion can be performed.
💡	This icon represents a tip. It identifies information that can help simplify or clarify tasks.
⚠	This icon represents a warning. It is used to identify significant information that must be read before proceeding.

Guides in the Documentation Set and Associated Users

- The *SA User's Guide: Server Automation* is intended for system administrators responsible for all aspects of managing servers in an operational environment. It describes how to use SA, introducing the system and the user interface. It provides information about managing servers, remediating servers, script execution, configuration tracking, deploying and rolling back code, and agent deployment. It also explains how to use the Global Shell and open a Remote Terminal on managed servers.

- The *SA User's Guide: Application Automation* is intended for system administrators responsible for performing the day-to-day functions of managing servers. It reviews auditing and compliance, software packaging, visual application management, application configuration, and software and operating system installation on managed servers.
- The *SA Administration Guide* is intended for administrators responsible for monitoring and diagnosing the health of the SA core components. It also documents how to set up SA user groups and permissions.
- The *SA Planning and Installation Guide* is intended for advanced system administrators responsible for planning all facets of an HP Server Automation installation. It documents all the main features of HP Server Automation, scopes out the planning tasks necessary to successfully install HP Server Automation, explains how to run the BSA Installer, and details how to configure each of the components. It also includes information on system sizing and checklists for installation.
- The *SA Policy Setter's Guide* is intended for system administrators responsible for setting up OS provisioning, configuration tracking, code deployment, and software management.
- The *Content Utilities Guide* is intended for advanced system administrators responsible for importing content such as software packages into HP Server Automation. It documents the following command-line utilities: OCLI 1.0, IDK, and DET (CBT).
- The *Automation Platform Developer's Guide* is intended for software developers responsible for customizing, extending, and integrating HP Server Automation. It documents how to create Web Services, Java RMI, Python, and CLI clients that invoke methods on the SA API.

Chapter 1: Overview

IN THIS CHAPTER

This chapter discusses the following topics:

- Supported Operating Systems
- Supported Storage Device Hardware

Supported Operating Systems

Table 1-1 lists the operating systems that support the Storage Host Agent Extension (SHA). For information about installing and configuring the Storage Host Agent Extension, see “Storage Host Agent Extension (SHA) Installation” on page 49.

Table 1-1: Supported Operating Systems for the Storage Host Agent Extension

OPERATING SYSTEM	VERSION	ARCHITECTURE
AIX	AIX 5.2 AIX 5.3	POWER POWER
HP-UX	HP-UX 11i v1 (11.11) HP-UX 11i v2 (11.23) HP-UX 11i v3 (11.31)	S700, S800 and Itanium S700, S800 and Itanium S700, S800 and Itanium
Linux	RHEL 3 RHEL 4	32 bit x86 32 bit x86
Solaris	Solaris 8 Solaris 9 Solaris 10 (Update 1, Update 2, Update 3)	Sun SPARC Sun SPARC Sun SPARC, 64 bit x86, 32 bit x86 and UltraSPARC
Windows	Windows 2000 Advanced Server Windows 2003 Advanced Server	32 bit x86 32 bit x86

As a prerequisite, the runtime version must be at least xlC version xlC.aix50.rte 7.0.0.0 for the Storage Host Agent proxies to run.

Supported Storage Device Hardware

Table 1-2 through Table 1-8 list the supported storage device hardware from various vendors.

SAN Storage Arrays

ASAS supports the SAN storage arrays described in Table 1-2.

Table 1-2: Supported SAN Storage Arrays

VENDOR	MODEL	FIRMWARE VERSION	PREREQUISITE SOFTWARE & VERSION
EMC CLARiiON	CX300, CX400 CX500, CX600 CX700	Navisphere Management Server	Navisphere CLI V6.16, V6.19.4 V6.22.21, V6.24.0
EMC Symmetrix DMX	800, 1000 2000, 3000	5669 5670	Solutions Enabler Kit (Full Version) 6.0.3, 6.2.2, 6.3.2
EMC Symmetrix	8000 series 3000 series	5x67 5x68 Match latest firmware	Solutions Enabler Kit (Full Version) 6.0.3, 6.2.2, 6.3.2
Hitachi Thunder 9500™ V Series	95xxV	N/A	HiCommand Device Manager 5.1.0-03
Lightning 9900™ V Series	9910, 9960	N/A	HiCommand Device Manager 5.1.0-03
Hitachi AMS, WMS	XXXX	N/A	HiCommand Device Manager 5.1.0-03
Hitachi Lightning Storage V-Series	9970V, 9980V	N/A	HiCommand Device Manager 5.1.0-03
Sun StorEdge	9990 Series	N/A	HiCommand Device Manager 5.1.0-03
Sun StorEdge	9910 9960	N/A	HiCommand Device Manager 5.1.0-03

Table 1-2: Supported SAN Storage Arrays (continued)

VENDOR	MODEL	FIRMWARE VERSION	PREREQUISITE SOFTWARE & VERSION
Sun StorEdge	9970 9980	N/A	HiCommand Device Manager 5.1.0-03

SAN Fibre Switches

ASAS supports the SAN fibre switches described in Table 1-3.

Table 1-3: SAN Fibre Switches

SWITCH/ DIRECTOR	MODEL	FIRMWARE SUPPORTED	MANAGEMENT SOFTWARE NAME & VERSION
Brocade	3250, 3850, 3014, 3106, 3900, 12000, 24000, 48000, 4100, 4900, 7500, 5000, Brocade 200E, 4102/16, 4018/20, 4024	5.0.1d	N/A
EMC Connectrix	DS-220B, DS-4100B, DS-4900B, DS-5000B, Ed-48000B	5.0.1d	N/A
The following configuration is NOT supported: • One Connectrix (McDATA) fabric. • Managed by two Connectrix Manager (EFCM) 9.0 instances (each managing a different fabric switch).			
EMC Connectrix	DS-16M, DS-16M2, DS-24M2 DS-32M, DS-32M2 ED-64M, ED-140M	v5.01.xx – v6.02.00	Connectrix Manager v9.1
The following configuration is NOT supported: • One McDATA fabric. • Managed by two EFCM 9.0 instances (each managing a different fabric switch).			
McDATA (Brocade)	Intrepid, 6140, 6064 Sphereon, 3016, 3032, 3216, 3232, 4500	v4.01.02 – v5.03.00	EFCM 9.0
McDATA (Brocade)	Intrepid, 6140, 6064 Sphereon, 3016, 3032, 3216, 3232, 4300, 4500	v6.00.00 – v6.03.00	EFCM 9.0
StorageTek	Any OEM versions that correspond to supported Brocade models.		

NA Storage Array

ASAS supports the NA storage arrays described in Table 1-4.

Table 1-4: NA Storage Arrays

VENDOR	MODEL	VERSION	OS
Network Appliance	FAS	ONTAP 7.0, 7.2	ONTAP OS

Fibre Channel Adapters

The minimum requirements for supporting FCAs are:

- The FCA vendor provides both FCA drivers and API libraries that comply with the SNIA FCA API standard.
- The driver and API libraries are installed and maintained as a matched set that came together from the specific vendor. Users must not upgrade or install drivers without also upgrading or installing the corresponding API libraries that were shipped with the driver from the vendor.

IBM FCAs on AIX do not require API libraries.

ASAS supports the Fibre Channel adapters described in Table 1-5.

Table 1-5: Supported Fibre Channel Adapters

VENDOR	HBA MODEL	OS
Emulex	LP10000ExDC, LP1050Ex, LP10000DC, LP10000, LP1050DC, LP1050, LP9802DC, LP9802, LP982, LP9402DC, LP9002L, LP9002DC, LP9000, LP952L, LP8000, LP8000DC, LP850	Linux, Red Hat Enterprise Linux 3.0, 4.0 (AS/ES/WS/ Desktop)
Emulex	LP10000DC, LP10000, LP9802DC, LP9802, LP9402DC, LP9002L, LP9002C, LP9002S, LP9002DC, LP9000, LP8000, LP8000DC, LP8000S, LP7000E	Solaris 8, Solaris 9, Solaris 10
Emulex	LP10000ExDC, LP1050Ex, LP10000DC, LP10000, LP1050DC, LP1050, LP9802DC, LP9802, LP982, LP9402DC, LP9002L, LP9002DC, LP9000, LP952L, LP8000, LP8000DC, LP850, LP7000E	Windows 2000 Server, Advanced Server Windows 2003 Server, Advanced Server

Table 1-5: Supported Fibre Channel Adapters (continued)

VENDOR	HBA MODEL	OS
HP	Tachyon Fibre Channel, A6684A, A6685A, A5158A, A6795A	HP-UX
HP	PCI-X Single-Port 4GB Fibre Channel HBA for HP-UX AB378B	HP-UX
HP	PCI-X Dual-Port 4GB Fibre Channel HBA for HP-UX AB379B	HP-UX
HP	Dual port 4 GB Fibre Channel, PCI-e AD300A	HP-UX
HP	Single port 4 GB Fibre Channel, PCI-e AD299A	HP-UX
HP	Dual Port 4 GB Fibre Channel, PCI-e AD355A	HP-UX
HP	PCI-X Dual Channel 2GB Fibre Channel HBA A6826A	HP-UX
HP	PCI-X Single-Port 4GB Fibre Channel HBA for HP-UX AB378B	HP-UX
HP	HP PCI-X Dual-Port 4GB Fibre Channel HBA for HP-UX AB378B	HP-UX
IBM		AIX
Qlogic	QLA2200 Series, QLA2202F, QLA2204F, QLA2300 (F), QLA2302F, QLA2310 (F), (FL)	Linux, Red Hat Enterprise Linux 3.0, 4.0 (AS/ES/WS/ Desktop)
Qlogic	QLA2200 Series, QLA2202F, QLA2204F, QLA2300 (F), QLA2302F, QLA2310 (F), (FL), QLA2340 (L), QLA2342 (L), QLA2344	Solaris 8 Solaris 9 Solaris 10
Qlogic	QLA2200 Series, QLA2202F, QLA2204F, QLA2302F, QLA2310 (F), (FL), QLA2340 (L), QLA2342 (L), QLA2344, QLA2350, QLA2352	Windows 2000 Server, Advanced Server Windows 2003 Server, Advanced Server
Sun	SG-XPCI1FC-JN2 SG-CPCI2FC-JN2 (OEM by AMCC)	Solaris 8 Solaris 9 Solaris 10

Volume Managers

ASAS supports the volume managers described in Table 1-6.

Table 1-6: Supported Volume Managers

VENDOR	VOLUME MANAGER	VERSION	OS
HP	HP-UX LVM	Same as OS	HP-UX 11i v1 (11.11) HP-UX 11i v2 (11.23) HP-UX 11i v3 (11.31)
IBM	AIX LVM	Same as OS	AIX 5.2 AIX 5.3
Microsoft	Native LDM	Same as OS	Windows 2000 Windows 2003
Red Hat	LVM2	2.6 kernels	Red Hat Linux 4.0
SUN	Solstice Disk Suite	4.2.1	Solaris 8
SUN	Solaris Volume Manager	Same as OS	Solaris 9, Solaris 10
Veritas	VxVM	3.1 SP1	Windows 2000
Veritas	Storage Foundation	v4.0 v4.1	Windows 2000 Windows 2003
Veritas	VxVM	v3.1 SP1	Windows 2000
Veritas	VxVM	v3.2 Update 1	RHEL 3, RHEL 4
Veritas	Storage Foundation	v4.0 v4.1	RHEL 3, RHEL 4
Veritas	VxVM	3.5	Solaris 8, 9, 10
Veritas	Storage Foundation	v4.0 v4.1	Solaris 8, 9, 10 HP-UX 11i v2
Veritas	Storage Foundation	v5.0	AIX 5.2, 5.3 HP-UX 11i v2 (PA-RISC and Itanium) RHEL 4 Solaris 8, 9, 10

MultiPath Software

ASAS supports multipath software described in Table 1-7.

Table 1-7: MultiPath Software

VENDOR	MULTIPATH SOFTWARE	VERSION	OS
EMC	PowerPath		AIX 5.2, 5.3
EMC	PowerPath	v3.0.0, v4.0.x through 4.4.x	Solaris 8
EMC	PowerPath	v3.0.4, v4.1.x through 4.4.x	Solaris 9, 10
EMC	PowerPath		RHEL 3, RHEL 4
Veritas	DMP	v5.0	AIX 5.2, 5.3
Veritas	DMP	v4.1	HP-UX 11.10 HP-UX 11i HP-UX 11i v2 HP-UX 11i v3
Veritas	DMP	v3.2 Update 1	RHEL 3, RHEL 4
Veritas	DMP	v4.0	RHEL 3, RHEL 4
Veritas	DMP	v3.5 v4.0 v4.1	Solaris 8, 9, 10
Veritas	DMP	v3.1 SP1 v4.0 v4.1 v5.0	Windows 2000, 2003
Sun	Native		Solaris 10
Red Hat	Native		RH 4 U2 and later
HP-UX	Native		Supported OS Versions

Databases/Middleware

ASAS supports the databases and middleware described in Table 1-8.

Table 1-8: Databases/Middleware

VENDOR	VERSION	APPLICATION INSTALLED ON OS
Oracle DB	9i	Solaris 8, Solaris 9, Solaris 10 Windows 2000, 2003 Red Hat Enterprise Linux v3.0, 4.0 (AS/ES/WS/Desktop)
Oracle DB	10g	Solaris 8, Solaris 9, Solaris 10 Windows 2000, 2003 Red Hat Enterprise Linux v3.0, 4.0 (AS/ES/WS/Desktop)

Supported Operating Systems for Storage Agents

Table 1-9 lists the operating systems that support Storage Agents. For information about installing and configuring Storage Agents, see “Storage Agent Installation” on page 25.

Table 1-9: Supported Operating Systems for Storage Agents

OPERATING SYSTEM	VERSION
Solaris	Solaris 9 Solaris 10
Windows	Windows 2000 Windows 2003

Chapter 2: Storage Agent Installation

IN THIS CHAPTER

This chapter discusses the following topics:

- Storage Agent
- Pre-Installation Requirements
- Installing a Storage Agent
- Deploying a Storage Agent
- Storage Agent File System Layout
- Removing a Storage Agent
- Uninstalling a Storage Agent

Storage Agent

A Storage Agent is a component that runs on managed servers and collects data about devices such as SAN arrays, SAN switches, SAN fabrics, and NAS filers. A Storage Agent must be installed and then deployed on a managed server.

ASAS includes an HP BSA Installer for each Storage Agent. The HP BSA Installer uploads the binaries (.zip files) to the core. During the upload process, ASAS creates one software policy for all supported Windows operating systems (Windows 2000 and Windows 2003) and for all supported Solaris operating systems (Solaris 9 and Solaris 10).

To deploy a Storage Agent, the storage administrator must explicitly schedule a remediate process for the software policy. See the *SA User's Guide: Application Automation* for more information about software policies.

To support the discovery of different types of storage data, Storage Agents are installed independently of each other—you are not required to install all Storage Agents, only the ones that your environment requires.

Only one Storage Agent can manage a storage device—multiple Storage Agents cannot manage the same storage device.

The following types of Storage Agents require a corresponding HP BSA Installer distribution:

- Brocade
- CLARiiON
- Hitachi
- McDATA
- NetApp
- Oracle
- Symmetrix

To minimize the dependency of Storage Agents on a certain version of the core, these distributions contain the minimum number of packages required to run Storage Agents on managed servers. Minimal dependencies are designed to simplify the upgrade process for Storage Agents.

The required packages are based on two types of Storage Agents:

- Java Storage Agent—for Brocade, CLARiiON, McDATA, Oracle, and Symmetrix
- XML Storage Agent—for NetApp and HiCommand

For Java Storage Agents, the HP BSA Installer uploads:

- Packages that are specific to the Storage Agent. These packages are stored in the folder for that particular type of Storage Agent.
- Packages that are common for all Java Storage Agents. These packages are stored in `/Opsware/Storage/Agents`.
- (Optional) Packages with native libraries. These packages are stored in the agent folder. The Brocade, McDATA, and Symmetrix Storage Agents have native libraries.

For XML Storage Agents, the HP BSA Installer uploads:

- Packages that are specific to the storage agent. These packages are stored in the folder for that particular type of Storage Agent.

- Packages that are shared for all XML Storage Agents. These packages are stored in `/Opsware/Storage/Agents`.

Pre-Installation Requirements

The Storage Agent installation process requires that all standard SA components have been installed on the server where the HP BSA Installer distribution will run. See the *SA Planning and Installation Guide* for information about installing SA.

ASAS Storage Agents require SA Agents 7.0 or later running on the managed servers.

The HP BSA Installer distribution is required to run on the core server that has the Software Repository installed. The core must be running when you install a storage agent.

Since there is a different distribution for each type of Storage Agent, response files are also different. The installers do not generate a complete response file for each Storage Agent in the sense that the Storage Agent response file contains a few entries specific to storage agent installation.

Installing a Storage Agent

If you are installing an Oracle Storage Agent, see “Prerequisites” on page 149.

To install the Storage Agent on a core, perform the following steps:

1. Log in to the server that you installed SA on and then launch a command prompt.
2. Mount the ASAS installation DVD using a command similar to `mount /dev/cdrom` or NFS-mount the directory that contains a copy of the DVD contents.

3. From the ASAS installation DVD, enter the `install_opsware.sh` command to start the HP BSA Installer.

   The following is an example of this command for a NetApp Storage Agent:

   ```
   /tmp/opsware_34.C.1959.0-pam-netapp/disk001/opsware_
   installer/install_opsware.sh -r /usr/tmp/oiresponse.storage-
   pam-netapp  --verbose
   ```

   A prompt similar to the following example appears:

   ```
   Welcome to the Opsware Installer.
   Please select the components to install.
   1 ( ) Storage Agent for Netapp (pam-netapp).
   Enter a component number to toggle ('a' for all, 'n' for
   none).
   When ready, press 'c' to continue, or 'q' to quit.
   Selection:
   ```

The sample command requires the user to have a pre-created response file. If it does not exist, then the user should run the command without using option '-r'. This will help the user go through an interview process. The simple interview mode will prompt the user to provide the Model Repository user password. The advance interview mode will require an additional password for internal user 'detuser'.

4. To select the Storage Agent, type `1` and then press Enter. There is one option for each type of Storage Agent. A prompt similar to the following appears:

   ```
   Welcome to the Opsware Installer.
   Please select the components to install.
   1 ( ) Storage Agent for Netapp (pam-netapp).
   Enter a component number to toggle ('a' for all, 'n' for
   none).
   When ready, press 'c' to continue, or 'q' to quit.
   Selection: 1
   ```

5. The HP BSA Installer saves your interview answer in a response file that is named to represent the Storage Agent, such as:

   `/usr/tmp/oiresponse.storage-pam-netapp`.

   The HP BSA Installer saves information similar to the following example in the response file:

   ```
   # Opsware Installer response file
   # Generated by Opsware Installer Tue May  1 16:31:19 2007
   ```

```
%oi.components
storage-pam-netapp

%oi.build_id
opsware_34.C.1507.0

%oi.layout
slices

%truth.detuserpwd
opsware_admin

%truth.oapwd
opsware_admin
```

Response file content is saved in plain text. At the end of the installation, you will be prompted to encrypt the response file. If you are providing a saved response file and want to use the installation interview, enter the `--interview` command line argument.

During the Storage Agent installation process, all changes are made in the core folders. No changes are made to the file system of the core server. If a folder does not exist, the Installation process creates a new folder for storage agent packages and policies. The folder location is predefined and cannot be modified.

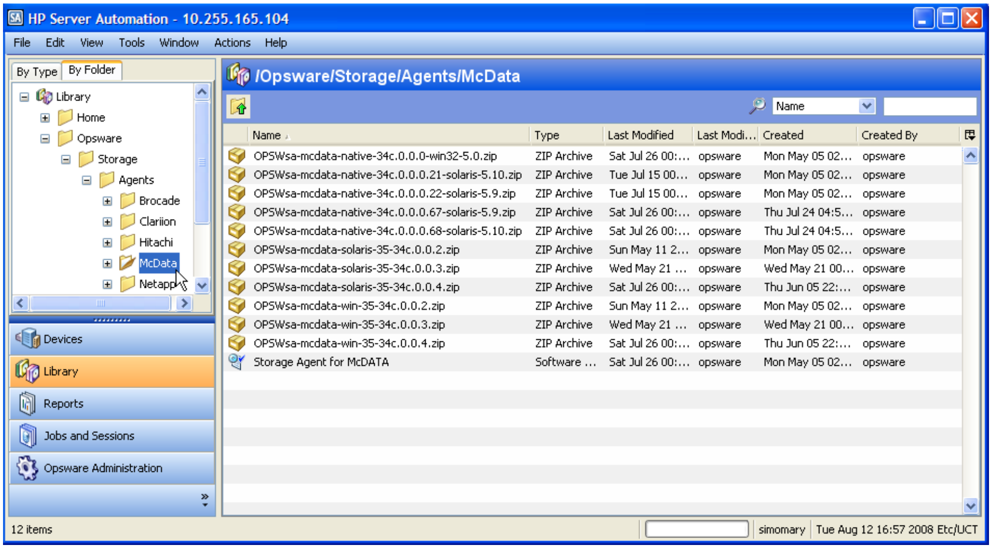
Deploying a Storage Agent

Storage Agent deployment is performed by a remediate process that ensures that the binaries on a managed server comply with a certain Storage Agent software policy. The storage administrator must explicitly schedule the remediation job. During the initial remediation, all binaries are copied to the managed server. If a package is deleted from a managed server, a subsequent remediation will restore that package on the server.

Storage Agent Folder

When a Storage Agent is deployed, a folder is created on the core for the Storage Agent during the installation process. For example, for a McDATA Storage Agent, a McDATA folder will be created in **Library ➤ Opsware ➤ Storage ➤ Agents**. See Figure 2-1.

Figure 2-1: Storage Agent Folder



Name	Type	Last Modified	Last Modi...	Created	Created By
OPSWsa-mcdata-native-34c.0.0.0-win32-5.0.zip	ZIP Archive	Sat Jul 26 00:...	opsware	Mon May 05 02...	opsware
OPSWsa-mcdata-native-34c.0.0.0.21-solaris-5.10.zip	ZIP Archive	Tue Jul 15 00...	opsware	Mon May 05 02...	opsware
OPSWsa-mcdata-native-34c.0.0.0.22-solaris-5.9.zip	ZIP Archive	Tue Jul 15 00...	opsware	Mon May 05 02...	opsware
OPSWsa-mcdata-native-34c.0.0.0.67-solaris-5.9.zip	ZIP Archive	Sat Jul 26 00:...	opsware	Thu Jul 24 04:5...	opsware
OPSWsa-mcdata-native-34c.0.0.0.68-solaris-5.10.zip	ZIP Archive	Sat Jul 26 00:...	opsware	Thu Jul 24 04:5...	opsware
OPSWsa-mcdata-solaris-35-34c.0.0.2.zip	ZIP Archive	Sun May 11 2...	opsware	Mon May 05 02...	opsware
OPSWsa-mcdata-solaris-35-34c.0.0.3.zip	ZIP Archive	Wed May 21 ...	opsware	Wed May 21 00...	opsware
OPSWsa-mcdata-solaris-35-34c.0.0.4.zip	ZIP Archive	Sat Jul 26 00:...	opsware	Thu Jun 05 22:...	opsware
OPSWsa-mcdata-win-35-34c.0.0.2.zip	ZIP Archive	Sun May 11 2...	opsware	Mon May 05 02...	opsware
OPSWsa-mcdata-win-35-34c.0.0.3.zip	ZIP Archive	Wed May 21 ...	opsware	Wed May 21 00...	opsware
OPSWsa-mcdata-win-35-34c.0.0.4.zip	ZIP Archive	Sat Jul 26 00:...	opsware	Thu Jun 05 22:...	opsware
Storage Agent for McDATA	Software ...	Sat Jul 26 00:...	opsware	Mon May 05 02...	opsware

The installation process uploads and configures packages that are in this folder. Storage Agent policies can only be attached to servers running Windows or Solaris.

To attach a server to a Storage Agent software policy, perform the following steps:

1. From the Navigation pane, select the By Folder tab and then select Library.

2. Go to the folder that corresponds to the Storage Agent you want to undeploy, such as **Library ➤ Opsware ➤ Storage ➤ Agents ➤ McDATA** for the McDATA Storage Agent.

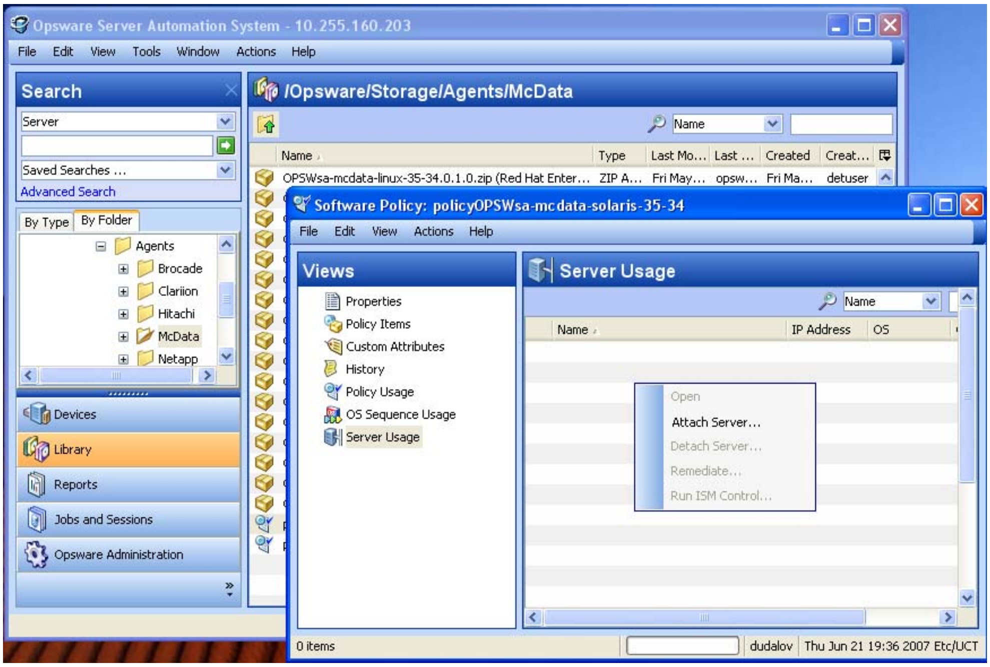
3. Select the software policy.

4. Open the software policy.

5. From the Views pane, select Server Usage.

6 From the Actions menu, select Attach Server.

Figure 2-2: Storage Agent Software Policy



Opsware Server Automation System - 10.255.160.203

/Opsware/Storage/Agents/McData

Name	Type	Last Mo...	Last ...	Created	Creat...
OPSWsa-mcdata-linux-35-34.0.1.0.zip (Red Hat Enter...	ZIP A...	Fri May...	opsw...	Fri Ma...	detuser

Software Policy: policyOPSWsa-mcdata-solaris-35-34

Server Usage

Name	IP Address	OS

0 items

dudalov Thu Jun 21 19:36 2007 Etc/UCT

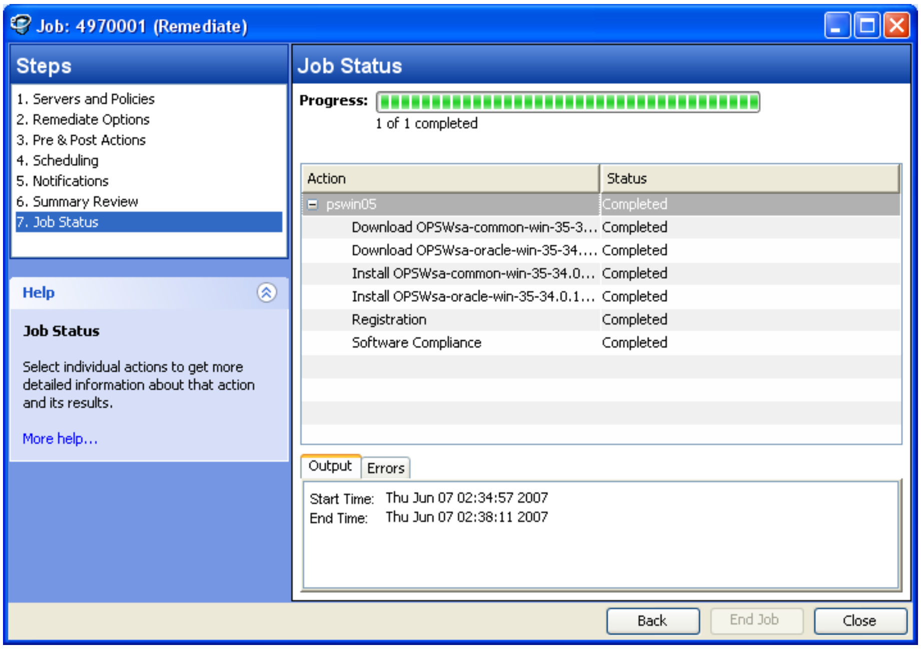
Storage Agent Software Policy

Each package that belongs to a software policy might have scripts defined for various steps, such as pre-install, post-install, pre-uninstall, and post-uninstall scripts. For a policy that contains multiple packages, the order of packages is important because these scripts are executed each time an individual package is processed during remediation.

Figure 2-3 illustrates the different steps taken during the remediate process (job) for the McDATA Storage Agent. This remediate job includes loading binaries on a managed server and running pre-install and post-install scripts.

To view detailed messages reported by the remediate process during any of these steps, open the Job Status and select a task.

Figure 2-3: Remediate Job for a Storage Agent Software Policy



Select individual actions to get more detailed information about that action and its results.

Progress: 1 of 1 completed

Action	Status
⊟ pswin05	Completed
Download OPSWsa-common-win-35-3...	Completed
Download OPSWsa-oracle-win-35-34....	Completed
Install OPSWsa-common-win-35-34.0...	Completed
Install OPSWsa-oracle-win-35-34.0.1...	Completed
Registration	Completed
Software Compliance	Completed

```
Start Time:   Thu Jun 07 02:34:57 2007
End Time:     Thu Jun 07 02:38:11 2007
```

Solaris Storage Agents

All Storage Agents (except Symmetrix Storage Agents deployed to Solaris managed servers) are grouped in an account called `opswstagent`. If this account does not already exist, a pre-install script will create it on the managed server. When you undeploy the last Solaris Storage Agent, the `opswstagent` account will be deleted. The Symmetrix Storage Agent runs under the `root` account.

On Solaris managed servers, the deployment process will also create an `opsware-pam-` entry in `/etc/init.d` and set required boot links.

Requirements for All Managed Servers

All managed servers require the following:

- All managed servers must have an agent installed and running.
- All managed servers use the agent gateway to communicate with the core.

Requirements for All Storage Agents

All Storage Agents on managed servers require that the managed servers also have an SA Agent running on them. This enables the Storage Agents to communicate with the core.

Requirements for Individual Storage Agents

There are no dependency checks made during the Storage Agent deployment process on a managed server. Depending on the operating system, each Storage Agent reports all errors in log files:

`%SYSTEMDRIVE%\Program Files\Common Files\Opsware\log\pam-<COMPONENT_NAME>` (Windows)

`/var/log/opsware/pam-<COMPONENT_NAME>/` (Unix)

The following sections describe additional installation requirements by each type of Storage Agent.

Brocade Storage Agent

The Brocade Storage Agent can be installed on a managed server that meets the following requirements:

- **Operating System**: Windows 2003 or Solaris 10
- **Free Space**: 150 MB for installation files, 20 MB (minimum) to 200 MB (maximum) for log files
- **RAM**: 256 MB
- **Open Firewall Ports**: when there is a firewall between the server running the Storage Agent and the Brocade switches

CLARiiON Storage Agent

Install and configure the EMC CLARiiON software tools to meet the following requirements:

- Navisphere Manager must be installed on each EMC CLARiiON array that the Storage Agent will manage.
- Navisphere CLI (command line interface) must be installed on the managed server where you will install the Storage Agent. (On a Solaris operating system, install this as root.) After Navisphere CLI is installed, restart the managed server. If you install Navisphere CLI to a location other than the default, you must modify the

`pam.properties` file to point to the correct location, such as `com.creekpath.pam.clariion.cli_path`.

- Access Logix must be installed on each EMC CLARiiON array that the Storage Agent will manage.

Hitachi Storage Agent

Install and configure the HiCommand management software to meet the following requirements:

- Verify that the HiCommand management software is installed and configured for the storage array. HiCommand version 4.0 is the minimum requirement; HiCommand versions 4.2 and 4.3 are also supported.

Do not install the HDS HiCommand client software on the same server as the core because the HiCommand client intercepts HiCommand Server messages that are intended only for the core.

- Only one HiCommand Storage Agent is required for managing multiple HiCommand storage arrays.

McDATA Storage Agent

Install and configure the McDATA software tools to meet the following requirements:

- **Bridge Agent**: The McDATA Storage Agent uses SWAPI (Switch Application Programming Interface) to communicate with McDATA's Bridge Agent. The Bridge Agent software must be installed on each system running the vendor's management software.
- **Vendor Management Software**: For McDATA switches, the Bridge Agent communicates with McDATA's Enterprise Fabric Connectivity Manager (EFCM) storage network software. For EMC Connectrix switches, the Bridge Agent communicates with EMC's Connectrix Manager. Use the appropriate vendor's switch management software to register each switch. Enterprise Fabric Connectivity Manager must be installed on the managed server.

NetApp Storage Agent

The NetApp Storage Agent must be installed on a server that meets the following requirements:

- **Operating System**: Windows 2003 or Solaris 10
- **Free Space**: 121 MB for installation files, 20 MB (minimum) to 200 MB (maximum) for log files
- **RAM**: 256 MB

Oracle Storage Agent

You must have a Storage Host Agent Extension (SHA) on the server where your Oracle instances are running. Without the SHA, you will not see any database information in the core. See *Chapter 3, Storage Host Agent Extension (SHA) Installation* for information about how to install SHAs.

If the Oracle database resides in a Unix environment and uses symbolic links for datafiles or log files, perform the following steps:

1 On the server where the Oracle Storage Agent will be installed, install an Oracle Client and enable Java for the databases.

2 Enable support for symbolic links:

1. Install the Oracle Client on the same server where you will install the Storage Agent.
2. Enable Java by running the following script:

```
$ORACLE_HOME/javavm/install/initjvm.sql
```

If Java is not enabled, the following errors can occur during Storage Manager synchronization:

```
ORA-29541: Class ORACLEPAM.com/creekpath/managedapp/util/
GetCannonicalPath could not be resolved.
ORA-06512: at  ORACLEPAM.GETCANNONICALPATHLOCAL,  line 0
ORA-06512: at  ORACLEPAM.GETCANONICALPATH,  line 8
```

Symmetrix

Install and configure the EMC software tools to meet the following requirements:

- **Solutions Enabler Kit**: The full version of the EMC Solutions Enabler Kit (SYMCLI), Version 5.5 or Version 6.0, must be installed on the server where you will install the EMC Symmetrix Storage Agent. Do not install the monitoring only version (known as EMC Solutions Enabler Kit Lite). The EMC Solutions Enabler Kit installs the EMC shared libraries that the Storage Agent uses to communicate with the Symmetrix array. These kits are part of the EMC Control Center (ECC) software.

- **TimeFinder and SRDF Licenses**: If you want to collect replication information, make sure the TimeFinder and SRDF licenses are installed on the server where the Storage Agent is installed. For arrays that use SRDF/TimeFinder replication software, you must install the EMC Solutions Enabler kit (SYMCLI) Version 6.0 on the server where the Storage Agent is installed.

To install and configure the EMC Solutions Enabler Kit, perform the following steps:

1. Make sure you have the following EMC license keys: SERVER, BASE, ConfigChange, and DevMasking. If you do not have these license keys, contact your EMC vendor.

2. For the Solutions Enabler Kit Version 6.0, change the defaults for the following prompts to these values:

   ```
   Install Single-threaded Symapi Shared Libraries? [N]Y
   ```

3. Make sure there is a zone from the server where EMC Solutions Enabler is installed to each Symmetrix array that is managed by that server.

4. Map a minimum of four EMC Gatekeepers to the server for each Symmetrix array managed by that server. The Storage Agent uses the Gatekeepers as communication channels to gather information from the arrays, such as events and metrics. To enable the Storage Agent to discover the Gatekeepers for a given Symmetrix frame, the Gatekeepers must be flagged as Gatekeeper devices.

   Run the SYMCLI command `symgate` on the server where the Storage Agent is installed, such as:

   ```
   symgate -sid <Sym_ID>define dev <Sym_Dev_Name>
   ```

   `<Sym_ID>` is the Symmetrix ID for devices that are defined as the Gatekeepers.

   `<Sym_Dev_Name>` is the Symmetrix device name that must be flagged as a Gatekeeper device.

5. Make sure the Volume Configuration Management Database (VCMDB) is visible to the server where the Storage Agent is installed. By default, the VCMDB is configured to be visible to every connected managed server on every storage array port. If the VCMDB does not use the default configuration, you must map the Storage Agent server using the storage array ports to which it is connected.

   1. If the server for the EMC Symmetrix Storage Agent runs on Solaris, verify that you have enough semaphores. (See the EMC Solutions Enabler installation documentation for more information.)

2. If the server for your EMC Symmetrix Storage Agent runs on Solaris, verify that EMC Solutions Enabler can communicate with Symmetrix arrays by running the SYMCLI command `symcfg discover`. If the command fails, the EMC Solutions Enabler server either could not find any Gatekeepers to communicate with the Symmetrix arrays or there is a zoning problem. To resolve these problems, refer to EMC documentation or contact EMC Customer Support.

Configuring Pre-Install and Post-Install Scripts

The following sections describe additional configuration requirements by each type of Storage Agent.

XML Storage Agent Ports

Some Storage Agents, such as the XML Storage Agents HiCommand and NetApp, allow you to specify a port. If the default port is already being used by another service running in your environment, you must modify the default setting.

