FUJITSU

FUJITSU Software
Systemwalker Operation Manager

Upgrade Guide

UNIX/Windows(R)

J2X1-8184-03ENZ0(00)
January 2022

Preface

Purpose of This Document

This document describes the migration method, and notes when updating another version level of Systemwalker Operation Manager.

Intended Readers

This document is intended for users who will upgrade Systemwalker Operation Manager.

Abbreviations and Generic Terms Used

- The term "Windows Server 2019 " is used to refer to all of the following products:
  - Microsoft(R) Windows Server(R) 2019 Standard (x64)
  - Microsoft(R) Windows Server(R) 2019 Datacenter (x64)
- The term "Windows Server 2016" is used to refer to all of the following products:
  - Microsoft(R) Windows Server(R) 2016 Standard (x64)
  - Microsoft(R) Windows Server(R) 2016 Datacenter (x64)
- The term "Server Core" is used to refer to all of the following products:
  - Microsoft(R) Windows Server(R) 2019 Standard Server Core
  - Microsoft(R) Windows Server(R) 2019 Datacenter Server Core
  - Microsoft(R) Windows Server(R) 2016 Standard Server Core
  - Microsoft(R) Windows Server(R) 2016 Datacenter Server Core
- The term "Windows(R) 10" is used to refer to all of the following products:
  - Windows(R) 10 Home (x64)
  - Windows(R) 10 Pro (x64)
  - Windows(R) 10 Enterprise (x64)
- The term "Windows(R) 8.1" is used to refer to all of the following products:
  - Windows(R) 8.1 (x64)
  - Windows(R) 8.1 Pro (x64)
  - Windows(R) 8.1 Enterprise (x64)
- Windows Internet Explorer(R) is abbreviated as "Internet Explorer".
- Versions of Systemwalker Operation Manager that run on all of the following operating systems are referred to as "Windows versions of Systemwalker Operation Manager" or simply "Windows versions":
  - Windows
  - 64-bit versions of Windows, except Itanium
- Articles specific to the version of Systemwalker Operation Manager that runs on 32-bit versions of Windows are referred to as "Windows x86 version".
- Articles specific to the version of Systemwalker Operation Manager that runs on Itanium-compatible versions of Windows are referred to as "Windows for Itanium version".
- Articles specific to the version of Systemwalker Operation Manager that runs on 64-bit versions of Windows, except Itanium, are referred to as "Windows x64 version".

- Server Core, Windows Server 2019, and Windows Server 2016 may be abbreviated as "Windows servers".
- Oracle Solaris may be referred to as Solaris, Solaris Operating System or Solaris OS.
- Versions of Systemwalker Operation Manager that run on Solaris are referred to as "Solaris versions of Systemwalker Operation Manager" or simply "Solaris versions".
- Articles specific to the version of Systemwalker Operation Manager that runs on 32-bit versions of Solaris are referred to as "Solaris 32-bit version".
- Articles specific to the version of Systemwalker Operation Manager that runs on 64-bit versions of Solaris are referred to as "Solaris 64-bit version".
- Versions of Systemwalker Operation Manager that run on HP-UX are referred to as "HP-UX versions of Systemwalker Operation Manager" or simply "HP-UX versions".
- Versions of Systemwalker Operation Manager that run on AIX are referred to as "AIX versions of Systemwalker Operation Manager" or simply "AIX versions".
- Articles specific to the version of Systemwalker Operation Manager that runs on 64-bit versions of Linux, except Itanium, are referred to as "Linux x64 version" or simply "Linux versions".
- Articles specific to the version of Systemwalker Operation Manager that runs on 32-bit versions of Linux are referred to as "Linux x86 version".
- Articles specific to the version of Systemwalker Operation Manager that runs on Itanium-compatible version of Linux are referred to as "Linux for Itanium version".
- Solaris, HP-UX, AIX, Linux and Linux for Itanium versions of Systemwalker Operation Manager are referred to collectively as "UNIX versions of Systemwalker Operation Manager" or simply "UNIX versions".
- Solaris, HP-UX, AIX and Linux may be referred to as "UNIX servers".
- Systemwalker Operation Manager Standard Edition may be abbreviated as "SE".
- Systemwalker Operation Manager Enterprise Edition may be abbreviated as "EE".
- Standard Edition may be abbreviated as "SE" and Enterprise Edition may be abbreviated as "EE".
- Arcserve(R) Backup for Windows is abbreviated as "Arcserve".
- Microsoft(R)-Mail that is provided as a standard feature with Windows NT(R) is abbreviated as "MS-Mail".

Export Restriction

Exportation/release of this document may require necessary procedures in accordance with the regulations of your resident country and/or US export control laws.

Trademarks

Contents

Chapter 1 Migration Overview 1
1.1 Target Products for Migration 1
1.2 Conditions and Notes for Migration 2

Chapter 2 Migration Procedure 4
2.1 Procedure for Migrating on the Same Machine 4
2.2 Procedure for Migrating to Another Machine 6
2.2.1 Migration of Windows Version 6
2.2.2 Migration of UNIX Version 7
2.3 Procedure for Aggregating Multiple Systemwalker Operation Manager Servers on a Single Machine 12
2.3.1 Pre-Migration Tasks [Tasks at the Migration Source/Migration Destination] 16
2.3.2 Changing a Calendar Name on the Migration Source Server [Tasks at the Migration Source/Migration Destination] (Schedule Server) 16
2.3.3 Migrating Assets Manually [Tasks at the Migration Source/Migration Destination] (Schedule Server) 18
2.3.4 Migrating Assets by Extracting and Distributing Policy Data [Tasks at the Migration Source/Migration Destination] (Schedule Server) 21
2.3.5 Migration Tasks on the Execution Server [Tasks at the Migration Source/Migration Destination] 22
2.3.6 Post-Migration Tasks [Tasks at the Migration Destination] 23
2.4 Procedure for Migration in a Cluster Environment 23
2.5 Migrating Certificate/Key Management Environment 23

Chapter 3 OS Upgrading 28
3.1 OS Upgrading Procedure 1 (Upgrading Operation Manager Servers) 28
3.2 OS Upgrading Procedure 2 (Upgrading Operation Manager Clients) 30
3.3 OS Upgrading Procedure 3 (Reinstalling Systemwalker Operation Manager) 30

Chapter 1 Migration Overview

This chapter describes the major changes when Systemwalker Operation Manager is migrated to this product. It also describes the products that can be migrated and related important notes on migration.

