

HP Server Automation

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

Software Version: 7.50

Content Migration 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

© Copyright 2000-2008 Hewlett-Packard Development Company, L.P.

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

Chapter 1: Migrating SA Content to Version 7.50	7
Content Migration Overview	7
Software Migration Tool Overview	8
Content Migration Process	8
Full Migration	10
Complete Migration	13
Migration of Software Installation Dependencies	13
Configuration Tracking in SA 7.50	13
Prerequisite for the Software Migration Tool	14
How to Run the Software Migration Tool	15
Content Migration Best Practices	16
Command Syntax for the Script	16
Content Migration Example	18
Special Cases for Software Tree Migration	22
Service Level Migration	23
Template Migration	23
Inheritance and Negative Overrides	23
Migration of Software Tree Permissions	25
Synchronizing Permissions After a Content Migration	26
RPM Metadata Migration	27
Running the RPM Metadata Migration Script	27
ISM Tool Runtime Migration	29

Migration of RPMs Created by ISMTool	29
Migrating RPMs Created by ISMTool	29
Compliance Data Migration Tool	30
Running the Compliance Data Migration Tool	30
Command Syntax For the Script	32
Chapter 2: Audit and Remediation Compliance Data Migration	33
<hr/>	
Introduction to Audit and Remediation Compliance Data Migration:	33
What the Migration Script Does	34
Migrating Script Functioning	34
Invoking the Migration Script	34
Testing the script	35
Chapter 3: AIX Software Provisioning Changes	37
<hr/>	
Introduction to AIX Software Provisioning Changes	37
The AIX Metadata Migration Tool	37
Procedure	38
The AIX Package Import Tool	38
Location	39
Usage	39
Software Provisioning Action Script	39
AIX Volume Manager Integration Example	41
Index	45
<hr/>	

Preface

Welcome to Server Automation System (SA) – an enterprise-class software solution that enables customers to get all the benefits of the SA data center automation platform and support services. SA provides a core foundation for automating formerly manual tasks associated with the deployment, support, and growth of server and server application infrastructure.

This guide describes how to use SA, starting with an introduction to the system and how to navigate the user interface. It provides information about managing servers, operating system provisioning, managing software packages, provisioning applications, reconciling servers, and configuration tracking. This guide is intended for system administrators who are responsible for all aspects of managing and provisioning the servers in an operational environment.

Contents of this Guide

This guide contains the following chapters and appendices:

This guide contains the following chapters and appendices:

Chapter 1: Migrating SA Content to Version 7.50: Provides an overview of the Content Migration process, explains how to run the Software Migration Tool, and describes the impact that the Software Migration Tool has on the SAS Web Client and SA Client.

Chapter 2: Audit and Remediation Compliance Data Migration: Describes what the Audit and Remediation compliance result Migration Script does, how to invoke the script and how to test it.

Chapter 3: AIX Software Provisioning Changes: Describes how to use the AIX meta-data migration and the AIX package import tools and run the software provisioning action script. It also provides a fully functional AIX volume manager integration example.




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.
<code>Courier</code>	Identifies text that is entered or displayed at the command-line prompt, such as Unix commands, SA 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.
<i>Italics</i>	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.

ICON	DESCRIPTION
	<p>This icon represents a warning. It is used to identify significant information that must be read before proceeding.</p>

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 SA installation. It documents all the main features of SA, scopes out the planning tasks necessary to successfully install SA, 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 *SA Content Utilities Guide* is intended for advanced system administrators responsible for importing content such as software packages into SA. It documents the following command-line utilities: OCLI 1.0, IDK, and DET (CBT).
- The *Platform Developer's Guide* is intended for software developers responsible for customizing, extending, and integrating SA. It documents how to create Web Services, Java RMI, Python, and CLI clients that invoke methods on the SA API.

Chapter 1: Migrating SA Content to Version 7.50

IN THIS CHAPTER

This section discusses the following topics:

- Content Migration Overview
- Software Migration Tool Overview
- Prerequisite for the Software Migration Tool
- How to Run the Software Migration Tool
- Command Syntax for the Script
- Content Migration Example
- Special Cases for Software Tree Migration
- Migration of Software Tree Permissions
- RPM Metadata Migration
- ISM Tool Runtime Migration
- Migration of RPMs Created by ISMTool
- Compliance Data Migration Tool

Content Migration Overview

The Software Migration Tool is a pre-requisite to upgrading to SA 7.50. It is assumed that customers have run the Software Migration Tool before upgrading to SA 7.50. After upgrading your core to SA 7.50, perform the following content migration tasks:

- After upgrading an SA core to 7.50 from a release earlier than 6.0, run the software migration tool to migrate the software tree nodes and package information to the Library in the SA Client. See “Software Migration Tool Overview” on page 8 in this chapter for information about running the Software Migration Script.

- After upgrading an SA core to 7.50 from a release earlier than 6.0 or 6.1, run the RPM metadata migration script to import the metadata of any pre-existing RPMs to the Model Repository. See “RPM Metadata Migration” on page 27 in this chapter for information about running the RPM metadata script.
- After upgrading an SA core to 7.50 from a release earlier than 6.0, run the ISM Tool runtime migration script to migrate the runtime packages of 3.2 and earlier ISMs to 3.3. See “ISM Tool Runtime Migration” on page 29 in this chapter for more information.
- After upgrading an SA core to 7.50, run the `ismpolicyrpm-migrate.sh` script to update the RPMs in the core that were created by ISMTool shipped with SA 6.1.1 or earlier. See “Migration of RPMs Created by ISMTool” on page 29 in this chapter for more information.
- After upgrading an SA core to 7.50 from a release earlier than 6.5, you are required to run the Compliance Data Migration Tool to migrate compliance data to the new database schema in the core. See “Compliance Data Migration Tool” on page 30 in this chapter for more information.



It is recommended that users must ensure that the Software Migration must be done before the 7.50 upgrade. The Software Migration Tool is a pre-requisite to upgrading to SA 7.50.

Software Migration Tool Overview

The Software Migration Tool is a pre-requisite to upgrading to SA 7.50. It is assumed that customers have run the Software Migration Tool before upgrading to SA 7.50.

Content Migration Process

The content migration process consists of two primary phases:

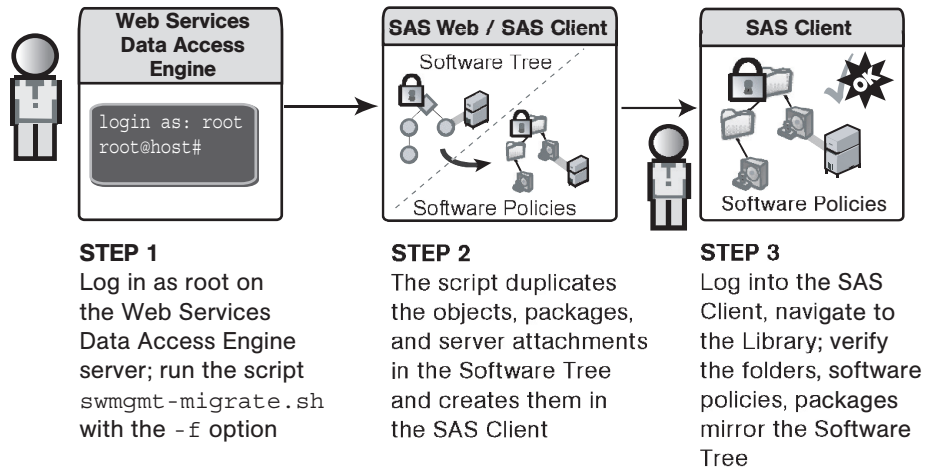
Part 1: Run the Software Migration Tool to duplicate the data and packages in the Software Tree in the SA Client Library and software policies.