To modify the default port for an operating system, you must modify the post-install script for that operating system. This script is located in the corresponding Storage Agent folder on the core. The following example shows the editable port parameter in a post-install script for a Solaris Hitachi Agent:

```
################# USER PARAMETERS ################
HTTP_PORT_VALUE=7031
################# USER PARAMETERS ################
```

The hashmark lines before and after `HTTP_PORT_VALUE` are part of the script. These lines enclose the editable part of the script. The valid port range is 7031 to 7050, such as 7031 for Hitachi, 7032 for NetApp, and so on. There is no validation on this port.

The following example is for a Symmetrix Storage Agent for Solaris. The `SYMCLI_HOME` parameter *must* be specified before deployment. This parameter can be modified repeatedly—different packages might have different values. These parameters must be independently set for each managed server prior to remediation.

```
################# USER PARAMETERS ################
SYMCLI_HOME=Provide your path here
REPLICATION_ENABLED=0
################# USER PARAMETERS ################
```

Options for Individual Storage Agents

The following sections describe additional configuration options by each type of Storage Agent.

To modify these options, perform the following steps:

1. Navigate to the folder for a certain Storage Agent.
2. Open the package for the operating system where you want to deploy the Storage Agent.
3. Scroll down to the Install Scripts section.
4. Edit the content of Post-Install Script.
5. From the **File** menu, select **Save** to save changes to the post-install script.

Some Storage Agents contain packages with native libraries and exclude post-install scripts—the post-install scripts are empty. These types of packages do not require any changes.

CLARiiON: This post-install script specifies settings in `NAVICLI_HOME`, such as:

`C:/Program Files/EMC/Navisphere CLI/navicli` (Windows)

`/opt/Navisphere/bin/navicli` (Solaris)

You must verify that the script settings on each managed server match those in the post-install script because other processes may modify the server configuration.

Hitachi: `HTTP_PORT_VALUE` is the port on which the Storage Agent listens for new http connections to its management console. The default is `7031`, such as `HTTP_PORT_VALUE = 7031`.

McDATA: Before deployment, you can modify this post-install script to set a different version of the Enterprise Fabric Connectivity Manager (EFCM). The default is `9`, such as `EFCM_VER = 9`.

NetApp: `HTTP_PORT_VALUE` is the port on which the Storage Agent listens for new http connections to its management console. The default value is `7032`, such as `HTTP_PORT_VALUE = 7032`.

Symmetrix: This post-install script specifies settings in `SYMCLI_HOME` such as:

`C:/Program Files/EMC/SYMCLI/bin` (Windows)

`/opt/emc/SYMCLI/V6.2.1/bin` (Solaris)

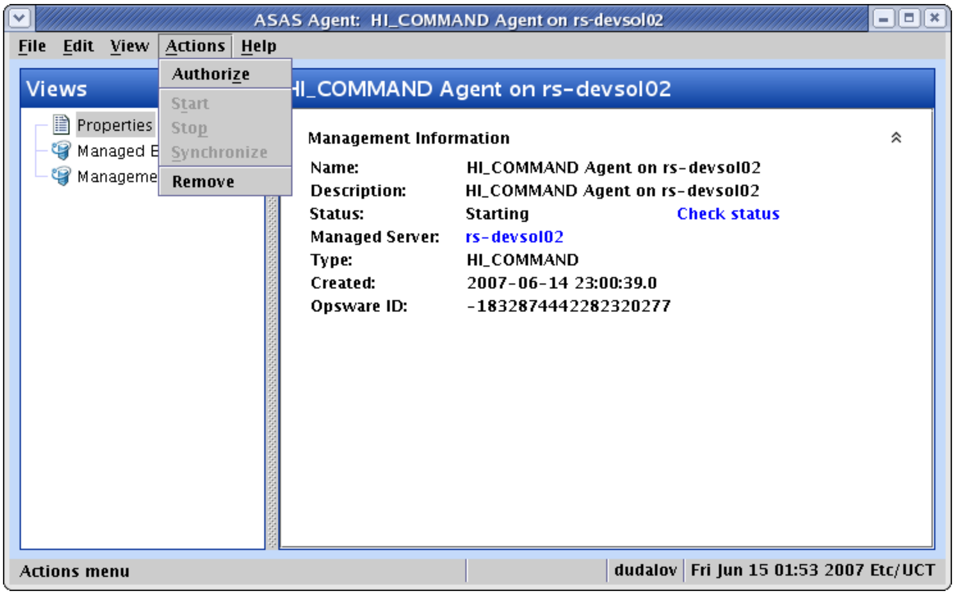
`REPLICATION_ENABLED` (The default is `1`.)

You must verify that the script settings on each managed server match those in the post-install script because other processes may modify the server configuration.

Authorizing a Deployed Storage Agent

Each Storage Agent must be authorized before messages from that agent are accepted by the core. You can authorize the Storage Agent using the object browser for that Storage Agent. See Figure 2-4.

Figure 2-4: Storage Agent Object Browser



Management Information

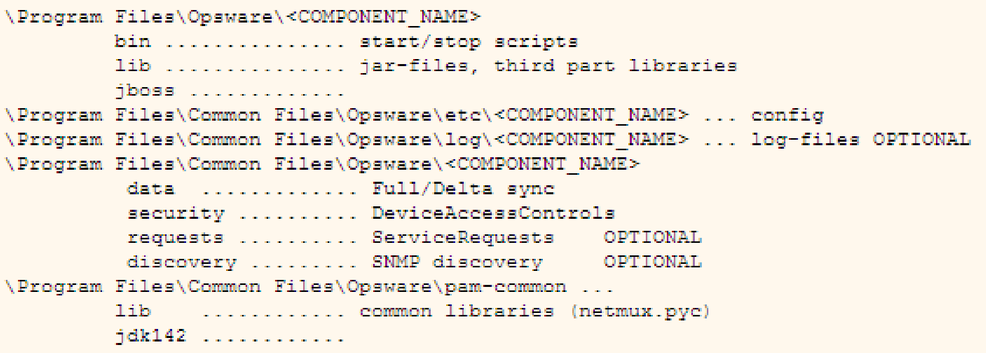
Name:	HI_COMMAND Agent on rs-devsol02	
Description:	HI_COMMAND Agent on rs-devsol02	
Status:	Starting	Check status
Managed Server:	rs-devsol02	
Type:	HI_COMMAND	
Created:	2007-06-14 23:00:39.0	
Opsware ID:	-1832874442282320277	

dudalov Fri Jun 15 01:53 2007 Etc/UCT

Storage Agent File System Layout

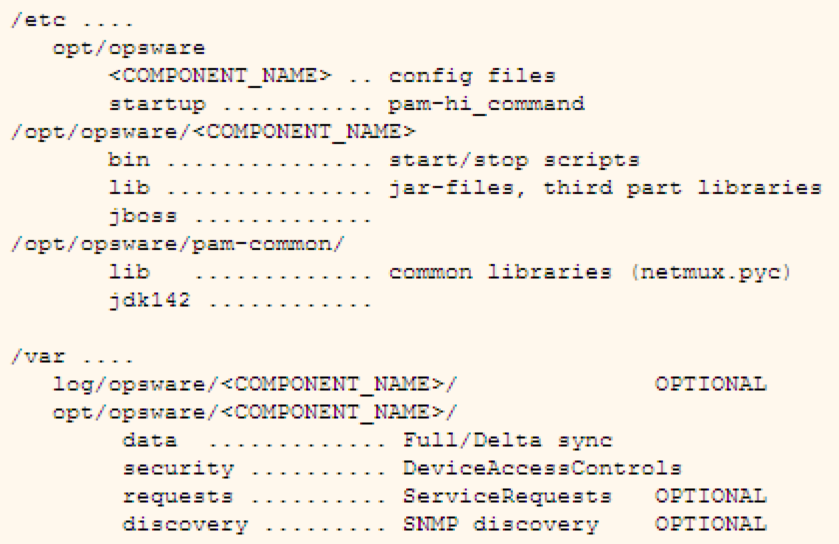
The following figures define the file system layouts for XML Storage Agents and Java Storage Agents for Windows and Unix operating systems.

Figure 2-5: XML Storage Agent File System for Windows.



```
\Program Files\Opsware\<COMPONENT_NAME>
         bin ............... start/stop scripts
         lib ............... jar-files, third part libraries
         jboss .............
\Program Files\Common Files\Opsware\etc\<COMPONENT_NAME> ... config
\Program Files\Common Files\Opsware\log\<COMPONENT_NAME> ... log-files OPTIONAL
\Program Files\Common Files\Opsware\<COMPONENT_NAME>
          data  ............ Full/Delta sync
          security .......... DeviceAccessControls
          requests .......... ServiceRequests    OPTIONAL
          discovery ......... SNMP discovery     OPTIONAL
\Program Files\Common Files\Opsware\pam-common ...
         lib    ............ common libraries (netmux.pyc)
         jdk142 ............
```

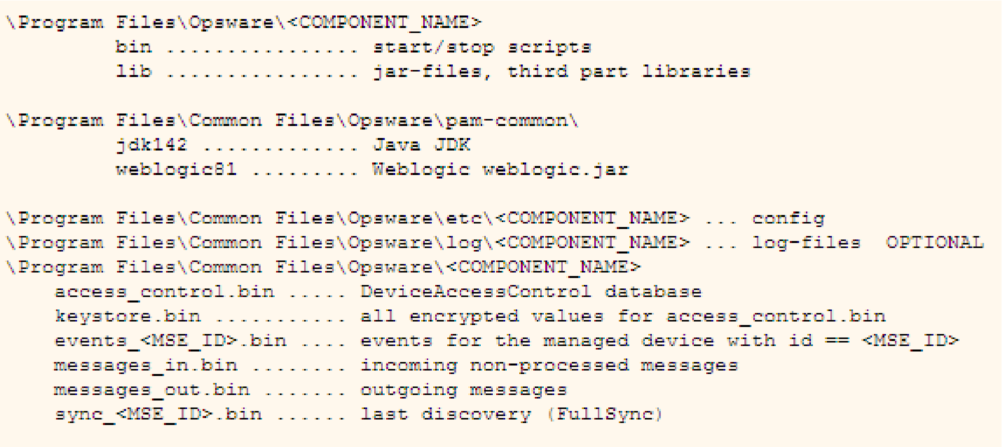
Figure 2-6: XML Storage Agent File System for Unix



```
/etc ....
   opt/opsware
       <COMPONENT_NAME> .. config files
       startup ........... pam-hi_command
/opt/opsware/<COMPONENT_NAME>
       bin ............... start/stop scripts
       lib ............... jar-files, third part libraries
       jboss .............
/opt/opsware/pam-common/
       lib   ............. common libraries (netmux.pyc)
       jdk142 ............

/var ....
   log/opsware/<COMPONENT_NAME>/             OPTIONAL
   opt/opsware/<COMPONENT_NAME>/
        data  ............. Full/Delta sync
        security .......... DeviceAccessControls
        requests .......... ServiceRequests   OPTIONAL
        discovery ......... SNMP discovery    OPTIONAL
```

Figure 2-7: Java Storage Agent File System for Windows

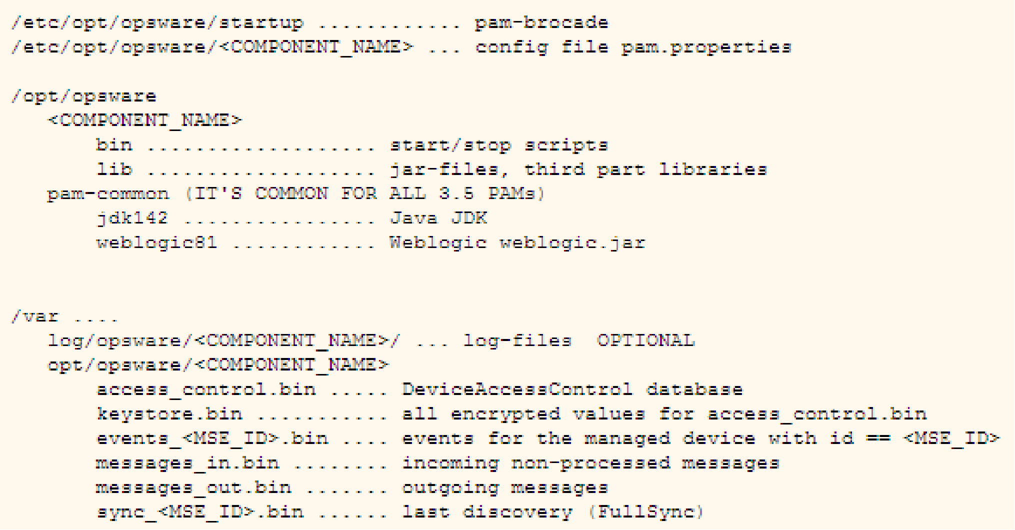


```
\Program Files\Opsware\<COMPONENT_NAME>
         bin ................ start/stop scripts
         lib ................ jar-files, third part libraries

\Program Files\Common Files\Opsware\pam-common\
         jdk142 ............. Java JDK
         weblogic81 ......... Weblogic weblogic.jar

\Program Files\Common Files\Opsware\etc\<COMPONENT_NAME> ... config
\Program Files\Common Files\Opsware\log\<COMPONENT_NAME> ... log-files  OPTIONAL
\Program Files\Common Files\Opsware\<COMPONENT_NAME>
    access_control.bin ..... DeviceAccessControl database
    keystore.bin ........... all encrypted values for access_control.bin
    events_<MSE_ID>.bin .... events for the managed device with id == <MSE_ID>
    messages_in.bin ........ incoming non-processed messages
    messages_out.bin ....... outgoing messages
    sync_<MSE_ID>.bin ...... last discovery (FullSync)
```

Figure 2-8: Java Storage Agent File System for Unix



```
/etc/opt/opsware/startup ............ pam-brocade
/etc/opt/opsware/<COMPONENT_NAME> ... config file pam.properties

/opt/opsware
   <COMPONENT_NAME>
       bin ................... start/stop scripts
       lib ................... jar-files, third part libraries
   pam-common (IT'S COMMON FOR ALL 3.5 PAMs)
       jdk142 ................ Java JDK
       weblogic81 ............ Weblogic weblogic.jar


/var ....
   log/opsware/<COMPONENT_NAME>/ ... log-files  OPTIONAL
   opt/opsware/<COMPONENT_NAME>
       access_control.bin ..... DeviceAccessControl database
       keystore.bin ........... all encrypted values for access_control.bin
       events_<MSE_ID>.bin .... events for the managed device with id == <MSE_ID>
       messages_in.bin ........ incoming non-processed messages
       messages_out.bin ....... outgoing messages
       sync_<MSE_ID>.bin ...... last discovery (FullSync)
```

Removing a Storage Agent

Before you can remove a Storage Agent from a core, you must undeploy it. This section explains how to undeploy a Storage Agent from a managed server and then remove that Storage Agent from the core. This section also discusses the changes that occur on a managed server when a Storage Agent is undeployed.

Undeploying a Storage Agent from a Managed Server

When you undeploy a Storage Agent, you remove the binaries from a managed server. A Storage Agent must be undeployed when a storage administrator wants to move a Storage Agent from one managed server to another managed server. This action will not change any data description in the database. Arrays, volumes, and switches controlled by that Storage Agent will be exactly the same after deploying that Storage Agent to another managed server. Objects are not removed from the database and may be discovered by a different Storage Agent.

See the *SA User's Guide: Application Automation* for more information about software policies and the remediate process.

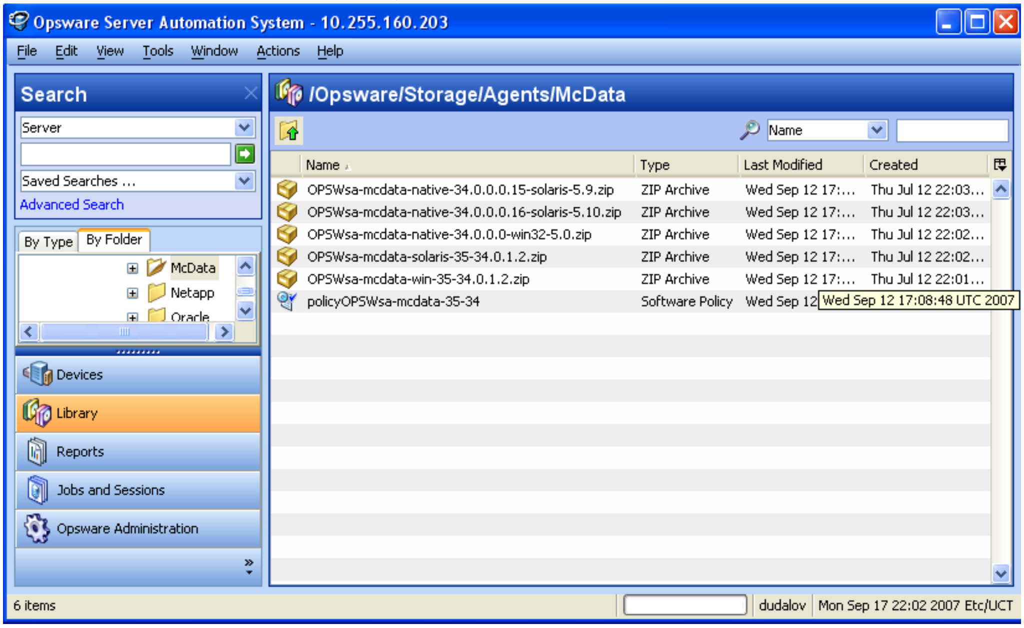
To undeploy a Storage Agent from a managed server, perform the following steps:

1. From the Navigation pane, select the By Folder tab and then select Library.

2. Go to the folder that corresponds to the Storage Agent you want to undeploy, such as **Library ➤ Opsware ➤ Storage ➤ Agents ➤ Brocade** for the Brocade Storage Agent.

3 Select the software policy.

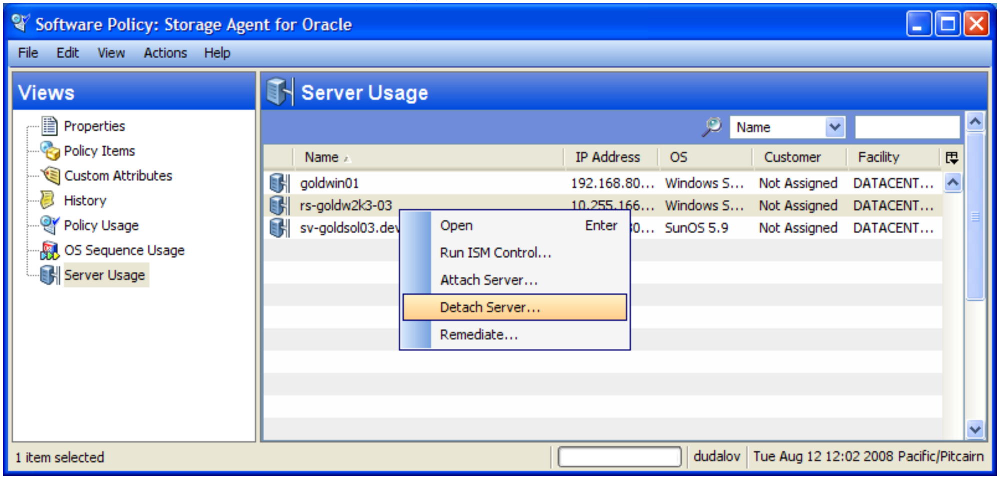
Figure 2-9: Selecting a Software Policy for a Storage Agent



Name	Type	Last Modified	Created
OPSWsa-mcdata-native-34.0.0.0.15-solaris-5.9.zip	ZIP Archive	Wed Sep 12 17:...	Thu Jul 12 22:03...
OPSWsa-mcdata-native-34.0.0.0.16-solaris-5.10.zip	ZIP Archive	Wed Sep 12 17:...	Thu Jul 12 22:03...
OPSWsa-mcdata-native-34.0.0.0-win32-5.0.zip	ZIP Archive	Wed Sep 12 17:...	Thu Jul 12 22:02...
OPSWsa-mcdata-solaris-35-34.0.1.2.zip	ZIP Archive	Wed Sep 12 17:...	Thu Jul 12 22:02...
OPSWsa-mcdata-win-35-34.0.1.2.zip	ZIP Archive	Wed Sep 12 17:...	Thu Jul 12 22:01...
policyOPSWsa-mcdata-35-34	Software Policy	Wed Sep 12	Wed Sep 12 17:08:48 UTC 2007

4 Open the software policy.

Figure 2-10: Detaching a Software Policy from a Managed Server



Name	IP Address	OS	Customer	Facility
goldwin01	192.168.80...	Windows S...	Not Assigned	DATACENT...
rs-goldw2k3-03	10.255.166...	Windows S...	Not Assigned	DATACENT...
sv-goldsol03.dev	0...	SunOS 5.9	Not Assigned	DATACENT...

5 From the Views pane, select Server Usage.

6 Select the managed server that you want to remove the Storage Agent from.

7 From the Action menu, select Detach Server.

8. In the Remediate window, select options to schedule the remediate job. The remediate process will stop and then remove the Storage Agent from the managed server.

After the Storage Agent is stopped or undeployed, the status does not change. For more information, see “Checking the Oracle Storage Agent Status” on page 162. For more information about stopping a certain type of Storage Agent, see “Storage Agent Configuration and Operation” on page 66.

Removing a Storage Agent from the Core

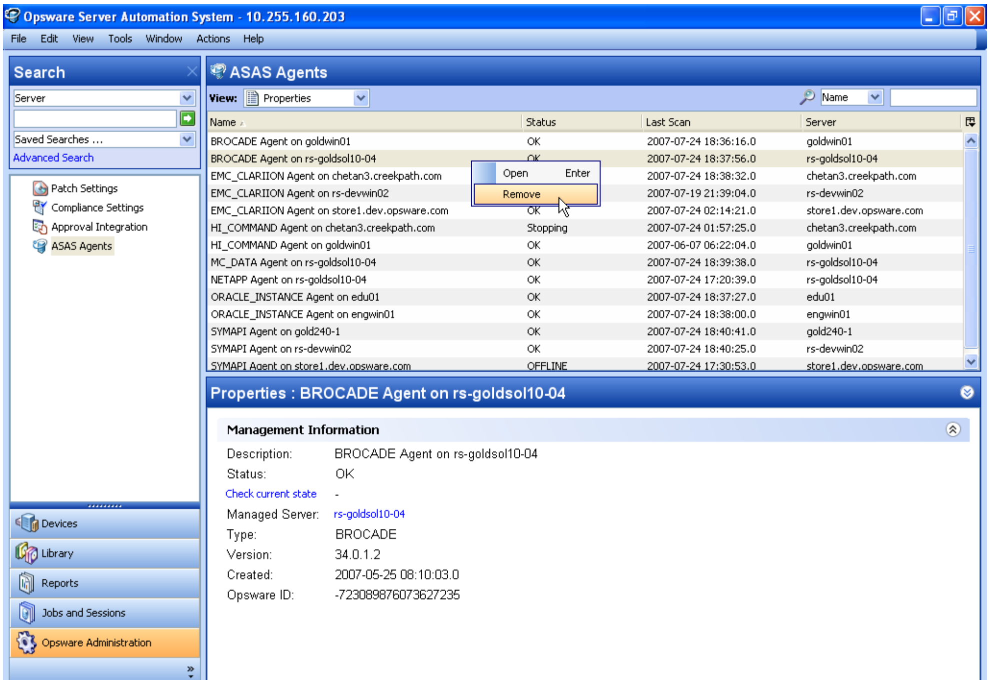
When you remove a Storage Agent from the core, you remove the entry in the database that represents the existence of a Storage Agent on a particular managed server. The Storage Agent software policy is not removed. The software policy is removed when you uninstall the Storage Agent. See “Uninstalling With the HP Server Automation Client (Recommended)” on page 46.

To remove these binaries from the managed server, use the corresponding software policy.

To remove a Storage Agent from the core, perform the following steps:

1. From the Navigation pane, select **Opsware Administration**.

Figure 2-11: Removing a Storage Agent from the Core



Name	Status	Last Scan	Server
BROCADE Agent on goldwin01	OK	2007-07-24 18:36:16.0	goldwin01
BROCADE Agent on rs-goldsol10-04	OK	2007-07-24 18:37:56.0	rs-goldsol10-04
EMC_CLARIION Agent on chetan3.creekpath.com		2007-07-24 18:38:32.0	chetan3.creekpath.com
EMC_CLARIION Agent on rs-devwin02		2007-07-19 21:39:04.0	rs-devwin02
EMC_CLARIION Agent on store1.dev.opsware.com	OK	2007-07-24 02:14:21.0	store1.dev.opsware.com
HI_COMMAND Agent on chetan3.creekpath.com	Stopping	2007-07-24 01:57:25.0	chetan3.creekpath.com
HI_COMMAND Agent on goldwin01	OK	2007-06-07 06:22:04.0	goldwin01
MC_DATA Agent on rs-goldsol10-04	OK	2007-07-24 18:39:38.0	rs-goldsol10-04
NETAPP Agent on rs-goldsol10-04	OK	2007-07-24 17:20:39.0	rs-goldsol10-04
ORACLE_INSTANCE Agent on edu01	OK	2007-07-24 18:37:27.0	edu01
ORACLE_INSTANCE Agent on engwin01	OK	2007-07-24 18:38:00.0	engwin01
SYMAPI Agent on gold240-1	OK	2007-07-24 18:40:41.0	gold240-1
SYMAPI Agent on rs-devwin02	OK	2007-07-24 18:40:25.0	rs-devwin02
SYMAPI Agent on store1.dev.opsware.com	OFFLINE	2007-07-24 17:30:53.0	store1.dev.opsware.com

Properties : BROCADE Agent on rs-goldsol10-04

Management Information

Description: BROCADE Agent on rs-goldsol10-04
Status: OK
Check current state -
Managed Server: rs-goldsol10-04
Type: BROCADE
Version: 34.0.1.2
Created: 2007-05-25 08:10:03.0
Opsware ID: -7230898760736227235

2. Select ASAS Agents.

3. Select the Storage Agent you want to remove.

4. From the **Action** menu, select **Remove**.

Managed Server Changes During Undeployment

The following changes occur on a managed server when its Storage Agent is undeployed:

- The undeployment process does not remove DeviceAccessControls or discovered data. This is intended to simplify the installation of the next version of the Storage Agent to the managed server. By keeping device access controls and data on a managed server, the newer version of a Storage Agent does not need to be configured after installation.
- Not every package deployed as a part of the software policy is removed from the managed server during the undeployment process. Packages that are shared by more

than one Storage Agent are removed by the remediate process only when there are no more deployed policies that have that package associated with them.

- When the last Storage Agent is removed from a Solaris managed server, the `opswstagent` account is also removed.

Uninstalling a Storage Agent

When you uninstall a Storage Agent, you remove the ability from the core to deploy or undeploy binaries to a managed server. All Storage Agents must be undeployed from a managed server before uninstalling that Storage Agent from the core. See “Undeploying a Storage Agent from a Managed Server” on page 42.

The following sections explain how you can uninstall a Storage Agent from the core by using the HP Server Automation Client and the HP BSA Installer distribution. It is recommended that you perform all uninstallation processes using the HP Server Automation Client.

Uninstalling With the HP Server Automation Client (Recommended)

To uninstall a Storage Agent using the HP Server Automation Client, perform the following steps:

1. Detach managed servers from a software policy. See “Undeploying a Storage Agent from a Managed Server” on page 42.
2. Remove packages that are assigned to that software policy.
3. Delete the software policy and packages.

See the *SA User’s Guide: Application Automation* for more information about software policies.

Uninstalling With the HP BSA Installer

You can uninstall a Storage Agent from the core using the HP BSA Installer distribution. The Storage Agent must be undeployed from the managed servers before you uninstall it. If there are any Storage Agents deployed on managed servers, the process fails with a non-zero exit code and an error message that lists all managed servers attached to the software policy.

To uninstall a Storage Agent from the core using HP BSA Installer distribution, perform the following steps:

1. Mount the Storage Agent distribution.
2. Invoke the `uninstall_opsware.sh` script. This script completes the following actions:
   - From the folder that corresponds to the selected Storage Agent, it checks all software policies with a name that was generated during Storage Agent installation.
   - If the software policy has a managed server attached to it, the uninstall process logs a list of attached managed servers and quits with a non-zero exit code.
   - If a managed server is not attached to the policy, the uninstallation process removes all packages assigned to the policy.
   - The uninstaller removes the software policy.
   - The uninstaller removes packages from the folder where the names match the pattern for the Storage Agent. The pattern is `OPSWsa-<COMPONENTNAME>`, such as `OPSWsa-brocade%` or `OPSWsa-netapp%`.

The HP BSA Installer distribution does not remove folders from the core. These are the folders that were created during the installation process, such as **Library ➤ Opsware ➤ Storage ➤ Agents ➤ Brocade**. There is no impact on the server where the core is running. The file system of that server does not keep any packages or software policies–everything is stored in the core.

If there are any shared packages that belong to another software policy, the uninstallation process tries to remove these packages. The process does not stop if it cannot remove them. It will continue after logging a `FINE` log-message saying that the package cannot be removed. If the uninstallation process fails to remove one of the main packages of a Storage Agent, the uninstallation fails with a non-zero exit code.

Chapter 3: Storage Host Agent Extension (SHA) Installation

IN THIS CHAPTER

This chapter discusses the following topics:

Storage Host Agent Extension

Storage Host Agent Extension (SHA) is an HP Server Automation 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, devices
- Volume manager (VM) assets, configuration, devices
- File systems

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

Supported Operating Systems

ASAS supports the operating systems listed in Table 1-1, “Supported Operating Systems for the Storage Host Agent Extension,” on page 17.

Pre-Installation Requirements

The SHA installation process is required to run on the core server that has the Software Repository installed. See the *SA Planning and Installation Guide* for information about installing HP Server Automation. The core must be running when you install the SHA distribution.

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

Installing a Storage Host Agent Extension

SHA is supplied in the ASAS Server Storage Extensions distribution. The distribution uses the HP BSA Installer to upload server module content into an existing SA core.

The HP BSA Installer uploads packages and creates software policies for the SHA modules. The simple interview mode prompts you to enter one parameter - the password for the Model Repository user `opsware_admin`. The advanced interview mode also requires an additional parameter - the password for the user `detuser`.

To install the SHA on a managed server, perform the following steps:

1. Log in to the server that you installed HP Server Automation on and then launch a command prompt.

2. Mount the ASAS installation DVD using a command similar to `mount /dev/cdrom` or NFS-mount the directory that contains a copy of the DVD contents.

3. From the ASAS installation DVD, enter the `install_opsware.sh` command to start the HP BSA Installer, such as:

```
/tmp/opsware_34.C.2434.0-storex/disk001/opsware_installer/
install_opsware.sh --verbose -r /usr/tmp/oiresponse.storex
```

A prompt similar to the following example appears:

```
Welcome to the Opsware Installer.
Please select the components to install.
1 ( ) Host Storage Extensions Server Modules
Enter a component number to toggle ('a' for all, 'n' for
none).
When ready, press 'c' to continue, or 'q' to quit.
Selection: 1
```

The sample command requires the user to have a pre-created response file, see page 56 for an example. If it does not exist, then the user should run the command without using option '-r'. This helps the user go through an interview process. The simple interview mode prompts the user to provide the Model Repository user password. The advance interview mode requires an additional password for internal user 'detuser'.

4. To select the SHA, type `1` and then press Enter. A prompt similar to the following appears:

   ```
   Welcome to the Opsware Installer.
   Please select the components to install.
   1 (*) Host Storage Extensions Server Modules
   Enter a component number to toggle ('a' for all, 'n' for
   none).
   When ready, press 'c' to continue, or 'q' to quit.
   Selection: c
   ```

5. The HP BSA Installer saves your interview answer in a file that is named to represent the SHA. such as:

   `/usr/tmp/oiresponse.storex`.

   See “Installation Transcript Example” on page 57 for an example of a response file.

Upgrading a Storage Host Agent Extension

SHA is upgraded when an administrator chooses to install SHA on an SA core that already contains a SHA module. During an upgrade, 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 intact and are ready for execution with the upgraded SHA module. Prior to running the upgrade, you should verify there are no storage inventory snapshot jobs running.

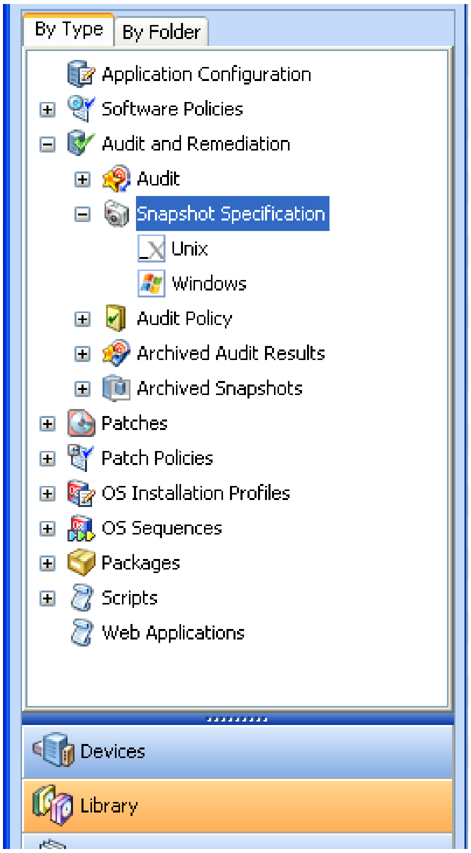
Creating a Storage Inventory Snapshot

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.

To create a snapshot specification, perform the following steps:

1 From the Navigation pane, select **Library ➤ Audit and Remediation ➤ Snapshot Specification**.

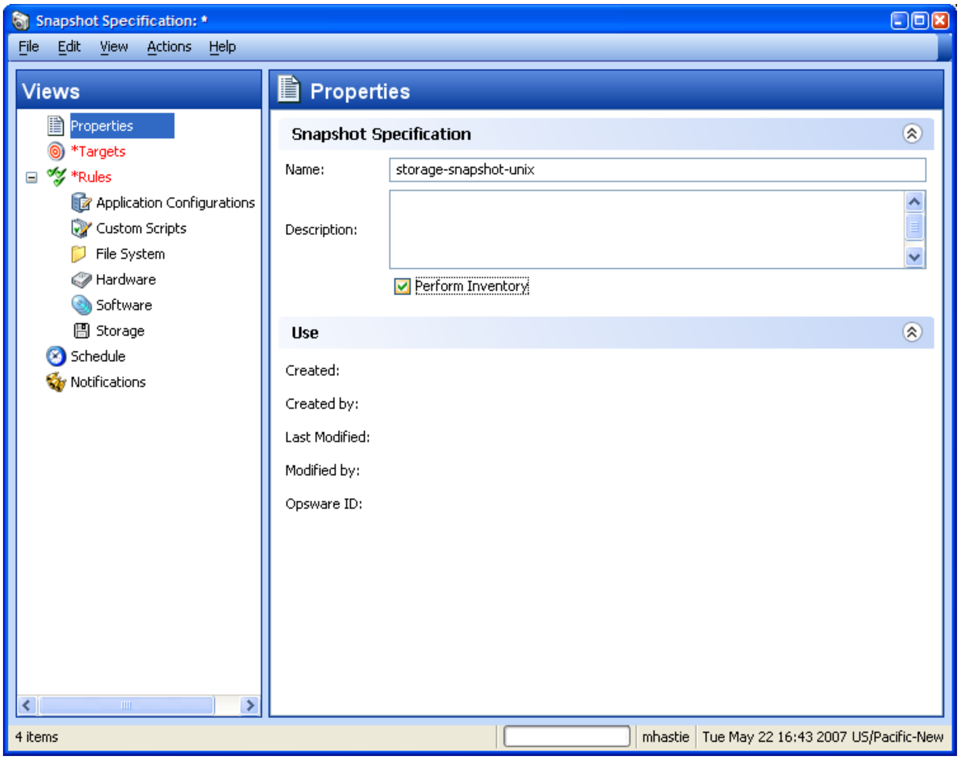
Figure 3-1: Snapshot Specification Folder in the SA Client



2 From the expanded Snapshot Specification folder, select the operating system that you are creating the snapshot specification for–Unix or Windows.

3 From the **Actions** menu, select **New** to display the Snapshot Specification Properties window.

Figure 3-2: Snapshot Specification Properties Window



Snapshot Specification

Name: storage-snapshot-unix

Description:

☑ Perform Inventory

Use

Created:

Created by:

Last Modified:

Modified by:

Opsware ID:

4 items | mhastie | Tue May 22 16:43 2007 US/Pacific-New

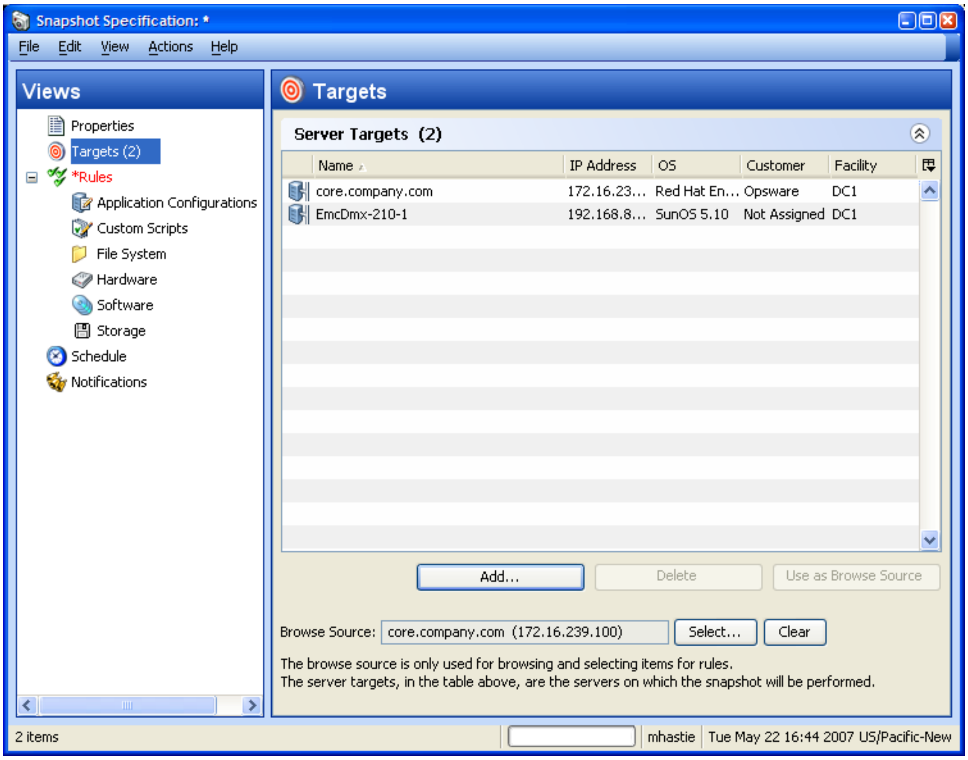
4 Enter a name for the inventory snapshot.