1.1 Target Products for Migration

The following products can be migrated.

Server

[Windows]

	Architecture and Edition of Product	Source Version	Destination	
			V17.0.0	
			x64 SE	x64 EE
Source	x86 SE	V13.8.0 and earliler	P	P
	x86 EE		N/A	P
	x64 SE	V13.8.0 - V17.0.0	A	A
	x64 EE		N/A	A

A:The upgrade installation or reinstall between the same version is available.
P:Migration of definition information for extracting/distributing policy is available.
N/A: Migration is not available.

[Solaris]

	Architecture and Edition of Product	Source Version	Destination	
			V17.0.0	
			64bit SE	64bit EE
Source	32bit SE	V13.8.0 and earliler	P	P
	32bit EE		N/A	P
	64bit SE	V13.8.0 - V17.0.0	A	A
	64bit EE		N/A	A

A:The upgrade installation or reinstall between the same version is available.
P:Migration of definition information for extracting/distributing policy is available.
N/A: Migration is not available.

[Linux]

	Architecture and Edition of Product	Source Version	Destination	
			V17.0.0	
			x64 SE	x64 EE
Source	x86 SE	V13.8.0 and earliler	P	P
	x86 EE		N/A	P
	Itanium SE	V13.2.0 - V13.3.1	(Note)	(Note)
	Itanium EE	V12.0L10 - V13.3.1	N/A	(Note)

	Architecture and Edition of Product	Source Version	Destination	
			V17.0.0	
			x64 SE	x64 EE
	x64 SE	V13.3.1 - V17.0.0	A	A
	x64 EE		N/A	A

```
A:The upgrade installation or reinstall between the same version is available.
P:Migration of definition information for extracting/distributing policy is available.
N/A: Migration is not available.

Note: You can migrate if you meet all of the following prerequisites:
    [Prerequisite]
    - Migration to another machine
    - Destination OS: Red Hat Enterprise Linux 7/8
```

Client

	Architecture and Edition of Product	Source Version	Destination	
			V17.0.0	
			[Windows] 64bit SE/EE	[UNIX] 64bit SE/EE
Source	[Windows] x86/x64 SE/EE	V17.0.0 and earlier	A	A
	[UNIX] 32bit/64bit SE/EE	V17.0.0 and earlier	A	A

```
A:The upgrade installation or reinstall between the same version is available.
```

Refer to "Chapter 2 Migration Procedure" for the migration procedure.

1.2 Conditions and Notes for Migration

This section describes the conditions required for migration to this version and related notes.

Conditions for migration

The following conditions should be met for version migration to this version:

- The directory to back up the migration data should be located in the local disk (hard disk) of the migration source computer.
- The drive to back up the migration data should have an idle capacity that is large enough to back up the user's assets.
- The installation type of the migration source and migration target should be identical.
- The drive and directory names of the Systemwalker installation directory of the migration source machine should be respectively identical to those of the migration target machine.
- The migration data specified for restoration in the migration target computer should be the data collected by the tool (program) provided by this product.
- The code system of the migration source and migration target systems should be identical.

Notes on migration

The following notes are required for migration.

Information that is not migrated

If the following information is changed from the default in the source, the changed contents are not migrated, and they restore to default. Change them in the destination environment as necessary.

- Port number of Web console/Web API
- Environment definition file (httpd.conf) of Web server
- Port number of mpaclmgr
- Startup account [Windows]

Also, if the following was deleted, it returnes to the state immediately after installation.

- [SampleProject] project [Windows]

Migrating Systemwalker Operation Manager from V13.8.0 to V17.0.0 or later

- In the pre-migration environment, if you created the definition of encrypted communication (HTTPS communication) of Web console and you will use same certificate in the post-migration environment, you need to migrate certificate/key management environment. For the migration procedure, refer to the "2.5 Migrating Certificate/Key Management Environment".
- In the pre-migration environment, if you used the user/group definition on the Systemwalker authentication repository to set permissions for project, the target definition is deleted and registered in the destination.

Tasks required before migration

Check and perform the following tasks before migration:

- Back up the previous version.

  It is recommended to back up the operating environment of the previous version before proceeding with migration in order to prepare for unexpected problems during migration. Perform backup as described in the manuals for the previous version.

Tasks required after migration

Check and perform the following tasks after migration:

- Re-compiling applications that use Systemwalker Operation Manager APIs

  After migration, in case of applications that use Systemwalker Operation Manager APIs, it is necessary to compile them using header files for this version and libraries.

Chapter 2 Migration Procedure

This section describes the procedures to be employed in migrating Systemwalker Operation Manager's operating environments to this version.

2.1 Procedure for Migrating on the Same Machine

Use Systemwalker upgrade installation when migrating Systemwalker Operation Manager on the same machine. Systemwalker upgrade installation allows migration from an earlier version to this version and also migration from SE edition of this version to EE edition of this version.

For upgrade installation procedure, see *Systemwalker Operation Manager Installation Guide*.

Notes on migrating on the same machine

Definition of Process Monitoring function and daemon startup command

Automatic migration of the definition of Process Monitoring function and Daemon Startup command is not available.

The definition given prior to the migration is saved in the same folder with a file name appended with ".XXXXXXXX_trans" or ".beforeXXXXXXXX". You can therefore modify the definition file of this version as needed, referring the saved file. ("XXXXXXXX" shows the version level of this product.)

The definition files to be backed up are as listed below. For details on the definition files, see *Systemwalker Operation Manager Installation Guide*.