Part 2: Run the Software Migration Tool again on the SA core to remove the Software Tree data from the SAS Web Client and unlock the packages in the SAS Client Library and software policies.

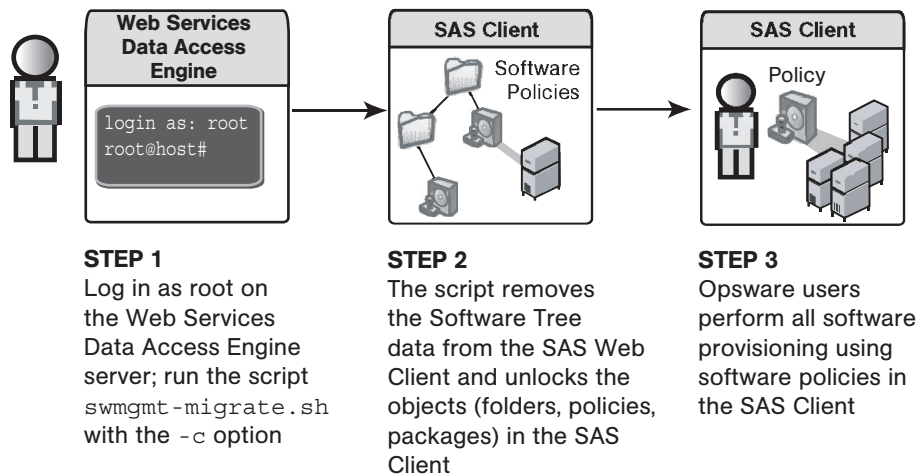
Figure 1-1: Content Migration Process

CONTENT MIGRATION PROCESS

Part 1: Run Software Migration Tool with “full migration”



Part 2: Run Software Migration Tool to **Complete** the Migration



Full Migration

Full migration occurs when you run the Software Migration Tool with the -f option.

Impact on the Software Tree

The Software Migration Tool copies all data for the following objects in the Software Tree:

- All nodes in the Software Tree (**Software** ► **Applications** in the navigation panel)
- All Service Levels except for the Service Levels under (**Service Levels** ► **Opware**)
- All templates except for the templates under (**Templates** ► **Opware**)
- All packages in the Package Management feature

After you run the Software Migration Tool, the container and leaf nodes in the Software Tree are locked. Users cannot delete nodes or modify them (which includes changing their properties, package lists, custom attributes, or installation order settings). Users with the manage lock permission for the nodes cannot change the lock state.

With a locked node, users can still:

- Assign, reassign, install, uninstall, and reconcile the nodes against servers and groups
- Utilize configuration tracking for nodes in the Software Tree
- Add child nodes to the Software Tree



It is recommended that users do not add child nodes to the Software Tree after the migration script is run and that complete migration should be performed on the SA core as soon as possible. See “Content Migration Best Practices” on page 16 in this chapter for more information about the preferred way to perform the migration.

Packages included in the nodes are locked and cannot be deleted, replaced, or have their properties modified. With a locked package, users can still:

- Assign or reassign the package to unlocked nodes.
- Install, uninstall, and reconcile nodes with locked packages against servers and groups.

Opware-specific Nodes

When you perform a full migration, the following Opware-specific nodes are not migrated because their software policy equivalents already exist in the SA Client:

- Templates under /Opware
- Templates under /Opware Tools
- Service levels under /Opware
- Applications under /System Utilities/Opware Tools

Impact on the SA Client

The Software Migration Tool creates the equivalent objects in the SA Client Library under the Migrated folder.

In the Migrated folder, the folder hierarchy mirrors the object hierarchy in the Software Tree. Each Software Tree node has a corresponding folder in the SA Client Library; the path of the folder mirrors the full path of the Software Tree node.

The folders have the same name as the display names of the nodes and the same customer associations as the nodes.

In each folder, the Software Migration Tool creates a software policy. Each software policy has a .p suffix and has properties that mirror the properties of the node it was duplicated from; for example, the OS assignment of the node becomes an OS attribute of the software policy.

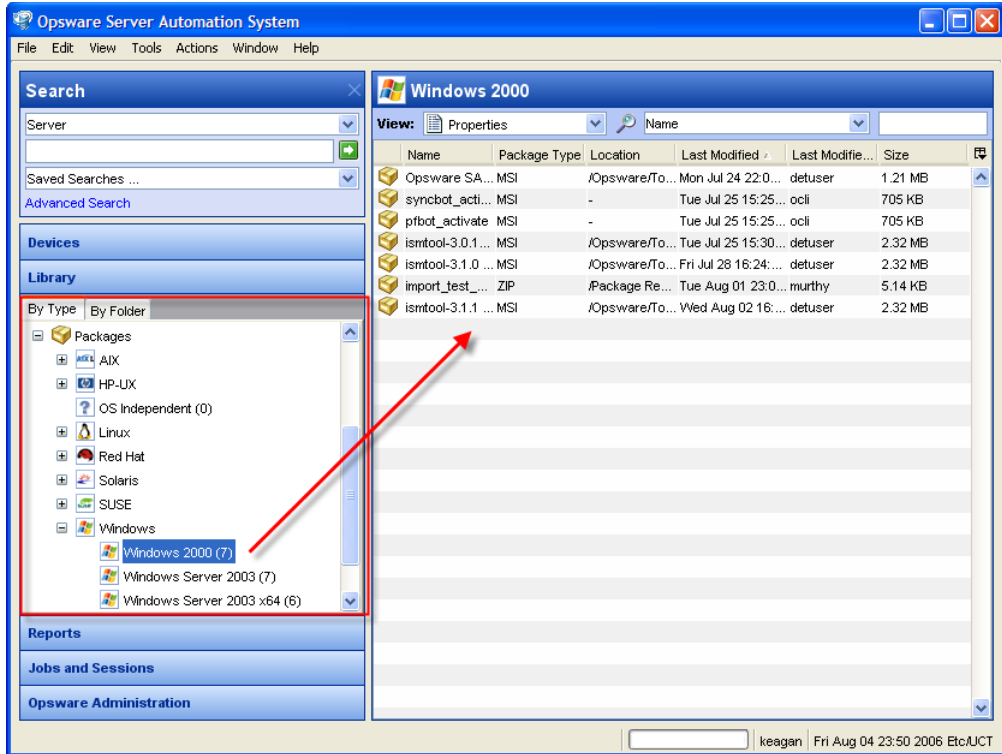
Once the folders and software policies are created in the SA Client Library, they are marked as in the "in migration" state and they cannot be modified while in this state.

All history entries for a migrated node are copied to the node's software policy equivalent. Additionally, the Software Migration Tool adds an entry to the history for each node and software policy that a migration event occurred. The history description references the corresponding objects.