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 to display the Snapshot Specification Targets window.

Figure 3-3: Snapshot Specification Targets Window



Server Targets (2)

Name	IP Address	OS	Customer	Facility
core.company.com	172.16.23...	Red Hat En...	Opsware	DC1
EmcDmx-210-1	192.168.8...	SunOS 5.10	Not Assigned	DC1

Browse Source: core.company.com (172.16.239.100)

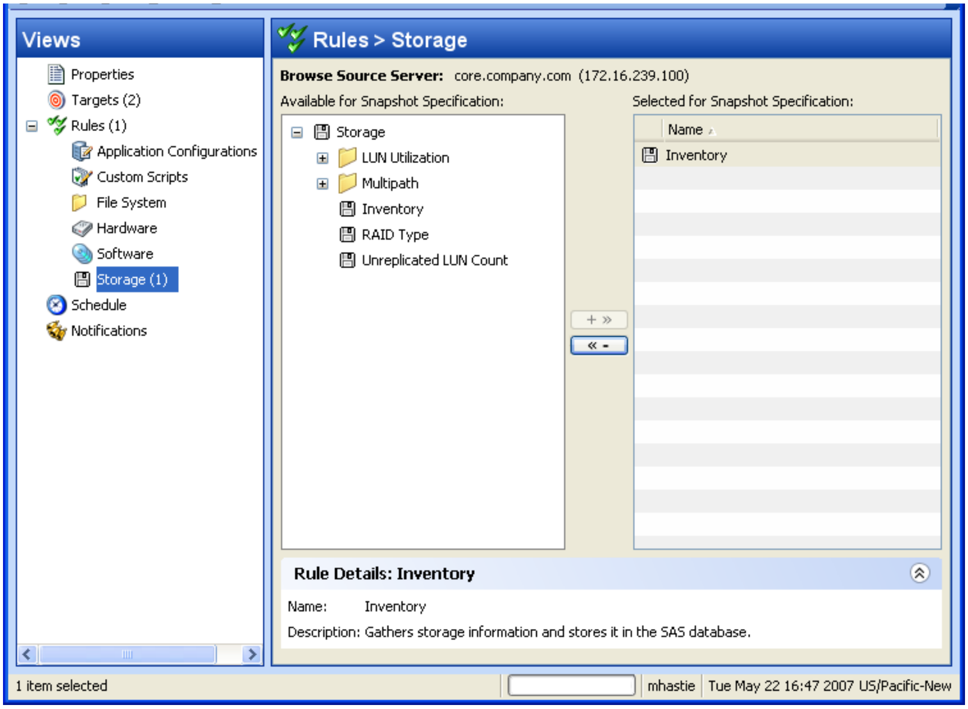
The browse source is only used for browsing and selecting items for rules.
The server targets, in the table above, are the servers on which the snapshot will be performed.

2 items | mhastie | Tue May 22 16:44 2007 US/Pacific-New

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 ➤ Storage** to display the Snapshot Specification Rules window.

Figure 3-4: Snapshot Specification Rules Window



Browse Source Server: core.company.com (172.16.239.100)

Name: Inventory

Description: Gathers storage information and stores it in the SAS database.

1 item selected | mhastie | Tue May 22 16:47 2007 US/Pacific-New

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

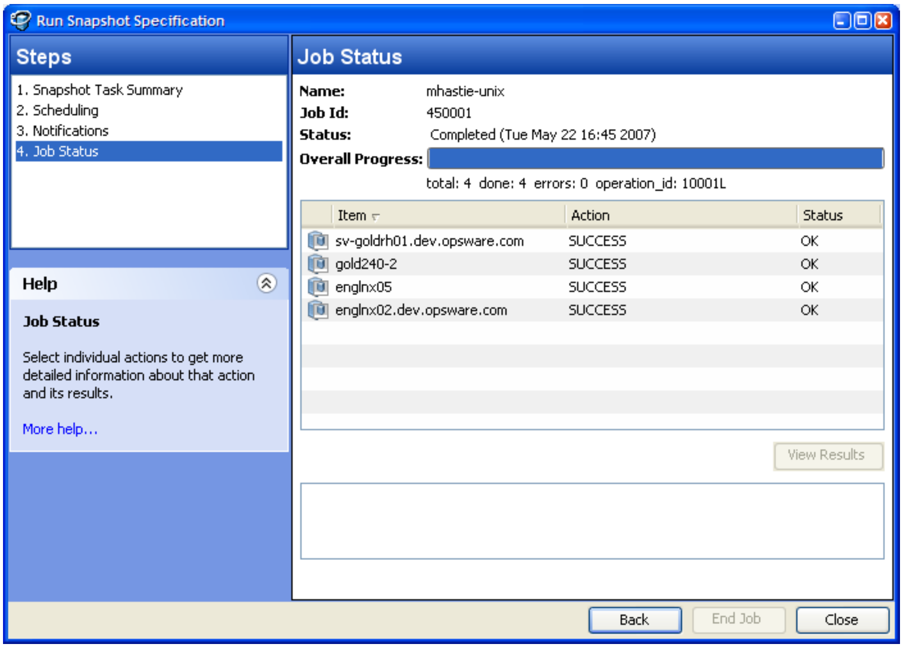
11 Click the **+ >>** button to move Inventory to the Selected for Snapshot Specification section.

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.

Figure 3-5: Inventory Snapshot Job Status Window



1. Snapshot Task Summary
2. Scheduling
3. Notifications
4. Job Status

Name: mhastie-unix
Job Id: 450001
Status: Completed (Tue May 22 16:45 2007)
Overall Progress:
total: 4 done: 4 errors: 0 operation_id: 10001L

Item	Action	Status
sv-goldrh01.dev.opsware.com	SUCCESS	OK
gold240-2	SUCCESS	OK
englnx05	SUCCESS	OK
englnx02.dev.opsware.com	SUCCESS	OK

Job Status

Select individual actions to get more detailed information about that action and its results.

More help...

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

SHA File System Layout

The SHA module is a server module called `com.opsware.storage.storex`. Depending on the operating system, the SHA module is installed in the following directories:

`%ProgramFiles%\Opsware\sm\com.opsware.storage.storex` (Windows)

`/opt/opsware/sm/com.opsware.storage.storex` (Unix)

The SHA module exposes an executable on both the Windows and Unix operating systems:

`/opt/opsware/storage/bin/sync.py [get <url>|xml <hostname>]` (Unix)

`"%ProgramFiles%\Opsware\storage\bin\symc.cmd" [get <url>|xml <hostname>]` (Windows)

`get <url>`	invoked by the server module framework
`xml`	for diagnosis only; requests `sync.py` to write the `storex` XML to stdout

Installation Transcript Example

The following is an example of a HP BSA Installer transcript. It shows the sequence of user actions required to install the SHA distribution.

```
[root@red-core1 tmp]# /tmp/opsware_34.C.2678.0-storex/disk001/
opsware_installer/install_opsware.sh
<opsware_34.0.2678.C-storex/disk001/opsware_installer/install_
opsware.sh

Distribution version = opsware_34.C
Script started, file is /var/log/opsware/install_opsware/
install_opsware.2007-06-21.20:27:29.log
/tmp/opsware_34.C.2678.0-storex/disk001/python_installations/
Linux/python/bin/python /tmp/opsware_34.C.2678.0-storex/
disk001/opsware_installer/install_opsware.pyc  --os_type Linux -
-os_version 3AS --base_dir /tmp/opsware_34.C.2678.0-storex/
disk001 --progname /var/tmp/oitmp//install_opsware.sh  --logfile
install_opsware.2007-06-21.20:27:29_verbose.log

Install Type: "Opsware ASAS Host Storage Extensions"
Please select the interview mode. Simple mode uses default
values for many of the configuration parameters. Advanced mode
allows you to fully configure the installation.

1 - Simple Interview Mode
2 - Advanced Interview Mode

Please select the interview mode from the menu, type 'h' for
help, 'q' to quit: 1

The Opsware Installer will now interview you to obtain the
installation parameters it needs. You can use the following keys
to navigate forward and backward through the list of parameters:
```

```
Control-P - go to the previous parameter
Control-N - go to the next parameter
Return - accept the default (if any) and go to the next
parameter
Control-F - finish parameter entry
Control-I - show this menu, plus information about the current
parameter

Press Control-F when you are finished. The Opsware Installer
will perform a final validation check and write out a response
file that will be used to install the Opsware components.

Parameter 1 of 1 (truth.oaPwd)Please enter the password for the
opsware_admin user. This is the password used to connect to the
Oracle database.: opsware_admin
Validating... OK.

All parameters have values.  Do you wish to finish the
interview? (y/n): y

Concluding interview.

Interview complete.

Name of response file to write [/usr/tmp/oiresponse.storex]:
Response file written to /usr/tmp/oiresponse.storex.

Would you like to continue the installation using this response
file? (y/n): y
Welcome to the Opsware Installer.
Please select the components to install.
1 ( ) Host Storage Extensions Server Modules
Enter a component number to toggle ('a' for all, 'n' for none).
When ready, press 'c' to continue, or 'q' to quit.

Selection: 1
Welcome to the Opsware Installer.
Please select the components to install.
1 (*) Host Storage Extensions Server Modules
Enter a component number to toggle ('a' for all, 'n' for none).
When ready, press 'c' to continue, or 'q' to quit.

Selection: c
[Jun-21-2007 20:27:43] >>>>Installing preliminary components

..........
[Jun-21-2007 20:28:23] Opsware Installer ran successfully.
```

```
For more details, please see the following file:
/var/log/opsware/install_opsware/install_opsware.2007-06-
21.20:27:29_verbose.log

###############################################################
#####
WARNING: to make sure that no sensitive information is left
on this server, please remove,encrypt or copy to a secure
location
the following files and directories:
  -- /var/opt/opsware/install_opsware/resp/*
  -- /var/log/opsware/install_opsware/*
  -- /var/tmp/*.sh
Also, please encrypt or store in a secure location the response
file that you used to install this core.
###############################################################
#####

Script done, file is /var/log/opsware/install_opsware/install_
opsware.2007-06-21.20:27:29.log
[root@red-core1 tmp]#

Here is an example response file:

# Opsware Installer response file
# Generated by Opsware Installer Thu Jun 21 20:27:39 2007

%oi.components
storex

%oi.build_id
opsware_34.C.2678.0

%truth.oaPwd
opsware_admin

%truth.detuserpwd
opsware_admin
```

Chapter 4: Administration

IN THIS CHAPTER

This section discusses the following topics:

- SA Permissions
- Storage Agent Configuration and Operation
- Storage Agent Properties
- Storage Agent Managed Elements
- Storage Agent Settings
- Storage Agent Management Console

SA Permissions

SA permissions allow users to view storage devices and related data. Table 4-1 specifies the permissions required by users to perform specific actions in the ASAS Client. For storage administrators, the table answers this question: To perform a particular action, what permissions does a user need?

In Table 4-1, most of the entries in the User Action column correspond to menu items in the ASAS Client. In addition to feature permissions, server permissions are required on the managed servers affected by the storage discovery operation.

Table 4-1: ASAS Permissions Required for User Actions

USER ACTION	FEATURE PERMISSION	SERVER PERMISSION (CUSTOMER, FACILITY, DEVICE GROUP)
ASAS Database Agent Administration		
Get a list of Database Agents managed by ASAS	Manage Database Agent	Read
Authorize a Database Agent	Manage Database Agent	Read
Start a Database Agent	Manage Database Agent	Read
Stop a Database Agent	Manage Database Agent	Read
Create access controls for databases managed by the Database Agent	Manage Database Agent	Read
Issue a synchronization request for databases managed by the Database Agent	Manage Database Agent	Read
Remove (unauthorize) a Database Agent	Manage Database Agent	Read
Checking the current state of a Database Agent	Manage Database Agent	Read
Modifying the settings for a Database Agent	Manage Database Agent	Read
ASAS Storage Agent Administration		
Get a list of Storage Agents managed by ASAS	Manage Storage Agent	Read
Authorize a Storage Agent	Manage Storage Agent	Read
Start a Storage Agent	Manage Storage Agent	Read
Stop a Storage Agent	Manage Storage Agent	Read

Table 4-1: ASAS Permissions Required for User Actions (continued)

USER ACTION	FEATURE PERMISSION	SERVER PERMISSION (CUSTOMER, FACILITY, DEVICE GROUP)
Create access controls for storage arrays/ NAS Filers managed by the Storage Agent	Manage Storage Agent	Read
Issue a synchronization request for storage arrays/NAS Filers managed by the Storage Agent	Manage Storage Agent	Read
Remove (unauthorize) a Storage Agent	Manage Storage Agent	Read
Checking the current state of a Storage Agent	Manage Storage Agent	Read
Modifying the settings for a Storage Agent	Manage Storage Agent	Read
ASAS Fabric Agent Administration		
Get a list of Fabric Agents managed by ASAS	Manage Fabric Agent	Read
Authorize a Fabric Agent	Manage Fabric Agent	Read
Start a Fabric Agent	Manage Fabric Agent	Read
Stop a Fabric Agent	Manage Fabric Agent	Read
Create access controls for fabrics managed by the Fabric Agent	Manage Fabric Agent	Read
Issue a synchronization request for fabrics managed by the Fabric Agent	Manage Fabric Agent	Read
Remove (unauthorize) a Fabric Agent	Manage Fabric Agent	Read
Checking the current state of a Fabric Agent	Manage Fabric Agent	Read
Modifying the settings for a Fabric Agent	Manage Fabric Agent	Read
View information for a database	Manage Databases	Read

Table 4-1: ASAS Permissions Required for User Actions (continued)

USER ACTION	FEATURE PERMISSION	SERVER PERMISSION (CUSTOMER, FACILITY, DEVICE GROUP)
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
View information for a storage array/NAS Filer	Manage Storage Systems	Read
View inventory for a storage array/NAS Filer	Manage Storage Systems	Read
Modify properties of a storage array/NAS Filer, such as updating a caption for a storage array/NAS Filer	Manage Storage Systems	Read & Write
Delete (remove) a storage array/NAS Filer	Manage Storage Systems	Read & Write
View information for a switch	Manage Fabrics	Read
View inventory for a switch	Manage Fabrics	Read
Modify properties of a storage switch, such as updating a caption for a storage switch	Manage Fabrics	Read & Write
Delete (remove) a switch	Manage Fabrics	Read & Write
Add a storage switch to a Public Device Group	Manage Public Device Group (Fabrics)	N/A
Remove a storage switch from a Public Device Group	Manage Public Device Group (Fabrics)	N/A

Table 4-1: ASAS Permissions Required for User Actions (continued)

USER ACTION	FEATURE PERMISSION	SERVER PERMISSION (CUSTOMER, FACILITY, DEVICE GROUP)
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
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 4-1, 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. For more information about users, groups, and permissions, see the *SA User’s 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 Users pane appears.
3. Click the Groups tab.
4. Select a group. The group is displayed in the View Groups pane.
5. Click the SA Features tab.

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

Storage Agent Configuration and Operation

Each type of Storage Agent requires configuration, such as setting access controls, starting and stopping the Storage Agent, and modifying Storage Agent settings.

To configure a Storage Agent on a managed server, you must have read permission on that server.

The following sections describe how to configure and run certain types of Storage Agents:

- “Brocade Storage Agent” on page 71
- “CLARiiON Storage Agent” on page 89
- “HiCommand Storage Agent” on page 107

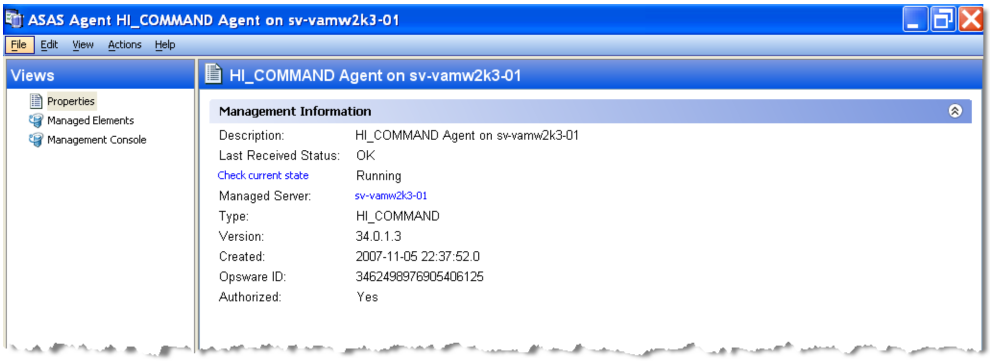
- “McDATA Storage Agent” on page 119
- “NetApp Storage Agent” on page 137
- “Oracle Storage Agent” on page 149
- “Symmetrix Storage Agent” on page 171

Storage Agent Properties

To view the properties for a Storage Agent, perform the following steps:

1. From the Navigation pane, select **Opsware Administration ➤ ASAS Agents**.
2. From the View drop-down list, select **Properties**.
3. In the ASAS Agents content pane, open a Storage Agent.
4. (Optional) Select the “Check current state” link to get the latest status of the Storage Agent.

Figure 4-1: Storage Agent Properties



HI_COMMAND Agent on sv-vamw2k3-01

Management Information

Description:	HI_COMMAND Agent on sv-vamw2k3-01
Last Received Status:	OK
Check current state	Running
Managed Server:	sv-vamw2k3-01
Type:	HI_COMMAND
Version:	34.0.1.3
Created:	2007-11-05 22:37:52.0
Opsware ID:	3462498976905406125
Authorized:	Yes

Important to Know

Description: The Storage Agent type and the managed server that it is installed and deployed on.

Last Received Status: The current status of the Storage Agent, such as OK, Starting, Stopping, or OFFLINE.

Check current state: Displays the latest status of the Storage Agent, such as Receiving…, Starting, Unavailable, and Running.

Managed Server: The name of the managed server that the Storage Agent is installed and deployed on.

Type: The type of Storage Agent.

Version: The version of the Storage Agent.

Created: The date and time when the Storage Agent was installed and deployed on the managed server.

Opsware ID: The name assigned to the Storage Agent.

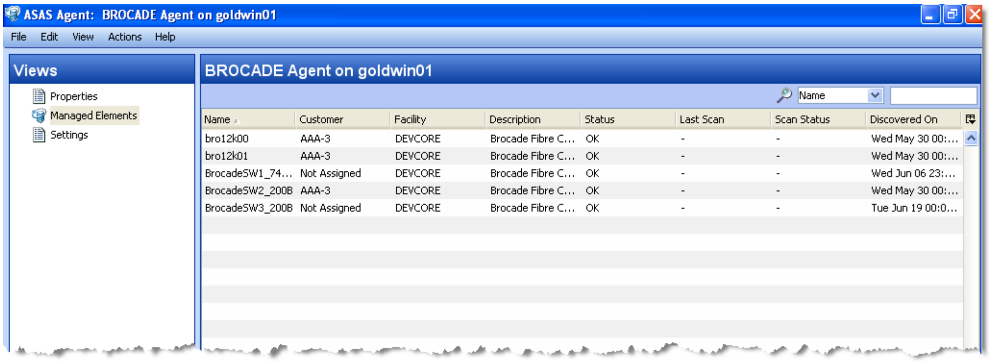
Authorized: The current authorization status, such as Yes or No.

Storage Agent Managed Elements

To view managed elements associated with the Storage Agent, perform the following steps:

1. From the Navigation pane, select **Opsware Administration ➤ ASAS Agents**.
2. From the View drop-down list, select **Managed Elements**.
3. In the ASAS Agents content pane, open a Storage Agent.

Figure 4-2: Storage Agent Managed Elements



Name	Customer	Facility	Description	Status	Last Scan	Scan Status	Discovered On
bro12k00	AAA-3	DEVCORE	Brocade Fibre C...	OK	-	-	Wed May 30 00:...
bro12k01	AAA-3	DEVCORE	Brocade Fibre C...	OK	-	-	Wed May 30 00:...
BrocadeSW1_74...	Not Assigned	DEVCORE	Brocade Fibre C...	OK	-	-	Wed Jun 06 23:...
BrocadeSW2_200B	AAA-3	DEVCORE	Brocade Fibre C...	OK	-	-	Wed May 30 00:...
BrocadeSW3_200B	Not Assigned	DEVCORE	Brocade Fibre C...	OK	-	-	Tue Jun 19 00:0...

Important to Know

Name: The name of the elements managed by the Storage Agent.

Customer: The customer assigned to the managed device.

Facility: The facility of the managed device.

Description: The Storage Agent type and the managed server that it is installed and deployed on.

Status: The current status of the Storage Agent, such as OK, Starting, Stopping, or OFFLINE.

Last Scan: The date and time when the managed device was last discovered.

Scan Status: The status of the last discovery, such as SUCCESS, INCOMPLETE, or FAILURE.

Discovered On: The date and time when the managed device was initially discovered.

Customer and Facility are determined based on similar properties of the managed server where the Storage Agent is running. This is the Storage Agent that discovered the managed device (array, fabric, and so on).

Storage Agent Settings

For information about Java Storage Agent settings, see:

- “Brocade Storage Agent” on page 71
- “CLARiiON Storage Agent” on page 89
- “McDATA Storage Agent” on page 119
- “Oracle Storage Agent” on page 149
- “Symmetrix Storage Agent” on page 171

For information about XML Storage Agent Settings, see:

- “HiCommand Storage Agent” on page 107
- “NetApp Storage Agent” on page 137

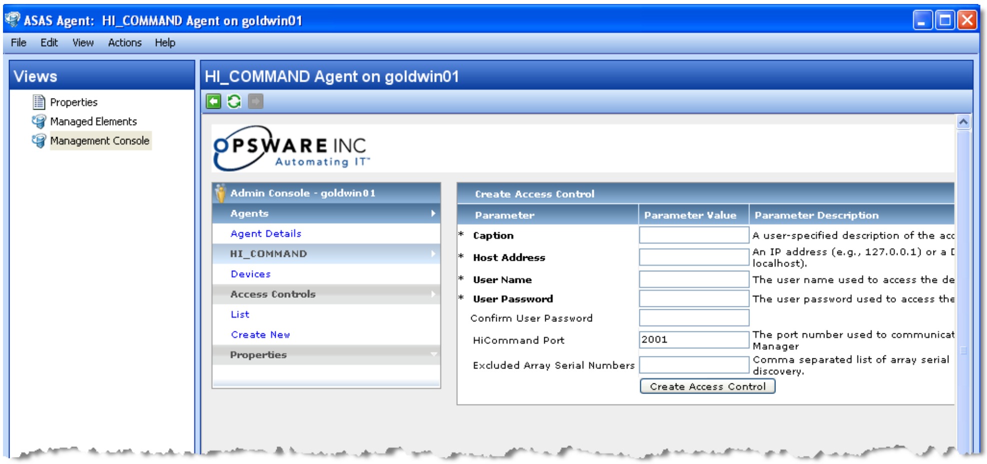
Storage Agent Management Console

The Management Console is used for XML Storage Agents only (NetApp and HiCommand).

To access the Management Console for an XML Storage Agent, perform the following steps:

1. From the Navigation pane, select **Opsware Administration ➤ ASAS Agents**.
2. In the ASAS Agents content pane, open a NetApp or HiCommand Storage Agent.
3. From the Views pane, select **Management Console**.

Figure 4-3: Management Console for a HiCommand Storage Agent



Create Access Control

	Parameter	Parameter Value	Parameter Description
*	**Caption**		A user-specified description of the acc
*	**Host Address**		An IP address (e.g., 127.0.0.1) or a D localhost).
*	**User Name**		The user name used to access the de
*	**User Password**		The user password used to access the
	Confirm User Password		
	HiCommand Port	2001	The port number used to communicat Manager
	Excluded Array Serial Numbers		Comma separated list of array serial discovery.

Create Access Control

Chapter 5: Brocade Storage Agent

IN THIS CHAPTER

This section discusses the following topics:

- Access Controls
- Storage Agent Operation
- Storage Agent Settings

Access Controls

This section describes how to configure the Storage Agent so it can gather information from the Brocade switches. To enable this process, you must define an access control for each fabric the Storage Agent manages. An access control contains values, such as the IP address of a switch in the fabric, that allows the Storage Agent to communicate with the fabric. Table 5-1 describes the access control values you must create before running the Brocade Storage Agent for the first time.

Table 5-1: Brocade Storage Agent Access Controls

ACCESS CONTROL VALUE	DESCRIPTION
Caption	A name used to uniquely identify each access control entry. The default is `Brocade AccessControl`.
User name	The user name authorized to access the Brocade fabric. The user name must be admin-level.
Password	The password authorized to access the Brocade fabric. The password must be admin-level.

Table 5-1: Brocade Storage Agent Access Controls (continued)

ACCESS CONTROL VALUE	DESCRIPTION
IP addresses	The IP address of at least one switch that belongs to the fabric. If you have a multiple-switch fabric, specify the IP address of the switch that has the highest firmware level. While you only need to enter one IP address (the Storage Agent discovers all other switches on the fabric from this switch), specify two IP addresses (separated by a comma) in case your principal switch goes offline. IP addresses are separated by a comma. **Important**: You can enter a maximum of two IP addresses.

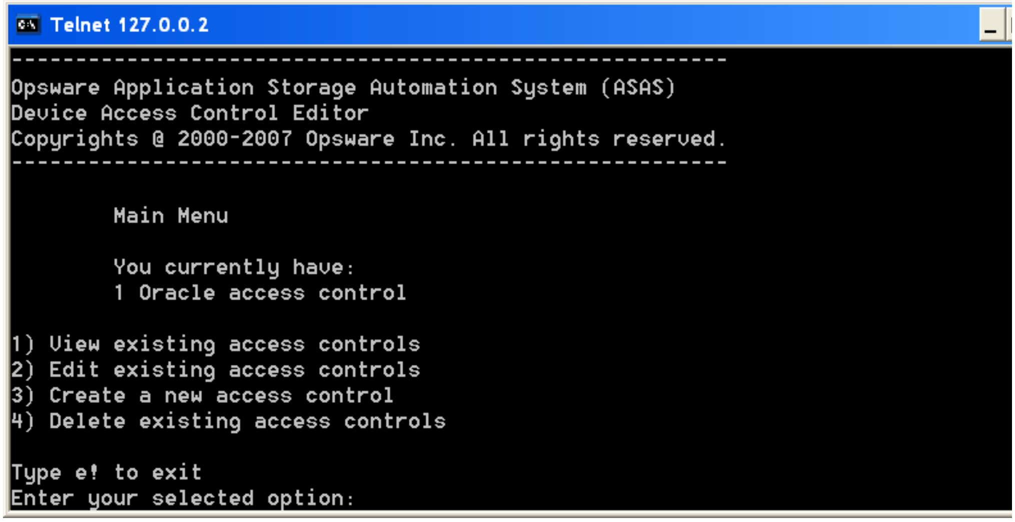
Opening the Device Access Control Editor

To open the Device Access Control Editor on a certain operating system, perform the following steps:

1. In the ASAS Agents window, select a Storage Agent and then select **Actions ➤ Open**.
2. In the ASAS Agents window for the selected Storage Agent, select **Actions ➤ DeviceAccessControl editor**.

The command line interface opens similar to the following, displaying the main menu for the Device Access Control Editor.

Figure 5-1: Device Access Control Editor Example



```
--------------------------------------------------------
Opsware Application Storage Automation System (ASAS)
Device Access Control Editor
Copyrights @ 2000-2007 Opsware Inc. All rights reserved.
--------------------------------------------------------

        Main Menu

        You currently have:
        1 Oracle access control

1) View existing access controls
2) Edit existing access controls
3) Create a new access control
4) Delete existing access controls

Type e! to exit
Enter your selected option:
```

3 Navigate through the Device Access Control Editor using the commands described in Table 5-2. All commands are case-sensitive.

Table 5-2: Device Access Control Editor Commands

COMMAND	ACTION
`b!`	Returns to the previous menu.
`c!`	Corrects the values entered for an access control. This command is only available from the Verify Values screen after you have entered all access control values for the Storage Agent.
`d!`	Deletes an existing access control.
`e!`	Exits the command line interface.
`r!`	Returns to the main menu.
`s!`	Saves a set of access control values.
`u!`	Undo an access control value by returning to the previous entry. This command is only available while you are entering access control values.

Configuring Access Controls

To configure access controls for the Brocade Storage Agent, perform the following steps:

1. Type `3` to select the `Create a new access control` option and then press Enter.

2. Type the number of the access control type you want to create or edit and then press Enter. For example, if `Brocade` is listed as option 1, type `1` and then press Enter.

3. At the `Caption` prompt, type a caption that identifies this access control and then press Enter. To accept the default value, just press Enter.

   If you are creating more than one access control, enter a caption that uniquely identifies each access control entry, such as Brocade-1, Brocade-2, and so on.

4. At the `User name` prompt, type an admin-level user name and then press Enter. This is the user name that is authorized to access the Brocade fabric instance.

5. At the `Password` prompt, type the password and then press Enter. This is the password that is authorized to access the Brocade fabric database instance.

6. Re-enter the password and then press Enter.

7. At the IP addresses prompt, type the IP address for a Brocade switch that belongs to the fabric and press Enter.

   While you only need to enter one IP address (the storage agent discovers all other switches on the fabric from this switch), you should specify two IP addresses (separated by a comma) in case your principal switch goes offline.

   If you have a multiple-switch fabric, you must specify the IP address of the switch that has the highest firmware level.
   You can enter a maximum of two IP addresses at this prompt.

   After you enter the IP addresses, the access control values you entered are displayed on the screen so that you can verify them.

8. Type `s!` (a lowercase `s`) and then press Enter to save your access control configuration.

   Access controls are saved in the `access_control.bin` file in the following directories, depending on the operating system:

`c:\Program Files\Common Files\Opsware\pam-brocade\` (Windows)

Or

`/var/opt/opsware/pam-brocade` (Unix)

9. If you need to create additional access controls, return to the main menu (`r!)` and repeat step 2 through step 8.

   OR

   Type one of the following options:

   `c!` Correct an access control entry.

   `b!` Go back to the previous menu.

10. After you have entered access control values for all Brocade fabrics you want to manage, type `e!` (a lowercase `e`) and then press Enter to exit the Access Control Editor.

Editing Access Controls

You can edit access controls while the Brocade Storage Agent is running or stopped. If you edit access controls while the Storage Agent is running, changes will be picked during the next synchronization. To edit access controls for the Brocade Storage Agent, perform the following steps:

1. Open the main menu for the Access Control Editor.
2. Type 2 to select the `Edit existing access controls` option and then press Enter.
3. Type the number of the access control type you want to edit and then press Enter.
4. Modify each value as desired. If you want to leave an access control value as is, press Enter.

   After you enter the last access control value, a summary is displayed on the screen so that you can verify them.

5. Type `s!` (a lowercase `s`) and then press Enter to save your access control configuration.

   Access controls are saved in the `access_control.bin` file in the following directories, depending on the operating system:

`c:\Program Files\Common Files\Opsware\pam-brocade\` (Windows)

Or

`/var/opt/opsware/pam-brocade` (Unix)

6. If you need to edit additional access controls, return to the main menu `(r!)` and repeat step 2 through step 5.
7. Type `e!`(a lowercase `e`) and press Enter to exit the program.

Deleting Access Controls

You can delete access controls while the Brocade Storage Agent is running or stopped. If you edit access controls while the Storage Agent is running, changes will be picked during the next synchronization. To delete access controls for the Brocade Storage Agent, perform the following steps:

1. Open the main menu for the Access Control Editor.
2. Type 4 to select the `Delete existing access controls` option and then press Enter.
3. From the **Actions** menu, select **Open** to display the Brocade Agent browser.
4. Type the number of the access control type you want to delete and then press Enter.
5. Type `d!` (a lowercase `d`) and then press Enter to delete the access control.

   The Access Control Editor confirms the deletion.
6. Type `e!` (a lowercase `e`) and then press Enter to exit access control configuration.

Storage Agent Operation

This section describes how to authorize, start, stop, synchronize, and check the discovery status of a Brocade Storage Agent.

Authorizing the Brocade Storage Agent

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 Brocade Storage Agent is deployed. When a Storage Agent is initially deployed to a managed server, you must authorize it so that messages from the Storage Agent are accepted by the core server. As a result of the authorization process, a security token is generated and given to the Storage Agent.

If you are not sure whether the security token in the core and on the managed server match, you can authorize the Brocade Storage Agent repeatedly. A security token mismatch can occur as a result of unintentional editing or removal of tokens.

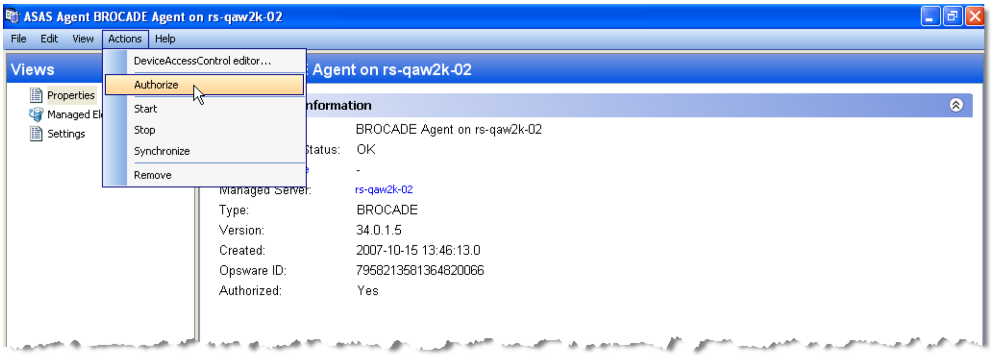
To authorize a Brocade Storage Agent, perform the following steps:

1. From the Navigation pane, select **Opsware Administration ➤ ASAS Agents**.

2. Open the Brocade Storage Agent that needs to be authorized.

3. From the **Actions** menu, select **Authorize**.

Figure 5-2: Authorize Action for a Brocade Storage Agent



BROCADE Agent on rs-qaw2k-02
tatus: OK
-
Managed Server: rs-qaw2k-02
Type: BROCADE
Version: 34.0.1.5
Created: 2007-10-15 13:46:13.0
Opsware ID: 7958213581364820066
Authorized: Yes

Starting the Brocade Storage Agent

When the Brocade Storage Agent starts for the first time, the agent begins discovering Brocade switches and synchronizing device data. During this process, the Brocade Storage Agent gathers information from various Oracle elements and reports that information to the Web Services Data Access Engine so that the device data for the Oracle switches are synchronized. Depending on the size of the Brocade fabric, device synchronization could require several hours. You can start the Storage Agent by using the ASAS Client on a managed server or by running a saved script on a remote managed server.

For performance reasons, you should start the Brocade Storage Agent during off-peak hours.

To start a Brocade Storage Agent on a managed server by using the ASAS Client, perform the following steps:

1. In the ASAS Agent window, select a Brocade Storage Agent and then select **Actions ➤ Open** to display the Brocade Storage Agent browser.
2. Select **Actions ➤ Start**.
3. In the Management Information section click the “Check current state” link to verify that the Storage Agent is running.

Starting the Brocade Storage Agent on a Remote Windows Server

To start a Brocade Storage Agent 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 OpswareBrocadeStorageAgent and then select **Action ➤ Start.**

Starting the Brocade Storage Agent on a Remote Unix Server

To start a Brocade Storage Agent on a remote Unix server, perform the following steps:

1. Navigate to the `/etc/opt/opsware/startup` directory.
2. Enter the `./pam-brocade start` command to run the saved script that starts the Storage Agent.

   When the Storage Agent starts, it begins the discovery and synchronization process. To monitor the discovery process, see “Checking the Brocade Storage Agent Status” on page 80.

Stopping the Brocade Storage Agent

You must stop the Brocade Storage Agent before you modify Storage Agent settings. See “Storage Agent Settings” on page 80.

You should also stop and then restart the Brocade Agent after any fabric changes are made. This action does not interfere with any fabric changes that are in progress.

You can stop the Storage Agent by using the ASAS Client on a managed server or by running a saved script on a remote managed server.

After the Storage Agent is stopped or undeployed, the status does not change. For more information, see “Undeploying a Storage Agent from a Managed Server” on page 42 and “Checking the Brocade Storage Agent Status” on page 80.

To stop a Brocade Storage Agent on a managed server by using the ASAS Client, perform the following steps:

1. In the ASAS Agent window, select a Brocade Storage Agent and then select **Actions ➤ Open** to display the Brocade Storage Agent browser.
2. Select **Actions ➤ Stop**.
3. In the Management Information section click the “Check current state” link to verify that the Storage Agent is Unavailable.

Stopping the Brocade Storage Agent on a Remote Windows Server

To stop a Brocade Storage Agent 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 **OpswareBrocadeStorageAgent** and then select **Action ➤ Stop.**

Stopping the Brocade Storage Agent on a Remote Unix Server

To stop a Brocade Storage Agent on a Remote Unix server, perform the following steps:

1. Navigate to the `/etc/opt/opsware/startup` directory.
2. Enter the `./pam-brocade stop` command to run the saved script that stops the Storage Agent.

   When the Storage Agent is stopped, discovery and synchronization processes will not run. See “Synchronizing the Brocade Storage Agent” on page 79.

Synchronizing the Brocade Storage Agent

Synchronization is a request to the Storage Agent to gather the latest data from managed devices and then send this data to the core. Synchronization is performed when the Storage Agent starts and then again at the interval specified in the `pam.properties` file.

Synchronization can occur only when the Storage Agent is running.