[Windows version]

- Systemwalker installation directory \mpwalker.jm\mpcmtool\pmon\etc\mppmon.usr
- Systemwalker installation directory \mpwalker.jm\mpcmtool\pmon\etc\mppmon.ini
- Systemwalker installation directory \mpwalker.jm\mpcmtool\pmon\bin\mppmonsnd.bat

[UNIX version]

- /etc/opt/FJSVftlo/pmon/mppmon.usr
- /etc/opt/FJSVftlo/pmon/mppmon.ini
- /opt/FJSVftlo/pmon/bin/mppmonsnd.sh
- /etc/opt/FJSVftlo/daemon/custom/rc3.ini

Job execution history information and operation record information

If any of the directories listed below, or their respective subdirectories, is specified as **Saved Directory** under **Save job execution history information**, or as **Saved Directory** under **Save operation results data**, in the **Logging** sheet of the **Define Operating Information** window on the machine from where the information is migrated, the job execution history information and the operation record information are not migrated.

[Windows version]

- <*Systemwalker installation directory*>\MPWALKER.JM\mpmjessv\mjespool
- <*Systemwalker installation directory*>\MPWALKER.JM\mpmjessv\mjes*n*\mjespool

  The "*n*" in "mjes*n*" is the subsystem number for subsystems 1 to 9.

[UNIX version]

- /opt/<*package name*> (*1)
- /etc/opt/<*package name*>
- /var/opt/<*package name*>
- /var/spool/mjes (*2)

*1

<*package name*> is the name of a package noted in the list of packages in the Release Note.

*2

Note that /var/spool/mjes, the directories below, and their respective subdirectories are not migrated:

- /var/spool/mjes/_jctl
- /var/spool/mjes/jclinfo
- /var/spool/mjes/log
- /var/spool/mjes/mjes*n* (*n*: 1-9)
- /var/spool/mjes/mjespool
- /var/spool/mjes/mjsinfo

All directories, except for those above, are migrated. For example, /var/spool/mjes/hist (directory that stores the job execution history immediately after installation) is migrated.

If the job execution history information and the operation record information are required when a saved directory that will not be migrated has been specified, back them up before performing the upgrade installation.

After performing the upgrade installation, change **Saved Directory** to a directory other than those listed above, and copy the backed up information files to the new directory. Note, however, that information files for the day of the upgrade installation itself must not be copied by overwriting. To reference pre-upgrade installation information on the day of the upgrade, refer to the files at the backup destination.

Information

Displaying the Gantt chart for executed job nets

If job nets have been executed on the day of the upgrade but prior to it, they will not be displayed in the Gantt chart after the upgrade.

The history of job nets not displayed in the Gantt chart can be checked in the **Job Net History** window.

From the next day, these jobs will be displayed in the Gantt chart when you specify a past date.

Remaining package without deleting [UNIX]

If you upgrade the Systemwalker Operation Manager from the V13.8.0 and earlier to the V17.0.0 or later, the following package of the bundled products remain without deleting.

[Solaris]

FJSVsmee

FJSVsclr

FJSVsme64

FJSVscl64

You can delete package listed above by executing the following command.

```
pkgrm Package name
```

[Linux]

FJSVsmee64

FJSVsclr64

You can delete package listed above by executing the following command.

```
rpm -e Package name
```

- When you created the definition of encrypted communication (HTTPS communication) of Web console in the source server

  Refer to the "2.5 Migrating Certificate/Key Management Environment" and migrate certificate as necessary. After migrating certificate, delete it with checking that other products are not using it.

- When you did not create the definition of encrypted communication (HTTPS communication) of Web console in the source server

  Delete it with checking that other products are not using it.

2.2 Procedure for Migrating to Another Machine

This section describes the procedure for migrating Systemwalker Operation Manager to a different machine.

2.2.1 Migration of Windows Version

Use the policy information extraction/distribution functions when migrating Systemwalker Operation Manager of the Windows version to another machine.

Prepare a machine for a client of Systemwalker Operation Manager separately from a target machine to install the Systemwalker Operation Manager client functions of the same version with the target machine.

1. Extracting policy information

   To extract the policy information, connect to the source machine from the client of Systemwalker Operation Manager of this version.

   For details on the policy information extraction procedure, see "Definitions when Constructing the Existing Environment on Another Server" in the *Systemwalker Operation Manager Installation Guide*.

   Note

   When Systemwalker Centric Manager is installed on the target machine, remove the followings from the target of policy extraction.

   - **Extract Policy** window - **Environment definition** sheet: **Action** checkbox under **Action Control**.
   - **Extract Policy** window - **Registration information** sheet: **Event monitoring condition** checkbox under **Event monitoring**.

2. Installing Systemwalker Operation Manager to a target machine

   Install Systemwalker Operation Manager of this version to the target machine. Pay attention to the followings for installation.

   - Use the same installation directory for both the target machine and source machine.
   - If the "shutdown process" job net has been defined in Jobscheduler, it becomes necessary to make settings again for the shutdown process job net. Refer to "Shutting Down the System at Optional Times [Windows version]" in the *Systemwalker Operation Manager User's Guide* for details on "shutdown process job net".
   - Register the user ID used as the project owner on the source machine in the target machine. Likewise, register in the target machine the user ID that has been used on the source machine for setting up the access rights.
   - If an environment for multi-subsystem operation is migrated, it is necessary to build the same multi-subsystem operation environment on the target machine, beforehand.

   For more information on the installation procedure and environment settings, see the *Systemwalker Operation Manager Installation Guide*.

3. Distributing policy information

   Distribute the policy information extracted in step 1 by connecting to the target machine from a client of Systemwalker Operation Manager of this version.

   Distributing the policy information copies the resources on the source machine to the target machine.

   For details on the policy information distribution procedure, see "Definitions when Constructing the Existing Environment on Another Server" in the *Systemwalker Operation Manager Installation Guide*.

4. Changing IP Address and Host Names

   If an IP address differs between the source and target machines, review the IP address and host name-related definition data of the target machine and other Systemwalker Operation Manager machines to be linked. Then modify the setting as needed.

   For the definition information to be reviewed, see "Changing the IP Addresses and Host Names" in the *Systemwalker Operation Manager Installation Guide*.

5. Define user restrictions

   When the **Define Operation Manager Shared Parameter** window is opened by clicking the **Shared parameter** button in the **Systemwalker Operation Manager Environment Setup** window on the source machine and **Operation Manager user restrictions** is disabled by checking, **Operation Manager user restrictions** in the **Define Operation Manager Shared Parameter** window of the target machine must be disabled, too.