After the migration, servers and groups that are attached to Software Tree nodes are also attached to the equivalent software policy objects. For example, if a group of servers has three node attachments, three software policies will be created and attached to the same group of servers.

The Software Migration Tool also duplicates all package information in the Package Management feature in the SAS Web Client (**Software ► Packages** in the navigation panel). The package information is displayed in the SA Client Library as shown in Figure 1-2.

Figure 1-2: Packages in the SA Client Library



Reconcile Behavior After Full Migration

Users can still reconcile servers with nodes that are in the "in migration" state. Likewise, users can remediate servers with the software policy counterparts that are also in the "in migration" state.

However, the two functions are separate: node reconcile in the SAS Web Client operates only on Software Tree node attachments, and software policy remediation in the SA Client operates only on software policy attachments.

Complete Migration

The Complete Migration step is the second part of the Content Migration process for the Software Tree data. When you run the Software Migration Tool with the `-c` option, the tool performs the following actions:

- Removes all Software Tree nodes along the path that leads to migrated nodes.
- Removes all server attachments to nodes in the SAS Web Client.
- Unlocks the software policy and folder counterparts in the SA Client.
- Clears the “in migration” state from the software policy objects so that users (with the necessary SA Client permissions) can modify them.
- Removes packages that are no longer referenced by any node, (whether they are in migration or not) from the SAS Web Client; but they are still available in the SA Client.

Migration of Software Installation Dependencies

The Software Migration Tool automatically preserves installation order data set for Software Tree nodes in the following ways:

- Within a node, package installation order is based on the order in which the packages were encountered while traversing the Software Tree node hierarchy to get to a leaf node.
- When a Software Tree node contains a software installation dependency, the Software Migration Tool preserves the data about dependent nodes in the software policy equivalent so that when a server is remediated with the software policy, the software is installed in the correct order. The data about dependent nodes is stored internally and is not modifiable in the SA Client.
- The the top-level categories in the Software Tree have a default installation order when servers are reconciled. This default installation order based on software category is preserved in the software policy equivalents. The data about the installation order of software categories is stored internally and is not modifiable in the SA Client.

Configuration Tracking in SA 7.50

As of SA 6.0, newly installed cores do not provide functionality to set up configuration tracking for Software Tree nodes. Configuration tracking for servers is still available. See the *SA User's Guide: Server Automation* for information.

While your upgraded SA 7.50 core is still in the “in migration” state, you can continue to use the Configuration Tracking feature with Software Tree nodes.

Prerequisite for the Software Migration Tool

Before you run the Software Migration Tool, you must verify if the database statistics for LCREP user have been collected. If the statistics have not been collected in the last 24 hours, then you must run the `dba_jobs` for the LCREP user. If the statistics collection job has not run at all, then you must run the `dba_job` for LCREP, Model Repository and the AAA users. For a database with approximately 50M records, this process might take up to 5 hours.

Perform the following steps to collect the statistics for the LCREP table:

- 1** Log on to the Model Repository server as user `oracle`.
`su - oracle`
- 2** Run `sqlplus`:
`sqlplus "/ as sysdba"`
- 3** Enter the following `sqlplus` commands to verify if the statistics collection jobs have been run:

```
set line 200
col last format a20
col next format a20
col this format a20
col what format a30
select job, priv_user, to_char(LAST_DATE, 'MM/DD/YY
HH:MI:SS')
last, to_char(THIS_DATE, 'MM/DD/YY HH:MI:SS')
this, to_char(NEXT_DATE, 'MM/DD/YY HH:MI:SS')
next, what from dba_jobs;
```

In the statistics collections jobs the `WHAT` has the following values:

```
gather_lcrep_stats
DBMS_STATS.GATHER_SCHEMA*
```

- 4** If the statistics collection jobs have not been run in the last twenty four hours, then you can run the statistics collection jobs manually. See the *SA Planning and Installation Guide*, Appendix A: Oracle Setup for Model Repository for instructions on running the statistics collection job.

How to Run the Software Migration Tool

- 1** Log on as root to the server running the Web Services Data Access Engine (twist) component. This component is installed on the same server as the SAS Web Client component.

(Recommended) Run the script from your source core, which is the first core installed in a multimaster mesh. See the *SA Planning and Installation Guide* for information about source and target cores.

You only run a migration operation once per multimaster mesh. The multimaster functionality will propagate the change to the rest of the cores in the mesh.

- 2** Locate the script in the following directory:

```
/opt/opsware/twist/migration/swmgtmigrate.sh
```

- 3 (Recommended)** To preview the migration, enter the following command:

```
swmgtmigrate -f -n
```

The script displays a detailed report indicating what will occur when the migration operation is run. The detailed information is important in disclosing what changes will be made and the scope of the changes. Use this information to schedule an appropriate time to perform the actual migration.

The detailed information includes metrics on the amount time the operation might take. Use the metrics as an estimate of how much time in bytes per second (bps) it might take to complete the operation for the core the script is run against. The metrics factor in the requirements of multimaster propagation. These metrics serve as a guideline and should not be interpreted as the exact time the migration operation will run.

- 4** To perform a full migration of the Software Tree data, enter the following command:

```
swmgtmigrate -f
```

Optionally, you can specify the `-s` option to skip the detailed report. The script still displays a basic report.

- 5** At the confirmation prompt, specify that you are ready to proceed with the full migration.

The migration proceeds and displays result information and success/failure details as it runs.

You can access the script logs in the `/var/log/opsware/swmgtm` directory.

- 6** On successful completion of the full migration operation, log into the SA Client for a core in the mesh and verify the results of the migration.
- 7** Log on as root to the server running the Web Services Data Access Engine (twist) component and rerun the script to complete the migration:

```
swmgmt-migrate -c -f
```



To optimize the execution speed of the migration operation, use the `-f` option.

See “Complete Migration” on page 13 in this chapter for more information.

Content Migration Best Practices

- Make the upgraded release public only after the Software Migration Tool runs and completes successfully.
- After the full migration, existing Software Tree nodes are locked in the SAS Web Client. However, by default, users can still create new nodes in Software Tree. It is recommended that you modify SAS Web Client permissions so that SA users (excluding System Administrators) do not have write permissions to the Software Tree, Software Provisioning Wizards, Package Management feature, and Templates after the migration.
- To prevent further use of unused packages, the Software Migration Tool moves packages that are not included in any nodes to the Software Repository folder in the SA Client. Therefore, if a package does not exist in a folder in the SA Client after the migration, add it to the folders where you need it.

Command Syntax for the Script

```
swmgmt-migrate.sh [options]
```

Table 1-1 provides a description of each option for the Software Migration Tool.

Options `-c`, `-o`, `-p`, and `-r` cannot be combined.