If the Storage Agent is stopped or the default schedule does not synchronize the Storage Agent as frequently as you need it to, you must explicitly request a synchronization. For example, you need to explicitly request a synchronization whenever the storage administrator applies changes and needs to immediately see them–instead of waiting for the next scheduled synchronization.

To change the intervals at which the Storage Agent performs synchronization, see "Modifying the Synchronization Schedule" on page 85.

To synchronize a Brocade Storage Agent on a managed server, perform the following steps:

1. In the ASAS Agent window, select a Brocade Storage Agent and then select **Actions ➤ Open** to display the Brocade Storage Agent browser.
2. Select **Actions ➤ Synchronize** to run the synchronization process. When the synchronization request is successfully completed, a confirmation window displays.
3. Click **OK** to close this window.

Checking the Brocade Storage Agent Status

When the Storage Agent starts, it begins the discovery and synchronization process.

To check Storage Agent discovery status, perform the following steps:

1. From the Navigation pane, select **Opsware Administration ➤ ASAS Agents**.
2. In the content pane, check the Last Received Status column to see whether the Storage Agent is OK, Starting, Stopping, or OFFLINE. The Last Scan column displays the date and time the status was captured.
3. (Optional) Select a Storage Agent and then click the "Check current state" link in the Properties pane to display the latest status, such as Running, Available, or Unavailable. The Last Scan column displays the date and time the state was captured.

Storage Agent Settings

Storage Agent settings (properties) manage Storage Agent behavior. After you install and configure the Storage Agent, you can adjust these settings in the `pam.properties` file.

Before modifying the `pam.properties` file, make sure the Storage Agent is not running. See “Stopping the Brocade Storage Agent” on page 78.

You can modify the following values in the `properties` file:

- **Log file size and level**. Conserve disk space by modifying the maximum size for log files and level of detail gathered for log messages.
- **Synchronization and polling**. Tune system performance by adjusting the intervals at which synchronizations run.

Contact Hewlett Packard if you need to modify thread pools.

Controlling Log File Sizes and Logging Levels

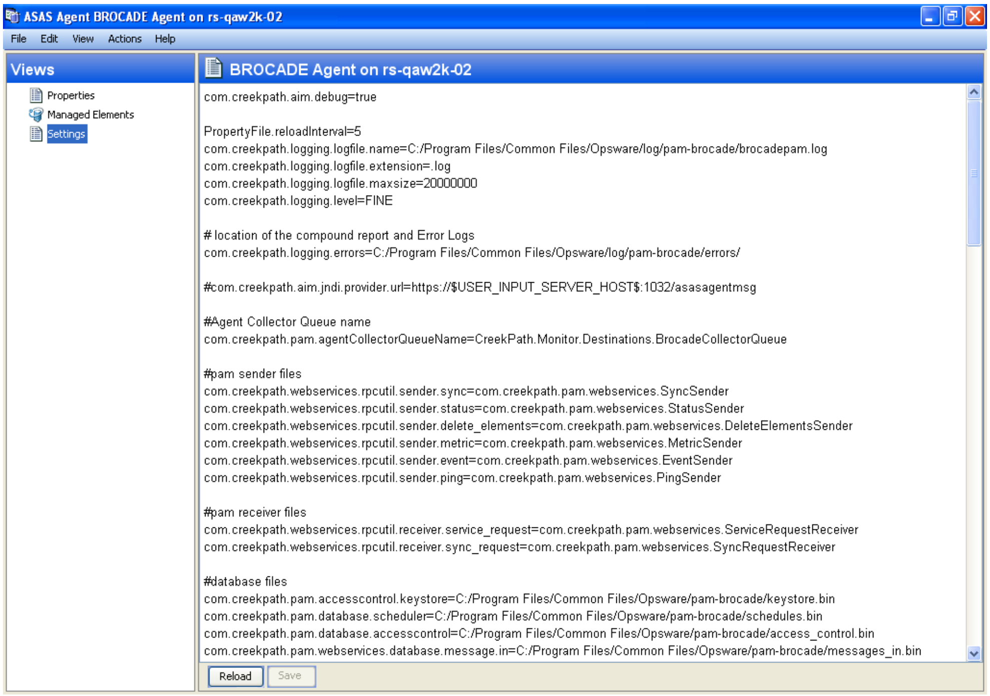
To conserve disk space and control the types of log messages that ASAS gathers, you can adjust the maximum size of log files and the logging level in the log file settings.

To modify the log file settings, perform the following steps:

1. Stop the Storage Agent.
2. In the ASAS Agent window, select a Storage Agent.
3. Select **Actions ➤ Open** to display the Storage Agent browser.
4. From the Views pane, select **Settings** to display the log file settings in the content pane.

5 Change any of the log file settings. For a list of these parameters and their descriptions, see Table 5-3 on page 83.

Figure 5-3: Storage Agent Log File Settings



```
com.creekpath.aim.debug=true

PropertyFile.reloadInterval=5
com.creekpath.logging.logfile.name=C:/Program Files/Common Files/Opsware/log/pam-brocade/brocadepam.log
com.creekpath.logging.logfile.extension=.log
com.creekpath.logging.logfile.maxsize=20000000
com.creekpath.logging.level=FINE

# location of the compound report and Error Logs
com.creekpath.logging.errors=C:/Program Files/Common Files/Opsware/log/pam-brocade/errors/

#com.creekpath.aim.jndi.provider.url=https://$USER_INPUT_SERVER_HOST$:1032/asasagentmsg

#Agent Collector Queue name
com.creekpath.pam.agentCollectorQueueName=CreekPath.Monitor.Destinations.BrocadeCollectorQueue

#pam sender files
com.creekpath.webservices.rpcutil.sender.sync=com.creekpath.pam.webservices.SyncSender
com.creekpath.webservices.rpcutil.sender.status=com.creekpath.pam.webservices.StatusSender
com.creekpath.webservices.rpcutil.sender.delete_elements=com.creekpath.pam.webservices.DeleteElementsSender
com.creekpath.webservices.rpcutil.sender.metric=com.creekpath.pam.webservices.MetricSender
com.creekpath.webservices.rpcutil.sender.event=com.creekpath.pam.webservices.EventSender
com.creekpath.webservices.rpcutil.sender.ping=com.creekpath.pam.webservices.PingSender

#pam receiver files
com.creekpath.webservices.rpcutil.receiver.service_request=com.creekpath.pam.webservices.ServiceRequestReceiver
com.creekpath.webservices.rpcutil.receiver.sync_request=com.creekpath.pam.webservices.SyncRequestReceiver

#database files
com.creekpath.pam.accesscontrol.keystore=C:/Program Files/Common Files/Opsware/pam-brocade/keystore.bin
com.creekpath.pam.database.scheduler=C:/Program Files/Common Files/Opsware/pam-brocade/schedules.bin
com.creekpath.pam.database.accesscontrol=C:/Program Files/Common Files/Opsware/pam-brocade/access_control.bin
com.creekpath.pam.webservices.database.message.in=C:/Program Files/Common Files/Opsware/pam-brocade/messages_in.bin
```

6 Click **Save** to save your settings.

Or

Click **Reload** to restore the settings to their previous values—before you made changes.

Log File Settings

The following table describes the Storage Agent log file settings you can change.

Table 5-3: Log File Settings for Storage Agent

PARAMETER	DESCRIPTION
`logfile.name`	Specifies the directory for all log files and compound reports for errors encountered during synchronization, such as `/var/log/opsware/pam-oracle/oraclepam.log`. This directory is created after ASAS begins gathering logging information. **Note:** If you change the default logging path on a Solaris system and you also created a server group and User ID, you must change the ownership of the new log directory using the `chown` command.
`logfile.extension`	Specifies the extension for log file names.
`logfile.maxsize`	Controls the maximum size of each log file (in bytes). By default, the Storage Agent will populate a log file until it reaches its maximum capacity (20 MB), then it will wrap any remaining log information into a new log file. The Storage Agent can create up to 10 individual log files before it overwrites previous log files.

Table 5-3: Log File Settings for Storage Agent (continued)

PARAMETER	DESCRIPTION
`logging.level`	Controls the type of messages gathered or turns off logging. Each subsequent level also includes the logging information that precedes it, such as INFO includes logging information for SEVERE and WARNING. Enter one of the following values: • OFF: Does not collect logging information. • SEVERE: Collects messages indicating a serious failure. • WARNING: Collects exception messages. • INFO (default): Collects informational messages, such as storage volume creation. • CONFIG: Collects static configuration messages. • FINE: Provides tracing information; used for system debugging. • FINER: Provides fairly detailed tracing information; used for system debugging. • FINEST: Provides highly detailed tracing information; used for system debugging. **Note**: The FINE, FINER, and FINEST settings affect Storage Agent performance and scalability. You should only use these settings if HP Support has instructed you to do so.

Modifying the Synchronization Schedule

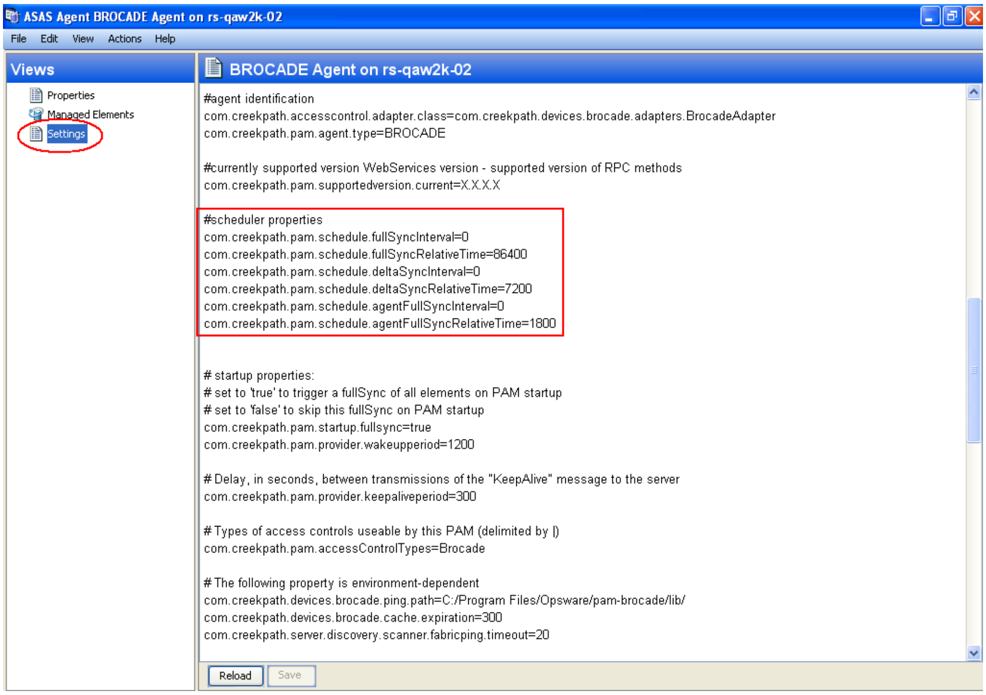
To change the intervals at which the Storage Agent performs synchronization, you can modify the values in the scheduler properties. Synchronization is a process by which the Storage Agent gathers data from the Brocade fabric and then transfers that data to the Domain Data Store, so that the Domain Data Store and Brocade fabric are synchronized.

Synchronization is performed when the Storage Agent starts and then again at the interval specified in the `pam.properties` file. For example, if you initially start the Storage Agent at midnight and the full synchronization is scheduled to run every 12 hours, the full synchronization will always run at noon and at midnight. As needed, you can run immediate synchronization requests. See “Synchronizing the Brocade Storage Agent” on page 79.

To modify synchronization intervals, perform the following steps:

1. Stop the Storage Agent.
2. From the Brocade Storage Agent browser, from the Views pane, select **Settings**.
3. In the content pane, locate the lines for #scheduler properties, as Figure 5-4 illustrates.

Figure 5-4: Storage Agent Schedule Settings


ASAS Agent BROCADE Agent on rs-qaw2k-02
File Edit View Actions Help
Views
Properties
Managed Elements
Settings
BROCADE Agent on rs-qaw2k-02
Reload
Save

```
#agent identification
com.creekpath.accesscontrol.adapter.class=com.creekpath.devices.brocade.adapters.BrocadeAdapter
com.creekpath.pam.agent.type=BROCADE

#currently supported version WebServices version - supported version of RPC methods
com.creekpath.pam.supportedversion.current=X.X.X.X

#scheduler properties
com.creekpath.pam.schedule.fullSyncInterval=0
com.creekpath.pam.schedule.fullSyncRelativeTime=86400
com.creekpath.pam.schedule.deltaSyncInterval=0
com.creekpath.pam.schedule.deltaSyncRelativeTime=7200
com.creekpath.pam.schedule.agentFullSyncInterval=0
com.creekpath.pam.schedule.agentFullSyncRelativeTime=1800


# startup properties:
# set to 'true' to trigger a fullSync of all elements on PAM startup
# set to 'false' to skip this fullSync on PAM startup
com.creekpath.pam.startup.fullsync=true
com.creekpath.pam.provider.wakeupperiod=1200

# Delay, in seconds, between transmissions of the "KeepAlive" message to the server
com.creekpath.pam.provider.keepaliveperiod=300

# Types of access controls useable by this PAM (delimited by |)
com.creekpath.pam.accessControlTypes=Brocade

# The following property is environment-dependent
com.creekpath.devices.brocade.ping.path=C:/Program Files/Opsware/pam-brocade/lib/
com.creekpath.devices.brocade.cache.expiration=300
com.creekpath.server.discovery.scanner.fabricping.timeout=20
```

4. To change the metrics and synchronization schedule, enter new times (in seconds) in the appropriate fields. For a list of these parameters and their descriptions, see Table 5-4 on page 86.

5. If desired, you can change the startup setting so that full synchronizations do not occur when the Storage Agent starts. Locate the following field and change the value from `true` to `false`:

   ```
   com.creekpath.pam.startup.fullsync=false
   ```

6. Click **Save** to save your changes.

   Or

   Click **Reload** to restore the settings to their previous values—before you made changes.

Scheduler Parameter Settings

The following table describes the Storage Agent scheduler parameter settings you can change.

Table 5-4: Scheduler Parameters

PARAMETER	DESCRIPTION
`fullSyncInterval` `fullSyncRelativeTime`	Controls full synchronizations, in which all data is gathered since the last synchronization: **Interval field**: Turns synchronizations on and off. Enter `-1` to turn off synchronizations. Enter `0` to turn on synchronizations. • **RelativeTime field**: Controls the interval at which synchronization occurs (in seconds). To improve scalability of the Manager and Management Server, adjust the Relative Time to a higher value so that synchronizations occur less frequently.

Table 5-4: Scheduler Parameters (continued)

PARAMETER	DESCRIPTION
`deltaSyncInterval` `deltaSyncRelativeTime`	Controls delta synchronizations, in which modified data is gathered since the last synchronization: • **Interval field**: Turns synchronizations on and off. Enter `-1` to turn off synchronizations. Enter `0` to turn on synchronizations. • **RelativeTime field**: Controls the interval at which synchronization occurs (in seconds). To improve scalability of the Manager and Management Server, adjust the Relative Time to a higher value so that synchronizations occur less frequently.

ASAS does not capture events and metrics.

Chapter 6: CLARiiON Storage Agent

IN THIS CHAPTER

This section discusses the following topics:

- Access Controls
- Storage Agent Operation
- Storage Agent Settings

Access Controls

This section describes how to configure the Storage Agent so that it can gather information from the EMC CLARiiON array. To enable this process, you must define an access control for each array the Storage Agent will manage. An access control contains values, such as the array's controller IP address of the vendor host, that allows the CLARiiON Storage Agent to communicate with the array. Table 6-1 describes the access control values you must create before running the CLARiiON Storage Agent for the first time.

Table 6-1: CLARiiON Storage Agent Access Controls

ACCESS CONTROL VALUE	DESCRIPTION
Caption	A name used to uniquely identify each access control entry. (If the Storage Agent will be managing more than one array, you must create more than one access control, each with a unique caption.)
User name	The user name authorized to access Navisphere.
Password	The password authorized to access Navisphere.

Table 6-1: CLARiiON Storage Agent Access Controls (continued)

ACCESS CONTROL VALUE	DESCRIPTION
Controller IP Address	The controller IP address(es) for the storage array. **Note**: You must enter all controller IP addresses for a given array.

Opening the Device Access Control Editor

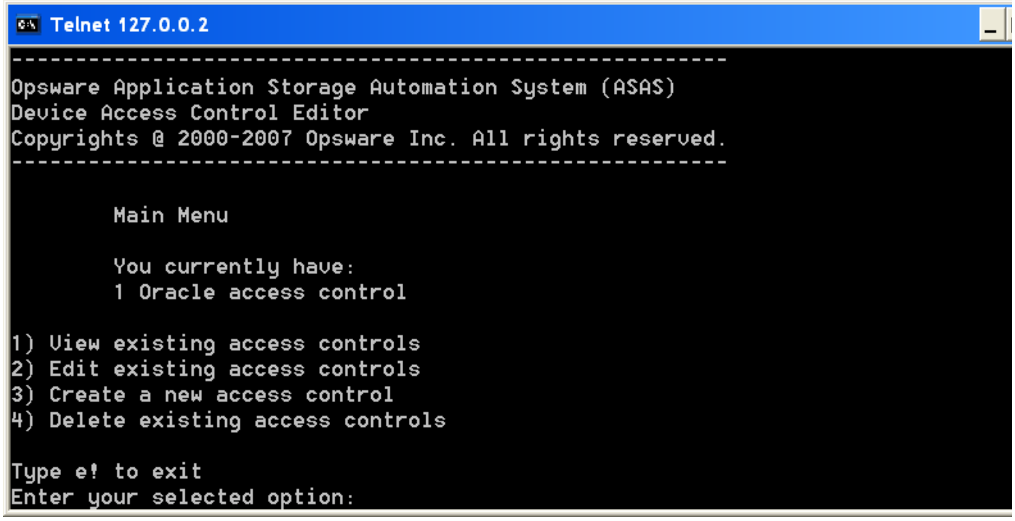
To open the Device Access Control Editor on a certain operating system, perform the following steps:

1. In the ASAS Agents window, select a Storage Agent and then select **Actions ➤ Open**.

2. In the ASAS Agents window for the selected Storage Agent, select **Actions ➤ DeviceAccessControl editor**.

   The command line interface opens similar to the following, displaying the main menu for the Device Access Control Editor.

Figure 6-1: Device Access Control Editor Example



```
--------------------------------------------------------
Opsware Application Storage Automation System (ASAS)
Device Access Control Editor
Copyrights @ 2000-2007 Opsware Inc. All rights reserved.
--------------------------------------------------------

        Main Menu

        You currently have:
        1 Oracle access control

1) View existing access controls
2) Edit existing access controls
3) Create a new access control
4) Delete existing access controls

Type e! to exit
Enter your selected option:
```

3. Navigate through the Device Access Control Editor using the commands described in Table 6-2. All commands are case-sensitive.

Table 6-2: Device Access Control Editor Commands

COMMAND	ACTION
`b!`	Returns to the previous menu.
`c!`	Corrects the values entered for an access control. This command is only available from the Verify Values screen after you have entered all access control values for the Storage Agent.
`d!`	Deletes an existing access control.
`e!`	Exits the command line interface.
`r!`	Returns to the main menu.
`s!`	Saves a set of access control values.
`u!`	Undo an access control value by returning to the previous entry. This command is only available while you are entering access control values.

Configuring Access Controls

To configure access controls for the EMC CLARiiON Storage Agent, perform the following steps:

1. Type `3` to select the `Create a new access control` option and then press Enter.

2. Type the number of the access control type you want to create or edit and then press Enter. For example, if `EMC CLARiiON` is listed as option 1, type `1` and then press Enter.

3. At the `Caption` prompt, type a caption that identifies this access control and then press Enter. To accept the default value, just press Enter.

   If you are creating more than one access control, enter a caption that uniquely identifies each access control entry, such as Clar-1, Clar-2, and so on.

4. At the `User name` prompt, type an admin-level user name and then press Enter. This is the user name that is authorized to access Navisphere.

5. At the `Password` prompt, type the password and then press Enter. This is the password that is authorized to access Navisphere.

6. Re-enter the password and then press Enter.

7. At the IP addresses prompt, type the controller IP address for the EMC CLARiiON system that is managed by the Storage Agent. If applicable, use a comma to separate each address. Press Enter.

   For the Storage Agent to discover all controllers, you must enter an IP address for each controller in the Access Control Editor. If you enter one IP address, the Storage Agent will only discover that controller, even if there is more than one controller for the array.

8. Type `s!` (a lowercase `s`) and then press Enter to save your access control configuration.

   Access controls are saved in the `access_control.bin` file in the following directories, depending on the operating system:

   `c:\Program Files\Common Files\Opsware\pam-clariion\` (Windows)

   Or

   `/var/opt/opsware/pam-clariion` (Unix)

9. If you need to create additional access controls, return to the main menu (`r!`) and repeat step 1 through step 8.

   Or

   Type one of the following options:

   `c!` Correct an access control entry.

   `b!` Go back to the previous menu.

10. After you have entered access control values for all CLARiiON arrays you want to manage, type `e!` (a lowercase `e`) and then press Enter to exit the Access Control Editor.

Editing Access Controls

You can edit access controls while the CLARiiON Storage Agent is running or stopped. If you edit access controls while the Storage Agent is running, changes will be picked during the next synchronization. To edit access controls for the CLARiiON Storage Agent, perform the following steps:

1. Open the main menu for the Access Control Editor.

2. Type 2 to select the `Edit existing access controls` option and then press Enter.

3. Type the number of the access control type you want to edit and then press Enter.

4. Modify each value as desired. If you want to leave an access control value as is, press Enter.

   After you enter the last access control value, a summary is displayed on the screen so that you can verify them.

5. Type `s!` (a lowercase `s`) and then press Enter to save your access control configuration.

   Access controls are saved in the `access_control.bin` file in the following directories, depending on the operating system:

   `c:\Program Files\Common Files\Opsware\pam-clariion\` (Windows)

   Or

   `/var/opt/opsware/pam-clariion` (Unix)

6. If you need to edit additional access controls, return to the main menu (`r!)` and repeat step 2 through step 5.

7. Type `e!`(a lowercase `e`) and press Enter to exit the program.

Deleting Access Controls

You can delete access controls while the CLARiiON Storage Agent is running or stopped. If you delete access controls while the Storage Agent is running, changes will be picked during the next synchronization. To delete access controls for the CLARiiON Storage Agent, perform the following steps:

1. Open the main menu for the Access Control Editor.

2. Type 4 to select the `Delete existing access controls` option and then press Enter.

3. Type the number of the access control type you want to delete and then press Enter.

4. Type the number of the access control that you want to delete and then press Enter.

5. Type `d!` (a lowercase `d`) and then press Enter to delete the access control.

   The Access Control Editor confirms the deletion.

6 Type `e!` (a lowercase `e`) and then press Enter to exit access control configuration.

Storage Agent Operation

This section describes how to authorize, start, stop, synchronize, and check the discovery status of a CLARiiON Storage Agent.

Authorizing the CLARiiON Storage Agent

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 CLARiiON Storage Agent is deployed. When a Storage Agent is initially deployed to a managed server, you must authorize it so that messages from the Storage Agent will be accepted by the core server. As a result of the authorization process, a security token is generated and given to the Storage Agent.

If you are not sure whether the security token in the core and on the managed server match, you can authorize the CLARiiON Storage Agent repeatedly. A security token mismatch can occur as a result of unintentional editing or removal of tokens.

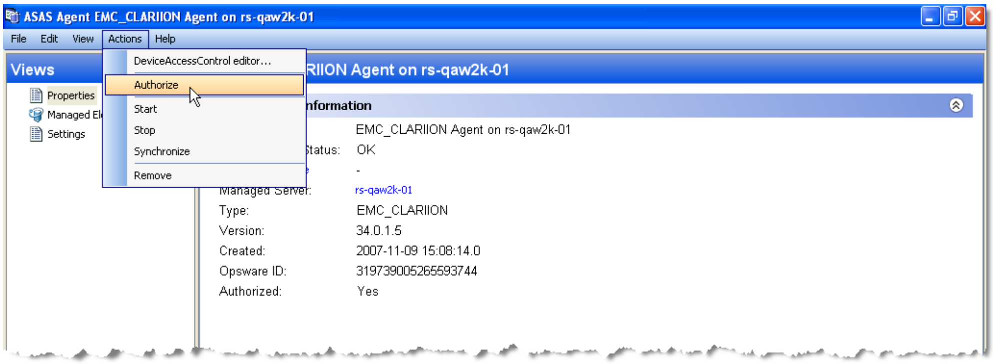
To authorize a CLARiiON Storage Agent, perform the following steps:

1 From the Navigation pane, select **Opsware Administration ➤ ASAS Agents**.

2 Open the CLARiiON Storage Agent that needs to be authorized.

3 From the **Actions** menu, select **Authorize**.

Figure 6-2: Authorize Action for a CLARiiON Storage Agent



EMC_CLARIION Agent on rs-qaw2k-01

tatus: OK

-

Managed Server: rs-qaw2k-01

Type: EMC_CLARIION

Version: 34.0.1.5

Created: 2007-11-09 15:08:14.0

Opsware ID: 319739005265593744

Authorized: Yes

Starting the CLARiiON Storage Agent

When the CLARiiON Storage Agent starts for the first time, the agent begins discovering and synchronizing device data. During this process, the CLARiiON Storage Agent gathers information from various Oracle elements and reports that information to the Web Services Data Access Engine so that the device data for the CLARiiON arrays is synchronized. Depending on the size of the CLARiiON arrays, device synchronization could require several hours. You can start the Storage Agent by using the ASAS Client on a managed server or by running a saved script on a remote managed server.

For performance reasons, you should start the CLARiiON Storage Agent during off-peak hours.

To start a CLARiiON Storage Agent on a managed server by using the ASAS Client, perform the following steps:

1. From the Navigation pane, select **Opsware Administration ➤ ASAS Agents**.
2. In the ASAS Agent window, select a CLARiiON Storage Agent and then select **Actions ➤ Open** to display the CLARiiON Storage Agent browser.
3. Select **Actions ➤ Start**.
4. In the Management Information section click “Check current state” link to verify that the Storage Agent is running.

Starting the CLARiiON Storage Agent on a Remote Windows Server

To start a CLARiiON Storage Agent 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 OpswareCLARiiONStorageAgent and then select **Action ➤ Start.**

Starting the CLARiiON Storage Agent on a Remote Unix Server

To start a CLARiiON Storage Agent on a remote Unix server, perform the following steps:

1. Navigate to the `/etc/opt/opsware/startup` directory.
2. Enter the `./pam-clariion start` command to run the saved script that starts the Storage Agent.

When the Storage Agent starts, it begins the discovery and synchronization process. To monitor the discovery process, see “Checking the CLARiiON Storage Agent Status” on page 97.

Stopping the CLARiiON Storage Agent

You must stop the CLARiiON Storage Agent before you modify Storage Agent settings. See “Storage Agent Settings” on page 98.

To stop a CLARiiON Storage Agent on a managed server by using the ASAS Client, perform the following steps:

1. From the Navigation pane, select **Opsware Administration ➤ ASAS Agents**.
2. In the ASAS Agent window, select a CLARiiON Storage Agent and then select **Actions ➤ Open** to display the CLARiiON Storage Agent browser.
3. Select **Actions ➤ Stop**.
4. In the Management Information section click the “Check current state” link to verify that the Storage Agent is Unavailable.

Stopping the CLARiiON Storage Agent on a Remote Windows Server

To stop an CLARiiON Storage Agent 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 OpswareCLARiiONStorageAgent and then select **Action ➤ Stop**.

Stopping the CLARiiON Storage Agent on a Remote Unix Server

To stop a CLARiiON Storage Agent on a remote Unix managed server, perform the following steps:

1. Navigate to the `/etc/opt/opsware/startup` directory.
2. Enter the `./pam-clariion stop` command to run the saved script that stops the Storage Agent.

When the Storage Agent is stopped, discovery and synchronization processes will not run. See “Synchronizing the CLARiiON Storage Agent” on page 97.

Synchronizing the CLARiiON Storage Agent

Synchronization is a request to the Storage Agent to gather the latest data from managed devices and then send this data to the core. Synchronization is performed when the Storage Agent starts and then again at the interval specified in the `pam.properties` file.

Synchronization can occur only when the Storage Agent is running.

If the Storage Agent is stopped or the default schedule does not synchronize the Storage Agent as frequently as you need it to, you must explicitly request a synchronization. For example, you need to explicitly request a synchronization whenever the storage administrator applies changes and needs to immediately see them—instead of waiting for the next scheduled synchronization.

To change the intervals at which the Storage Agent performs synchronization, see “Modifying the Synchronization Schedule” on page 103.

To synchronize a CLARiiON Storage Agent on a managed server, perform the following steps:

1. From the Navigation pane, select **Opsware Administration ➤ ASAS Agents**.
2. In the ASAS Agent window, select a CLARiiON Storage Agent and then select **Actions ➤ Open** to display the CLARiiON Storage Agent browser.
3. Select **Actions ➤ Synchronize** to run the synchronization process. When the synchronization request is successfully completed, a confirmation window displays.
4. Click **OK** to close this window.

Checking the CLARiiON Storage Agent Status

When the Storage Agent starts, it begins the discovery and synchronization process.

To check Storage Agent discovery status, perform the following steps:

1. From the Navigation pane, select **Opsware Administration ➤ ASAS Agents**.
2. In the content pane, check the Last Received Status column for the status of the tree structure in the left panel.

3. Select the EMC_CLARIION Storage Agent and make sure the Properties tab is selected in the right display panel. The Last Received Status indicates the state of the array, such as OK or offline.

Modifying the Navisphere CLI Path

The `pam.properties` file includes a setting that instructs the Storage Agent where to locate the EMC Navisphere CLI. If you upgrade your version of Navisphere or if you install Navisphere to a directory other than the default, you need to verify the path to the CLI in the `pam.properties` file and update the path as necessary.

To modify the Navisphere CLI path, perform the following steps:

1. Make sure the Storage Agent is not running. See “Stopping the CLARiiON Storage Agent” on page 96.

   In a text editor, open the `pam.properties` file in the following directories, depending on the operating system:

   `c:\Program Files\Common Files\Opsware\etc\pam-clariion` (Windows)

   Or

   `/etc/opt/opsware/etc/pam-clariion` (Unix)

2. Locate the following field and enter a new path for the CLI:
   `com.creekpath.pam.clariion.cli_path=`
3. Save the `pam.properties` file.

Storage Agent Settings

Storage Agent settings (properties) manage Storage Agent behavior. After you install and configure the Storage Agent, you can adjust these settings in the `pam.properties` file.

✔ Before modifying the `pam.properties` file, make sure the Storage Agent is not running. See “Stopping the CLARiiON Storage Agent” on page 96.

You can modify the following values in the `properties` file:

- **Log file size and level**. Conserve disk space by modifying the maximum size for log files and level of detail gathered for log messages.
- **Synchronization and polling**. Tune system performance by adjusting the intervals at which synchronizations run.

Contact Hewlett Packard if you need to modify thread pools.

Controlling Log File Sizes and Logging Levels

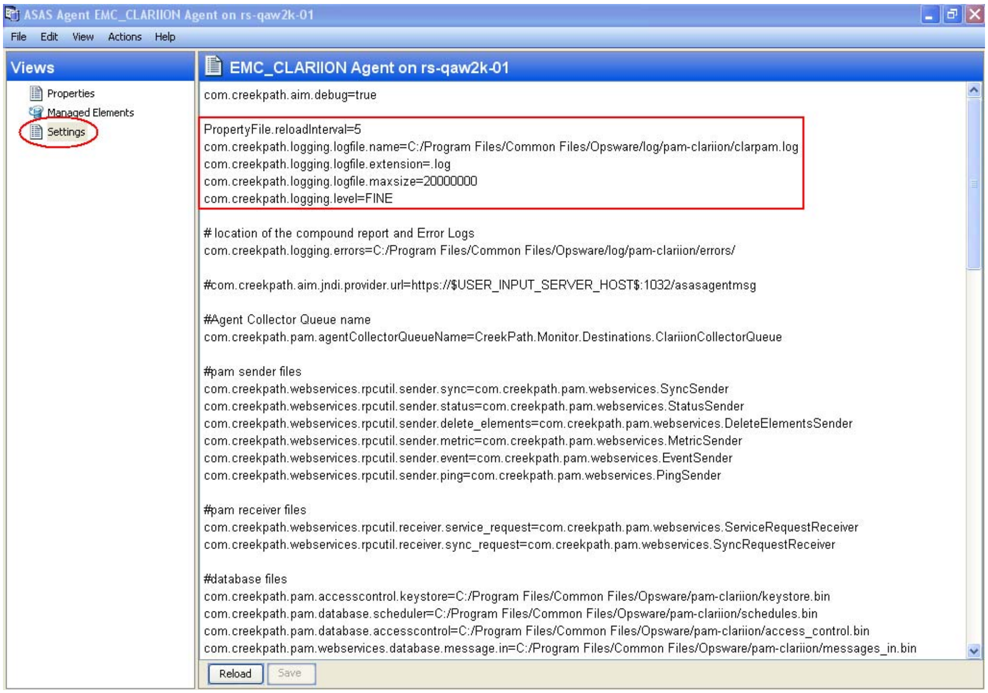
To conserve disk space and control the types of log messages that ASAS gathers, you can adjust the maximum size of log files and the logging level in the log file settings.

To modify the log file settings, perform the following steps:

1. Stop the Storage Agent.
2. In the ASAS Agent window, select a Storage Agent.
3. Select **Actions** ➤ **Open** to display the Storage Agent browser.
4. From the Views pane, select Settings to display the log file settings in the content pane.

5 Change any of the log file settings. For a list of these parameters and their descriptions, see Table 6-3 on page 101.

Figure 6-3: Storage Agent Log File Settings


ASAS Agent EMC_CLARIION Agent on rs-qaw2k-01
File
Edit
View
Actions
Help
Views
Properties
Managed Elements
Settings
EMC_CLARIION Agent on rs-qaw2k-01
Reload
Save

```
com.creekpath.aim.debug=true

PropertyFile.reloadInterval=5
com.creekpath.logging.logfile.name=C:/Program Files/Common Files/Opsware/log/pam-clariion/clarpam.log
com.creekpath.logging.logfile.extension=.log
com.creekpath.logging.logfile.maxsize=20000000
com.creekpath.logging.level=FINE

# location of the compound report and Error Logs
com.creekpath.logging.errors=C:/Program Files/Common Files/Opsware/log/pam-clariion/errors/

#com.creekpath.aim.jndi.provider.url=https://$USER_INPUT_SERVER_HOST$:1032/asasagentmsg

#Agent Collector Queue name
com.creekpath.pam.agentCollectorQueueName=CreekPath.Monitor.Destinations.ClariionCollectorQueue

#pam sender files
com.creekpath.webservices.rpcutil.sender.sync=com.creekpath.pam.webservices.SyncSender
com.creekpath.webservices.rpcutil.sender.status=com.creekpath.pam.webservices.StatusSender
com.creekpath.webservices.rpcutil.sender.delete_elements=com.creekpath.pam.webservices.DeleteElementsSender
com.creekpath.webservices.rpcutil.sender.metric=com.creekpath.pam.webservices.MetricSender
com.creekpath.webservices.rpcutil.sender.event=com.creekpath.pam.webservices.EventSender
com.creekpath.webservices.rpcutil.sender.ping=com.creekpath.pam.webservices.PingSender

#pam receiver files
com.creekpath.webservices.rpcutil.receiver.service_request=com.creekpath.pam.webservices.ServiceRequestReceiver
com.creekpath.webservices.rpcutil.receiver.sync_request=com.creekpath.pam.webservices.SyncRequestReceiver

#database files
com.creekpath.pam.accesscontrol.keystore=C:/Program Files/Common Files/Opsware/pam-clariion/keystore.bin
com.creekpath.pam.database.scheduler=C:/Program Files/Common Files/Opsware/pam-clariion/schedules.bin
com.creekpath.pam.database.accesscontrol=C:/Program Files/Common Files/Opsware/pam-clariion/access_control.bin
com.creekpath.pam.webservices.database.message.in=C:/Program Files/Common Files/Opsware/pam-clariion/messages_in.bin
```

6 Click **Save** to save your settings.

Or

Click **Reload** to restore the settings to their previous values—before you made changes.

7 Start the Storage Agent.

Log File Settings

The following table describes the Storage Agent log file settings you can change.

Table 6-3: Log File Settings for Storage Agent

PARAMETER	DESCRIPTION
`logfile.name`	Specifies the directory for all log files and compound reports for errors encountered during synchronization, such as `/var/log/opsware/pam-clariion/clariionpam.log`. This directory is created after ASAS begins gathering logging information. **Note:** If you change the default logging path on a Solaris system and you also created a server group and User ID, you must change the ownership of the new log directory using the `chown` command.
`logfile.extension`	Specifies the extension for log file names.
`logfile.maxsize`	Controls the maximum size of each log file (in bytes). By default, the Storage Agent will populate a log file until it reaches its maximum capacity (20 MB), then it will wrap any remaining log information into a new log file. The Storage Agent can create up to 10 individual log files before it overwrites previous log files.

Table 6-3: Log File Settings for Storage Agent (continued)

PARAMETER	DESCRIPTION
`logging.level`	Controls the type of messages gathered or turns off logging. Each subsequent level also includes the logging information that precedes it, such as INFO includes logging information for SEVERE and WARNING. Enter one of the following values: • OFF: Does not collect logging information. • SEVERE: Collects messages indicating a serious failure. • WARNING: Collects exception messages. • INFO (default): Collects informational messages, such as storage volume creation. • CONFIG: Collects static configuration messages. • FINE: Provides tracing information; used for system debugging. • FINER: Provides fairly detailed tracing information; used for system debugging. • FINEST: Provides highly detailed tracing information; used for system debugging. **Note**: The FINE, FINER, and FINEST settings affect Storage Agent performance and scalability. You should only use these settings if HP Support has instructed you to do so.