6. Definitions of Process Monitoring function

   Definitions of the Process Monitoring function are not migrated automatically.

   If any of the following files has been customized on the migration source machine, it must be customized also on the target machine.

   The following three definition files are saved. For details on the definition files, see *Systemwalker Operation Manager Installation Guide*.

   - Systemwalker installation directory \mpwalker.jm\mpcmtool\pmon\etc\mppmon.usr
   - Systemwalker installation directory \mpwalker.jm\mpcmtool\pmon\etc\mppmon.ini
   - Systemwalker installation directory \mpwalker.jm\mpcmtool\pmon\bin\mppmonsnd.bat

Note

- When the job owner information has been defined, redefine the job owner information. For how to set it, see "Defining the Job Owner Information [Windows version]" in the *Systemwalker Operation Manager Installation Guide.*
- The job execution history information and the operation record information are not migrated. If this information needs to be migrated, perform migration by transferring files between servers. Note that information files for the day of migration itself must not be copied by overwriting. To reference pre-migration information on the day of migration, refer to the copy source files.
- If a directory under <*Systemwalker installation directory*>\MPWALKER.JM\mpmjessv\mjespool is specified as **Saved Directory** under **Save job execution history information**, or as **Saved Directory** under **Save operation results data**, in the **Logging** sheet of the **Define Operating Information** window, it must be changed to a directory other than the one in <*Systemwalker installation directory*>\MPWALKER.JM\mpmjessv\mjespool after policy application.

2.2.2 Migration of UNIX Version

Use the backup command for migration and the conversion/registration command for migration when migrating Systemwalker Operation Manager of the UNIX version to another machine.

It is possible to perform migration between the machines with the same architecture or from the Linux for Itanium machine to the Linux x64 machine.

1. Installing Systemwalker Operation Manager to a target machine

   Install Systemwalker Operation Manager of this version to the target machine. Pay attention to the followings for installation.

   - Use the same installation directory for both the target machine and source machine.
   - Register the user ID used as the project owner on the source machine in the target machine. Likewise, register in the target machine the user ID that has been used on the source machine for setting up the access rights.
   - In migrating an environment where multi-subsystem operation is running, the target system is automatically caused to be the subsystem environment, making it unnecessary to newly build the subsystem environment on it. Note, however, you need to specify a port number for the subsystems in the services file.

   See the *Systemwalker Operation Manager Installation Guide* for more information on installation, environment settings and setting port numbers for subsystems.

2. Shutting down the operations of jobs by Systemwalker Operation Manager

   Shut down the operations of jobs by Systemwalker Operation Manager on both the source and target machines. Since the daemons used by Systemwalker Operation Manager is stopped automatically when the backup command for migration or the conversion/registration command for migration is executed. So you don't have to stop them.

   In environments that also include Systemwalker Centric Manager, each daemon of Systemwalker Centric Manager will also be stopped automatically.

3. Executing the backup command for migration

   Insert the product media for this version of Systemwalker Operation Manager into the drive on the source machine, and then execute the backup command for migration as below:

   Refer to "Executing the backup command for migration on a Solaris (Non-global Zone) system" when executing the backup command for migration on a Solaris 10 or later (Non-global Zone) system.

   [Solaris version]

   ```
   <DVD root>/Solaris/unx/tool/swmove -b <backup destination directory>
   ```

   [Linux version]

   ```
   <DVD root>/Linux/unx/tool/swmove -b <backup destination directory>
   ```

   [HP-UX/AIX version]

   ```
   <cdrom root>/unx/tool/swmove -b <backup destination directory>
   ```

   Note

   If the migration is performed from the Linux for Itanium machine to the Linux x64 machine, use the product media for Linux x64 and execute the command.

4. Executing the conversion/registration command for migration

   Insert the product media for this version of Systemwalker Operation Manager into the drive on the source machine, and then execute the conversion/registration command for migration as below:

   Refer to "Executing the conversion/registration command for migration on a Solaris (Non-global Zone) system" when executing the conversion/registration command for migration on a Solaris 10 or later (Non-global Zone) system.

   [Solaris version]

   ```
   <DVD root>/Solaris/unx/tool/swtrans -b <backup destination directory>
   ```

   [Linux version]

```
<DVD root>/Linux/unx/tool/swtrans -b <backup destination directory>
```

[HP-UX/AIX version]

```
<cdrom root>/unx/tool/swtrans -b <backup destination directory>
```

5. Changing IP address and host name

   If an IP address differs between the source and target machines, review the IP address and host name-related definition data of the target machine and other Systemwalker Operation Manager machines to be linked. Then modify the setting as needed.

   For the definition information to be reviewed, see "Changing the IP Addresses and Host Names" in the *Systemwalker Operation Manager Installation Guide*.

6. Definitions of process monitoring function and daemon startup command

   If the version level differs between the source and target machines, definitions for the process monitoring function and daemon startup command are not migrated automatically.

   In this case, the definition given prior to the migration is saved in the same folder with a file name appended with ".beforeXXXXXXXX ". You can therefore modify the definition file of this version as needed, referring the saved file. ("XXXXXXXX" shows the version level of this product.)

   The following four definition files are saved. For details on the definition files, see *Systemwalker Operation Manager Installation Guide*.

   - /etc/opt/FJSVftlo/pmon/mppmon.usr
   - /etc/opt/FJSVftlo/pmon/mppmon.ini
   - /opt/FJSVftlo/pmon/bin/mppmonsnd.sh
   - /etc/opt/FJSVftlo/daemon/custom/rc3.ini

Note

When the Extended User Management Function is used, Operation Manager User Information and Access Right Information are migrated as described below.

- When the Extended User Management function is enabled on the source machine, the Extended User Management function will be enabled on the target machine regardless of whether or not it is enabled on it. And the Operation Manager User information and Operation Manager User's access right to the project will be migrated.
- When the Extended User Management Function is disabled on the source machine, it will be disabled on the target machine regardless of whether or not it is enabled or disabled on it, and OS user's access right to the project will be migrated.

If Operation Manager User is existent on the target machine, Operation Manager User Information is replaced with Operation Manager User Information of the source machine.