Table 1-1: Command Syntax for the `swmgmt-migrate.sh` Script

OPTION	DESCRIPTION
<code>-c</code>	Completes a migration. See “Complete Migration” on page 13 in this chapter for more information.
<code>-f</code>	Migrates all nodes in the Software Tree (Software ► Applications in the navigation panel), Service Levels, and templates, leaving nothing except the top-level categories under Software ► Applications, /Templates/Opware, and /Service Levels/Opware. See “Full Migration” on page 10 in this chapter for more information. Full migration also syncs permissions, sets installation orders, and migrates packages automatically.
<code>-m</code>	When used in conjunction with other options, displays all migrated Software Tree nodes.
<code>-n</code>	Displays a report on how the migration will be performed; does not perform the actual migration.
<code>-o</code>	Sets global ordering by taking a snapshot of existing installation order for nodes and recording the global order numbers by using custom attributes.
<code>-p</code>	Synchronizes permissions by granting equivalent software policy permissions for user groups that have existing software tree-related permissions. See “Synchronizing Permissions After a Content Migration” on page 26 in this chapter for more information about when to use the <code>-p</code> option.
<code>-r</code>	Rolls back a migration by undoing the "in migration" Software Tree nodes. "Completed" nodes are removed; therefore, it's not possible to roll them back.
<code>-s</code>	Performs the migration in silent mode (no preview).
<code>--help</code>	Shows usage and examples for the <code>swmgmt-migrate.sh</code> script.

Command Syntax Examples

To perform a full migration, enter the following command:

```
swmgmt-migrate -f
```

To roll back the last full migration, enter the following command:

```
swmgmt-migrate -r -f
```

To complete a migration, enter the following command:

```
swmgmt-migrate -c -f
```



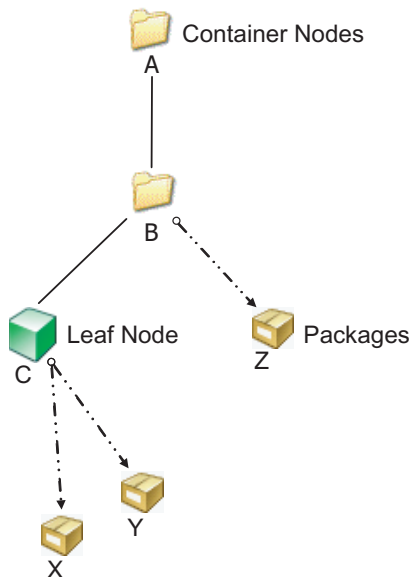
To optimize the execution speed of the migration operation, use the `-f` option, as shown in the examples above.

Content Migration Example

The following example illustrates the process for migrating Software Tree nodes to SA 7.50.

In this example, the Software Tree has two container nodes (node A and node B) and one leaf node (node C) in the Application Servers category of the Software Tree. Node C has packages X and Y and node B has package Z.

Figure 1-3: Software Tree Before Running the Migration Script



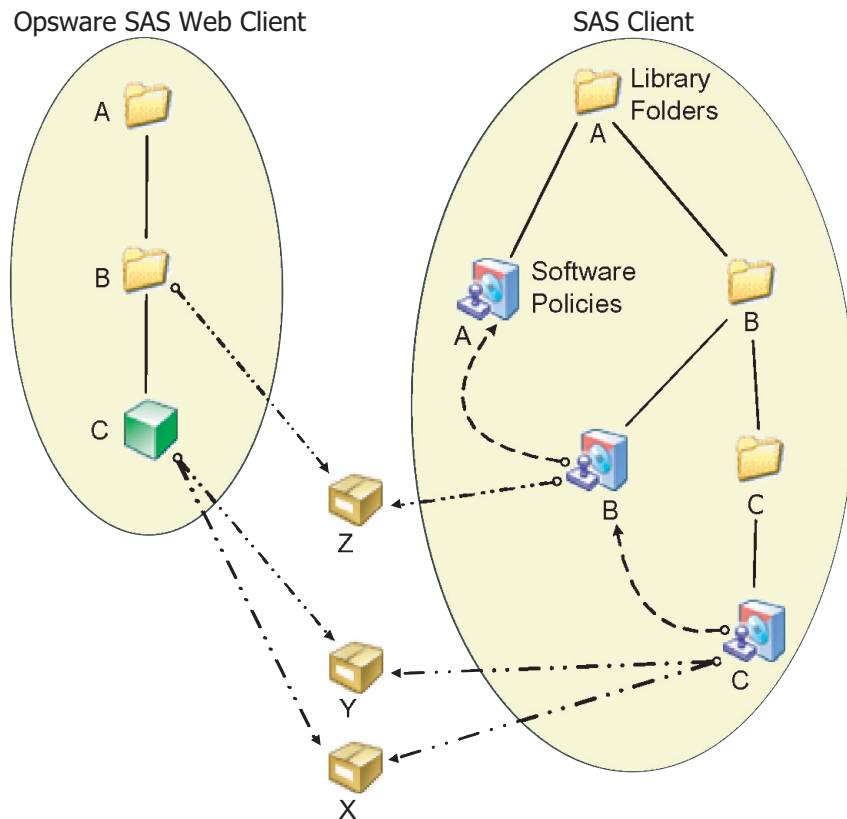
In this example, these three nodes have the properties shown in Table 1-2:

Table 1-2: Node Properties Before Migration

NODE	TYPE	CUSTOM ATTRIBUTES	PACKAGES/PATCHES	CUSTOMER
A	Container	Yes	None	Independent
B	Container	Yes	Z	Independent
C	Leaf	Yes	X, Y	Marketing

An administrator runs the Software Migration script to migrate node C as shown by Figure 1-4:

Figure 1-4: Full Migration of Node C



The script migrates everything that formulates the path to node C, which means it also migrates container nodes A and B.

In the SA Client, the Software Migration script creates folders that correspond to container nodes A and B. Additionally, because nodes A and B have custom attributes and packages defined, the script creates software policies that correspond to nodes A and B to capture the custom attribute and package information.

Software policy B includes A as a nested policy so that the custom attribute inheritance is captured.

For leaf node C, the script creates software policy C and folder C so that the Marketing customer constraint can be placed on folder C. The net effect is that software policy C is constrained to the customer Marketing.

Software policy C includes software policy B to capture custom attribute and package Z associations due to inheritance in the Software Tree. Lastly, the packages X and Y are associated to software policy C. The existing packages (X and Y) are associated with both Software Tree nodes and software policies.

At this point, all the nodes, folders, software policies, and packages involved are in an "in migration" state. All objects in the Software Tree and in the SA Client are "locked" and "in migration" mode.

The following table lists the properties of the software policies created as a result:

Table 1-3: Node Properties After Full Migration

OBJECT	TYPE	CUSTOM ATTRIBUTES	PACKAGES	CUSTOMER CONSTRAINTS
A	Folder	N/A	N/A	Independent
A	Software Policy	Those of node A's	None	N/A
B	Folder	N/A	N/A	Independent
B	Software Policy	Those of node B's	W	N/A
C	Folder	N/A	N/A	Marketing
C	Software Policy	Those of node C's	X, Y	N/A

If the "complete the migration" operation is done with the migration script, then both the Software Tree notes and software policy representation would be "unlocked" so that modifications are allowed for involved objects in both areas. Then the Software Tree branch would be entirely removed, leaving just the software policy representation.