Modifying the Synchronization Schedule

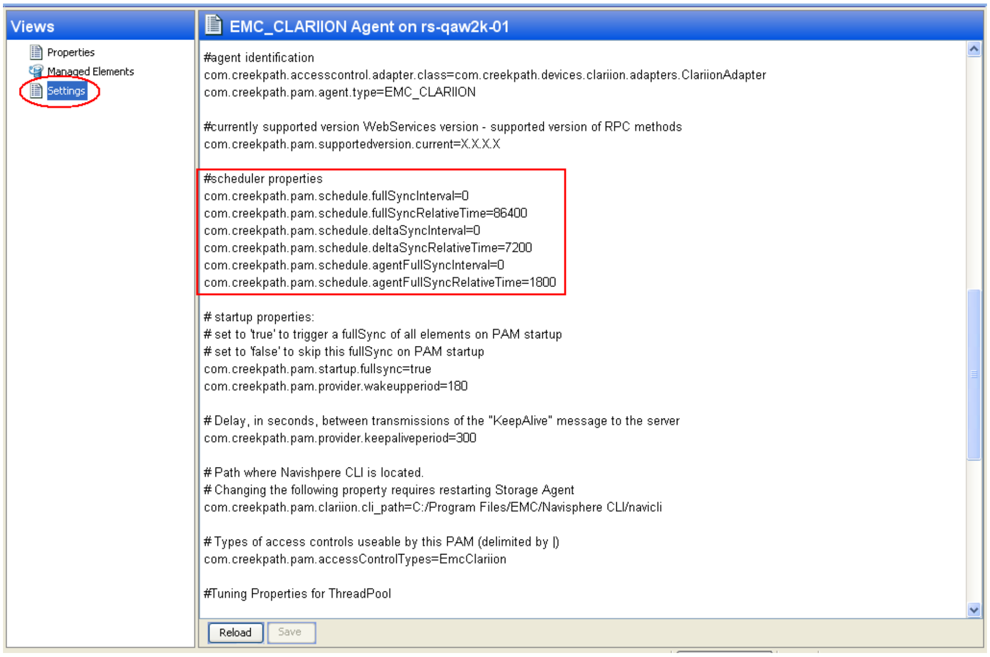
To change the intervals at which the Storage Agent performs synchronization, you can modify the values in the scheduler properties. Synchronization is a process by which the Storage Agent gathers data from the CLARiiON arrays and then transfers that data to the Domain Data Store, so that the Domain Data Store and CLARiiON arrays are synchronized.

Synchronization is performed when the Storage Agent starts and then again at the interval specified in the `pam.properties` file. For example, if you initially start the Storage Agent at midnight and the full synchronization is scheduled to run every 12 hours, the full synchronization will always run at noon and at midnight. As needed, you can run immediate synchronization requests. See “Synchronizing the CLARiiON Storage Agent” on page 97.

To modify synchronization intervals, perform the following steps:

1. Stop the Storage Agent.
2. From the CLARiiON Storage Agent browser, from the Views pane, select **Settings**.
3. In the content pane, locate the lines for #scheduler properties, as Figure 6-4 illustrates.

Figure 6-4: Storage Agent Schedule Settings



```
#agent identification
com.creekpath.accesscontrol.adapter.class=com.creekpath.devices.clariion.adapters.ClariionAdapter
com.creekpath.pam.agent.type=EMC_CLARIION

#currently supported version WebServices version - supported version of RPC methods
com.creekpath.pam.supportedversion.current=X.X.X.X

#scheduler properties
com.creekpath.pam.schedule.fullSyncInterval=0
com.creekpath.pam.schedule.fullSyncRelativeTime=86400
com.creekpath.pam.schedule.deltaSyncInterval=0
com.creekpath.pam.schedule.deltaSyncRelativeTime=7200
com.creekpath.pam.schedule.agentFullSyncInterval=0
com.creekpath.pam.schedule.agentFullSyncRelativeTime=1800

# startup properties:
# set to 'true' to trigger a fullSync of all elements on PAM startup
# set to 'false' to skip this fullSync on PAM startup
com.creekpath.pam.startup.fullsync=true
com.creekpath.pam.provider.wakeupperiod=180

# Delay, in seconds, between transmissions of the "KeepAlive" message to the server
com.creekpath.pam.provider.keepaliveperiod=300

# Path where Navishpere CLI is located.
# Changing the following property requires restarting Storage Agent
com.creekpath.pam.clariion.cli_path=C:/Program Files/EMC/Navisphere CLI/navicli

# Types of access controls useable by this PAM (delimited by |)
com.creekpath.pam.accessControlTypes=EmcClariion

#Tuning Properties for ThreadPool
```

4. To change the metrics and synchronization schedule, enter new times (in seconds) in the appropriate fields. For a list of these parameters and their descriptions, see Table 6-4 on page 104.

5. If desired, you can change the startup setting so that full synchronizations do not occur when the Storage Agent starts. Locate the following field and change the value from `true` to `false`:

   ```
   com.creekpath.pam.startup.fullsync=false
   ```

6. Click **Save** to save your changes.

   Or

   Click **Reload** to restore the settings to their previous values—before you made changes.

7. Start the Storage Agent.

Scheduler Parameter Settings

The following table describes the Storage Agent scheduler parameter settings you can change.

Table 6-4: Scheduler Parameters

PARAMETER	DESCRIPTION
`fullSyncInterval` `fullSyncRelativeTime`	Controls full synchronizations, in which all data is gathered since the last synchronization: **Interval field**: Turns synchronizations on and off. Enter `-1` to turn off synchronizations. Enter `0` to turn on synchronizations. • **RelativeTime field**: Controls the interval at which synchronization occurs (in seconds). To improve scalability of the Manager and Management Server, adjust the Relative Time to a higher value so that synchronizations occur less frequently.

Table 6-4: Scheduler Parameters (continued)

PARAMETER	DESCRIPTION
`deltaSyncInterval` `deltaSyncRelativeTime`	Controls delta synchronizations, in which modified data is gathered since the last synchronization: • **Interval field**: Turns synchronizations on and off. Enter `-1` to turn off synchronizations. Enter `0` to turn on synchronizations. • **RelativeTime field**: Controls the interval at which synchronization occurs (in seconds). To improve scalability of the Manager and Management Server, adjust the Relative Time to a higher value so that synchronizations occur less frequently.

ASAS does not capture events and metrics.

Chapter 7: HiCommand Storage Agent

IN THIS CHAPTER

This section discusses the following topics:

- Access Controls
- HiCommand Management Console
- Storage Agent Operation
- Storage Agent Settings

Access Controls

This section describes how to configure access controls so that the Storage Agent can gather information from the arrays managed by the HiCommand software. To enable this process, you must define an access control for each HiCommand server the Storage Agent will manage. An access control contains values, such as a server address, that allow the Storage Agent to communicate with the HiCommand software. Table 7-1 describes the access control values you must create before running the HiCommand Storage Agent for the first time.

Table 7-1: HiCommand Storage Agent Access Controls

ACCESS CONTROL VALUE	DESCRIPTION
Caption	A name used to uniquely identify each access control entry. (If the Storage Agent is managing more than one HiCommand server, you must create more than one access control, each with a unique caption.) **Note**: After this access control is created, you cannot change the caption.
Host Address	An IP address or a DNS host name of the HiCommand server.

Table 7-1: HiCommand Storage Agent Access Controls (continued)

ACCESS CONTROL VALUE	DESCRIPTION
User Name	The user name needed to access the HiCommand server.
Password	The password needed to access the HiCommand server.
HiCommand Port	The port on the server used for communicating with the HiCommand server.
Excluded Array Serial Numbers	Optional. A comma-separated list of serial numbers for arrays that you want to exclude from being discovered by ASAS.

HiCommand Management Console

This section describes how to use the HiCommand Management Console to enable the Storage Agent to communicate with and gather data from HiCommand servers. You can establish communication links by creating access controls for each HiCommand server. The Management Console is installed with the HiCommand Storage Agent.

After you configure the access controls in the Management Console, ASAS begins discovering HiCommand servers and synchronizing device data. During this process, the Storage Agent gathers information from various HiCommand servers and reports that information to the Web Service Data Access Engine, so that ASAS and the device data for the HiCommand servers are synchronized.

Depending on the number of HiCommand servers the Storage Agent is controlling, device synchronization may require several hours. For performance reasons, you should start the HiCommand Storage Agent during off-peak hours.

Opening the Management Console

To open the Management Console for a HiCommand Storage Agent, perform the following steps:

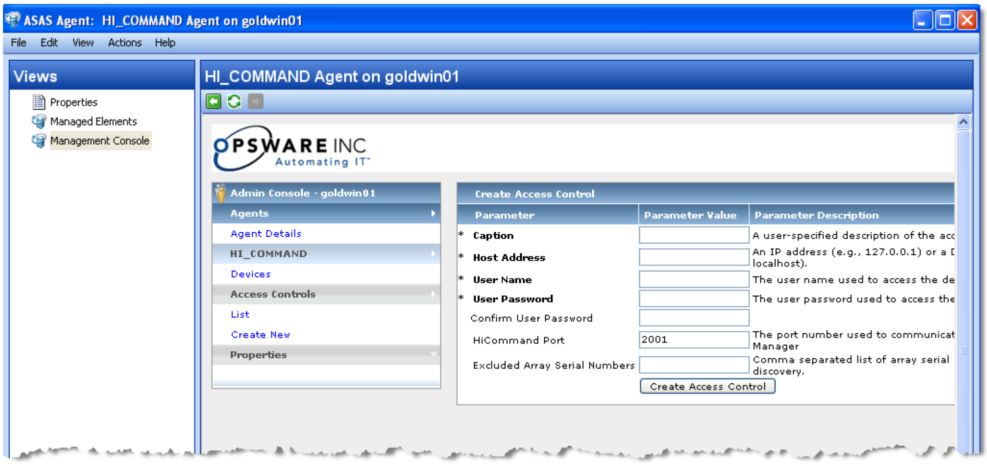
1. From the Navigation pane, select **Opsware Administration ➤ ASAS Agents**.

2 In the content pane, open a HiCommand Storage Agent to display the Agent Browser.

3 In the Last Received Status field, verify that the Storage Agent is OK.

4 In the Views pane, select **Management Console** to open the Management Console for the selected HiCommand Storage Agent.

Figure 7-1: HiCommand Management Console



	Parameter	Parameter Value	Parameter Description
*	**Caption**		A user-specified description of the acc
*	**Host Address**		An IP address (e.g., 127.0.0.1) or a D localhost).
*	**User Name**		The user name used to access the de
*	**User Password**		The user password used to access the
	Confirm User Password		
	HiCommand Port	2001	The port number used to communicat Manager
	Excluded Array Serial Numbers		Comma separated list of array serial discovery.

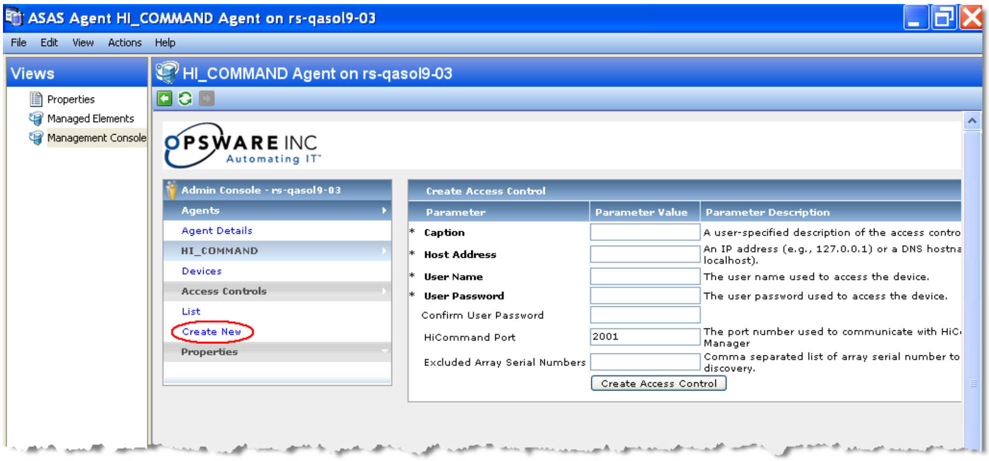
Creating an Access Control

To create an access control for a HiCommand Storage Agent, perform the following steps:

1 In the Admin Console, click the Access Control down arrow to expand the actions.

2 **Select Create New** to display the Create Access Control editor.

Figure 7-2: Create Access Control Editor in the Management Console.



	Parameter	Parameter Value	Parameter Description
*	**Caption**		A user-specified description of the access contro
*	**Host Address**		An IP address (e.g., 127.0.0.1) or a DNS hostna localhost).
*	**User Name**		The user name used to access the device.
*	**User Password**		The user password used to access the device.
	Confirm User Password		
	HiCommand Port	2001	The port number used to communicate with HiC Manager
	Excluded Array Serial Numbers		Comma separated list of array serial number to discovery.

3. Enter the access controls, as described in Table 7-1 on page 107.

4. After you have entered the access controls, click **Create Access Control** to save your changes. The new access controls are listed in the Admin Console.

5. (Optional) Select List in the Admin Console to review all access controls.

6. If there is another HiCommand server running in the network, repeat step 1 through step 5 to create another access control.

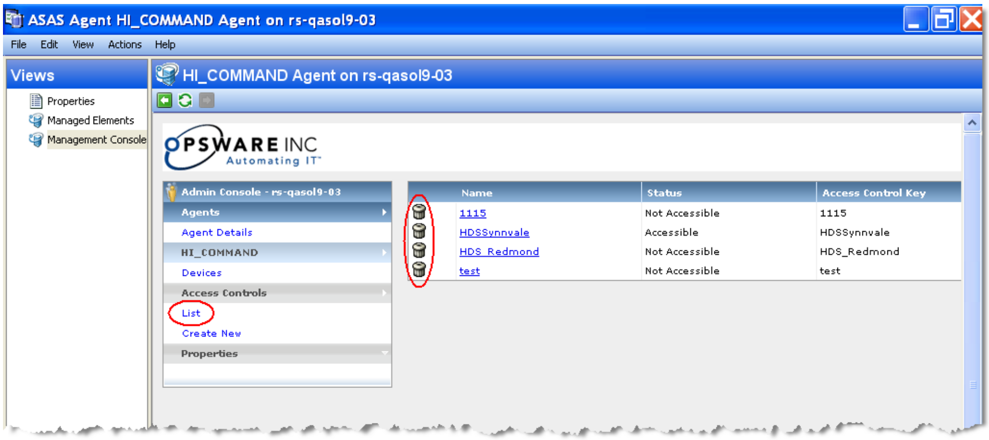
Deleting an Access Control

You can delete access controls while the HiCommand Storage Agent is running or stopped. If you edit access controls while the Storage Agent is running, changes are picked up during the next synchronization. To delete access controls for the HiCommand Storage Agent, perform the following steps:

1. In the Admin Console, click the Access Control down arrow to expand the actions.

2. Select List to display a list of access controls for the HiCommand Storage Agent.

Figure 7-3: Access Control List in the Management Console.



	Name	Status	Access Control Key
🗑	1115	Not Accessible	1115
🗑	HDSSynnvale	Accessible	HDSSynnvale
🗑	HDS_Redmond	Not Accessible	HDS_Redmond
🗑	test	Not Accessible	test

3. Click the trash can icon next to the access control you want to delete.

Storage Agent Operation

This section describes how to authorize, start, stop, synchronize, and check the discovery status of a HiCommand Storage Agent.

Authorizing the HiCommand Storage Agent

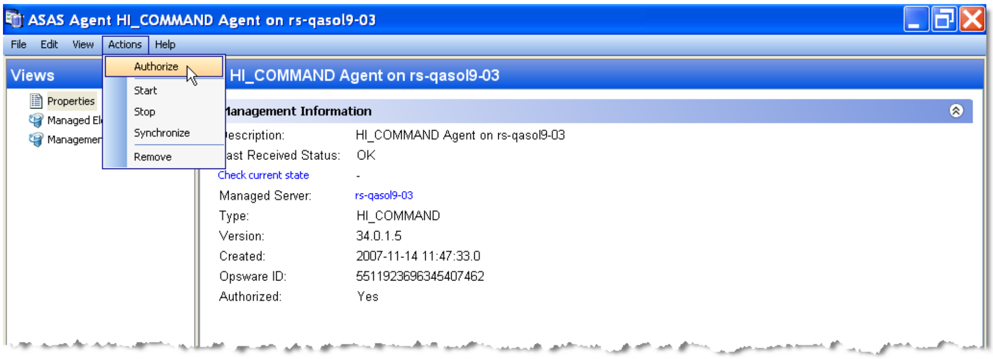
The purpose of authorization is to provide a matching pair of security tokens–one token in the core and the other token on the managed server where the HiCommand Storage Agent is deployed. When a Storage Agent is initially deployed to a managed server, you must authorize it so that messages from the Storage Agent will be accepted by the core server. As a result of the authorization process, a security token is generated and given to the Storage Agent.

If you are not sure whether the security token in the core and on the managed server match, you can authorize the HiCommand Storage Agent repeatedly. A security token mismatch can occur as a result of unintentional editing or removal of tokens.

To authorize a HiCommand Storage Agent, perform the following steps:

1. From the Navigation pane, select **Opsware Administration ➤ ASAS Agents**.
2. Open the HiCommand Storage Agent that needs to be authorized.
3. From the **Actions** menu, select **Authorize**.

Figure 7-4: Authorize Action for a HiCommand Storage Agent



escription: HI_COMMAND Agent on rs-qasol9-03
ast Received Status: OK
Check current state -
Managed Server: rs-qasol9-03
Type: HI_COMMAND
Version: 34.0.1.5
Created: 2007-11-14 11:47:33.0
Opsware ID: 5511923696345407462
Authorized: Yes

Starting the HiCommand Storage Agent

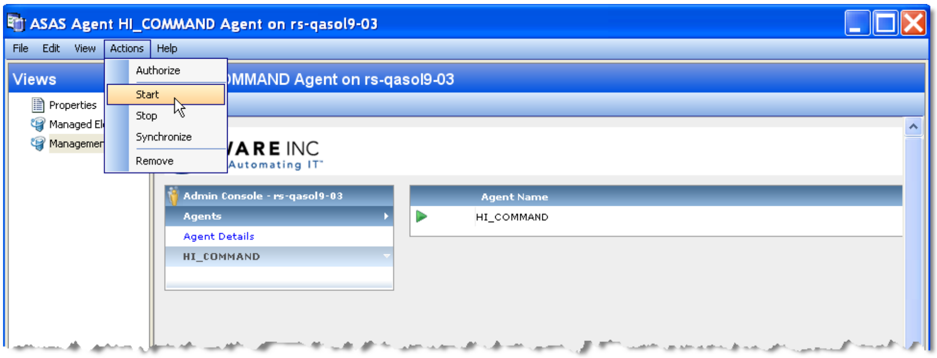
When the HiCommand Storage Agent starts for the first time, the agent begins discovering and synchronizing device data. During this process, the HiCommand Storage Agent gathers information from various device elements and reports that information to the Web Services Data Access Engine so that the device data for the HiCommand servers is synchronized. Depending on the size of the HiCommand servers, device synchronization could require several hours. You can start the Storage Agent by using the ASAS Client on a managed server or by running a saved script on a remote managed server.

For performance reasons, you should start the HiCommand Storage Agent during off-peak hours.

To start a HiCommand Storage Agent on a managed server by using the Management Console, perform the following steps:

1. In the Admin Console, select **Agent Details**.
2. From the Actions menu, select **Start**. The Storage Agent runs as a service in the operating system's background.

Figure 7-5: Starting the Storage Agent



Stopping the HiCommand Storage Agent

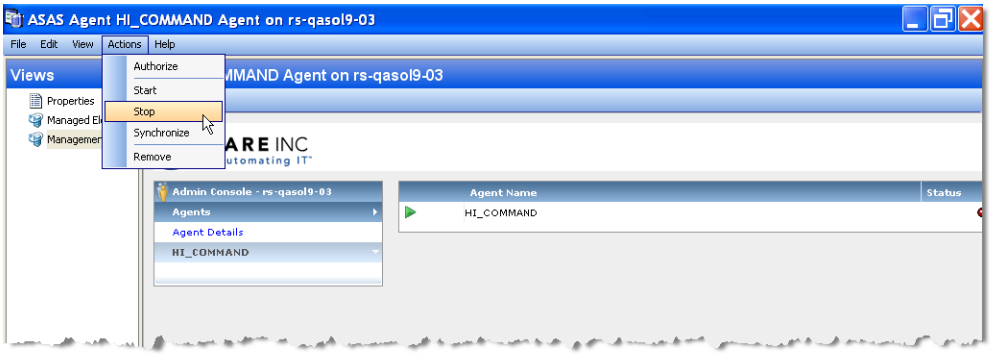
You must stop the HiCommand Storage Agent before you modify Storage Agent settings. See "Storage Agent Settings" on page 114.

After the Storage Agent is stopped or undeployed, the status does not change. For more information, see "Undeploying a Storage Agent from a Managed Server" on page 42 and "Checking the HiCommand Storage Agent Status" on page 114.

To stop a HiCommand Storage Agent on a managed server by using the Management Console, perform the following steps:

1. In the Admin Console, select Agent Details.
2. From the Actions menu, select **Stop**.

Figure 7-6: Stopping the Storage Agent



Synchronizing the HiCommand Storage Agent

Synchronization is a request to the Storage Agent to gather the latest data from managed devices and then send this data to the core. Synchronization is performed when the Storage Agent starts. You can monitor the status of this process in the Storage Management Console or the Central Admin Console.

Synchronization can occur only when the Storage Agent is running.

If the Storage Agent is stopped or the default schedule does not synchronize the Storage Agent as frequently as you need it to, you can explicitly request a synchronization. For example, you will need to explicitly request a synchronization whenever the storage administrator applies changes and needs to immediately see them—instead of waiting for the next scheduled synchronization.

To change the intervals at which the Storage Agent performs synchronization, see “Modifying the Synchronization Schedule” on page 116.

To synchronize a HiCommand Storage Agent on a managed server, perform the following steps:

1. In the ASAS Agent window, select a HiCommand Storage Agent and then select **Actions ➤ Open** to display the HiCommand Storage Agent browser.
2. Select **Actions ➤ Synchronize** to run the synchronization process. When the synchronization request is successfully completed, a confirmation window displays.
3. Click **OK** to close this window.

Checking the HiCommand Storage Agent Status

When the Storage Agent starts, it begins the discovery and synchronization process.

To check Storage Agent discovery status, perform the following steps:

1. From the Navigation pane, select **Opsware Administration ➤ ASAS Agents**.
2. In the content pane, check the Last Received Status column to see whether the Storage Agent is OK, Starting, Stopping, or OFFLINE. The Last Scan column displays the date and time the status was captured.
3. (Optional) Select a Storage Agent and then click the “Check current state” link in the Properties pane to display the latest status, such as Running, Available, or Unavailable. The Last Scan column displays the date and time the state was captured.

Storage Agent Settings

Storage Agent settings (properties) manage Storage Agent behavior. After you install and configure the Storage Agent, you can adjust these settings in the `pam.properties` file.

Before modifying the `pam.properties` file, make sure the Storage Agent is not running. See “Stopping the HiCommand Storage Agent” on page 112.

You can modify the following values in the `properties` file:

- **Log file size and level**. Conserve disk space by modifying the maximum size for log files and level of detail gathered for log messages.
- **Synchronization and polling**. Tune system performance by adjusting the intervals at which synchronizations run.

Contact Hewlett Packard if you need to modify thread pools.

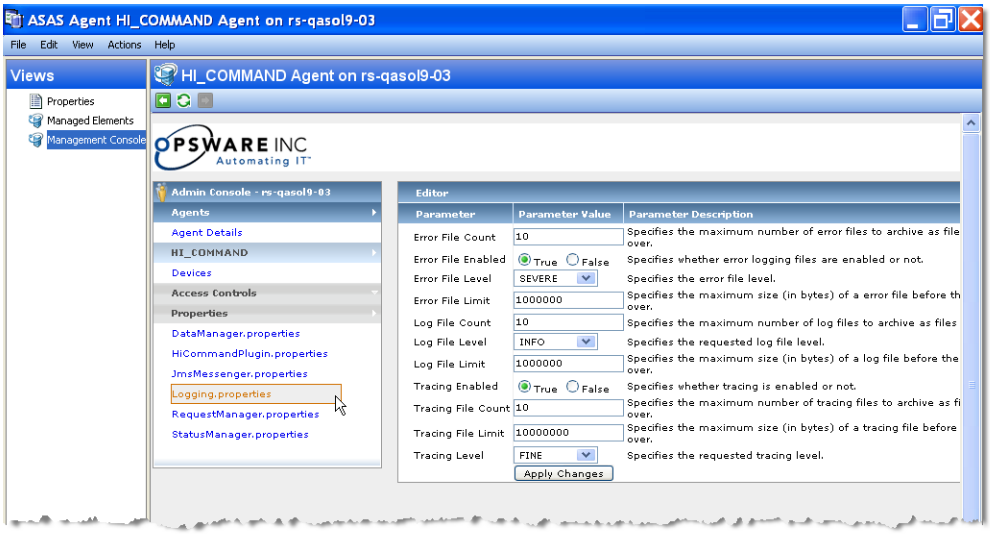
Controlling Log File Sizes and Logging Levels

To conserve disk space and control the types of log messages that ASAS gathers, you can adjust the maximum size of log files and the logging level in the log file settings.

To modify the log file settings, perform the following steps:

1. Stop the Storage Agent.
2. From the HiCommand Storage Agent browser, from the Views pane, select Management Console.
3. In the Admin Console, select Properties and then select Logging.properties to display the logging parameters for error files, log files, and tracing files. For descriptions of the logging levels, see Table 7-2 on page 116.

Figure 7-7: Storage Agent Log File Settings



Parameter	Parameter Value	Parameter Description
Error File Count	10	Specifies the maximum number of error files to archive as file over.
Error File Enabled	● True ○ False	Specifies whether error logging files are enabled or not.
Error File Level	SEVERE	Specifies the error file level.
Error File Limit	1000000	Specifies the maximum size (in bytes) of a error file before th over.
Log File Count	10	Specifies the maximum number of log files to archive as files
Log File Level	INFO	Specifies the requested log file level.
Log File Limit	1000000	Specifies the maximum size (in bytes) of a log file before the over.
Tracing Enabled	● True ○ False	Specifies whether tracing is enabled or not.
Tracing File Count	10	Specifies the maximum number of tracing files to archive as fi over.
Tracing File Limit	10000000	Specifies the maximum size (in bytes) of a tracing file before over.
Tracing Level	FINE	Specifies the requested tracing level.

4. After you make changes, click **Apply Changes.**

Logging Levels

You can also specify logging levels (the types of messages gathered), as described in Table 7-2 on page 116.

Each subsequent level includes the logging information that precedes it. For example, INFO includes logging information for SEVERE and WARNING.

Table 7-2: Logging Levels for a HiCommand Storage Agent

LEVEL	DESCRIPTION
SEVERE	Collects messages indicating a serious failure.
WARNING	Collects exception messages.
INFO	Collects informational messages, such as storage volume creation. This is the default Error File Level.
CONFIG	Collects static configuration messages.
FINE	Provides tracing information; used for system debugging.
FINER	Provides fairly detailed tracing information; used for system debugging.
FINEST	Provides highly detailed tracing information; used for system debugging.

The FINE, FINER, and FINEST settings affect performance and scalability. Use these settings if HP has instructed you to do so.

Modifying the Synchronization Schedule

To change the intervals at which the Storage Agent performs synchronization, you can modify the values in the scheduler properties. Synchronization is a process by which the Storage Agent gathers data from the HiCommand servers and then transfers that data to the Domain Data Store, so that the Domain Data Store and HiCommand servers are synchronized.

Synchronization is performed when the Storage Agent starts and then again at the interval specified in the `pam.properties` file. For example, if you initially start the Storage Agent at midnight and the full synchronization is scheduled to run every 12 hours, the full synchronization always runs at noon and at midnight. As needed, you can run immediate synchronization requests. See “Synchronizing the HiCommand Storage Agent” on page 113.

To modify synchronization intervals, perform the following steps:

1. Verify that the HiCommand Storage Agent is running.

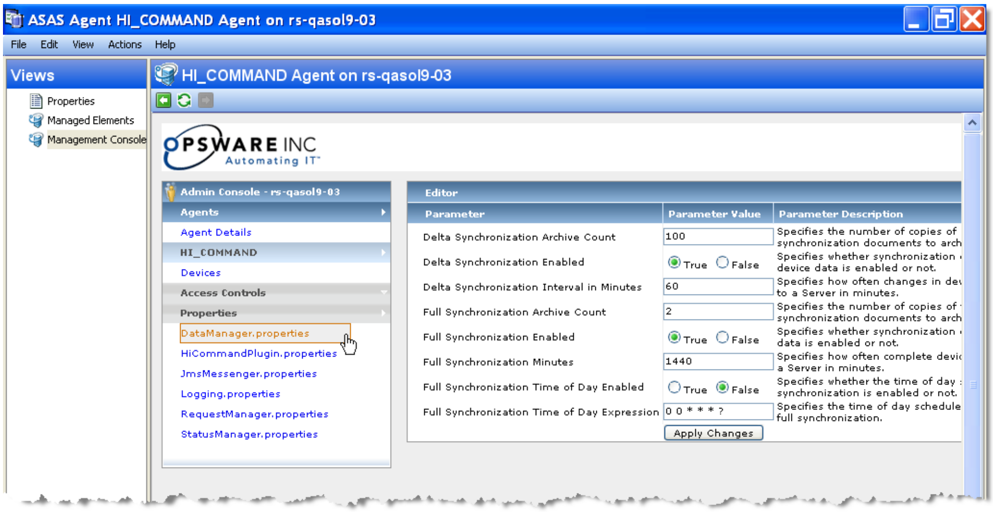
2. From the HiCommand Storage Agent browser, from the Views pane, select Management Console.

3. In the Admin Console, select Properties and then select DataManager.properties to display the schedule parameters. A description of each parameter is provided in the last column.

   Delta synchronization parameters control delta synchronizations where modified data is gathered since the last synchronization.

   Full synchronization parameters control full synchronizations where all data is gathered since the last synchronization.

Figure 7-8: Storage Agent Schedule Settings



Parameter	Parameter Value	Parameter Description
Delta Synchronization Archive Count	100	Specifies the number of copies of synchronization documents to arch
Delta Synchronization Enabled	● True ○ False	Specifies whether synchronization device data is enabled or not.
Delta Synchronization Interval in Minutes	60	Specifies how often changes in dev to a Server in minutes.
Full Synchronization Archive Count	2	Specifies the number of copies of synchronization documents to arch
Full Synchronization Enabled	● True ○ False	Specifies whether synchronization data is enabled or not.
Full Synchronization Minutes	1440	Specifies how often complete devic a Server in minutes.
Full Synchronization Time of Day Enabled	○ True ● False	Specifies whether the time of day synchronization is enabled or not.
Full Synchronization Time of Day Expression	0 0 * * * ?	Specifies the time of day schedule full synchronization.

4. After you make changes, click **Apply Changes**.

Chapter 8: McDATA Storage Agent

IN THIS CHAPTER

This section discusses the following topics:

- Access Controls
- Storage Agent Operation
- Storage Agent Settings

Access Controls

This section describes how to configure the Storage Agent so that it can gather information from the McDATA fabric. To enable this process, you must define an access control for each EFCM server the Storage Agent manages. An access control contains values, such as the IP address of the vendor server, which allows the McDATA Storage Agent to communicate with the vendor management software. Table 8-1 describes the access control values you must create before running the McDATA Storage Agent for the first time.

✔ Each server where the vendor management software resides requires a unique access control. For example, if you have two fabrics, one managed by EFCM and the other managed by EFCM and Connectrix Manager, you need to create three access controls— one for each vendor server to manage the two fabrics.

Table 8-1: McDATA Storage Agent Access Controls

ACCESS CONTROL VALUE	DESCRIPTION
Caption	A name used to uniquely identify each access control entry. The default is `McDATA EFCM AccessControl`.

Table 8-1: McDATA Storage Agent Access Controls (continued)

ACCESS CONTROL VALUE	DESCRIPTION
User name	The user name authorized to access the McDATA vendor management software server. The user name must be admin-level.
Password	The password authorized to access the McDATA vendor management software server. The password must be admin-level.
IP Address	The IP address for the vendor management software server.

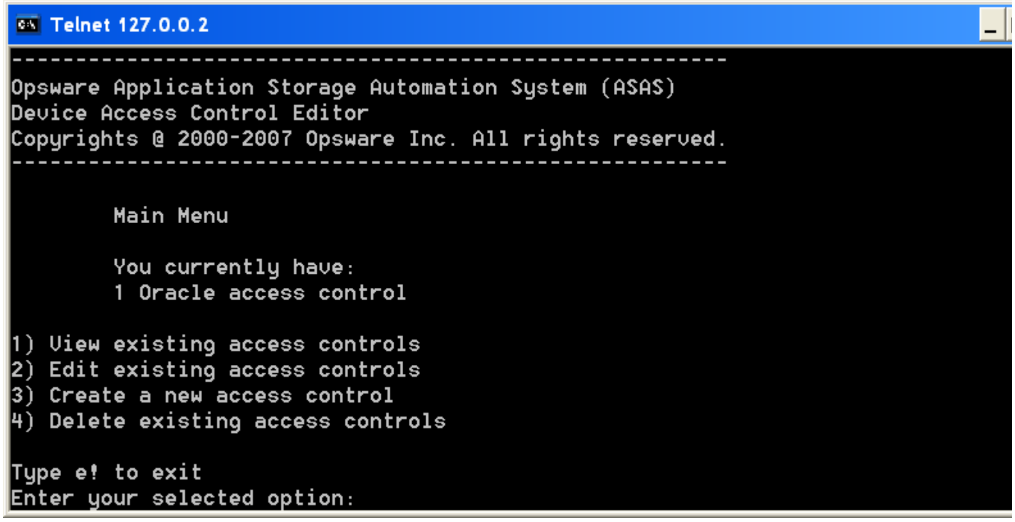
Opening the Device Access Control Editor

To open the Device Access Control Editor on a certain operating system, perform the following steps:

1. In the ASAS Agents window, select a Storage Agent and then select **Actions ➤ Open**.
2. In the ASAS Agents window for the selected Storage Agent, select **Actions ➤ DeviceAccessControl editor**.

The command line interface opens similar to the following, displaying the main menu for the Device Access Control Editor.

Figure 8-1: Device Access Control Editor Example



```
-------------------------------------------------------
Opsware Application Storage Automation System (ASAS)
Device Access Control Editor
Copyrights @ 2000-2007 Opsware Inc. All rights reserved.
-------------------------------------------------------

        Main Menu

        You currently have:
        1 Oracle access control

1) View existing access controls
2) Edit existing access controls
3) Create a new access control
4) Delete existing access controls

Type e! to exit
Enter your selected option:
```

3 Navigate through the Device Access Control Editor using the commands described in Table 8-2. All commands are case-sensitive.

Table 8-2: Device Access Control Editor Commands

COMMAND	ACTION
`b!`	Returns to the previous menu.
`c!`	Corrects the values entered for an access control. This command is only available from the Verify Values screen after you have entered all access control values for the Storage Agent.
`d!`	Deletes an existing access control.
`e!`	Exits the command line interface.
`r!`	Returns to the main menu.
`s!`	Saves a set of access control values.
`u!`	Undo an access control value by returning to the previous entry. This command is only available while you are entering access control values.

Configuring Access Controls

To configure access controls for the McDATA Storage Agent, perform the following steps:

1. Type `3` to select the `Create a new access control` option and then press Enter.
2. Type the number of the access control type you want to create or edit and then press Enter. For example, if `McDATA EFCM` is listed as option 1, type `1` and then press Enter.
3. At the `Caption` prompt, type a caption that identifies this access control and then press Enter. To accept the default value, just press Enter.

   If you are creating more than one access control, enter a caption that uniquely identifies each access control entry, such as McDATA-1, McDATA-2, and so on.
4. At the `User name` prompt, type an admin-level user name and then press Enter. This is the user name that is authorized to access the McDATA fabric instance.
5. At the `Password` prompt, type the password and then press Enter. This is the password that is authorized to access the McDATA fabric instance.
6. Re-enter the password and then press Enter.
7. At the IP addresses prompt, type the IP address for the server running the vendor management software and press Enter.

   The prompt for specifying a Fibre Switch World Wide Name for the fabric is optional and exists only for the remote Unix version of the McDATA Storage Agent. If you do enter a World Wide Name, the Storage Agent only accesses the switches on that given fabric.

   If the vendor management software (EFCM or Connectrix Manager) manages more than one fabric, you should skip this access control by pressing Enter.

   After you enter the IP addresses or WWN, if you chose to enter a value for this option, the access control values you entered are displayed on the screen so that you can verify them.
8. Type `s!` (a lowercase `s`) and then press Enter to save your access control configuration.

Access controls are saved in the `access_control.bin` file in the following directories, depending on the operating system:

`c:\Program Files\Common Files\Opsware\pam-mcdata\` (Windows)

Or

`/var/opt/opsware/pam-mcdata` (Unix)

9 If you need to create additional access controls, return to the main menu (`r!)` and repeat step 2 through step 8.

OR

Type one of the following options:

`c!` Correct an access control entry.

`b!` Go back to the previous menu.

10 After you have entered access control values for all McDATA EFCMs you want to manage, type `e!` (a lowercase `e`) and then press Enter to exit the Access Control Editor.

Editing Access Controls

You can edit access controls while the McDATA Storage Agent is running or stopped. If you edit access controls while the Storage Agent is running, changes are picked during the next synchronization. To edit access controls for the McDATA Storage Agent, perform the following steps:

1 Open the main menu for the Access Control Editor.

2 Type 2 to select the `Edit existing access controls` option and then press Enter.

3 Type the number of the access control type you want to edit and then press Enter.

4 Modify each value as desired. If you want to leave an access control value as is, press Enter.

After you enter the last access control value, a summary is displayed on the screen so that you can verify them.