Note

Job execution history information and operation record information

The job execution history and the operation record information are migrated only if one of the directories listed below, or their respective subdirectories, is specified as **Saved Directory** under **Save job execution history information**, or as **Saved Directory** under **Save operation results data**, in the **Logging** sheet of the **Define Operating Information** window on the machine from where the information is migrated.

- /var/spool/mjes/*XXX*

  XXX is optional.

  However, migration will not take place if any of the directories below, or their respective subdirectories, is specified:

- /var/spool/mjes/_jctl
- /var/spool/mjes/jclinfo
- /var/spool/mjes/log
- /var/spool/mjes/mjes*n* (*n*: 1-9)
- /var/spool/mjes/mjespool
- /var/spool/mjes/mjsinfo

If the job execution history information and the operation record information are required when a saved directory that will not be migrated has been specified, perform migration by transferring files between servers. Note that information files for the day of migration itself must not be copied by overwriting. To reference pre-migration information on the day of migration, refer to the copy source files.

Executing the backup command for migration on a Solaris (Non-global Zone) system

The following explains the procedure for executing the backup command for migration on a Solaris 10 or later (Non-global Zone) system.

1. Log in to the Global Zone.

   Log in to the Global Zone as the root user (administrator).

2. Insert the Systemwalker Operation Manager product media into the drive.

   Insert the product media for this version of Systemwalker Operation Manager into the drive device. If the volume management daemon is not being used, it is necessary to mount the drive device manually. Since the device name of the drive device will vary depending on the environment, check it beforehand.

   The following is an example of how to mount:

   ```
   # mount -F hsfs /dev/dsk/<device name> <mount destination directory>
   ```

3. Copy the contents of the product media to the disk on the Global Zone.

   (In the following example, the contents of the product media are copied to the "/PKG" directory.)

   ```
   # cp -rfp <mount point>/unx/tool /PKG
   ```

4. Stop the Non-global Zone on the migration source.

   Use the following command to stop the Non-global Zone that has been already created.

   (In the following example, the name of Non-global Zone on the migration source is "SWZONE".)

   ```
   # /usr/sbin/zoneadm -z SWZONE halt
   ```

5. Set up the zone configuration.

   Use the following commands to enable the product media contents that were copied in step 3 to be viewed from the Non-global Zone as well.

   ```
   # zonecfg -z SWZONE
   zonecfg:SWZONE> add fs                <- Enter "add fs".
   zonecfg:SWZONE:fs> set dir=/SWPKG     <- Enter "set dir=/SWPKG".
   zonecfg:SWZONE:fs> set special=/PKG   <- Enter "set special=/PKG".
   zonecfg:SWZONE:fs> set type=lofs      <- Enter "set type=lofs".
   zonecfg:SWZONE:fs> set options=ro     <- Enter "set options=ro".
   zonecfg:SWZONE:fs> end                <- Enter "end".
   zonecfg:SWZONE> commit                <- Enter "commit".
   zonecfg:SWZONE> exit                  <- Enter "exit".
   ```

   Once specified, the product media contents copied to the Global Zone can be referred to as the read-only file system from the /SWPKG directory of Non-global Zone after the next startup of Non-global Zone.

6. Start the Non-global Zone on the migration source.

   Use the following command to start the Non-global Zone that already exists.

   ```
   # /usr/sbin/zoneadm -z SWZONE boot
   ```

7. Execute the backup command for migration.

   Log in to the Non-global Zone and execute the backup command for migration from the directory that was set in step 5 so that it can be viewed from the Non-global Zone.

   ```
   # /SWPKG/swmove -b backup destination directory
   ```

When it is no longer necessary to refer to the /SWPKG directory from the Non-global Zone after the command was executed, it is possible to cancel the settings using the command below.

At this time, stop the Non-global Zone before deleting the /PKG directory.

```
# zonecfg -z SWZONE
zonecfg:SWZONE> remove fs dir=/SWPKG
zonecfg:SWZONE> commit
zonecfg:SWZONE> exit
# rm -fr /PKG
```

Executing the conversion/registration command for migration on a Solaris (Non-global Zone) system

The following explains the procedure for executing the conversion/registration command on a Solaris 10 or later (Non-global Zone) system.

1. Log in to the Global Zone.

   Log in to the Global Zone as the root user (administrator).

2. Insert the Systemwalker Operation Manager product media into the drive.

   Insert the product media for this version of Systemwalker Operation Manager into the drive device. If the volume management daemon is not being used, it is necessary to mount the drive device manually. Since the device name of the drive device will vary depending on the environment, check it beforehand.

   The following is an example of how to mount:

   ```
   # mount -F hsfs /dev/dsk/<device name> <mount destination directory>
   ```

3. Copy the contents of the product media to the disk on the Global Zone.

   (In the following example, the contents of the product media are copied to the "/PKG" directory.)

   ```
   # cp -rfp <mount point>/unx/tool /PKG
   ```

4. Stop the Non-global Zone on the migration target.

   Use the following command to stop the Non-global Zone that has been already created.

   (In the following example, the name of Non-global Zone on the migration target is "SWZONE".)

   ```
   # /usr/sbin/zoneadm -z SWZONE halt
   ```

5. Set up the zone configuration.

   Use the following commands to enable the product media contents that were copied in step 3 to be viewed from the Non-global Zone as well.

   ```
   # zonecfg -z SWZONE
   zonecfg:SWZONE> add fs                <- Enter "add fs".
   zonecfg:SWZONE:fs> set dir=/SWPKG     <- Enter "set dir=/SWPKG".
   zonecfg:SWZONE:fs> set special=/PKG   <- Enter "set special=/PKG".
   ```

```
zonecfg:SWZONE:fs> set type=lofs      <- Enter "set type=lofs".
zonecfg:SWZONE:fs> set options=ro     <- Enter "set options=ro".
zonecfg:SWZONE:fs> end                <- Enter "end".
zonecfg:SWZONE> commit                <- Enter "commit".
zonecfg:SWZONE> exit                  <- Enter "exit".
```

Once specified, the product media contents copied to the Global Zone can be referred to as the read-only file system from the /SWPKG directory of Non-global Zone after the next startup of Non-global Zone.