Table 1-4: Software Policy Properties After Complete Migration

OBJECT	TYPE	CUSTOM ATTRIBUTES	PACKAGES	CUSTOMER CONSTRAINT
A	Folder	N/A	N/A	Independent
A	Software Policy	Those of node A's	None	N/A
B	Folder	N/A	N/A	Independent
B	Software Policy	Those of node B's	Z	N/A
C	Folder	N/A	N/A	Nike
C	Software Policy	Those of node C's	X, Y	N/A

Figure 1-5: Software Policy Hierarchy for Node C After Complete Migration

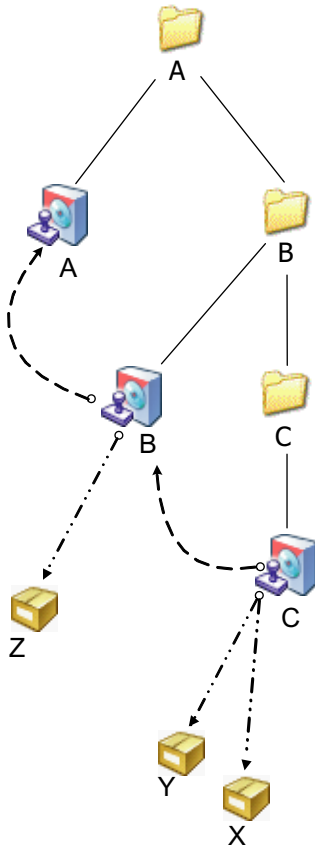


Figure 1-5 shows the software policy hierarchy with C migrated. The Software Tree source is completely removed. The software policy equivalents are no longer in migration mode. Packages are reused as they were.

Special Cases for Software Tree Migration

When you migrate the Software Tree data to the SA Client, you should understand how the following Software Tree objects are migrated because their data equivalents in the SA Client have unique properties:

- Service Levels
- Templates
- Inheritance and Negative Overrides in the Software Tree

Service Level Migration

Unlike application nodes in the Software Tree, service levels cannot have packages as part of their specification and they can have multiple customer assignments (whereas an application nodes can only have one).

The software policy equivalent of a service level is combination of a folder and a software policy. A folder is needed so that the node's customer assignments can be transformed to multiple customer constraints on the folder.

Template Migration

Templates can include application nodes, OS nodes, patches, and service levels.

When an application node or service level is migrated, all templates that include the nodes still function normally.

If a template includes the installation of an operating system, it is used for OS provisioning. Templates that include OS installation are migrated to the SA Client to Software Policy Templates or to OS sequences. The migrated OS sequences reside in the /Migrated/Templates folder in the SA Client Library.

Migrated OS sequences are locked in the SA Client and cannot be modified until after the migration is completed. See "Complete Migration" on page 13 for information.

If the OS Installation Profile in the SAS Web Client is customer independent, the customer field of the Install OS Task can be empty or set to a specific customer when migrated to the SA Client.

Inheritance and Negative Overrides

In the Software Tree, inheritance and negative overrides can be set for custom attributes and packages that are assigned to nodes.

In the SA Client, software policies do not support inheritance for custom attributes. Therefore, for custom attributes that use inheritance or negative overrides, the Software Migration Tool simply creates the corresponding custom attributes on the software policies directly.

When a node has negative overrides of packages, the software policy counterpart is a flattened out version of the node hierarchy. The software policy includes all packages that the node would inherit, minus the packages that were negatively overridden.

For example, assume you have two nodes – A (parent node) and B (child node of A) – and node A has packages X and Y. If child node B has negative inheritance on package Y, then a software policy B would be created with straight inclusion of package X but not Y, and it would not nest policy A.

Template Inheritance

Applications, patches, and service levels can be attached to templates. They can be inherited and blocked.

When you run the Software Migration Tool, it handles a blocked node attached to a template in the following way:

- Two objects are created in the SA Client – a software policy equivalent of the template and a software policy equivalent of the node
- The software policy equivalent of the template does not include the software policy equivalent of the node

For example, if G and H are templates, H is a child of G, and G includes application nodes R and V.

Figure 1-6: Example of Template Inheritance in the SAS Web Client

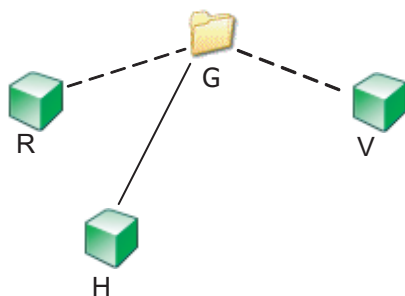


Figure 1-6 shows the template hierarchy with H migrated. R and V are members of G. H is a child of G. H has an override on V so that it only gets R through inheritance.

Continuing with this example, the software policy equivalent to G, say G' would not have the software policy equivalent of V, say V', as a nested policy, but would have R'. Also, H specifies that V is negatively overridden, so that H only inherits R from G as a result.

Figure 1-7: Example of Template Inheritance After Migration to the SA Client

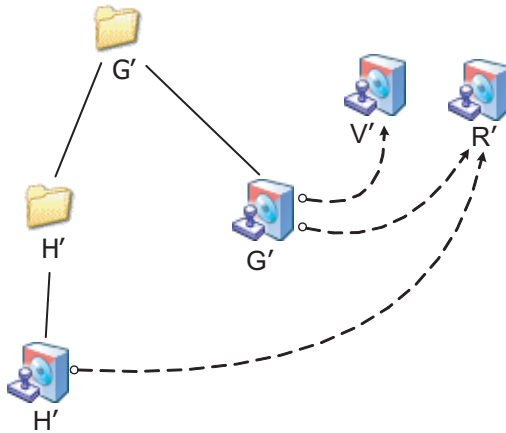


Figure 1-7 shows all of G, H, R, and V are migrated. H' only nests R' however. It does not nest G' or V'.

Migration of Software Tree Permissions

As of SA 6.0, software policies and folders have new permissions for the Software Management feature in the SA Client.

As part of the Content Migration, SA user groups that had permission to perform software provisioning in the SAS Web Client are granted the corresponding Software Management permissions in the SA Client.

Table 1-5: Mapping of SAS Web Client Permissions to SA Client Permissions

SAS WEB CLIENT PERMISSION:	SA CLIENT PERMISSION:
<ul style="list-style-type: none"> • Model: Applications • Model: Service Levels • Templates 	<ul style="list-style-type: none"> • Manage Application Policies: Read/Write • Manage Folders: Read/Write

Table 1-5: Mapping of SAS Web Client Permissions to SA Client Permissions

SAS WEB CLIENT PERMISSION:	SA CLIENT PERMISSION:
<ul style="list-style-type: none"> • Packages 	<ul style="list-style-type: none"> • Manage Folders: Read/Write • Manage Packages: Read/Write • Allow Install Packages • Allow Uninstall Packages
<ul style="list-style-type: none"> • Wizard: Install Software • Wizard: Uninstall Software 	<ul style="list-style-type: none"> • Allow Attach/Detach Application Policy: Yes • Allow Remediate Application Policy: Yes
<ul style="list-style-type: none"> • ISM Controls 	<ul style="list-style-type: none"> • Allow Run ISM Controls: Yes
<ul style="list-style-type: none"> • Other ► Manage Server Permissions ► Model Public Device Groups 	<ul style="list-style-type: none"> • Client Features ► Server Group Permissions ► Model Public Device Groups

Folder-specific permissions are assigned as appropriate when nodes are migrated to the SA Client. See the *SA Administration Guide* for information about granting folder permissions in the SA Client.

Synchronizing Permissions After a Content Migration

After upgrading to SA 7.50, you can run the Software Migration Tool with the sync permissions (-p) option when you need to grant a user group that has the SAS Web Client software provisioning permissions the corresponding permissions in the SA Client.