5 Type `s!` (a lowercase `s`) and then press Enter to save your access control configuration.

Access controls are saved in the `access_control.bin` file in the following directories, depending on the operating system:

`c:\Program Files\Common Files\Opsware\pam-mcdata\` (Windows)

Or

`/var/opt/opsware/pam-mcdata` (Unix)

6 If you need to edit additional access controls, return to the main menu (`r!)` and repeat step 2 through step 5.

7 Type `e!`(a lowercase `e`) and press Enter to exit the program.

Deleting Access Controls

You can delete access controls while the McDATA Storage Agent is running or stopped. If you edit access controls while the Storage Agent is running, changes are picked during the next synchronization. To delete access controls for the McDATA Storage Agent, perform the following steps:

1 Open the main menu for the Access Control Editor.

2 Type 4 to select the `Delete existing access controls` option and then press Enter.

3 Type the number of the access control type you want to delete and then press Enter.

4 Type the number of the access control that you want to delete and then press Enter.

5 Type `d!` (a lowercase `d`) and then press Enter to delete the access control.

The Access Control Editor confirms the deletion.

6 Type `e!` (a lowercase `e`) and then press Enter to exit access control configuration.

Storage Agent Operation

This section describes how to authorize, start, stop, synchronize, and check the discovery status of a McDATA Storage Agent.

Authorizing the McDATA Storage Agent

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 McDATA Storage Agent is deployed. When a Storage Agent is initially deployed to a managed server, you must authorize it so that messages from the Storage Agent are accepted by the core server. As a result of the authorization process, a security token is generated and given to the Storage Agent.

If you are not sure whether the security token in the core and on the managed server match, you can authorize the McDATA Storage Agent repeatedly. A security token mismatch can occur as a result of unintentional editing or removal of tokens.

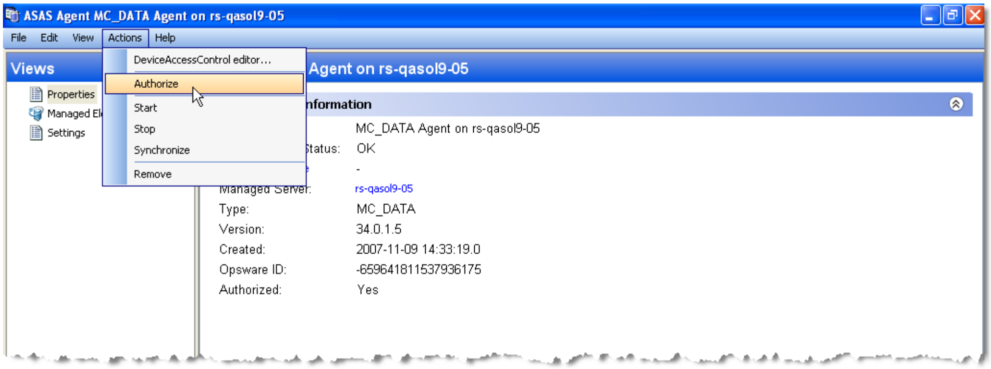
To authorize a McDATA Storage Agent, perform the following steps:

1. From the Navigation pane, select **Opsware Administration ➤ ASAS Agents**.

2. Open the McDATA Storage Agent that needs to be authorized.

3. From the **Actions** menu, select **Authorize**.

Figure 8-2: Authorize Action for a McDATA Storage Agent



MC_DATA Agent on rs-qasol9-05
tatus: OK
-
Managed Server: rs-qasol9-05
Type: MC_DATA
Version: 34.0.1.5
Created: 2007-11-09 14:33:19.0
Opsware ID: -659641811537936175
Authorized: Yes

Starting the McDATA Storage Agent

When the McDATA Storage Agent starts for the first time, the agent begins discovering McDATA switches and synchronizing device data. During this process, the McDATA Storage Agent gathers information from various switch elements and reports that information to the Web Services Data Access Engine so that the device data for the McDATA switches is synchronized. Depending on the size and number of the McDATA switches, device synchronization could require several hours. You can start the Storage Agent by using the ASAS Client on a managed server or by running a saved script on a remote managed server.

For performance reasons, you should start the McDATA Storage Agent during off-peak hours.

To start a McDATA Storage Agent on a managed server by using the ASAS Client, perform the following steps:

1. In the ASAS Agent window, select a McDATA Storage Agent and then select **Actions ➤ Open** to display the McDATA Storage Agent browser.
2. Select **Actions ➤ Start**.
3. In the Management Information section click the “Check current state” link to verify that the Storage Agent is Running.

Starting the McDATA Storage Agent on a Remote Windows Server

To start a McDATA Storage Agent 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 OpswareMcDATAStorageAgent and then select **Action ➤ Start.**

Starting the McDATA Storage Agent on a Remote Unix Server

To start a McDATA Storage Agent on a remote Unix server, perform the following steps:

1. Navigate to the `/etc/opt/opsware/startup` directory.
2. Enter the `./pam-mcdata start` command to run the saved script that starts the Storage Agent.

   When the Storage Agent starts, it begins the discovery and synchronization process. To monitor the discovery process, see “Checking the McDATA Storage Agent Status” on page 128.

Stopping the McDATA Storage Agent

You must stop the McDATA Storage Agent before you modify Storage Agent settings. See “Storage Agent Settings” on page 129.

You should also stop and then restart the McDATA Agent after any fabric changes are made. This action does not interfere with any fabric changes that are in progress.

You can stop the Storage Agent by using the ASAS Client on a managed server or by running a saved script on a remote managed server.

After the Storage Agent is stopped or undeployed, the status does not change. For more information, see “Undeploying a Storage Agent from a Managed Server” on page 42 and “Checking the McDATA Storage Agent Status” on page 128.

To stop a McDATA Storage Agent on a managed server by using the ASAS Client, perform the following steps:

1. In the ASAS Agent window, select a McDATA Storage Agent and then select **Actions ➤ Open** to display the McDATA Storage Agent browser.
2. Select **Actions ➤ Stop**.
3. In the Management Information section click the “Check current state” link to verify that the Storage Agent is unavailable.

Stopping the McDATA Storage Agent on a Remote Windows Server

To stop an McDATA Storage Agent 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 OpswareMcDATAStorageAgent and then select **Action ➤ Stop.**

Stopping the McDATA Storage Agent on a Remote Unix Server

To stop a McDATA Storage Agent on a remote Unix managed server, perform the following steps:

1. Navigate to the `/etc/opt/opsware/startup` directory.
2. Enter the `./pam-mcdata stop` command to run the saved script that stops the Storage Agent.

   When the Storage Agent is stopped, discovery and synchronization processes will not run. See “Synchronizing the McDATA Storage Agent” on page 127.

Synchronizing the McDATA Storage Agent

Synchronization is a request to the Storage Agent to gather the latest data from managed devices and then send this data to the core. Synchronization is performed when the Storage Agent starts and then again at the interval specified in the `pam.properties` file.

Synchronization can occur only when the Storage Agent is running.

If the Storage Agent is stopped or the default schedule does not synchronize the Storage Agent as frequently as you need it to, you can explicitly request a synchronization. For example, you will need to explicitly request a synchronization whenever the storage administrator applies changes and needs to immediately see them—instead of waiting for the next scheduled synchronization.

To change the intervals at which the Storage Agent performs synchronization, see "Modifying the Synchronization Schedule" on page 53.

To synchronize a McDATA Storage Agent on a managed server, perform the following steps:

1. In the ASAS Agent window, select a McDATA Storage Agent and then select **Actions ➤ Open** to display the McDATA Storage Agent browser.
2. Select **Actions ➤ Synchronize** to run the synchronization process. When the synchronization request is successfully completed, a confirmation window displays.
3. Click **OK** to close this window.

Checking the McDATA Storage Agent Status

When the Storage Agent starts, it begins the discovery and synchronization process.

To check Storage Agent discovery status, perform the following steps:

1. From the Navigation pane, select **Opsware Administration ➤ ASAS Agents**.
2. In the content pane, check the Last Received Status column for the status of the fabric tree structure in the left panel.
3. Select the fabric name and make sure the Properties tab is selected in the right display panel. Table 8-3 describes the general status values.

Table 8-3: McDATA Storage Agent Status Values

STATUS VALUE	DESCRIPTION
Last Received Status	Indicates the state of the fabric, such as OK, Starting, Stopping, or OFFLINE.
Lifecycle State	Indicates the state of storage agent communications: either **OK** or **MISSING**. If the storage agent has stopped running, the Lifecycle State changes to **MISSING**. When the storage agent is running again, the Lifecycle State returns to **OK**.

Table 8-3: McDATA Storage Agent Status Values

STATUS VALUE	DESCRIPTION
Last Sync	Indicates the last time the Storage Management Console received information in the synchronization process from the Storage Agent.
Synchronization Status	Indicates the status of the last synchronization for the storage agent. They are as follows: SUCCESS: The synchronization process completed without errors. INCOMPLETE: An error occurred during the synchronization process, which indicates that the Management Server or Storage Agent processed some element information successfully, but could not process all element information. FAILED: The synchronization process failed, which indicates that the Management Server or Storage Agent was not able to process any element information. **Note:** When an "INCOMPLETE" or "FAILED" status appears, view the Management Server and Storage Agent log file for more information about the errors.

Storage Agent Settings

Storage Agent settings (properties) manage Storage Agent behavior. After you install and configure the Storage Agent, you can adjust these settings in the `pam.properties` file.

Before modifying the `pam.properties` file, make sure the Storage Agent is not running. See "Stopping the McDATA Storage Agent" on page 126.

You can modify the following values in the `properties` file:

- **Log file size and level**. Conserve disk space by modifying the maximum size for log files and level of detail gathered for log messages.

- **Synchronization and polling**. Tune system performance by adjusting the intervals at which synchronizations run.

Contact Hewlett Packard if you need to modify thread pools.

Controlling Log File Sizes and Logging Levels

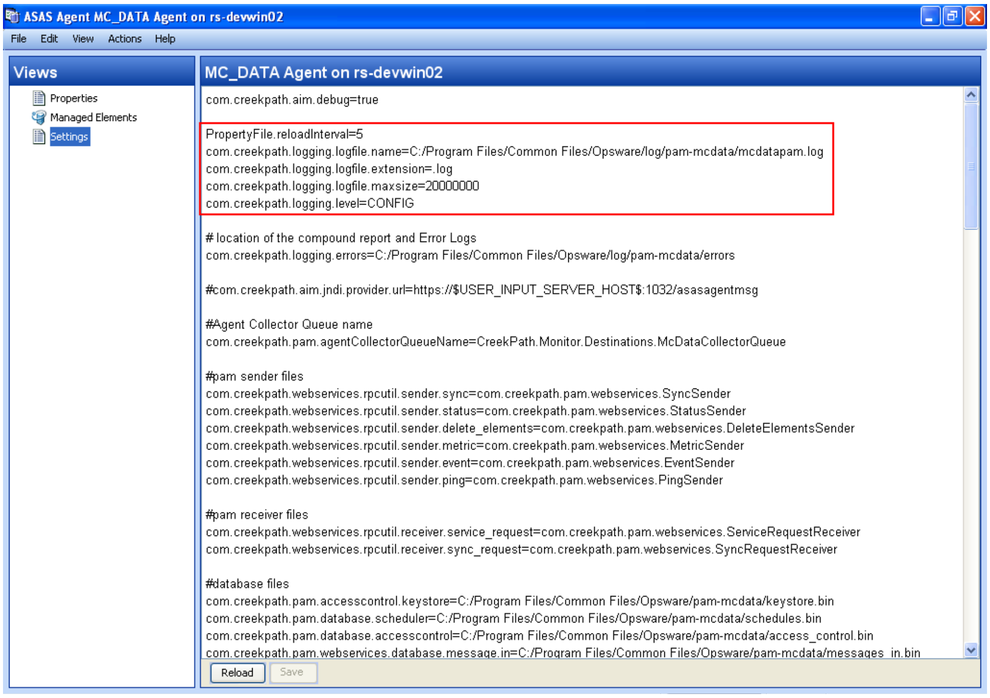
To conserve disk space and control the types of log messages that ASAS gathers, you can adjust the maximum size of log files and the logging level in the log file settings.

To modify the log file settings, perform the following steps:

1. Stop the Storage Agent.
2. In the ASAS Agent window, select a Storage Agent.
3. Select **Actions ➤ Open** to display the Storage Agent browser.
4. From the Views pane, select **Settings** to display the log file settings in the content pane.

5 Change any of the log file settings. For a list of these parameters and their descriptions, see Table 8-4 on page 132.

Figure 8-3: Storage Agent Log File Settings



```
com.creekpath.aim.debug=true

PropertyFile.reloadInterval=5
com.creekpath.logging.logfile.name=C:/Program Files/Common Files/Opsware/log/pam-mcdata/mcdatapam.log
com.creekpath.logging.logfile.extension=.log
com.creekpath.logging.logfile.maxsize=20000000
com.creekpath.logging.level=CONFIG

# location of the compound report and Error Logs
com.creekpath.logging.errors=C:/Program Files/Common Files/Opsware/log/pam-mcdata/errors

#com.creekpath.aim.jndi.provider.url=https://$USER_INPUT_SERVER_HOST$:1032/asasagentmsg

#Agent Collector Queue name
com.creekpath.pam.agentCollectorQueueName=CreekPath.Monitor.Destinations.McDataCollectorQueue

#pam sender files
com.creekpath.webservices.rpcutil.sender.sync=com.creekpath.pam.webservices.SyncSender
com.creekpath.webservices.rpcutil.sender.status=com.creekpath.pam.webservices.StatusSender
com.creekpath.webservices.rpcutil.sender.delete_elements=com.creekpath.pam.webservices.DeleteElementsSender
com.creekpath.webservices.rpcutil.sender.metric=com.creekpath.pam.webservices.MetricSender
com.creekpath.webservices.rpcutil.sender.event=com.creekpath.pam.webservices.EventSender
com.creekpath.webservices.rpcutil.sender.ping=com.creekpath.pam.webservices.PingSender

#pam receiver files
com.creekpath.webservices.rpcutil.receiver.service_request=com.creekpath.pam.webservices.ServiceRequestReceiver
com.creekpath.webservices.rpcutil.receiver.sync_request=com.creekpath.pam.webservices.SyncRequestReceiver

#database files
com.creekpath.pam.accesscontrol.keystore=C:/Program Files/Common Files/Opsware/pam-mcdata/keystore.bin
com.creekpath.pam.database.scheduler=C:/Program Files/Common Files/Opsware/pam-mcdata/schedules.bin
com.creekpath.pam.database.accesscontrol=C:/Program Files/Common Files/Opsware/pam-mcdata/access_control.bin
com.creekpath.pam.webservices.database.message.in=C:/Program Files/Common Files/Opsware/pam-mcdata/messages_in.bin
```

6 Click **Save** to save your settings.

Or

Click **Reload** to restore the settings to their previous values—before you made changes.

Log File Settings

The following table describes the Storage Agent log file settings you can change.

Table 8-4: Log File Settings for Storage Agent

PARAMETER	DESCRIPTION
`logfile.name`	Specifies the directory for all log files and compound reports for errors encountered during synchronization, such as `/var/log/opsware/pam-oracle/oraclepam.log`. This directory is created after ASAS begins gathering logging information. **Note:** If you change the default logging path on a Solaris system and you also created a server group and User ID, you must change the ownership of the new log directory using the `chown` command.
`logfile.extension`	Specifies the extension for log file names.
`logfile.maxsize`	Controls the maximum size of each log file (in bytes). By default, the Storage Agent will populate a log file until it reaches its maximum capacity (20 MB), then it will wrap any remaining log information into a new log file. The Storage Agent can create up to 10 individual log files before it overwrites previous log files.

Table 8-4: Log File Settings for Storage Agent (continued)

PARAMETER	DESCRIPTION
`logging.level`	Controls the type of messages gathered or turns off logging. Each subsequent level also includes the logging information that precedes it, such as INFO includes logging information for SEVERE and WARNING. Enter one of the following values: • OFF: Does not collect logging information. • SEVERE: Collects messages indicating a serious failure. • WARNING: Collects exception messages. • INFO (default): Collects informational messages, such as storage volume creation. • CONFIG: Collects static configuration messages. • FINE: Provides tracing information; used for system debugging. • FINER: Provides fairly detailed tracing information; used for system debugging. • FINEST: Provides highly detailed tracing information; used for system debugging. **Note**: The FINE, FINER, and FINEST settings affect Storage Agent performance and scalability. You should only use these settings if HP Support has instructed you to do so.

Modifying the Synchronization Schedule

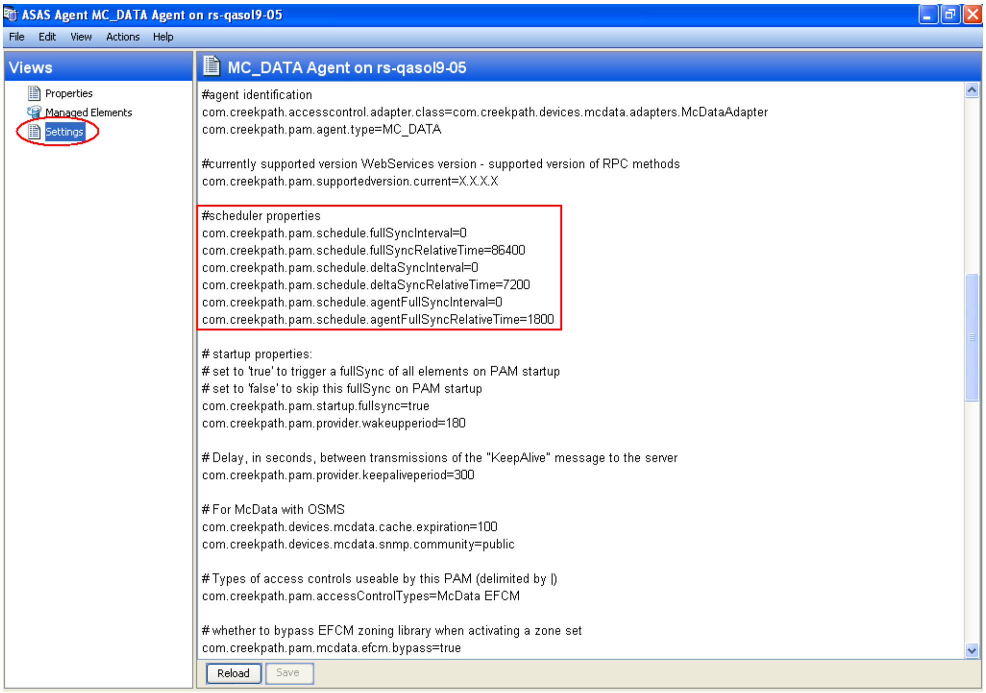
To change the intervals at which the Storage Agent performs synchronization, you can modify the values in the scheduler properties. Synchronization is a process by which the Storage Agent gathers data from the McDATA EFCM and then transfers that data to the Domain Data Store so that the Domain Data Store and McDATA switches are synchronized.

Synchronization is performed when the Storage Agent starts and then again at the interval specified in the `pam.properties` file. For example, if you initially start the Storage Agent at midnight and the full synchronization is scheduled to run every 12 hours, the full synchronization always runs at noon and at midnight. As needed, you can run immediate synchronization requests. See "Synchronizing the McDATA Storage Agent" on page 127.

To modify synchronization intervals, perform the following steps:

1. Stop the Storage Agent.
2. From the McDATA Storage Agent browser, from the Views pane, select Settings.
3. In the content pane, locate the lines for #scheduler properties, as Figure 8-4 illustrates.

Figure 8-4: Storage Agent Schedule Settings



```
#agent identification
com.creekpath.accesscontrol.adapter.class=com.creekpath.devices.mcdata.adapters.McDataAdapter
com.creekpath.pam.agent.type=MC_DATA

#currently supported version WebServices version - supported version of RPC methods
com.creekpath.pam.supportedversion.current=X.X.X.X

#scheduler properties
com.creekpath.pam.schedule.fullSyncInterval=0
com.creekpath.pam.schedule.fullSyncRelativeTime=86400
com.creekpath.pam.schedule.deltaSyncInterval=0
com.creekpath.pam.schedule.deltaSyncRelativeTime=7200
com.creekpath.pam.schedule.agentFullSyncInterval=0
com.creekpath.pam.schedule.agentFullSyncRelativeTime=1800

# startup properties:
# set to 'true' to trigger a fullSync of all elements on PAM startup
# set to 'false' to skip this fullSync on PAM startup
com.creekpath.pam.startup.fullsync=true
com.creekpath.pam.provider.wakeupperiod=180

# Delay, in seconds, between transmissions of the "KeepAlive" message to the server
com.creekpath.pam.provider.keepaliveperiod=300

# For McData with OSMS
com.creekpath.devices.mcdata.cache.expiration=100
com.creekpath.devices.mcdata.snmp.community=public

# Types of access controls useable by this PAM (delimited by |)
com.creekpath.pam.accessControlTypes=McData EFCM

# whether to bypass EFCM zoning library when activating a zone set
com.creekpath.pam.mcdata.efcm.bypass=true
```

4. To change the metrics and synchronization schedule, enter new times (in seconds) in the appropriate fields. For a list of these parameters and their descriptions, see Table 8-5 on page 135.
5. If desired, you can change the startup setting so that full synchronizations do not occur when the Storage Agent starts. Locate the following field and change the value from `true` to `false`:

   ```
   com.creekpath.pam.startup.fullsync=false
   ```
6. Click **Save** to save your changes.

   Or

   Click **Reload** to restore the settings to their previous values—before you made changes.

Scheduler Parameter Settings

The following table describes the Storage Agent scheduler parameter settings you can change.

Table 8-5: Scheduler Parameters

PARAMETER	DESCRIPTION
`fullSyncInterval` `fullSyncRelativeTime`	Controls full synchronizations, in which all data is gathered since the last synchronization: **Interval field**: Turns synchronizations on and off. Enter `-1` to turn off synchronizations. Enter `0` to turn on synchronizations. • **RelativeTime field**: Controls the interval at which synchronization occurs (in seconds). To improve scalability of the Manager and Management Server, adjust the Relative Time to a higher value so that synchronizations occur less frequently.

Table 8-5: Scheduler Parameters (continued)

PARAMETER	DESCRIPTION
`deltaSyncInterval` `deltaSyncRelativeTime`	Controls delta synchronizations, in which modified data is gathered since the last synchronization: • **Interval field**: Turns synchronizations on and off. Enter `-1` to turn off synchronizations. Enter `0` to turn on synchronizations. • **RelativeTime field**: Controls the interval at which synchronization occurs (in seconds). To improve scalability of the Manager and Management Server, adjust the Relative Time to a higher value so that synchronizations occur less frequently.

ASAS does not capture events and metrics.

Chapter 9: NetApp Storage Agent

IN THIS CHAPTER

This section discusses the following topics:

- Access Controls
- NetApp Management Console
- Storage Agent Operation
- Storage Agent Settings

Access Controls

This section describes how to configure access controls so that the Storage Agent can gather information from the NetApp NA systems. To enable this process, you must define an access control for each NAS filer the Storage Agent will manage. An access control contains values, such as the IP address that allows the NetApp Storage Agent to communicate with the NetApp NA systems. Table 9-1 describes the access control values you must create before running the NetApp Storage Agent for the first time.

Table 9-1: NetApp Storage Agent Access Controls

ACCESS CONTROL VALUE	DESCRIPTION
Caption	A name used to uniquely identify each access control entry. (If the Storage Agent is managing more than one NA system, you must create more than one access control, each with a unique caption.) **Note**: After this access control is created, you cannot change the caption.
Host Address	An IP address or a DNS host name of the filer.
User Name	The user name needed to access the NetApp system's ONTAPI interface.

Table 9-1: NetApp Storage Agent Access Controls (continued)

ACCESS CONTROL VALUE	DESCRIPTION
Password	The password needed to access the NetApp system's ONTAPI interface.
SNMP Community	The read community string needed to access the NetApp system through SNMP.

Filer Etc directory	The paths to the NetApp vfiler(s)' root volume `/etc` directories. The Storage Agent needs access to the root volumes to obtain information on exported directories and connected hosts.
	Enter the paths to the `/etc` directories for each vfiler using the following format:
	`vfilerx|/vol/voln/etc`
	where vfilerx is the name of the vfiler (for example, "vfiler0"), and voln is the name of the volume (for example, "vol0") containing the `/etc` directory.
	If multi-store is enabled, use a comma to separate each vfiler. For example:
	`vfiler0|/vol/vol0/etc, vfiler1|/vol/vol20/etc`

NetApp Management Console

This section describes how to use the NetApp Management Console to enable the Storage Agent to communicate with and gather data from NetApp systems. You can establish communication links by creating access controls for each NetApp system. The Management Console is installed with the NetApp Storage Agent.

After you configure the access controls in the Management Console, ASAS begins discovering NetApp servers and synchronizing device data. During this process, the Storage Agent gathers information from various NetApp systems and reports that information to the Web Service Data Access Engine, so that ASAS and the device data for the NetApp NA systems are synchronized.

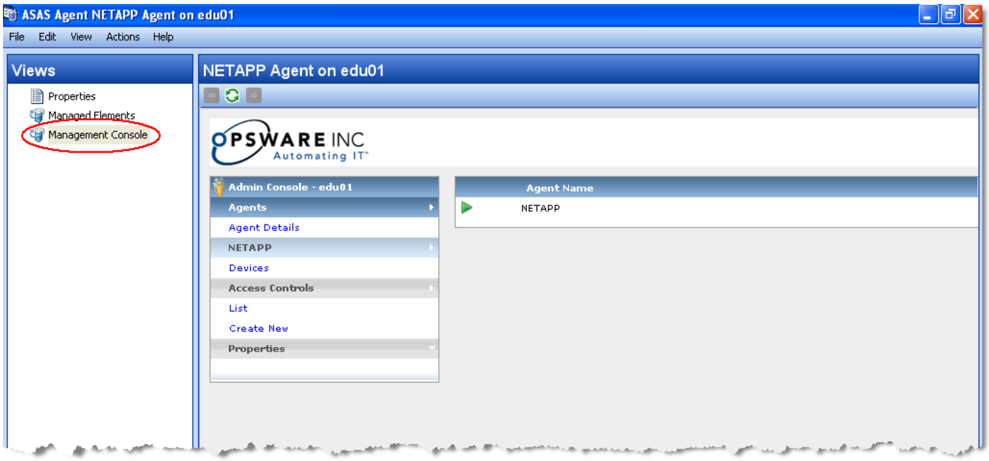
Depending on the number of NetApp NA systems the Storage Agent is controlling, device synchronization might require several hours. For performance reasons, you should start the NetApp Storage Agent during off-peak hours.

Opening the Management Console

To open the Management Console for a NetApp Storage Agent, perform the following steps:

1. From the Navigation pane, select **Opsware Administration ➤ ASAS Agents**.
2. In the content pane, open a NetApp Storage Agent to display the Agent Browser.
3. Select the “Check current status” link to verify that the Storage Agent is running.
4. In the Views pane, select Management Console to open the Management Console for the selected NetApp Storage Agent.

Figure 9-1: NetApp Management Console



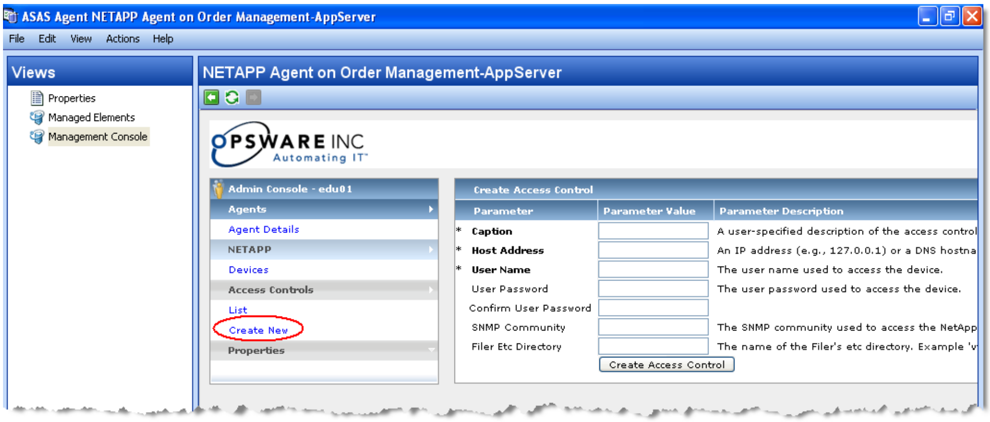
Creating an Access Control

To create an access control for a NetApp Storage Agent, perform the following steps:

1. In the Admin Console, click the Access Control down arrow to expand the actions.

2 Select Create New to display the Create Access Control editor.

Figure 9-2: Create Access Control Editor in the Management Console



Create Access Control

	Parameter	Parameter Value	Parameter Description
*	**Caption**		A user-specified description of the access control
*	**Host Address**		An IP address (e.g., 127.0.0.1) or a DNS hostna
*	**User Name**		The user name used to access the device.
	User Password		The user password used to access the device.
	Confirm User Password		
	SNMP Community		The SNMP community used to access the NetApp
	Filer Etc Directory		The name of the Filer's etc directory. Example 'v

Create Access Control

3 Enter the access controls, as described in Table 9-1 on page 137.

4 After you have entered the access controls, click **Create Access Control** to save your changes. The new access controls are listed in the Admin Console.

5 (Optional) Select List in the Admin Console to review all access controls.

6 If there is another NetApp server running in the network, repeat step 1 through step 5 to create another access control.

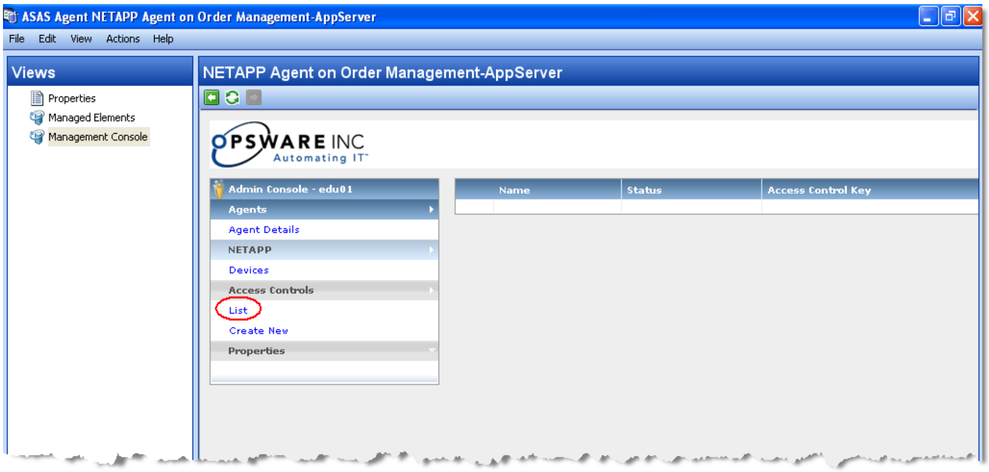
Deleting an Access Control

You can delete access controls while the NetApp Storage Agent is running or stopped. If you edit access controls while the Storage Agent is running, changes will be picked up during the next synchronization. To delete access controls for the NetApp Storage Agent, perform the following steps:

1 In the Admin Console, click the Access Control down arrow to expand the actions.

2 Select List to display a list of access controls for the NetApp Storage Agent.

Figure 9-3: Access Control List in the Management Console.



3 Click the trash can icon next to the access control you want to delete.

Storage Agent Operation

This section describes how to authorize, start, stop, synchronize, and check the discovery status of a NetApp Storage Agent.

Authorizing the NetApp Storage Agent

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 NetApp Storage Agent is deployed. When a Storage Agent is initially deployed to a managed server, you must authorize it so that messages from the Storage Agent will be accepted by the core server. As a result of the authorization process, a security token is generated and given to the Storage Agent.

If you are not sure whether the security token in the core and on the managed server match, you can authorize the NetApp Storage Agent repeatedly. A security token mismatch can occur as a result of unintentional editing or removal of tokens.

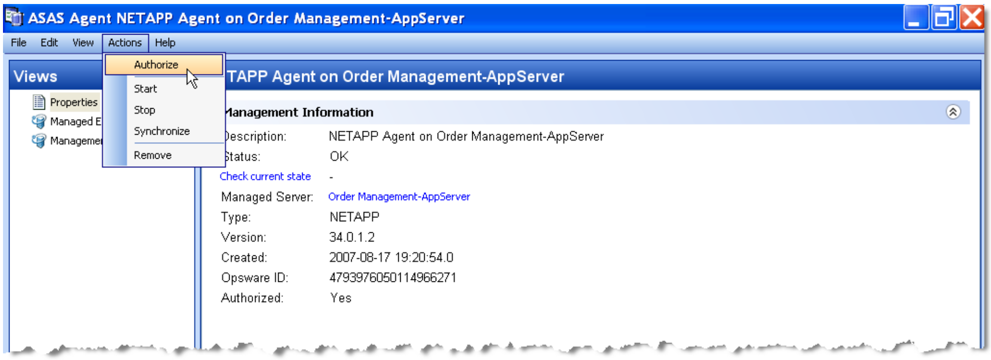
To authorize a NetApp Storage Agent, perform the following steps:

1 From the Navigation pane, select **Opsware Administration ➤ ASAS Agents**.

2 Open the NetApp Storage Agent that needs to be authorized.

3 From the **Actions** menu, select **Authorize**.

Figure 9-4: Authorize Action for a NetApp Storage Agent


ASAS Agent NETAPP Agent on Order Management-AppServer
File
Edit
View
Actions
Help
Authorize
Start
Stop
Synchronize
Remove
Views
Properties
Managed E
Managemer
TAPP Agent on Order Management-AppServer

Management Information

Description: NETAPP Agent on Order Management-AppServer
Status: OK
Check current state -
Managed Server: Order Management-AppServer
Type: NETAPP
Version: 34.0.1.2
Created: 2007-08-17 19:20:54.0
Opsware ID: 4793976050114966271
Authorized: Yes

Starting the NetApp Storage Agent

When the NetApp Storage Agent starts for the first time, the agent begins discovering and synchronizing device data. During this process, the NetApp Storage Agent gathers information from various NAS filer elements and reports that information to the Web Services Data Access Engine so that the device data for the NetApp NAS systems is synchronized. Depending on the size of the NetApp NAS systems, device synchronization could require several hours. You can start the Storage Agent by using the ASAS Client on a managed server or by running a saved script on a remote managed server.

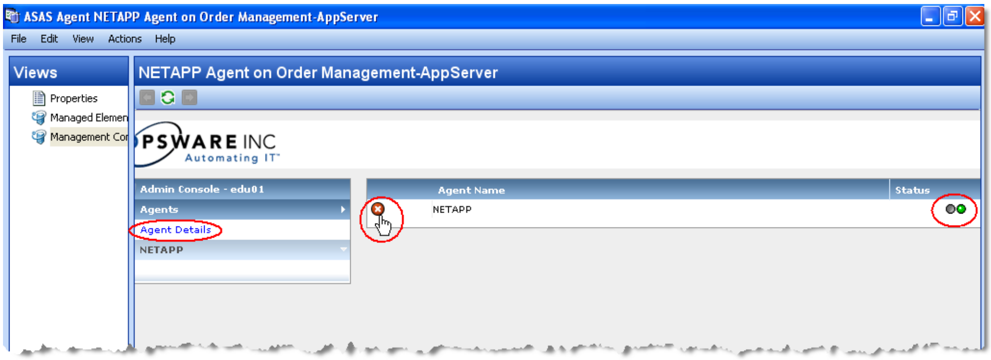
For performance reasons, you should start the NetApp Storage Agent during off-peak hours.

To start a NetApp Storage Agent on a managed server by using the Management Console, perform the following steps:

1 In the Admin Console, select Agent Details.

2 Click the green start icon to start the Storage Agent. This icon changes to a red stop icon and the Status indicator changes from red to green. The Storage Agent runs as a service in the operating system's background.

Figure 9-5: Starting the Storage Agent



Stopping the NetApp Storage Agent

You must stop the NetApp Storage Agent before you modify Storage Agent settings. See "Storage Agent Settings" on page 145.

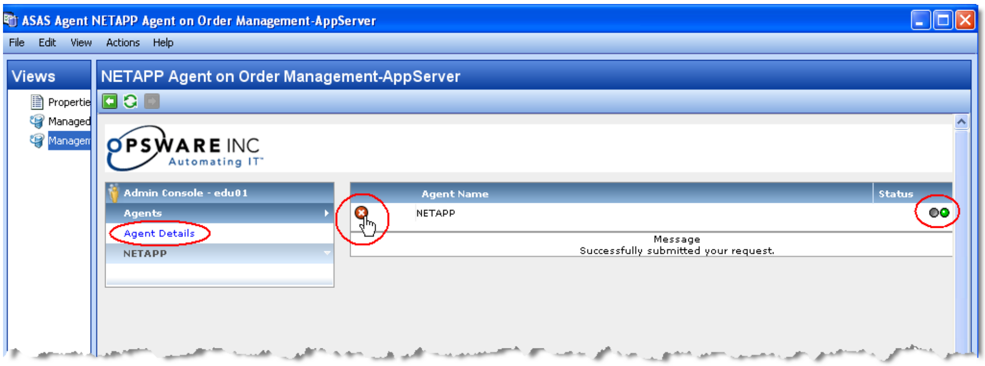
After the Storage Agent is stopped or undeployed, the status does not change. For more information, see "Undeploying a Storage Agent from a Managed Server" on page 42 and "Checking the NetApp Storage Agent Status" on page 145.

To stop a NetApp Storage Agent on a managed server by using the Management Console, perform the following steps:

1 In the Admin Console, select Agent Details.

2. Click the red icon to stop the Storage Agent. This icon changes to a green arrow icon and the Status indicator changes from red to green. The Storage Agent runs as a service in the operating system's background.

Figure 9-6: Stopping the Storage Agent



Agent Name	Status
NETAPP	●●

Message
Successfully submitted your request.

Synchronizing the NetApp Storage Agent

Synchronization is a request to the Storage Agent to gather the latest data from managed devices and then send this data to the core. Synchronization is performed when the Storage Agent starts. You can monitor the status of this process in the Storage Management Console or the Central Admin Console.

Synchronization can occur only when the Storage Agent is running.