6. Start the Non-global Zone on the migration target.

   Use the following command to start the Non-global Zone that already exists.

   ```
   # /usr/sbin/zoneadm -z SWZONE boot
   ```

7. Execute the conversion/registration command for migration.

   Log in to the Non-global Zone and execute the backup command for migration from the directory that was set in step 5 so that it can be viewed from the Non-global Zone.

   ```
   # /SWPKG/swtrans -b backup destination directory
   ```

When it is no longer necessary to refer to the /SWPKG directory from the Non-global Zone after the command was executed, it is possible to cancel the settings using the command below.

At this time, stop the Non-global Zone before deleting the /PKG directory.

```
# zonecfg -z SWZONE
zonecfg:SWZONE> remove fs dir=/SWPKG
zonecfg:SWZONE> commit
zonecfg:SWZONE> exit
# rm -fr /PKG
```

EE

2.3 Procedure for Aggregating Multiple Systemwalker Operation Manager Servers on a Single Machine

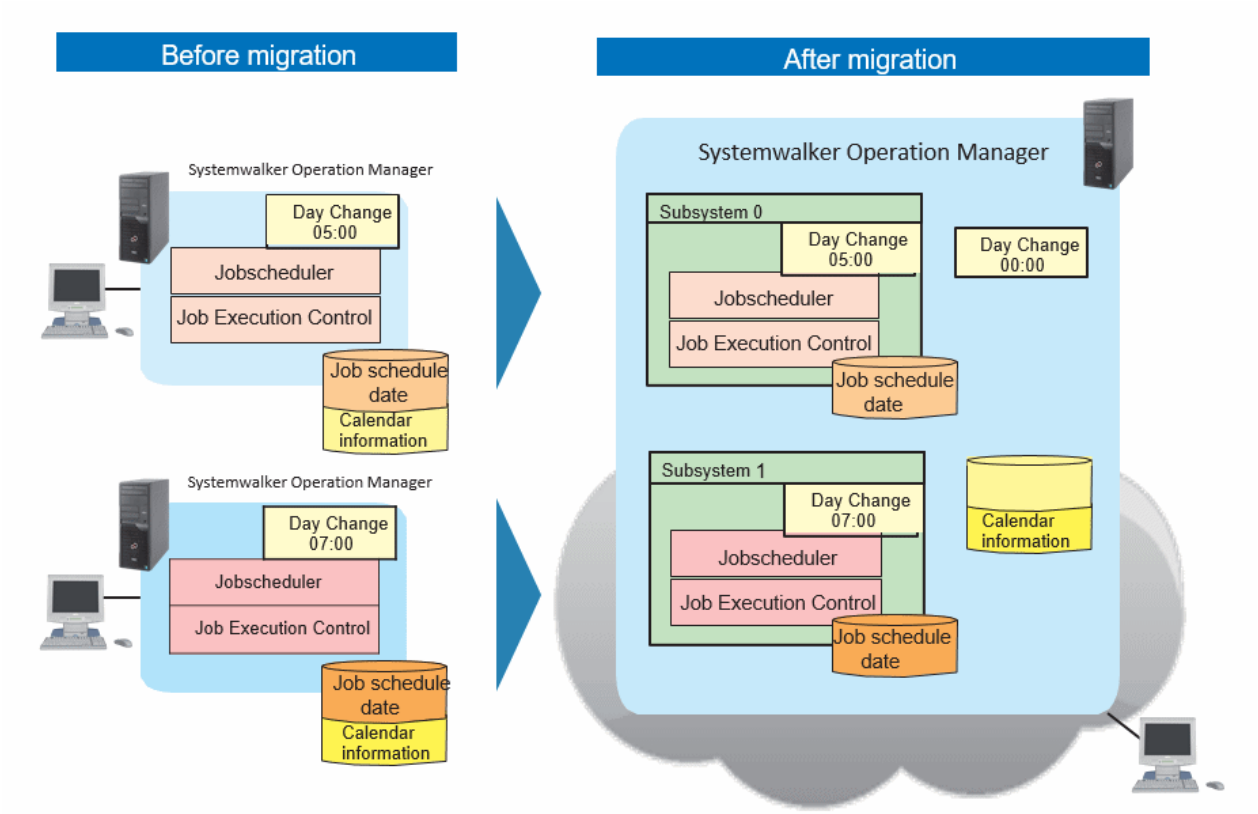
This section describes how to aggregate jobs that are running on multiple Systemwalker Operation Manager servers onto one machine.

Migrate the Systemwalker Operation Manager servers to a Systemwalker Operation Manager subsystem that runs on, for example, a virtual machine. This enables you to aggregate jobs that are distributed across multiple servers onto a single server while retaining mutually independent operation. This system aggregation reduces the costs required for management, operation, and maintenance.