For example, user group A is added and granted access to all categories in the **Software Tree (Software) ► Applications** in the SAS Web Client navigation panel) but the user group does not have permission to access folder and software policy features in the SA Client.

Later, you grant user group A access permission to certain folders. However, the members of user group A still cannot operate on these folder because their group does not have the feature permission for the SA Client. You can manually add these permission for the user group or run the Software Migration Tool with sync permission (-p) option.

RPM Metadata Migration

As of SAS 6.1, the RPM Deployment feature is available as part of the SA Client. SA allows you to deploy RPM packages on Red Hat Linux and SUSE Linux servers without manually specifying all the dependent packages required for installing the RPM packages. When you deploy a RPM package, SA determines the dependencies and installation order for the RPM package, and identifies if any conflicts exists between the dependencies. After you resolve the conflicts, SA installs the RPM packages on the managed server. See *SA Policy Setter's Guide* for more information on this feature.

When you upload an RPM package using SA, the metadata for the RPM package is extracted and stored in the Model Repository. After upgrading an SA core to 7.50, you must run the RPM metadata migration script to import any pre existing RPM metadata to the Model Repository. You are not required to run this script if you are upgrading from SA 6.1, 6.1.1, or 6.1.2 to 6.5. Running the RPM Metadata Migration script on your upgraded SA core thus allows you to use the new RPM Deployment feature with your existing data.

Running the RPM Metadata Migration Script

- 1 Log on as root to the server running the Software Repository (word) component.

Run the script on each core in a multimaster mesh. You should run the script on only one core at a time. After you complete running the script in a core, wait for several minutes before running the script in the next core.

- 2 Locate the script in the following directory:

```
/opt/opsware/mm_wordbot/util/import_rpm_metadata
```

- 3 Run the script as follows:

```
/opt/opsware/mm_wordbot/util/import_rpm_metadata -a
```

See Table 1-6 for the other options for the script.

- 4 You can verify the output of the script to confirm if the script ran successfully. The output of the script informs you of the number of RPMs imported and the number of RPMs that still needed to be imported. After running the script on each core in a multimaster mesh this final number should be 0.

Figure 1-8: Output of RPM Metadata Migration Script

```
# /opt/opsware/mm_wordbot/util/import_rpm_metadata -a
Downloading journal
Retrieving RPM IDs
```

```

(8/8): Step 8                               100%
[#####]
RPMs needing metadata import: 0
Retrieving RPM details
Looking for RPMs on local filesystem
RPMs found on local filesystem: 0
Verifying results
(8/8): Step 8                               100%
[#####]
RPMs needing metadata import: 0
Deleteing remote journal
Deleteing local journal
Completed
    
```

Command Syntax for the Script

Table 1-6: Command Syntax for the RPM Metadata Migration Script

OPTION	DESCRIPTION
-a	Re-imports the metadata of the existing RPM packages to the Model Repository automatically.
-f	Forces the re-import of metadata of the existing RPM packages. This option is always used in conjunction with -a.
-c FILE	Specifies the Software Repository configuration file.
{ID..... -}	Allows you to specify the IDS of the RPM packages. Only the metadata of the RPM packages whose IDS are specified will be imported into the Model Repository.
-s	Performs the migration in silent mode (no preview). This option is always used in conjunction with -a
-h	Shows usage and examples for the script.

ISM Tool Runtime Migration

The ISM Tool Runtime Migration should be done in SA 6.x before upgrading to 7.50.

Migration of RPMs Created by ISMTool

This section describes how to migrate the RPMs in your core that were created by ISMTool shipped with SA 6.1.1 or earlier. Unless you are certain that you have no such RPMs, follow the instructions in this section. If these RPMs are not migrated, they cannot be installed on managed servers by SA. For details on the ISMTool bugs that require this RPM migration, see “What’s Fixed in SA 6.1.2” in the *SA 6.1.2 Release Notes*.

Migrating RPMs Created by ISMTool

The following instructions explain how to migrate the RPMs by running the `ismpolicyrpm-migrate.sh` script. In a mutlimaster mesh, you only need to run the script once for the entire mesh. If you ran the `ismpolicyrpm-migrate.sh` script when applying the SA 6.1.2 patch, you do not need to run it again.

To migrate the RPMs, perform the following steps:

- 1** On the core server running the Command Center (occ) component, log on as root.
- 2** Change to the directory containing the `ismpolicyrpm-migrate.sh` script.

```
cd /opt/opsware/twist/migration
```
- 3** View a list of the RPMs that will be updated by the migration script by entering the following command:

```
./ismpolicyrpm-migrate.sh --preview
```

This command lists the IDs of the RPMs.

- 4** (Optional) To view the properties of an RPM, you can search for it by ID in the SA Client:
 1. In the Navigation pane, select **Library > By Type > Packages > platform**
 2. For the View, select Properties.
 3. In the field next to the magnifying glass, enter the ID.

- 5** To migrate the RPMs, enter the following command:

```
./ismpolicyrpm-migrate.sh --update
```

This command searches for all software policies created by ISMTool, locates RPMs associated with those policies, and then sets the following install and uninstall parameters on each RPM:

Upgrade: No

Install Flags: --nodeps

Uninstall Fags: --nodeps

Compliance Data Migration Tool

In SA 6.5, the Audit Exceptions feature is available as part of the SA Client. After upgrading an SA core to 7.50, you are required to run the Compliance Data Migration Tool to migrate compliance data to the new database schema in the core.

Running the Compliance Data Migration Tool on your upgraded SA 7.50 core allows you to use the new Audit Exceptions feature with your existing data. After the migration, the audit rules become available in the SA Client for constructing audit exceptions using the audit editor.

If you are migrating from SA 6.5 or later, there is no need to run the data migration tool. However, if you are migrating from a release earlier than SA 6.5, then you *must* run this tool. Running the tool when not required, does no harm.

See the *SA User's Guide: Application Automation* for more information about Audit exceptions.

Running the Compliance Data Migration Tool

- 1** Log on as root to the server running the Web Services Data Access Engine (twist) component. This component is installed on the same server as the SAS Web Client component.

(Recommended) Run the script from your source core, which is the first core installed in a multimaster mesh. See the *SA Planning and Installation Guide* for information about source and target cores.

You only run a migration operation once per multimaster mesh. The multimaster functionality will propagate the change to the rest of the cores in the mesh.

- 2** Locate the script in the following directory:

```
/opt/opsware/twist/compliance-migration/compliance-  
migration.sh
```

- 3** Run the script as follows:

```
compliance-migration.sh --host localhost --port 1026
```

You are required to specify the user name and password to run the script. It is recommended that you specify the DCML Exchange Tool (DET) user name and password to run the script. See the *SA Content Utilities Guide* for more information about DET.

The DET user name and password specified when the system was installed and are perhaps saved in the OI response file.

Running the script will migrate all the compliance rules data to the new schema. See Table 1-7 for the list of script options.

- 4** To display a list of options of to run the script without specifying any parameters:

```
/opt/opsware/twist/compliance-migration/compliance-  
migration.sh
```

or specify the `--help` option.