If the Storage Agent is stopped or the default schedule does not synchronize the Storage Agent as frequently as you need it to, you can explicitly request a synchronization. For example, you need to explicitly request a synchronization whenever the storage administrator applies changes and needs to immediately see them–instead of waiting for the next scheduled synchronization.

To change the intervals at which the Storage Agent performs synchronization, see "Modifying the Synchronization Schedule" on page 147.

To synchronize a NetApp Storage Agent on a managed server, perform the following steps:

1. In the ASAS Agent window, select a NetApp Storage Agent and then select **Actions ➤ Open** to display the NetApp Storage Agent browser.

2. Select **Actions ➤ Synchronize** to run the synchronization process. When the synchronization request is successfully completed, a confirmation window displays.
3. Click **OK** to close this window.

Checking the NetApp Storage Agent Status

When the Storage Agent starts, it begins the discovery and synchronization process.

To check Storage Agent discovery status, perform the following steps:

1. From the Navigation pane, select **Opsware Administration ➤ ASAS Agents**.
2. In the content pane, check the Last received Status column to see whether the Storage Agent is OK, Starting, Stopping, or OFFLINE. The Last Scan column displays the date and time the status was captured.
3. (Optional) Select a Storage Agent and then click the "Check current state" link in the Properties pane to display the latest status, such as Running, Available, or Unavailable. The Last Scan column displays the date and time the state was captured.

Storage Agent Settings

Storage Agent settings (properties) manage Storage Agent behavior. After you install and configure the Storage Agent, you can adjust these settings in the `pam.properties` file.

Before modifying the `pam.properties` file, make sure the Storage Agent is not running. See "Stopping the NetApp Storage Agent" on page 143.

You can modify the following values in the `properties` file:

- **Log file size and level**. Conserve disk space by modifying the maximum size for log files and level of detail gathered for log messages.
- **Synchronization and polling**. Tune system performance by adjusting the intervals at which synchronizations run.

Contact Hewlett Packard if you need to modify thread pools.

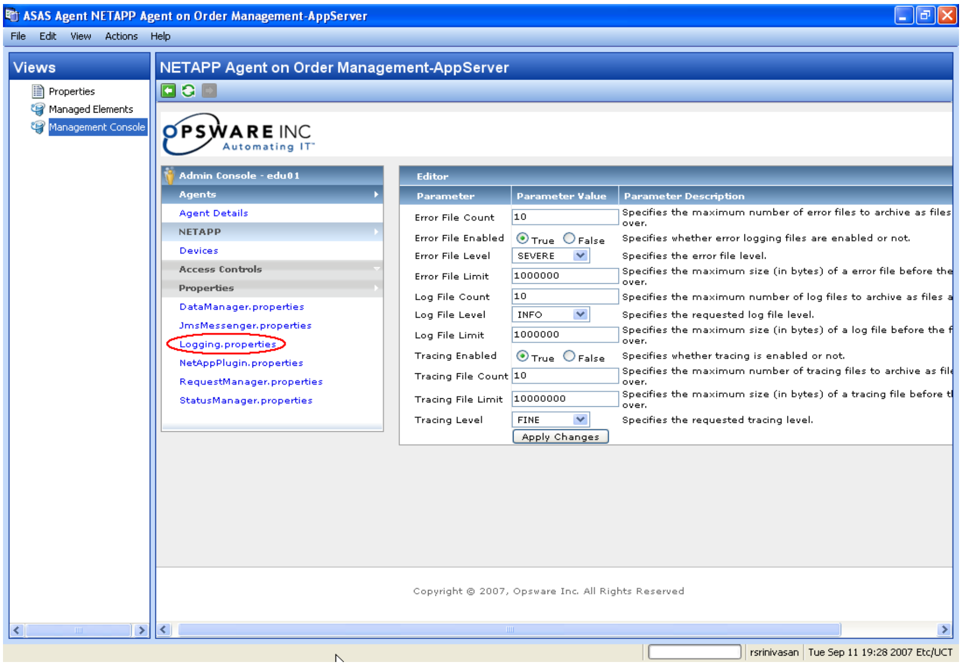
Controlling Log File Sizes and Logging Levels

To conserve disk space and control the types of log messages that ASAS gathers, you can adjust the maximum size of log files and the logging level in the log file settings.

To modify the log file settings, perform the following steps:

1. Stop the Storage Agent.
2. From the NetApp Storage Agent browser, from the Views pane, select Management Console.
3. In the Admin Console, select Properties and then select Logging.properties to display the logging parameters for error files, log files, and tracing files. For descriptions of the logging levels, see Table 9-2 on page 147.

Figure 9-7: Storage Agent Log File Settings



Parameter	Parameter Value	Parameter Description
Error File Count	10	Specifies the maximum number of error files to archive as files over.
Error File Enabled	● True ○ False	Specifies whether error logging files are enabled or not.
Error File Level	SEVERE	Specifies the error file level.
Error File Limit	1000000	Specifies the maximum size (in bytes) of a error file before the over.
Log File Count	10	Specifies the maximum number of log files to archive as files a
Log File Level	INFO	Specifies the requested log file level.
Log File Limit	1000000	Specifies the maximum size (in bytes) of a log file before the f over.
Tracing Enabled	● True ○ False	Specifies whether tracing is enabled or not.
Tracing File Count	10	Specifies the maximum number of tracing files to archive as file over.
Tracing File Limit	10000000	Specifies the maximum size (in bytes) of a tracing file before tl over.
Tracing Level	FINE	Specifies the requested tracing level.

Copyright © 2007, Opsware Inc. All Rights Reserved

rsrinivasan Tue Sep 11 19:28 2007 Etc/UCT

4. After you make changes, click **Apply Changes.**

Logging Levels

You can also specify logging levels (the types of messages gathered), as described in Table 9-2 on page 147.

Each subsequent level includes the logging information that precedes it. For example,

INFO includes logging information for SEVERE and WARNING.

Table 9-2: Logging Levels for a NetApp Storage Agent

LEVEL	DESCRIPTION
SEVERE	Collects messages indicating a serious failure.
WARNING	Collects exception messages.
INFO	Collects informational messages, such as storage volume creation. This is the default Error File Level.
CONFIG	Collects static configuration messages.
FINE	Provides tracing information; used for system debugging.
FINER	Provides fairly detailed tracing information; used for system debugging.
FINEST	Provides highly detailed tracing information; used for system debugging.

The FINE, FINER, and FINEST settings affect performance and scalability. Use these settings if HP has instructed you to do so.

Modifying the Synchronization Schedule

To change the intervals at which the Storage Agent performs synchronization, you can modify the values in the scheduler properties. Synchronization is a process by which the Storage Agent gathers data from the NetApp NAS systems and then transfers that data to the Domain Data Store, so that the Domain Data Store and NetApp NAS systems are synchronized.

Synchronization is performed when the Storage Agent starts and then again at the interval specified in the `pam.properties` file. For example, if you initially start the Storage Agent at midnight and the full synchronization is scheduled to run every 12 hours, the full synchronization always runs at noon and at midnight. As needed, you can run immediate synchronization requests. See “Synchronizing the NetApp Storage Agent” on page 144.

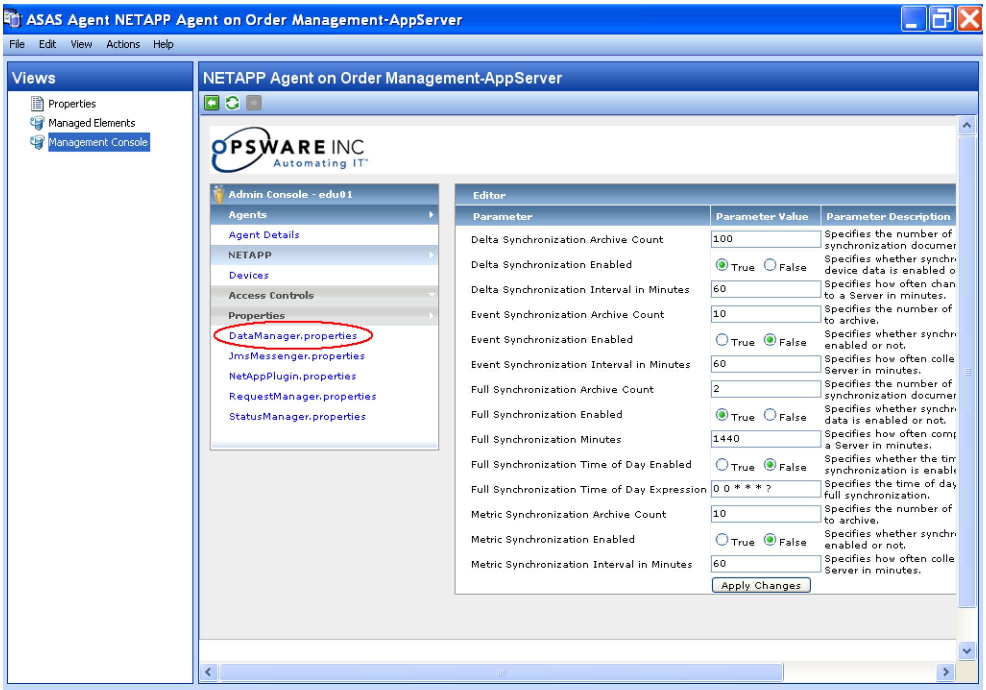
To modify synchronization intervals, perform the following steps:

1. Verify that the NetApp Storage Agent is running.
2. From the NetApp Storage Agent browser, from the Views pane, select **Management Console**.
3. In the Admin Console, select Properties and then select DataManager.properties to display the schedule parameters. A description of each parameter is provided in the last column.

   Delta synchronization parameters control delta synchronizations where modified data is gathered since the last synchronization.

   Full synchronization parameters control full synchronizations where all data is gathered since the last synchronization.

Figure 9-8: Storage Agent Schedule Settings



Parameter	Parameter Value	Parameter Description
Delta Synchronization Archive Count	100	Specifies the number of synchronization documer
Delta Synchronization Enabled	● True ○ False	Specifies whether synchr device data is enabled o
Delta Synchronization Interval in Minutes	60	Specifies how often chan to a Server in minutes.
Event Synchronization Archive Count	10	Specifies the number of to archive.
Event Synchronization Enabled	○ True ● False	Specifies whether synchr enabled or not.
Event Synchronization Interval in Minutes	60	Specifies how often colle Server in minutes.
Full Synchronization Archive Count	2	Specifies the number of synchronization documer
Full Synchronization Enabled	● True ○ False	Specifies whether synchr data is enabled or not.
Full Synchronization Minutes	1440	Specifies how often comp a Server in minutes.
Full Synchronization Time of Day Enabled	○ True ● False	Specifies whether the tir synchronization is enable
Full Synchronization Time of Day Expression	0 0 * * * ?	Specifies the time of day full synchronization.
Metric Synchronization Archive Count	10	Specifies the number of to archive.
Metric Synchronization Enabled	○ True ● False	Specifies whether synchr enabled or not.
Metric Synchronization Interval in Minutes	60	Specifies how often colle Server in minutes.

- After you make changes, click **Apply Changes**.

Chapter 10: Oracle Storage Agent

IN THIS CHAPTER

This section discusses the following topics:

- Prerequisites
- Access Controls
- Storage Agent Operation
- Storage Agent Settings

Prerequisites

This section describes the following prerequisites for setting up the Oracle Storage Agent:

- Storage Host Agent Extension and Realm
- Hardware Registration for the Model Repository
- Creating Tablespaces (Unix only)
- Granting User Privileges
- Loading the Oracle Storage Agent Symlink Add-on (Unix only)

Storage Host Agent Extension and Realm

The Storage Host Agent Extension (SHA) must be installed on the managed server where the Oracle instance or database is. See Chapter 3, “Installing a Storage Host Agent Extension” on page 50 of this guide for more information.

The Oracle Storage Agent and the managed server where the Oracle instance or database is must also be in the same realm. To support Agents in overlapping IP address spaces, a core supports realms. One or more Gateways service the managed servers contained within a realm. In SA, a realm is a routable IP address space, which is serviced by one or more Gateways. All managed servers that connect to a core by a Gateway are identified as being in that Gateway’s realm. For more information about realms, see the *SA Administration Guide*.

Hardware Registration for the Model Repository

The Agent must perform a hardware registration with the Model Repository so that the Oracle Storage Agent is able to discover any Oracle databases. For more information about hardware registration, see *SA User's Guide: Server Automation*.

Creating Tablespaces (Unix only)

For each Oracle instance residing on a Unix managed server and using symbolic links as the datafiles path, you must create tablespaces for each instance. If the Storage Agent will manage instances in a non-Unix environment or in a Unix environment that is not using symbolic links as the datafiles path, skip this procedure and go to "Granting User Privileges" on page 151.

After installing the Oracle Storage Agent on a server that will manage the Oracle instances, the necessary scripts for this process will become available. Copy the scripts from the Storage Agent server to the Oracle database server.

To create a tablespace for each Oracle instance, perform the following steps:

1. Log in to the server where the Oracle Storage Agent is installed.

2. Go to one of the following directories, depending on the operating system:

   `%SYSTEMDRIVE%\Program Files\Opsware\pam-oracle\bin` (Windows)

   Or

   `/opt/opsware/pam-oracle/bin` (Unix)

   For more information, see "Storage Agent File System Layout" on page 40.

3. Locate the `pamtablespace_symboliclink.sql` file and copy it to the server where the Oracle database is installed.

4. Log in to the Oracle database server.

5. Open the `pamtablespace_symboliclink.sql` file in a text editor.

6. In the `pamtablespace_symboliclink.sql` file, replace the data file's default path and database name for `CPSORACLEPAM` and `CPSORACLEPAMTEMP` with the appropriate path and database names for your environment.

7. To create the tablespaces, run the following script using a database account with the appropriate privileges:

   ```
   sqlplus -L <system_user>/<system_password>@<db_name>
   @pamtablespace_symboliclink > pamtablespace_symboliclink.out
   ```

   Repeat this process for each instance.

Granting User Privileges

The Oracle Storage Agent requires user privileges to access the database(s)—which is non-intrusive access to all required system dictionary views. After installing the Oracle Storage Agent on a server that will manage the Oracle instances, the necessary scripts for this process will become available. Copy the scripts from the Storage Agent server to the Oracle database server.

By default, this script will create the user name `oraclepam` and the password `pam`, which will be used to access the Oracle database instance(s). If desired, you can open the `pamuserprivilege` script and edit the user name and password.

To grant user database privileges to the Storage Agent on the database server, perform the following steps:

1. Log in to the server where the Oracle Storage Agent is installed.

2. Go to one of the following directories, depending on the operating system:

   `%SYSTEMDRIVE%\Program Files\Opsware\pam-oracle\bin` (Windows)

   Or

   `/opt/opsware/pam-oracle/bin` (Unix)

   See Chapter 2, “Storage Agent File System Layout” on page 40 of this guide for more information.

3. Locate the appropriate `pamuserprivilege` script and copy it to the server where the Oracle database is installed.

   - For Windows databases or Unix databases that do not use symbolic links as the datafiles path, use the `pamuserprivilege.sql` file.

   - For Unix databases that use symbolic links as the datafiles path, use the `pamuserprivilege_symboliclink.sql` file.

4. Log in to the Oracle database server.

5. As a `sysdba`, run `sqlplus` and execute the appropriate `pamuserprivilege` script.

- For Windows databases or Unix databases that do not use symbolic links as the datafiles path, use the `pamuserprivilege.sql` file.

  Example:

  ```
  sqlplus /nolog

  SQL> connect <sysdba_user>/<sysdba_user_password>@<db_
  name> as sysdba

  SQL> @pamuserprivilege.sql
  ```

- For Unix databases that use symbolic links as the datafiles path, use the `pamuserprivilege_symboliclink.sql` file.

  Example:

  ```
  sqlplus /nolog
  SQL> connect <sysdba_user>/<sysdba_user_password>@<db_
  name> as sysdba
  SQL> @pamuserprivilege_symboliclink.sql
  ```

Loading the Oracle Storage Agent Symlink Add-on (Unix only)

This procedure is optional for Solaris only. For each Oracle instance residing on a Unix managed server and using symbolic links in the datafiles path, you must load the Oracle Storage Agent Symlink Add-on for each instance. If the Storage Agent manages instances in a non-Unix environment or if you do not use symbolic links, skip this procedure.

Before you load the Oracle Storage Agent Symlink Add-on, perform the following steps:

1. Verify that the Oracle client is installed on the same managed server that contains the Oracle Storage Agent. The Oracle client contains the `loadjava` command, which is required for Oracle Storage Agent Symlink Add-on installation. See “Oracle Storage Agent” on page 35 for information about enabling Java for databases.
2. Verify that the `loadjava` Oracle command is in the path for the instance.
3. Verify that the TNS name for the database instance is properly configured on the Oracle Storage Agent host.
4. Verify that the target instance is Java-enabled.

To load the Oracle Storage Agent Symlink Add-on:

1. From a Unix prompt, switch to the `/bin` directory on the Oracle Storage Agent managed server.

2 Run the `oraclepaminit_symboliclink.sh` file (Unix) with the Oracle URL (user name, password, and instance name) as the argument.

Example:

```
oraclepaminit_symboliclink.sh <user name>/
<password>@<instance_name>
```

3 Repeat this procedure for each instance.

Access Controls

This section describes how to define an access control for each database instance the Oracle Storage Agent will manage. An access control contains values, such as a host name and port number, that direct the Oracle Storage Agent to where a specific instance resides. Table 10-1 describes the access control values you must create before running the Oracle Storage Agent for the first time.

Table 10-1: Oracle Storage Agent Access Controls

ACCESS CONTROL VALUE	DESCRIPTION
Caption	A name used to uniquely identify each access control entry. The default is `Oracle AccessControl`.
Enable support for Symbolic Link	This option allows you to activate Oracle Storage Agent support for symbolic links to Oracle database instances. Use this option only when your Oracle database instances reside on Unix managed servers that use symbolic links to resolve the location of the Oracle database instances.
Host name	The fully qualified domain name where the Oracle instance resides, such as `dev.corp.opsware.com`.
Instance name	The Oracle System Identifier (SID).

Table 10-1: Oracle Storage Agent Access Controls (continued)

ACCESS CONTROL VALUE	DESCRIPTION
JDBC Connect String	The managed server (either DNS or IP address) or server group name where the Oracle database instance is installed.
Password	The Oracle password authorized to access the Oracle database. The default password is `pam`.
Port number	The port that the Oracle listener uses. The default is `1521`. The Storage Agent communicates with the Oracle instance through this port.
User name	The Oracle user name authorized to access the Oracle database. The user name is `oraclepam`.

Opening the Device Access Control Editor

To open the Device Access Control Editor on a certain operating system, perform the following steps:

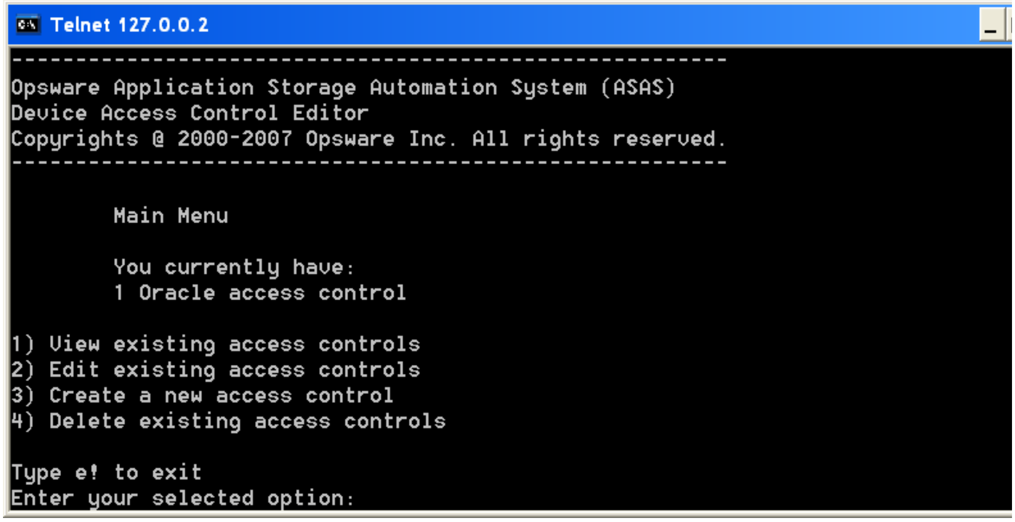
1. From the Navigation pane, select **Opsware Administration ➤ ASAS Agents**.

2. In the ASAS Agents window, select a Storage Agent and then select **Actions ➤ Open**.

3. In the ASAS Agents window for the selected Storage Agent, select **Actions ➤ DeviceAccessControl editor**.

The command line interface opens similar to the following, displaying the main menu for the Device Access Control Editor.

Figure 10-1: Device Access Control Editor Example



```
-----------------------------------------------------
Opsware Application Storage Automation System (ASAS)
Device Access Control Editor
Copyrights @ 2000-2007 Opsware Inc. All rights reserved.
-----------------------------------------------------

        Main Menu

        You currently have:
        1 Oracle access control

1) View existing access controls
2) Edit existing access controls
3) Create a new access control
4) Delete existing access controls

Type e! to exit
Enter your selected option:
```

4 Navigate through the Device Access Control Editor using the commands described in Table 10-2. All commands are case-sensitive.

Table 10-2: Device Access Control Editor Commands

COMMAND	ACTION
`b!`	Returns to the previous menu.
`c!`	Corrects the values entered for an access control. This command is only available from the Verify Values screen after you have entered all access control values for the Storage Agent.
`d!`	Deletes an existing access control.
`e!`	Exits the command line interface.
`r!`	Returns to the main menu.
`s!`	Saves a set of access control values.
`u!`	Undo an access control value by returning to the previous entry. This command is only available while you are entering access control values.

Configuring Access Controls

To configure access controls for the Oracle Storage Agent, perform the following steps:

1. Type `3` to select the `Create a new access control` option and then press Enter.

2. Type the number of the access control type you want to create or edit and then press Enter. For example, if `Oracle` is listed as option 1, type `1` and then press Enter.

3. At the `Caption` prompt, type a caption that identifies this access control and then press Enter. To accept the default value, just press Enter.

   If you are creating more than one access control, enter a caption that uniquely identifies each access control entry, such as Oracle-1, Oracle-2, and so on.

4. At the `Instance name` prompt, type the Oracle System Identifier (SID) and then press Enter.

5. At the `User name` prompt, type `oraclepam` and then press Enter. This is the user name that is authorized to access the Oracle database instance.

6. At the `Password` prompt, type `pam` and then press Enter. This is the password that is authorized to access the Oracle database instance.

7. Re-enter the password and then press Enter.

8. At the `Host name` prompt, specify the fully qualified domain name or IP address where the Oracle instance resides and then press Enter.

9. At the `JDBC Connect String` prompt, type the JDBC connect string (either DNS or IP address) where the Oracle instance is installed and then press Enter.

✓ An Agent must be installed on the managed server where the Oracle instance is also installed.

10. At the `Port number` prompt, type a port number if the Oracle listener uses a port number other than the default (`1521`) and then press Enter. To accept the default value, just press Enter.

11. At the `Enable support for Symbolic Link` prompt (Unix only), type `Y` to activate symbolic link resolution between the Oracle Storage Agent and the Oracle Storage Agent Add-on and then press Enter.

If you do not need to use symbolic link resolution, press Enter to continue.

12 Type `s!` (a lowercase `s`) and then press Enter to save your access control configuration.

Access controls are saved in the `access_control.bin` file in the following directories, depending on the operating system:

`c:\Program Files\Common Files\Opsware\pam-oracle\` (Windows)

Or

`/var/opt/opsware/pam-oracle` (Unix)

13 If you need to create additional access controls, return to the main menu (`r!)` and repeat step 1 through step 12.

Or

Type one of the following options:

`c!` Correct an access control entry.

`b!` Go back to the previous menu.

14 After you have entered access control values for all Oracle instances you want to manage, type `e!` (a lowercase `e`) and then press Enter to exit the Access Control Editor.

Editing Access Controls

You can edit access controls while the Oracle Storage Agent is running or stopped. If you edit access controls while the Storage Agent is running, changes are picked during the next synchronization. To edit access controls for the Oracle Storage Agent, perform the following steps:

1 Open the main menu for the Access Control Editor.

2 Type `2` to select the **`Edit existing access controls`** option and then press Enter.

3 Type the number of the access control type you want to edit and then press Enter.

4 Modify each value as desired. If you want to leave an access control value as is, press Enter.

After you enter the last access control value, a summary is displayed on the screen so that you can verify them.

5. Type `s!` (a lowercase `s`) and then press Enter to save your access control configuration.

   Access controls are saved in the `access_control.bin` file in the following directories, depending on the operating system:

   `c:\Program Files\Common Files\Opsware\pam-oracle\` (Windows)

   Or

   `/var/opt/opsware/pam-oracle` (Unix)

6. If you need to edit additional access controls, return to the main menu (`r!)` and repeat step 2 through step 5.

7. Type `e!`(a lowercase `e`) and press Enter to exit the program.

Deleting Access Controls

You can delete access controls while the Oracle Storage Agent is running or stopped. If you delete access controls while the Storage Agent is running, changes are picked during the next synchronization. To delete access controls for the Oracle Storage Agent, perform the following steps:

1. Open the main menu for the Access Control Editor.

2. Type 4 to select the `Delete existing access controls` option and then press Enter.

3. Type the number of the access control that you want to delete and then press Enter.

4. Type `d!` (a lowercase `d`) and then press Enter to delete the access control.

   The Access Control Editor confirms the deletion.

5. Type `e!` (a lowercase `e`) and then press Enter to exit access control configuration.

Storage Agent Operation

This section describes how to authorize, start, stop, synchronize, and check the discovery status of an Oracle Storage Agent.

Authorizing the Oracle Storage Agent

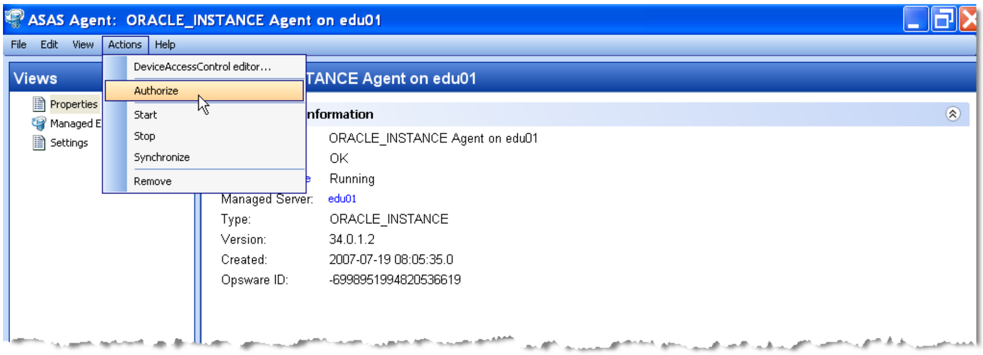
The purpose of authorization is to provide a matching pair of security tokens—one token in the core and the other token on the managed server where the Oracle Storage Agent is deployed. When a Storage Agent is initially deployed to a managed server, you must authorize it so that messages from the Storage Agent are accepted by the core server. As a result of the authorization process, a security token is generated and given to the Storage Agent.

If you are not sure whether the security token in the core and on the managed server match, you can authorize the Oracle Storage Agent repeatedly. A security token mismatch can occur as a result of unintentional editing or removal of tokens.

To authorize an Oracle Storage Agent, perform the following steps:

1. From the Navigation pane, select **Opsware Administration ➤ ASAS Agents**.
2. Open the Oracle Storage Agent that needs to be authorized.
3. From the **Actions** menu, select **Authorize**.

Figure 10-2: Authorize Action for an Oracle Storage Agent



ORACLE_INSTANCE Agent on edu01
OK
Running
Managed Server: edu01
Type: ORACLE_INSTANCE
Version: 34.0.1.2
Created: 2007-07-19 08:05:35.0
Opsware ID: -6998951994820536619

Starting the Oracle Storage Agent

When the Oracle Storage Agent starts for the first time, the agent begins discovering Oracle databases and synchronizing device data. During this process, the Oracle Storage Agent gathers information from various Oracle elements and reports that information to the Web Services Data Access Engine so that the device data for the Oracle databases is synchronized. Depending on the size of the Oracle databases, device synchronization could require several hours. You can start the Storage Agent by using the ASAS Client on a managed server or by running a saved script on a remote managed server.

For performance reasons, you should start the Oracle Storage Agent during off-peak hours.

To start an Oracle Storage Agent on a managed server by using the ASAS Client, perform the following steps:

1. In the ASAS Agent window, select an Oracle Storage Agent and then select **Actions ➤ Open** to display the Oracle Storage Agent browser.
2. Select **Actions ➤ Start**.
3. In the Management Information section click the "Check current state" link to verify that the Storage Agent is Running.

Starting the Oracle Storage Agent on a Remote Windows Server

To start an Oracle Storage Agent 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 OpswareOracleStorageAgent and then select **Action ➤ Start.**

Starting the Oracle Storage Agent on a Remote Unix Server

To start an Oracle Storage Agent on a remote Unix managed server, perform the following steps:

1. Navigate to the `/etc/opt/opsware/startup` directory.
2. Enter the `./pam-oracle start` command to run the saved script that starts the Storage Agent.

   When the Storage Agent starts, it begins the discovery and synchronization process. To monitor the discovery process, see "Checking the Oracle Storage Agent Status" on page 162.

Stopping the Oracle Storage Agent

You must stop the Oracle Storage Agent before you modify Storage Agent settings. See "Storage Agent Settings" on page 163.

You should also stop and then restart the Oracle Agent after any database changes are made. This action does not interfere with any database changes that are in progress.

You can stop the Storage Agent by using the ASAS Client on a managed server or by running a saved script on a remote managed server.

After the Storage Agent is stopped or undeployed, the status does not change. For more information, see “Undeploying a Storage Agent from a Managed Server” on page 42 and “Checking the Oracle Storage Agent Status” on page 162.

To stop an Oracle Storage Agent on a managed server by using the ASAS Client, perform the following steps:

1. In the ASAS Agent window, select an Oracle Storage Agent and then select **Actions ➤ Open** to display the Oracle Storage Agent browser.
2. Select **Actions ➤ Stop**.
3. In the Management Information section click the “Check current state” link to verify that the Storage Agent is Unavailable.

Stopping the Oracle Storage Agent on a Remote Windows Server

To stop an Oracle Storage Agent 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 **OpswareOracleStorageAgent** and then select **Action ➤ Stop.**

Stopping the Oracle Storage Agent on a Remote Unix Server

To stop an Oracle Storage Agent on a remote Unix managed server, perform the following steps:

1. Navigate to the `/etc/opt/opsware/startup` directory.
2. Enter the `./pam-oracle stop` command to run the saved script that stops the Storage Agent.

   When the Storage Agent is stopped, discovery and synchronization processes will not run. See “Synchronizing the Oracle Storage Agent” on page 161.

Synchronizing the Oracle Storage Agent

Synchronization is a request to the Storage Agent to gather the latest data from managed devices and then send this data to the core. Synchronization is performed when the Storage Agent starts and then again at the interval specified in the `pam.properties` file.

Synchronization can occur only when the Storage Agent is running.

If the Storage Agent is stopped or the default schedule does not synchronize the Storage Agent as frequently as you need it to, you must explicitly request a synchronization. For example, you need to explicitly request a synchronization whenever the storage administrator applies changes and needs to immediately see them—instead of waiting for the next scheduled synchronization.

To change the intervals at which the Storage Agent performs synchronization, see "Modifying the Synchronization Schedule" on page 167.

To synchronize an Oracle Storage Agent on a managed server, perform the following steps:

1. From the Navigation pane, select **Opsware Administration ➤ ASAS Agents**.
2. In the ASAS Agent window, select an Oracle Storage Agent and then select **Actions ➤ Open** to display the Oracle Storage Agent browser.
3. Select **Actions ➤ Synchronize** to run the synchronization process. When the synchronization request is successfully completed, a confirmation window displays.
4. Click **OK** to close this window.

Checking the Oracle Storage Agent Status

When the Storage Agent starts, it begins the discovery and synchronization process.

To check Storage Agent discovery status, perform the following steps:

1. From the Navigation pane, select **Opsware Administration ➤ ASAS Agents**.
2. Select a Storage Agent and then click the "Check current state" link in the Properties pane to verify that the Storage Agent is running.

Storage Agent Settings

Storage Agent settings (properties) manage Storage Agent behavior. After you install and configure the Storage Agent, you can adjust these settings in the `pam.properties` file.

Before modifying the `pam.properties` file, make sure the Storage Agent is not running. See “Stopping the Oracle Storage Agent” on page 160.

You can modify the following values in the `properties` file:

- **Log file size and level**. Conserve disk space by modifying the maximum size for log files and level of detail gathered for log messages.
- **Synchronization and polling**. Tune system performance by adjusting the intervals at which synchronizations run.

Contact Hewlett Packard if you need to modify thread pools.

Controlling Log File Sizes and Logging Levels

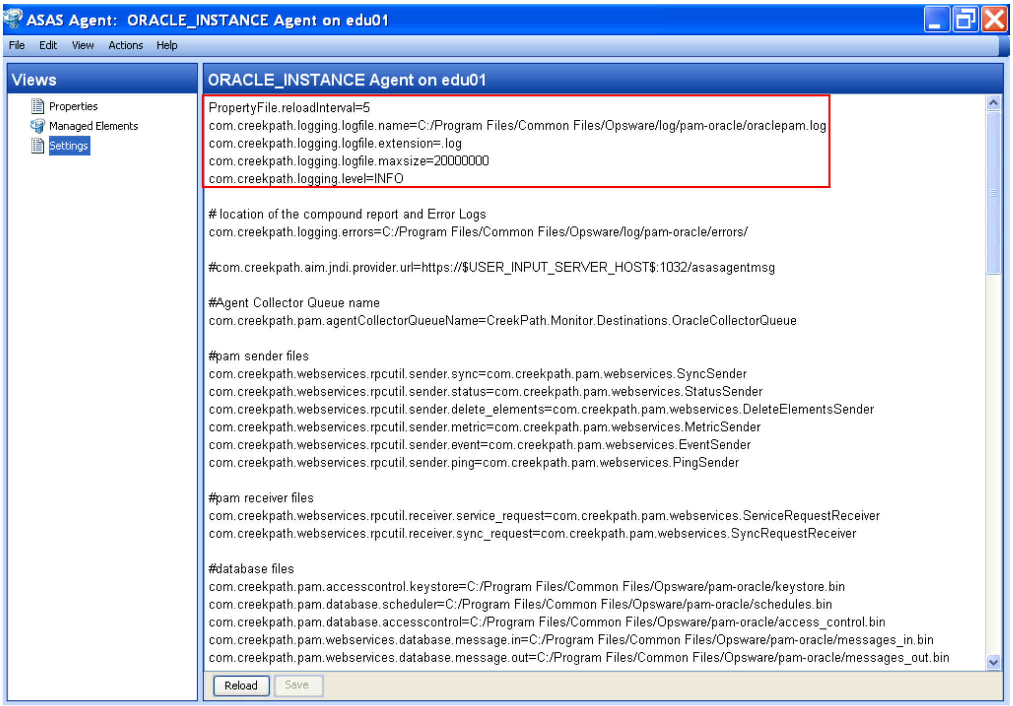
To conserve disk space and control the types of log messages that ASAS gathers, you can adjust the maximum size of log files and the logging level in the log file settings.

To modify the log file settings, perform the following steps:

1. Stop the Storage Agent.
2. In the ASAS Agent window, select a Storage Agent.
3. Select **Actions ➤ Open** to display the Storage Agent browser.
4. From the Views pane, select Settings to display the log file settings in the content pane.

5 Change any of the log file settings. For a list of these parameters and their descriptions, see Table 10-3 on page 165.

Figure 10-3: Storage Agent Log File Settings


ASAS Agent: ORACLE_INSTANCE Agent on edu01
File
Edit
View
Actions
Help
Views
Properties
Managed Elements
Settings
ORACLE_INSTANCE Agent on edu01
Reload
Save

```
PropertyFile.reloadInterval=5
com.creekpath.logging.logfile.name=C:/Program Files/Common Files/Opsware/log/pam-oracle/oraclepam.log
com.creekpath.logging.logfile.extension=.log
com.creekpath.logging.logfile.maxsize=20000000
com.creekpath.logging.level=INFO

# location of the compound report and Error Logs
com.creekpath.logging.errors=C:/Program Files/Common Files/Opsware/log/pam-oracle/errors/

#com.creekpath.aim.jndi.provider.url=https://$USER_INPUT_SERVER_HOST$:1032/asasagentmsg

#Agent Collector Queue name
com.creekpath.pam.agentCollectorQueueName=CreekPath.Monitor.Destinations.OracleCollectorQueue

#pam sender files
com.creekpath.webservices.rpcutil.sender.sync=com.creekpath.pam.webservices.SyncSender
com.creekpath.webservices.rpcutil.sender.status=com.creekpath.pam.webservices.StatusSender
com.creekpath.webservices.rpcutil.sender.delete_elements=com.creekpath.pam.webservices.DeleteElementsSender
com.creekpath.webservices.rpcutil.sender.metric=com.creekpath.pam.webservices.MetricSender
com.creekpath.webservices.rpcutil.sender.event=com.creekpath.pam.webservices.EventSender
com.creekpath.webservices.rpcutil.sender.ping=com.creekpath.pam.webservices.PingSender

#pam receiver files
com.creekpath.webservices.rpcutil.receiver.service_request=com.creekpath.pam.webservices.ServiceRequestReceiver
com.creekpath.webservices.rpcutil.receiver.sync_request=com.creekpath.pam.webservices.SyncRequestReceiver

#database files
com.creekpath.pam.accesscontrol.keystore=C:/Program Files/Common Files/Opsware/pam-oracle/keystore.bin
com.creekpath.pam.database.scheduler=C:/Program Files/Common Files/Opsware/pam-oracle/schedules.bin
com.creekpath.pam.database.accesscontrol=C:/Program Files/Common Files/Opsware/pam-oracle/access_control.bin
com.creekpath.pam.webservices.database.message.in=C:/Program Files/Common Files/Opsware/pam-oracle/messages_in.bin
com.creekpath.pam.webservices.database.message.out=C:/Program Files/Common Files/Opsware/pam-oracle/messages_out.bin
```

6 Click **Save** to save your settings.

Or

Click **Reload** to restore the settings to their previous values—before you made changes.