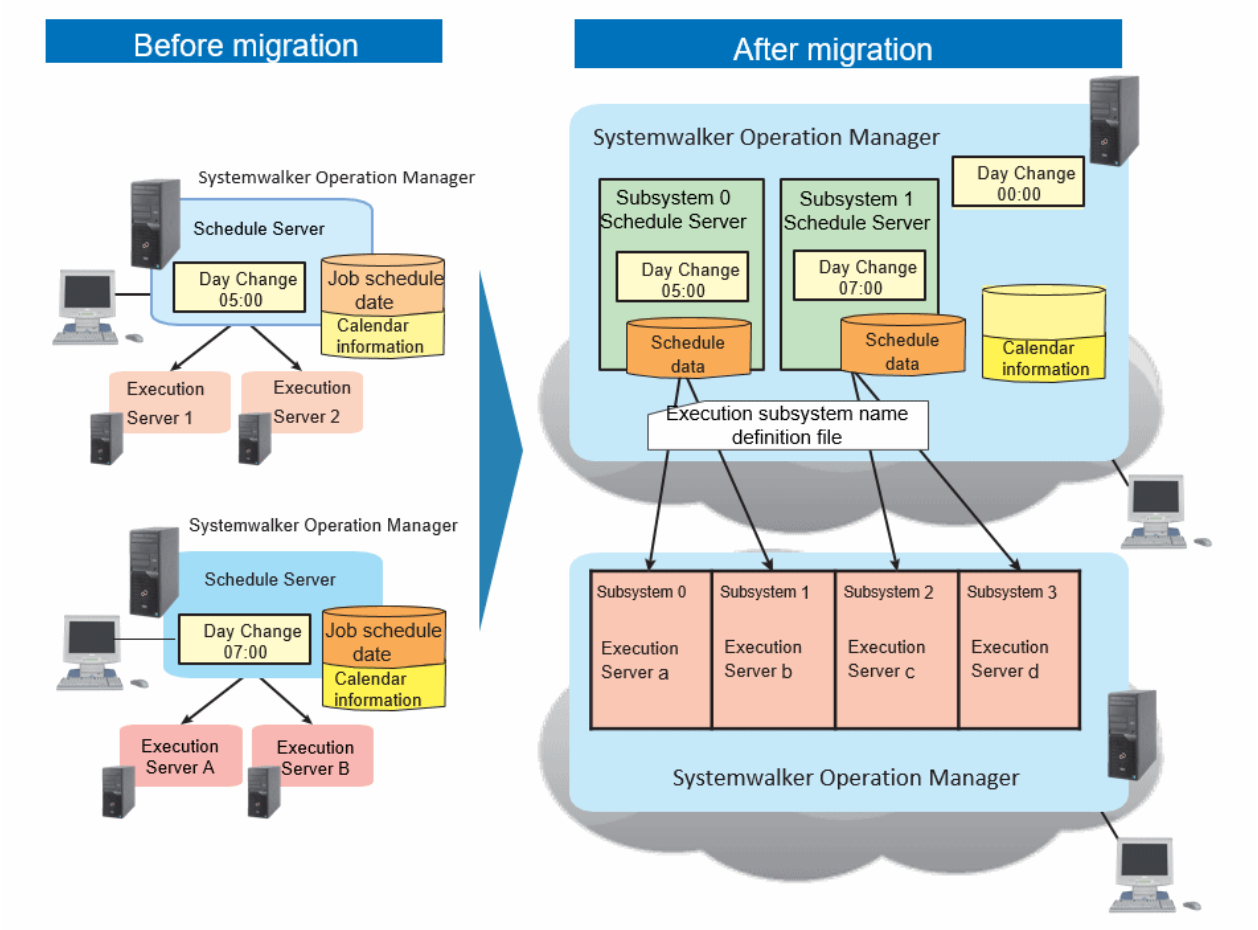
Overview of migration

The figure below provides an illustrated overview of migrating Systemwalker Operation Manager jobs as a Systemwalker Operation Manager subsystem that runs on a virtual machine.

Overview of migration for running jobs on a single server

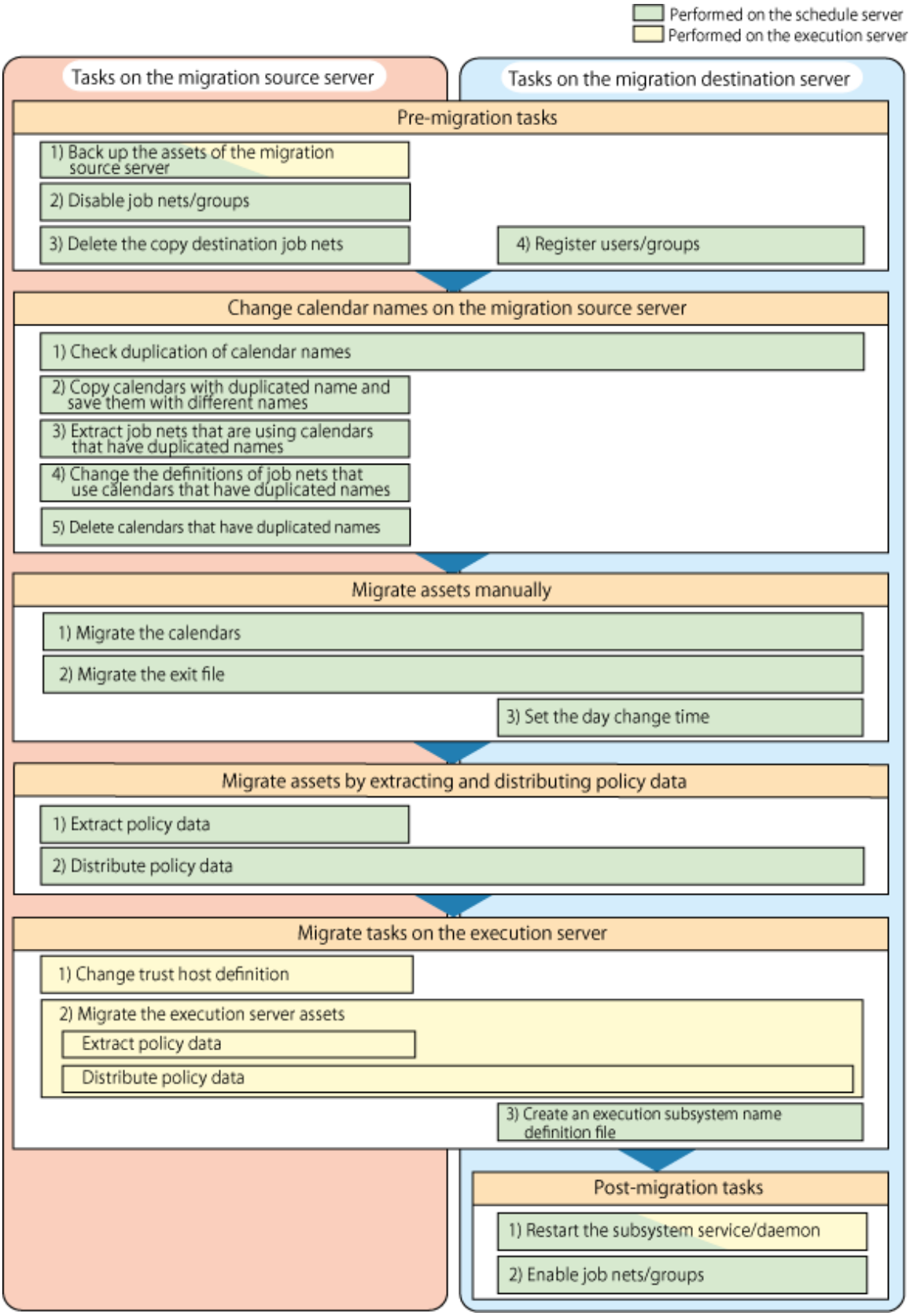


Overview of migration for scheduling and executing jobs on different servers



Migration steps

The following figure shows the migration steps:



Note

- Only a system administrator (a member of the Administrators group or the superuser) can perform migration.