- 5** To verify if the script has run successfully perform any one of the following steps:

- Run the script. The `-d` (debug) option is optional, it provides information when the program fails.
- Verify the log files to check for exceptions.

The log files can be located at the following location:

```
/var/log/opsware/compliance/
```

- Run the script as follows to display the output of the script:

```
compliance-migration.sh --user -passwd >output.txt
```

Command Syntax For the Script

Table 1-7: Command Syntax for the Compliance Data Migration Tool

OPTION	DESCRIPTION
-s	Performs the migration in silent mode (no preview).
-d	Shows debug information for the script.
--host	Specifies the host name to run the script.
--port	Specifies the connection port of the host machine. If the port number is not specified, the default port 1026 is used.
--protocol	Specifies the connection protocol (http or https) required to run the script.
--user	The user name required to run the script.
--passwd	The password required to run the script.
--id	Specifies the ID of the compliance data to migrate.
--AuditPoliciesOnly	Allows you to migrate only Audit Policies.
--AuditsOnly	Allows you to migrate only Audits.
--AuditResultsOnly	Allows you to migrate only Audit Results.
--SnapshotSpecsOnly	Allows you to migrate only Snapshot Specifications.
--SnapshotsOnly	Allows you to migrate only Snapshots.

Chapter 2: Audit and Remediation Compliance Data Migration

IN THIS CHAPTER

This section contains the following topics:

- Introduction to Audit and Remediation Compliance Data Migration:
- What the Migration Script Does
- Migrating Script Functioning
- Invoking the Migration Script
- Testing the script

Introduction to Audit and Remediation Compliance Data Migration:

This chapter describes what the Audit and Remediation compliance result Migration Script does, how to invoke the script and how to test it.

The Migration Script is located at the following location on the core:

```
/opt/opsware/twist/compliance-migration/compliance-result-migration.sh
```

This script is for migrating data to SA 7.50 from any release. It is run automatically by the SA 7.50 upgrade script. However, you may want or need to run it manually if there are any issues.

Source code is located at the following location:

```
/soft/lco/twist/tools/compliance/migration/compliance-result-migration.sh, /soft/lco/twist/tools/compliance/migration/src/com/opsware/migration/ComplianceResultMigration.java.
```

What the Migration Script Does

This Migration Script is used to migrate AuditResults and SnapShots data from SAS 6.x versions to SA 7.50. Prior to SA 7.50, the associations between AuditTask and AuditResults, SnapShot Specification and SnapShots are based on name, which is error prone, since AuditTask can be deleted or renamed. In SA 7.50, AuditResults/SnapShots are associated with AuditTask/SnapshotTask by task id. So when the user clicks on a task from SAS Web Client, the results generated by that task display at the bottom panel. Those results which do not have a task ID go to the "Archived" folder. The Migration Script tries to find task ID for the AuditResults/Snapshots and updates them accordingly.

Migrating Script Functioning

The Migrating Script first tries to update the AuditResults/Snapshots by going through all the non scheduled jobs for each audit task. Then it tries to update the AuditResults/Snapshots by finding the AuditTask/Snapshot Spec with the same name. If the `-byName` option is true, the default value is true. If there are still some results left behind, which do not have the task ID associated with them, those results go to the "Archived" folder.

Invoking the Migration Script

Perform the following steps to invoke the Migration Script:

- 1** Logon to the core as root 2. chmod as needed to run the script 3. `/opt/opsware/twist/compliance-migration/compliance-result-migration.sh --user dummy --passwd dummy`
- 2** You can use `builadmgr/builadmgr` (should be DET user and password) as user name and passwd.
- 3** You can run `/opt/opsware/twist/compliance-migration/compliance-result-migration.sh` only to see the usage message

```
[root@m171 root]# /opt/opsware/twist/compliance-migration/
compliance-result-migration.sh Usage: compliance-result-
migrate.sh [flags] Flags:
```

```
-s: silent mode. -d: debug. Options:
```

```
--host: The Opsware host machine. --port: The
connection port of the host machine. --protocol: The connection
protocol. --user: Login user name. --passwd: Login user
password. --byName: link results and task by name (default value
is true) --id: The Opsware ID of one object to migrate. --
AuditResultsOnly --SnapshotResultsOnly --All
```

The Log files are written at the following location:

```
/var/log/opsware/compliance/ compliance-migration/compliance-
result-migration.sh --user dummy --passwd dummy
```

Testing the script

Perform the following steps to test the script:

- 1** Have a SAS 6.x core ready
If you have audit results and snapshots data on that core already, skip Step. 2
- 2** Create some audit results and snapshots.
- 3** Upgrade the core to SA 7.50
- 4** Invoke the Migration Script when the upgrade is done and Web Services Data Access (twist) is running.
- 5** Log on to the SA Client to verify if the data are migrated successfully. You should see the AuditResults/SnapShots showing on the lower panel of Audits when the audit task is selected and if that audit task has audit results.

Chapter 3: AIX Software Provisioning Changes

IN THIS CHAPTER

This section contains the following topics:

- Introduction to AIX Software Provisioning Changes
- The AIX Metadata Migration Tool
- The AIX Package Import Tool
- Software Provisioning Action Script
- AIX Volume Manager Integration Example

Introduction to AIX Software Provisioning Changes

SA 7.50 offers improved support for working with AIX software.

- **Package dependencies** - when installing AIX software, fileset requisites are now resolved automatically. This functionality requires SA to store additional AIX package metadata as compared to prior versions of SA, so a one-time migration step is necessary upon upgrading to 7.50
- **Importing packages** - a new CLI makes the process of importing AIX software into SA much simpler.
- **Volume manager support** - new functionality allows the customer to integrate the software provisioning procedure with an OS volume manager. A sample AIX volume manager integration script is provided to demonstrate this functionality.

The AIX Metadata Migration Tool

After upgrading to SA 7.50, a one-time migration step is necessary before you may install AIX software. This step requires a CLI tool to be run on each Software Repository. The CLI tool must only be run on a single Software Repository at a time.

Procedure

Login to a Software Repository. As the root user, execute the following command:

```
/opt/opsware/mm_wordbot/util/migrate_aix_metadata -a
```

Wait for the command to complete. It may take several minutes depending upon how many AIX packages exist on the Software Repository.

Once the command completes, login to the next Software Repository and repeat the command above.

Once the command has been run on each Software Repository in turn, the final output should resemble the following:

```
[root]# /opt/opsware/mm_wordbot/util/migrate_aix_metadata -a
Retrieving AIX fileset IDs
(5/5): 100%
[#####
##]
Filesets needing metadata migration: 0
Deleting remote journal
Deleting local journal
Retrieving AIX APAR IDs
Retrieving APAR to fileset mappings
(9/9): 100%
[#####
##]
APAR to fileset mappings needing correcting: 0 Completed
```

Note in particular two lines in the output above:

1. Filesets needing metadata migration: 0
2. APAR to fileset mappings needing correcting: 0

Both of these lines should indicate "0" as shown.



The AIX Package Import Tool

The AIX Package Import Tool makes it easy to import AIX packages (*.bff files) into SA. In addition, the tool may optionally create a policy from the imported packages. This simplifies the process of importing a collection of packages which comprise an AIX fix pack (i.e. technology level or service pack).