Log File Settings

The following table describes the Storage Agent log file settings you can change.

Table 10-3: Log File Settings for Storage Agent

PARAMETER	DESCRIPTION
`logfile.name`	Specifies the directory for all log files and compound reports for errors encountered during synchronization, such as `/var/log/opsware/pam-oracle/oraclepam.log`. This directory is created after ASAS begins gathering logging information. **Note:** If you change the default logging path on a Solaris system and you also created a server group and User ID, you must change the ownership of the new log directory using the `chown` command.
`logfile.extension`	Specifies the extension for log file names.
`logfile.maxsize`	Controls the maximum size of each log file (in bytes). By default, the Storage Agent populates a log file until it reaches its maximum capacity (20 MB), then it wraps any remaining log information into a new log file. The Storage Agent can create up to 10 individual log files before it overwrites previous log files.

Table 10-3: Log File Settings for Storage Agent (continued)

PARAMETER	DESCRIPTION
`logging.level`	Controls the type of messages gathered or turns off logging. Each subsequent level also includes the logging information that precedes it, such as INFO includes logging information for SEVERE and WARNING. Enter one of the following values: • OFF: Does not collect logging information. • SEVERE: Collects messages indicating a serious failure. • WARNING: Collects exception messages. • INFO (default): Collects informational messages, such as storage volume creation. • CONFIG: Collects static configuration messages. • FINE: Provides tracing information; used for system debugging. • FINER: Provides fairly detailed tracing information; used for system debugging. • FINEST: Provides highly detailed tracing information; used for system debugging. **Note**: The FINE, FINER, and FINEST settings affect Storage Agent performance and scalability. You should only use these settings if HP Support has instructed you to do so.

Modifying the Synchronization Schedule

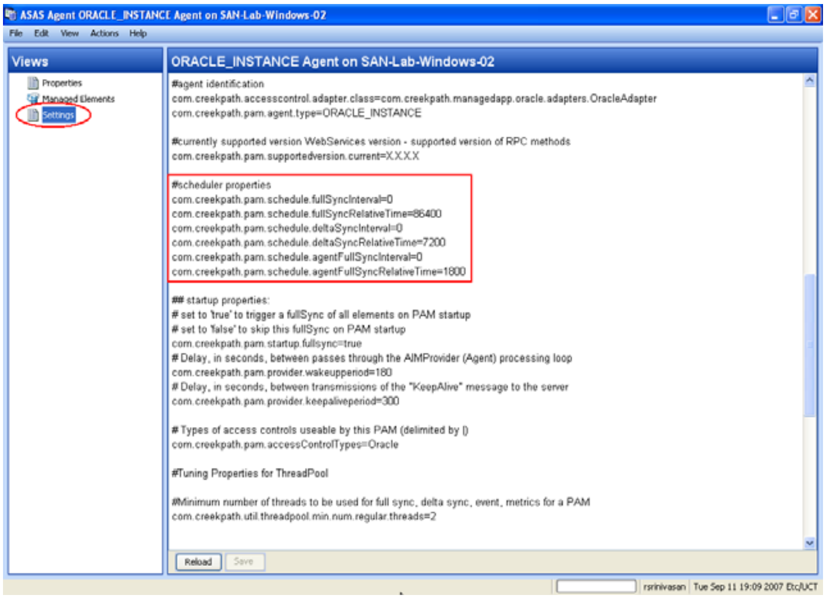
To change the intervals at which the Storage Agent performs synchronization, you can modify the values in the scheduler properties. Synchronization is a process by which the Storage Agent gathers data from the Oracle databases and then transfers that data to the Domain Data Store, so that the Domain Data Store and Oracle databases are synchronized.

Synchronization is performed when the Storage Agent starts and then again at the interval specified in the `pam.properties` file. For example, if you initially start the Storage Agent at midnight and the full synchronization is scheduled to run every 12 hours, the full synchronization always runs at noon and at midnight. As needed, you can run immediate synchronization requests. See “Synchronizing the Oracle Storage Agent” on page 161.

To modify synchronization intervals, perform the following steps:

1. Stop the Storage Agent.
2. From the Oracle Storage Agent browser, from the Views pane, select **Settings**.
3. In the content pane, locate the lines for #scheduler properties, as Figure 10-4 illustrates.

Figure 10-4: Storage Agent Schedule Settings



ASAS Agent ORACLE_INSTANCE Agent on SAN-Lab-Windows-02
File Edit View Actions Help
Views
Properties
Managed Elements
Settings
ORACLE_INSTANCE Agent on SAN-Lab-Windows-02
Reload
Save
rsrinivasan
Tue Sep 11 19:09 2007 Etc/UCT

```
#agent identification
com.creekpath.accesscontrol.adapter.class=com.creekpath.managedapp.oracle.adapters.OracleAdapter
com.creekpath.pam.agent.type=ORACLE_INSTANCE

#currently supported version WebServices version - supported version of RPC methods
com.creekpath.pam.supportedversion.current=X.X.X.X

#scheduler properties
com.creekpath.pam.schedule.fullSyncInterval=0
com.creekpath.pam.schedule.fullSyncRelativeTime=86400
com.creekpath.pam.schedule.deltaSyncInterval=0
com.creekpath.pam.schedule.deltaSyncRelativeTime=7200
com.creekpath.pam.schedule.agentFullSyncInterval=0
com.creekpath.pam.schedule.agentFullSyncRelativeTime=1800

## startup properties:
# set to 'true' to trigger a fullSync of all elements on PAM startup
# set to 'false' to skip this fullSync on PAM startup
com.creekpath.pam.startup.fullsync=true
# Delay, in seconds, between passes through the AIMProvider (Agent) processing loop
com.creekpath.pam.provider.wakeupperiod=180
# Delay, in seconds, between transmissions of the "KeepAlive" message to the server
com.creekpath.pam.provider.keepaliveperiod=300

# Types of access controls useable by this PAM (delimited by |)
com.creekpath.pam.accessControlTypes=Oracle

#Tuning Properties for ThreadPool

#Minimum number of threads to be used for full sync, delta sync, event, metrics for a PAM
com.creekpath.util.threadpool.min.num.regular.threads=2
```

4. To change the metrics and synchronization schedule, enter new times (in seconds) in the appropriate fields. For a list of these parameters and their descriptions, see Table 10-4 on page 168.

5. If desired, you can change the startup setting so that full synchronizations do not occur when the Storage Agent starts. Locate the following field and change the value from `true` to `false`:

   ```
   com.creekpath.pam.startup.fullsync=false
   ```

6. Click **Save** to save your changes.

   Or

   Click **Reload** to restore the settings to their previous values—before you made changes.

Scheduler Parameter Settings

The following table describes the Storage Agent scheduler parameter settings you can change.

Table 10-4: Scheduler Parameters

PARAMETER	DESCRIPTION
`fullSyncInterval` `fullSyncRelativeTime`	Controls full synchronizations, in which all data is gathered since the last synchronization: **Interval field**: Turns synchronizations on and off. Enter `-1` to turn off synchronizations. Enter `0` to turn on synchronizations. • **RelativeTime field**: Controls the interval at which synchronization occurs (in seconds). To improve scalability of the Manager and Management Server, adjust the Relative Time to a higher value so that synchronizations occur less frequently.

Table 10-4: Scheduler Parameters (continued)

PARAMETER	DESCRIPTION
`deltaSyncInterval` `deltaSyncRelativeTime`	Controls delta synchronizations, in which modified data is gathered since the last synchronization: • **Interval field**: Turns synchronizations on and off. Enter `-1` to turn off synchronizations. Enter `0` to turn on synchronizations. • **RelativeTime field**: Controls the interval at which synchronization occurs (in seconds). To improve scalability of the Manager and Management Server, adjust the Relative Time to a higher value so that synchronizations occur less frequently.

ASAS does not capture events and metrics.

Chapter 11: Symmetrix Storage Agent

IN THIS CHAPTER

This section discusses the following topics:

- Access Controls
- Storage Agent Operation
- Storage Agent Settings

Access Controls

This section describes how to configure access controls so that the Storage Agent can gather information from the EMC Symmetrix Storage array. To enable this process, you must define an access control for each array the Storage Agent will manage. An access control contains values, such as the array's controller location of the database bin file of the vendor server, which allows the Symmetrix Storage Agent to communicate with the array. Table 11-1 describes the access control values you must create before running the Symmetrix Storage Agent for the first time.

Table 11-1: Symmetrix Storage Agent Access Controls

ACCESS CONTROL VALUE	DESCRIPTION
Caption	A name used to uniquely identify each access control entry. (If the Storage Agent will be managing more than one array, you must create more than one access control, each with a unique caption.)
Init db filename	The default location of the database bin file for the EMC Solutions Enabler.

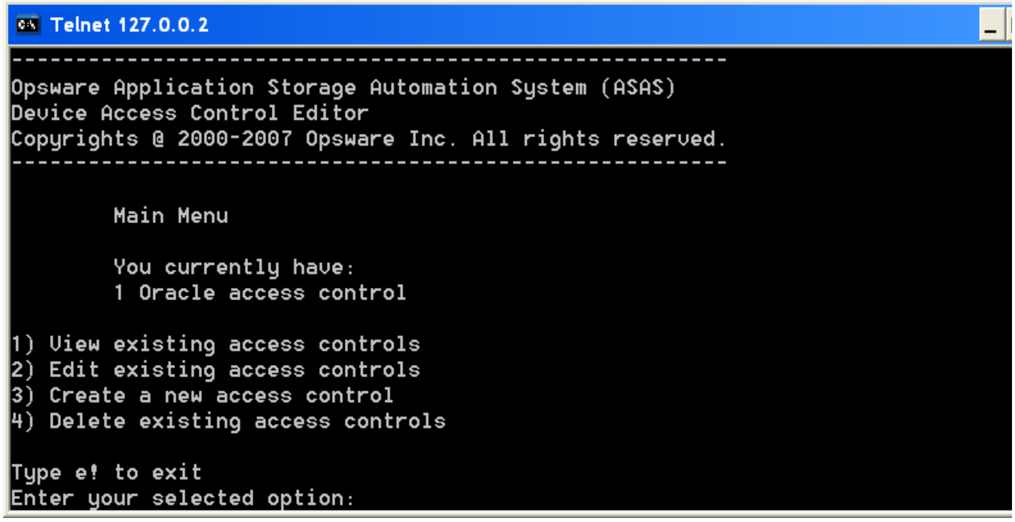
Opening the Device Access Control Editor

To open the Device Access Control Editor on a certain operating system, perform the following steps:

1. From the Navigation pane, select **Opsware Administration ➤ ASAS Agents**.
2. In the ASAS Agents window, select a Storage Agent and then select **Actions ➤ Open**.
3. In the ASAS Agents window for the selected Storage Agent, select **Actions ➤ DeviceAccessControl editor**.

   The command line interface opens similar to the following, displaying the main menu for the Device Access Control Editor.

Figure 11-1: Device Access Control Editor Example



```
--------------------------------------------------------
Opsware Application Storage Automation System (ASAS)
Device Access Control Editor
Copyrights @ 2000-2007 Opsware Inc. All rights reserved.
--------------------------------------------------------

        Main Menu

        You currently have:
        1 Oracle access control

1) View existing access controls
2) Edit existing access controls
3) Create a new access control
4) Delete existing access controls

Type e! to exit
Enter your selected option:
```

4. Navigate through the Device Access Control Editor using the commands described in Table 11-2. All commands are case-sensitive.

Table 11-2: Device Access Control Editor Commands

COMMAND	ACTION
b!	Returns to the previous menu.
c!	Corrects the values entered for an access control. This command is only available from the Verify Values screen after you have entered all access control values for the Storage Agent.

Table 11-2: Device Access Control Editor Commands (continued)

COMMAND	ACTION
`d!`	Deletes an existing access control.
`e!`	Exits the command line interface.
`r!`	Returns to the main menu.
`s!`	Saves a set of access control values.
`u!`	Undo an access control value by returning to the previous entry. This command is only available while you are entering access control values.

Configuring Access Controls

To configure access controls for the EMC Symmetrix Storage Agent, perform the following steps:

1. Type `3` to select the `Create a new access control` option and then press Enter.

2. Type the number of the access control type you want to create or edit and then press Enter. For example, if `EMC Symmetrix` is listed as option 1, type `1` and then press Enter.

3. At the `Caption` prompt, type a caption that identifies this access control and then press Enter. To accept the default value, just press Enter.

   If you are creating more than one access control, enter a caption that uniquely identifies each access control entry, such as Sym-1, Sym-2, and so on.

4. At the `Init db filename` prompt, type the directory path for the location of the database bin file (if you installed Solutions Enabler in a directory other than the default) and press Enter. To accept the default value, just press Enter.

5. Type `s!` (a lowercase `s`) and then press Enter to save your access control configuration.

Access controls are saved in the `access_control.bin` file in the following directories, depending on the operating system:

`c:\Program Files\Common Files\Opsware\pam-symmetrix\` (Windows)

Or

`/var/opt/opsware/pam-symmetrix` (Unix)

6. If you need to create additional access controls, return to the main menu (`r!`) and repeat step 2 through step 5.

   OR

   Type one of the following options:

   `c!` Correct an access control entry.

   `b!` Go back to the previous menu.

7. After you have entered access control values for all Symmetrix arrays you want to manage, type `e!` (a lowercase `e`) and then press Enter to exit the Access Control Editor.

Editing Access Controls

You can edit access controls while the Symmetrix Storage Agent is running or stopped. If you edit access controls while the Storage Agent is running, changes will be picked during the next synchronization. To edit access controls for the Symmetrix Storage Agent, perform the following steps:

1. Open the Device Access Control Editor.
2. Type `2` to select the `Edit existing access controls` option and then press Enter.
3. Type the number of the access control type you want to edit and then press Enter.
4. Modify each value as desired. If you want to leave an access control value as is, press Enter.

   After you enter the last access control value, a summary is displayed on the screen so that you can verify them.
5. Type `s!` (a lowercase `s`) and then press Enter to save your access control configuration.

Access controls are saved in the `access_control.bin` file in the following directories, depending on the operating system:

`c:\Program Files\Common Files\Opsware\pam-symmetrix` (Windows)

Or

`/var/opt/opsware/pam-symmetrix` (Unix)

6. If you need to edit additional access controls, return to the main menu (`r!)` and repeat step 2 through step 5.
7. Type `e!`(a lowercase `e`) and press Enter to exit the program.

Deleting Access Controls

You can delete access controls while the Symmetrix Storage Agent is running or stopped. If you edit access controls while the Storage Agent is running, changes are picked during the next synchronization. To delete access controls for the Symmetrix Storage Agent, perform the following steps:

1. Open the main menu for the Access Control Editor.
2. Type 4 to select the `Delete existing access controls` option and then press Enter.
3. Type the number of the access control type you want to delete and then press Enter.
4. Type the number of the access control that you want to delete and then press Enter.
5. Type `d!` (a lowercase `d`) and then press Enter to delete the access control.

   The Access Control Editor confirms the deletion.
6. Type `e!` (a lowercase `e`) and then press Enter to exit access control configuration.

Storage Agent Operation

This section describes how to authorize, start, stop, synchronize, and check the discovery status of a Symmetrix Storage Agent.

Authorizing the Symmetrix Storage Agent

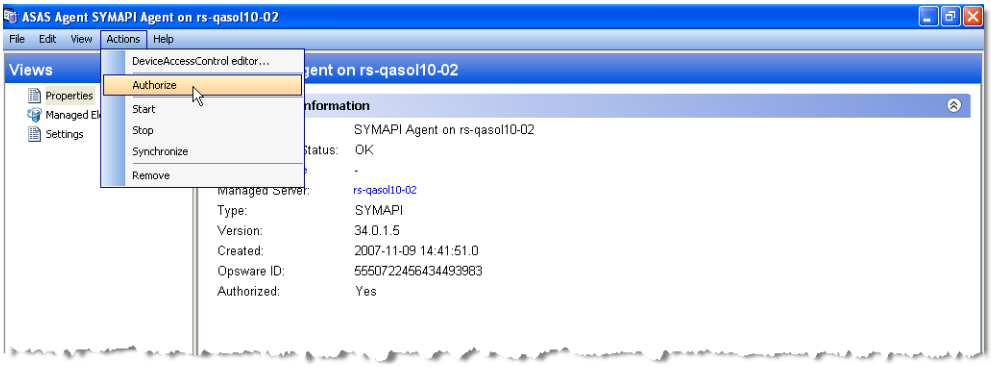
The purpose of authorization is to provide a matching pair of security tokens—one token in the core and the other token on the managed server where the Symmetrix Storage Agent is deployed. When a Storage Agent is initially deployed to a managed server, you must authorize it so that messages from the Storage Agent will be accepted by the core server. As a result of the authorization process, a security token is generated and given to the Storage Agent.

If you are not sure whether the security token in the core and on the managed server match, you can authorize the Symmetrix Storage Agent repeatedly. A security token mismatch can occur as a result of unintentional editing or removal of tokens.

To authorize a Symmetrix Storage Agent, perform the following steps:

1. From the Navigation pane, select **Opsware Administration ➤ ASAS Agents**.
2. Open the Symmetrix Storage Agent that needs to be authorized.
3. From the **Actions** menu, select **Authorize**.

Figure 11-2: Authorize Action for a Symmetrix Storage Agent



ASAS Agent SYMAPI Agent on rs-qasol10-02

SYMAPI Agent on rs-qasol10-02
Status: OK
-
Managed Server: rs-qasol10-02
Type: SYMAPI
Version: 34.0.1.5
Created: 2007-11-09 14:41:51.0
Opsware ID: 5550722456434493983
Authorized: Yes

Starting the Symmetrix Storage Agent

When the Symmetrix Storage Agent starts for the first time, the agent begins discovering and synchronizing device data. During this process, the Symmetrix Storage Agent gathers information from various Oracle elements and reports that information to the Web Services Data Access Engine so that the device data for the Symmetrix arrays is synchronized. Depending on the size of the Symmetrix arrays, device synchronization could require several hours. You can start the Storage Agent by using the ASAS Client on a managed server or by running a saved script on a remote managed server.

For performance reasons, you should start the Symmetrix Storage Agent during off-peak hours.

To start a Symmetrix Storage Agent on a managed server by using the ASAS Client, perform the following steps:

1. From the Navigation pane, select **Opsware Administration ➤ ASAS Agents**.
2. In the ASAS Agent window, select a Symmetrix Storage Agent and then select **Actions ➤ Open** to display the Symmetrix Storage Agent browser.
3. Select **Actions ➤ Start**.
4. In the Management Information section click “Check current state” link to verify that the Storage Agent is running.

Starting the Symmetrix Storage Agent on a Remote Windows Server

To start a Symmetrix Storage Agent 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 OpswareSymmetrixStorageAgent and then select **Action ➤ Start**.

Starting the Symmetrix Storage Agent on a Remote Unix Server

To start a Symmetrix Storage Agent on a remote Unix server, perform the following steps:

1. Navigate to the `/etc/opt/opsware/startup` directory.
2. Enter the `./pam-symmetrix start` command to run the saved script that starts the Storage Agent.

   When the Storage Agent starts, it begins the discovery and synchronization process. To monitor the discovery process, see “Checking the Symmetrix Storage Agent Status” on page 179.

Stopping the Symmetrix Storage Agent

You must stop the Symmetrix Storage Agent before you modify Storage Agent settings. See “Storage Agent Settings” on page 181.

To stop a Symmetrix Storage Agent on a managed server by using the ASAS Client, perform the following steps:

1. From the Navigation pane, select **Opsware Administration ➤ ASAS Agents**.
2. In the ASAS Agent window, select a Symmetrix Storage Agent and then select **Actions ➤ Open** to display the Symmetrix Storage Agent browser.

3. Select **Actions ➤ Stop**.

4. In the Management Information section click the “Check current state” link to verify that the Storage Agent is Unavailable.

Stopping the Symmetrix Storage Agent on a Remote Windows Server

To stop a Symmetrix Storage Agent 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 **OpswareSymmetrixStorageAgent** and then select **Action ➤ Stop.**

Stopping the Symmetrix Storage Agent on a Remote Unix Server

To stop a Symmetrix Storage Agent on a remote Unix managed server, perform the following steps:

1. Navigate to the `/etc/opt/opsware/startup` directory.

2. Enter the `./pam-symmetrix stop` command to run the saved script that stops the Storage Agent.

   When the Storage Agent is stopped, discovery and synchronization processes will not run. See “Synchronizing the Symmetrix Storage Agent” on page 178.

Synchronizing the Symmetrix Storage Agent

Synchronization is a request to the Storage Agent to gather the latest data from managed devices and then send this data to the core. Synchronization is performed when the Storage Agent starts and then again at the interval specified in the `pam.properties` file.

Synchronization can occur only when the Storage Agent is running.

If the Storage Agent is stopped or the default schedule does not synchronize the Storage Agent as frequently as you need it to, you must explicitly request a synchronization. For example, you need to explicitly request a synchronization whenever the storage administrator applies changes and needs to immediately see them–instead of waiting for the next scheduled synchronization.

To change the intervals at which the Storage Agent performs synchronization, see “Modifying the Synchronization Schedule” on page 185.

To synchronize a Symmetrix Storage Agent on a managed server, perform the following steps:

1. From the Navigation pane, select **Opsware Administration ➤ ASAS Agents**.
2. In the ASAS Agent window, select a Symmetrix Storage Agent and then select **Actions ➤ Open** to display the Symmetrix Storage Agent browser.
3. Select **Actions ➤ Synchronize** to run the synchronization process. When the synchronization request is successfully completed, a confirmation window displays.
4. Click **OK** to close this window.

Checking the Symmetrix Storage Agent Status

When the Storage Agent starts, it begins the discovery and synchronization process.

To check Storage Agent discovery status, perform the following steps:

1. From the Navigation pane, select **Opsware Administration ➤ ASAS Agents**.
2. In the content pane, view the Last Received Status column for the status of the tree structure in the left panel.
3. Select the Symmetrix Storage Agent and make sure the Properties tab is selected in the right display panel. The Last Received Status indicates the state of the array, such as OK or offline.

Modifying the EMC Solutions Enabler (SYMCLI) Path

The `pam.properties` file includes a setting that instructs the EMC Symmetrix Storage array where to locate the EMC Solutions Enabler (SYMCLI). If you upgrade your version of the SYMCLI, you need to verify the path to the SYMCLI in the `pam.properties` file and update the path as necessary.

To modify the EMC Solutions Enabler (SYMCLI) path, perform the following steps:

1. Make sure the Storage Agent is not running. See “Stopping the Symmetrix Storage Agent” on page 177.

   In a text editor, open the `pam.properties` file in the following directories, depending on the operating system:

`c:\Program Files\Common Files\Opsware\etc\pam-symmetrix` (Windows)

Or

`/etc/opt/opsware/etc/pam-symmetrix` (Unix)

2. Locate the following field and enter a new path for the SYMCLI:

   `com.creekpath.devices.symmetrix.symcli= <SYMCLI Path>`

3. Save the `pam.properties` file.

Modifying Performance Parameters

The `pam.properties` file provides a parameter enabling you to allow separate bin files for each array to increase the general performance of the Storage Agent.

The default setting for these parameters is **false**. If you set these parameters to **true**, you cannot change them back to false.

To improve performance, perform the following steps:

1. Make sure the Storage Agent is not running. See "Stopping the Symmetrix Storage Agent" on page 177.

2. In a text editor, open the `pam.properties` file in the following directories, depending on the operating system:

   `c:\Program Files\Common Files\Opsware\etc\pam-symmetrix` (Windows)

   Or

   `/etc/opt/opsware/etc/pam-symmetrix` (Unix)

3. To determine whether the Storage Agent should use a single bin file or use multiple bin files to communicate with arrays, change the following parameter to true: `com.creekpath.pam.symmetrix.use.multiple.infiledb=true`

   When you set this parameter to true, the Storage Agent creates a separate bin file for each managed array. To avoid communication collisions, you should maintain four gatekeepers and four semaphores for common processes, and one additional gatekeeper and one additional semaphore for each ServiceRequest that will run concurrently. For example, for six concurrently running ServiceRequests, you need ten gatekeepers and ten semaphores (six plus four for the common processes).

4. Save the `pam.properties` file.

Storage Agent Settings

Storage Agent settings (properties) manage Storage Agent behavior. After you install and configure the Storage Agent, you can adjust these settings in the `pam.properties` file.

Before modifying the `pam.properties` file, make sure the Storage Agent is not running. See “Stopping the Symmetrix Storage Agent” on page 177.

You can modify the following values in the `properties` file:

- **Log file size and level**. Conserve disk space by modifying the maximum size for log files and level of detail gathered for log messages.
- **Synchronization and polling**. Tune system performance by adjusting the intervals at which synchronizations run.

Contact Hewlett Packard if you need to modify thread pools.

Controlling Log File Sizes and Logging Levels

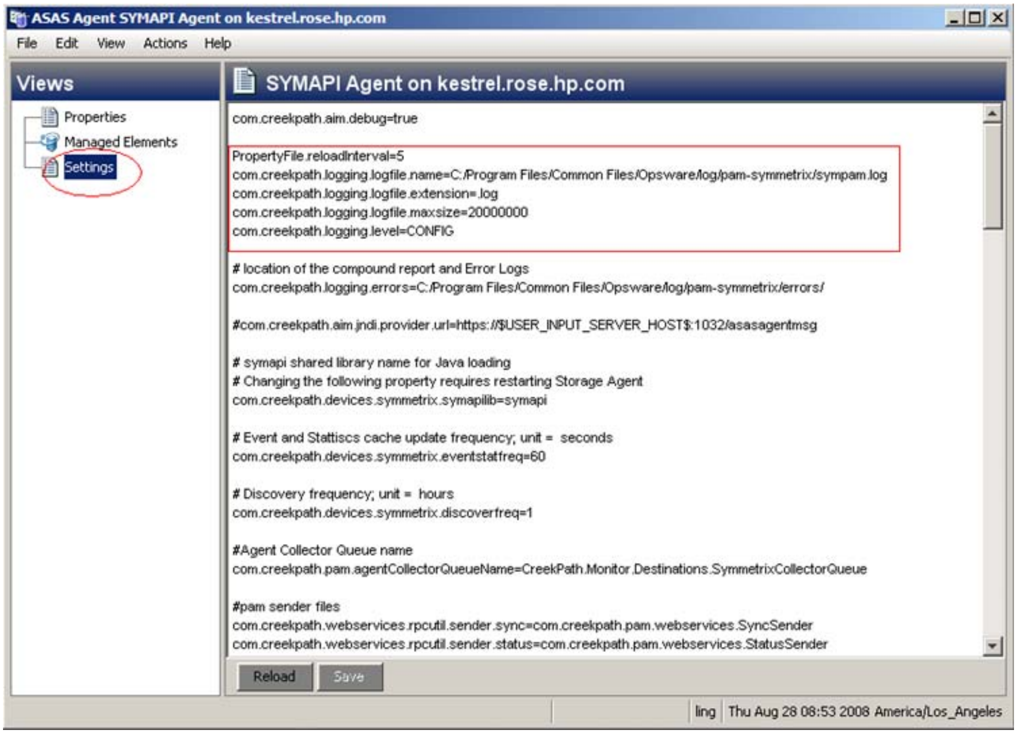
To conserve disk space and control the types of log messages that ASAS gathers, you can adjust the maximum size of log files and the logging level in the log file settings.

To modify the log file settings, perform the following steps:

1. Stop the Storage Agent.
2. In the ASAS Agent window, select a Storage Agent.
3. Select **Actions ➤ Open** to display the Storage Agent browser.
4. From the Views pane, select Settings to display the log file settings in the content pane.

5 Change any of the log file settings. For a list of these parameters and their descriptions, see Table 11-3 on page 183.

Figure 11-3: Storage Agent Log File Settings



ASAS Agent SYMAPI Agent on kestrel.rose.hp.com
File
Edit
View
Actions
Help
Views
Properties
Managed Elements
Settings
SYMAPI Agent on kestrel.rose.hp.com
Reload
Save
ling
Thu Aug 28 08:53 2008 America/Los_Angeles

```
com.creekpath.aim.debug=true

PropertyFile.reloadInterval=5
com.creekpath.logging.logfile.name=C:/Program Files/Common Files/Opsware/log/pam-symmetrix/sympam.log
com.creekpath.logging.logfile.extension=.log
com.creekpath.logging.logfile.maxsize=20000000
com.creekpath.logging.level=CONFIG

# location of the compound report and Error Logs
com.creekpath.logging.errors=C:/Program Files/Common Files/Opsware/log/pam-symmetrix/errors/

#com.creekpath.aim.jndi.provider.url=https://$USER_INPUT_SERVER_HOST$:1032/asasagentmsg

# symapi shared library name for Java loading
# Changing the following property requires restarting Storage Agent
com.creekpath.devices.symmetrix.symapilib=symapi

# Event and Stattiscs cache update frequency; unit =  seconds
com.creekpath.devices.symmetrix.eventstatfreq=60

# Discovery frequency; unit =  hours
com.creekpath.devices.symmetrix.discoverfreq=1

#Agent Collector Queue name
com.creekpath.pam.agentCollectorQueueName=CreekPath.Monitor.Destinations.SymmetrixCollectorQueue

#pam sender files
com.creekpath.webservices.rpcutil.sender.sync=com.creekpath.pam.webservices.SyncSender
com.creekpath.webservices.rpcutil.sender.status=com.creekpath.pam.webservices.StatusSender
```

6 Click **Save** to save your settings.

Or

Click **Reload** to restore the settings to their previous values—before you made changes.

7 Start the Storage Agent.

Log File Settings

The following table describes the Storage Agent log file settings you can change.

Table 11-3: Log File Settings for Storage Agent

PARAMETER	DESCRIPTION
`logfile.name`	Specifies the directory for all log files and compound reports for errors encountered during synchronization, such as `/var/log/opsware/pam-symmetrix/sympam.log`. This directory is created after ASAS begins gathering logging information. **Note:** If you change the default logging path on a Solaris system and you also created a server group and User ID, you must change the ownership of the new log directory using the `chown` command.
`logfile.extension`	Specifies the extension for log file names.
`logfile.maxsize`	Controls the maximum size of each log file (in bytes). By default, the Storage Agent populates a log file until it reaches its maximum capacity (20 MB), then it will wrap any remaining log information into a new log file. The Storage Agent can create up to 10 individual log files before it overwrites previous log files.

Table 11-3: Log File Settings for Storage Agent (continued)

PARAMETER	DESCRIPTION
`logging.level`	Controls the type of messages gathered or turns off logging. Each subsequent level also includes the logging information that precedes it, such as INFO includes logging information for SEVERE and WARNING. Enter one of the following values: • OFF: Does not collect logging information. • SEVERE: Collects messages indicating a serious failure. • WARNING: Collects exception messages. • INFO (default): Collects informational messages, such as storage volume creation. • CONFIG: Collects static configuration messages. • FINE: Provides tracing information; used for system debugging. • FINER: Provides fairly detailed tracing information; used for system debugging. • FINEST: Provides highly detailed tracing information; used for system debugging. **Note**: The FINE, FINER, and FINEST settings affect Storage Agent performance and scalability. You should only use these settings if HP Support has instructed you to do so.

Modifying the Synchronization Schedule

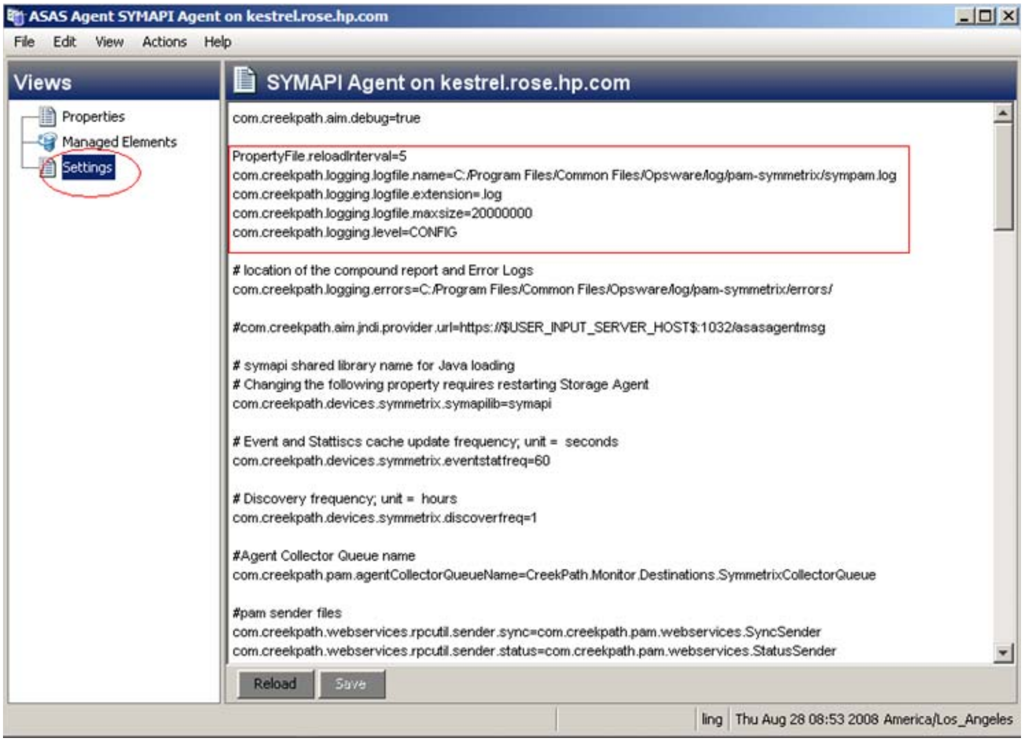
To change the intervals at which the Storage Agent performs synchronization, you can modify the values in the scheduler properties. Synchronization is a process by which the Storage Agent gathers data from the Symmetrix arrays and then transfers that data to the Domain Data Store, so that the Domain Data Store and Symmetrix arrays are synchronized.

Synchronization is performed when the Storage Agent starts and then again at the interval specified in the `pam.properties` file. For example, if you initially start the Storage Agent at midnight and the full synchronization is scheduled to run every 12 hours, the full synchronization always runs at noon and at midnight. As needed, you can run immediate synchronization requests. See “Synchronizing the Symmetrix Storage Agent” on page 178.

To modify synchronization intervals, perform the following steps:

1. Stop the Storage Agent.
2. From the Symmetrix Storage Agent browser, from the Views pane, select **Settings**.
3. In the content pane, locate the lines for #scheduler properties, as Figure 11-4 illustrates.

Figure 11-4: Storage Agent Schedule Settings



ASAS Agent SYMAPI Agent on kestrel.rose.hp.com
File
Edit
View
Actions
Help
Views
Properties
Managed Elements
Settings
SYMAPI Agent on kestrel.rose.hp.com
Reload
Save
ling
Thu Aug 28 08:53 2008 America/Los_Angeles

```
com.creekpath.aim.debug=true

PropertyFile.reloadInterval=5
com.creekpath.logging.logfile.name=C:/Program Files/Common Files/Opsware/log/pam-symmetrix/sympam.log
com.creekpath.logging.logfile.extension=.log
com.creekpath.logging.logfile.maxsize=20000000
com.creekpath.logging.level=CONFIG

# location of the compound report and Error Logs
com.creekpath.logging.errors=C:/Program Files/Common Files/Opsware/log/pam-symmetrix/errors/

#com.creekpath.aim.jndi.provider.url=https://$USER_INPUT_SERVER_HOST$:1032/asasagentmsg

# symapi shared library name for Java loading
# Changing the following property requires restarting Storage Agent
com.creekpath.devices.symmetrix.symapilib=symapi

# Event and Stattiscs cache update frequency; unit =  seconds
com.creekpath.devices.symmetrix.eventstatfreq=60

# Discovery frequency; unit =  hours
com.creekpath.devices.symmetrix.discoverfreq=1

#Agent Collector Queue name
com.creekpath.pam.agentCollectorQueueName=CreekPath.Monitor.Destinations.SymmetrixCollectorQueue

#pam sender files
com.creekpath.webservices.rpcutil.sender.sync=com.creekpath.pam.webservices.SyncSender
com.creekpath.webservices.rpcutil.sender.status=com.creekpath.pam.webservices.StatusSender
```

4 To change the metrics and synchronization schedule, enter new times (in seconds) in the appropriate fields. For a list of these parameters and their descriptions, see Table 11-4 on page 187.

5 If desired, you can change the startup setting so that full synchronizations do not occur when the Storage Agent starts. Locate the following field and change the value from `true` to `false`:

```
com.creekpath.pam.startup.fullsync=false
```

6 Click **Save** to save your changes.

Or

Click **Reload** to restore the settings to their previous values—before you made changes.

7 Start the Storage Agent.

Scheduler Parameter Settings

The following table describes the Storage Agent scheduler parameter settings you can change.

Table 11-4: Scheduler Parameters

PARAMETER	DESCRIPTION
`fullSyncInterval` `fullSyncRelativeTime`	Controls full synchronizations, in which all data is gathered since the last synchronization: **Interval field**: Turns synchronizations on and off. Enter `-1` to turn off synchronizations. Enter `0` to turn on synchronizations. • **RelativeTime field**: Controls the interval at which synchronization occurs (in seconds). To improve scalability of the Manager and Management Server, adjust the Relative Time to a higher value so that synchronizations occur less frequently.
`deltaSyncInterval` `deltaSyncRelativeTime`	Controls delta synchronizations, in which modified data is gathered since the last synchronization: • **Interval field**: Turns synchronizations on and off. Enter `-1` to turn off synchronizations. Enter `0` to turn on synchronizations. • **RelativeTime field**: Controls the interval at which synchronization occurs (in seconds). To improve scalability of the Manager and Management Server, adjust the Relative Time to a higher value so that synchronizations occur less frequently.

ASAS does not capture events and metrics.

Index