Location

```
/opt/opsware/mm_wordbot/util/import_aix_packages
```

Usage

```
import_aix_packages [options]
```

All *.bff packages in the current working directory are copied to the SA library.

```
import_aix_packages [options] <source-directory>
```

All *.bff packages in the specified directory are copied to the SA library.

```
import_aix_packages [options] <*.bff>
```

The explicitly specified packages are copied to the SA library.

```
import_aix_packages -h
```

Show additional options.

Packages already in the SA library will not be copied unless you specify the `--force` option.

The operating system version of the packages will be determined automatically as long as a `bos.*` package is in the source list. Otherwise you must provide the AIX OS version using the `--os` option.

When importing packages comprising a *fix pack*, use the `-p <policy_path>` option to create an SA software policy containing the imported packages. `<policy_path>` specifies the location and name of the policy to create. For example

```
-p /AIX Fix Packs/ 5.3/5300-07-04-0812
```

Software Provisioning Action Script

When provisioning software, SA first creates a temporary download directory on the managed server. SA transfers the software to be installed to this directory, installs the software, then removes the temporary download directory.

SA 7.50 provides a new mechanism for running a script during software provisioning. One use for such a script is to integrate with a volume manager on the managed server

Custom attributes, set on the managed server, control the functionality as shown in Table 3-1:

Table 3-1: Software Provisioning Custom Attributes

CUSTOM ATTRIBUTE	DESCRIPTION
OPSWremediate_action_script	The name of a shared script (SA Client ► Library ► By Type ► Scripts ► Unix). For security reasons, the script name must begin with Remediate:. For example Remediate:AIX LVM Actions. As of SA 7.50 scripts are located in folders, therefore, you must provide the path when invoking the script: <path>/Remediate:AIX LVM Actions
OPSWremediate_action_script_args	Command-line arguments to provide to the script.
OPSWremediate_action_script_timeout	Timeout for the script in minutes. The default value is 1.
OPSWremediate_action_script_abort_on_error	Whether or not to stop the job if the script returns an error or times out. Legal values are "true/false" (case-insensitive), "yes/no" (case-insensitive) and "1/0". The default is "true". (Note: this setting is effectively ignored if the "Attempt to continue running if an error occurs" checkbox which appears in the "Remediate Options" in the OCC Client is checked.)

A software provisioning action script is run at four different points during the provisioning process. Several environment variables provide contextual information about the provisioning process to the script at the time it is run:

- 6** OPSWremediate_phase – The value of this environment variable is one of:
 - *pre-stage* – This value indicates the script is being run just before the download operation is to begin.

- *post-stage* – This value indicates the script is being run just after the download operation has completed.
 - *pre-action* – This value indicates the script is being run just before the software install operation is to begin.
 - *post-action* – This value indicates the script is being run just after the software install operation has completed.
- 7** `OPSWremediate_job_id` – This value provides the ID of the current provisioning job.
 - 8** `OPSWremediate_space_required` - This environment variable is set only during the pre-stage phase. Its value is the space required in megabytes to download the software.
 - 9** `OPSWremediate_download_dir` – This environment variable is set only during the pre-stage phase. Its value is equivalent to the setting of the `package_download_dir` custom attribute on the managed server.

AIX Volume Manager Integration Example

SA 7.50 provides a fully functional AIX volume manager integration script as a sample. During software provisioning, the script will create a temporary filesystem when it is run in the *pre-stage* phase.

SA will download software into the temporary filesystem. After the software has been installed, the filesystem will be deallocated when the script is run in the *post-action* phase.

Preparing the LVM Script

To use this script, first perform these tasks:

- 1** Locate the file `aix-lvm-remediate-script.sh` on your distribution media and save it locally to a directory of your choosing.
- 2** Log in to the SA Client.
- 3** Select **Library** ► **By Type** ► **Scripts** ► **Unix** ► **Action** ► **New**.

- 4 The New Script window appears. Use this window to provide the following information:

Table 3-2: LVM Script Information

Name:	Remediate:AIX LVM Integration
Type:	Unix Shell
Shared?	Yes
Changes Server?	Yes
Upload Script:	Select this radio button. Set Encoding of script to English (US-ASCII). Click Browse... and locate <code>aix-lvm-integration.sh</code> on your local machine.
Usage Notes:	This script creates a temporary filesystem on AIX servers where remediate can download packages. After all packages have been installed, the filesystem is deallocated.

- 5 Click **Save**.
- 6 Log out of the SA Client.

The script is now prepared.

Using the LVM Script

The following tasks must be performed on each AIX managed server for which you wish to make use of the script.

- 1 Log in to the SA Client.
- 2 Locate the Managed Server in the SA Client.
- 3 Double-click the server to bring it up in its own window.
- 4 Click **Custom Attributes**.
- 5 Click **Add**. Name the first custom attribute to `OPSWremediate_action_script` and set its value to `<path>/Remediate:AIX LVM Integration`.
- 6 Click **Add**. Name the second custom attribute `package_download_dir`. Its value is the mount point for the temporary filesystem created by `aix-lvm-integration.sh`. A suggested value is `/OPSWremediate_tmp`.

- 7 (Optional)** Click **Add** again. Name the third custom attribute `OPSWremediate_action_script_args`. The `aix-lvm-integration.sh` script supports two arguments:
1. `-g VolumeGroup` – Specify a volume group from which to allocate the file-system. The default is `rootvg`.
 2. `-m Value` – Specify a minimum size in MB needed for temporary filesystem creation to occur. For example, specifying 100 means that the total download size in a given remediate needs to exceed 100MB for the temporary filesystem to be created, otherwise remediate will just use the default location under `/var/opt/opsware/agent`.
- 8** The default timeout should be sufficient for allocating/deallocating a filesystem. If for some reason, an AIX server takes longer than this to complete the `crfs` and `mount` operations, you can use the `OPSWremediate_action_script_timeout` custom attribute to increase the timeout beyond the default one minute.

The script will now be used whenever software is installed on the managed server.

Index

C

- configuration tracking
 - Opware SAS 6.0.1, availability in 13
- content migration
 - best practices of 16
 - complete migration, explained 13
 - example of 18
 - full migration, explained 10
 - inheritance and negative overrides 23
 - optimizing 18
 - preview only mode 15, 17
 - process for 8
 - rolling back 17
 - service levels 23
 - software installation dependencies 13
 - Software Tree permissions 25
 - sync permissions for 17, 26
 - template inheritance 24
 - templates 23
- custom attributes
 - migrating 23

E

- examples
 - content migration 18
 - Software Migration Tool, command syntax 18

N

- nodes
 - migrating 10

P

- packages
 - migrating 12
- permissions
 - Software Tree, migrating 25
 - synchronizing after content migration 26

R

- reconcile
 - content migration, affect on 12

S

- SAS Client Library
 - Migrated folder 11
- service levels
 - migrating 10, 23
- software installation dependencies
 - migrating 13
- Software Migration Tool
 - command syntax examples 17
 - command syntax for 16
 - running 15
- Software Tree
 - inheritance, migrating 23
 - migrating nodes 10
 - synchronizing permissions, migration 26
- Software Tree nodes
 - Opware-specific, migrating 10
- swmgmt-migrate.sh script, command syntax 16

T

- templates
 - inheritance, migrating 24
 - migrating 10, 23