- Do not perform migration while the calendar year will change.

2.3.1 Pre-Migration Tasks [Tasks at the Migration Source/Migration Destination]

Before starting migration, back up the assets and disable the job nets of the migration source server. This section describes these tasks.

1) Backing up the assets of the migration source server (schedule server/execution server) [migration source]

Back up the assets of the migration source server.

If jobs are being scheduled and executed on different servers and the execution server is also to be migrated, also back up the execution server assets of the migration source.

Refer to "Backing Up or Restoring Operation Environment" in the *Systemwalker Operation Manager Installation Guide* for details.

2) Disabling job nets/groups (schedule server) [migration source]

Disable the job nets and groups of the migration source server.

To ensure that the migrated job nets and groups do not run before operation starts on the migration destination server, disable the job nets and groups of the migration source server beforehand.

Perform the following procedure for all projects that are registered in the migration source server:

1. Select a project in the job selection tree of the Systemwalker Operation Manager client.
2. Click **File** >> **Batch Processing** >> **Disable All** to disable the job nets and groups in that project.

3) Deleting the copy destination job nets (schedule server) [migration source]

Delete the copy destination job nets that were created with copy and startup.

Perform the following procedure for all copy destination job nets that are registered in the migration source server:

1. Select a copy destination job net in the job selection tree of the Systemwalker Operation Manager client.
2. Click **File** >> **Delete** to delete the copy destination job net.

4) Registering users/groups (schedule server) [migration destination]

The same users/groups as those registered to the operating system on the migration source server are also registered to the operating system on the migration destination server. Perform the following procedure.

1. On the migration source server, execute the mplstacluser command to list the users and groups with access rights to the project.
2. The users and groups displayed in 1 are also registered to the operating system on the migration destination server.

2.3.2 Changing a Calendar Name on the Migration Source Server [Tasks at the Migration Source/Migration Destination] (Schedule Server)

If the same calendar name is registered in the migration source server and migration destination server, you must take advance action on the migration source server to prevent overwriting during migration.

This section describes how to change a duplicated calendar name and the job net definition that uses it on the migration source server.

1) Checking duplication of calendar names [migration source/migration destination]

Confirm that the same calendar name is not registered on both the migration source server and migration destination server.

Perform one of the following at the migration source and migration destination, and compare the calendar names of the source and destination:

- On the Systemwalker Operation Manager client, display the **Calendar List** window.
- On the server, execute the jobschprint command with the -v option to output a list of the calendar names.

2) Copying a calendar with a duplicated name and saving it with a different name [migration source]

Copy a calendar that has a duplicated name and create a calendar that has a different name from that at the migration destination.

Perform one of the procedures below for all calendars (including SYSTEM_CALENDAR) that have duplicated names.

On the client

1. Select the target calendar in the job selection tree and display the **Add Calendar** window.
2. Click **File** >> **Save** to display the **Save Calendar** dialog box.
3. Specify a name that is not registered at the migration destination, and save the calendar.

On the server

1. Execute the jobschprint command with the -rh option and the name of the target calendar to output the result (holiday information control statement) to a file.
2. Edit the file that you output in step 1 and change the calendar name in the calendarname control statement to a name that is not registered at the migration destination.
3. To register the calendar, execute the jobschsethol command with the -ent option and the name of the file that you edited in step 2.

3) Extracting job nets that are using a calendar that has a duplicated name [migration source]

Perform one of the procedures below for all calendars that have duplicated names to extract the job nets that are using the calendars.

On the client

1. Select the target calendar in the job selection tree and click **File** >> **Status** to display the **Calendar Status** dialog box.
2. Browse the **Used in Job net** list and confirm the job nets that are using a calendar.

On the server

1. Execute jobschprint with the -a option to output the result (property information for the registered job nets) to a file.
2. Use a text editor or similar program to open the file that you output in step 1 and search for job nets that have duplicate calendar names in the "Calendar Name" line.

4) Changing the definition of a job net that is using a calendar that has a duplicated name [migration source]

Perform one of the procedures below for all job nets that are using a calendar that has a duplicated name to change the job net definition:

On the client

1. Select the target job net in the job selection tree and click **File** >> **Export** to display the Systemwalker Operation Manager Export window.
2. Export the definition information.

3. Edit the definition file that you exported in step 2, changing the calendar name to the name of the calendar you copied and created in 2) above.
4. Specify the project in which the target job net has been registered, and click **File** >> **Import** to display the Systemwalker Operation Manager Import window.
5. Import the file that you edited in step 3.

On the server

1. Execute the jobschprint command with the -r, -detail, and -operate options and the name of the target job net to output the result (job net control statement) to a file.
2. Edit the file that you output in step 1, changing the calendar name that is specified in the holidaycalendar operand to the name of the calendar that you copied and created in 2).
3. Execute the jobschsetnet command with the -nche option and the name of the file that you edited in step 2.

5) Deleting a calendar that has a duplicated name [migration source]

Perform one of the following to delete a calendar (other than SYSTEM_CALENDAR) that has a duplicated name:

- Select the target calendar in the job selection tree of the Systemwalker Operation Manager client and click **File** >> **Delete**.
- On the server, execute the jobschsethol command with the -del option and the name of the target calendar.

2.3.3 Migrating Assets Manually [Tasks at the Migration Source/ Migration Destination] (Schedule Server)

This section explains how to migrate **Calendar** and **Exit file**, which cannot be migrated by extraction and distribution of policy data, from the migration source server to the migration destination server.

1) Migrating the calendar [migration source/migration destination]

Perform the procedures below to migrate the calendar:

On the migration source server

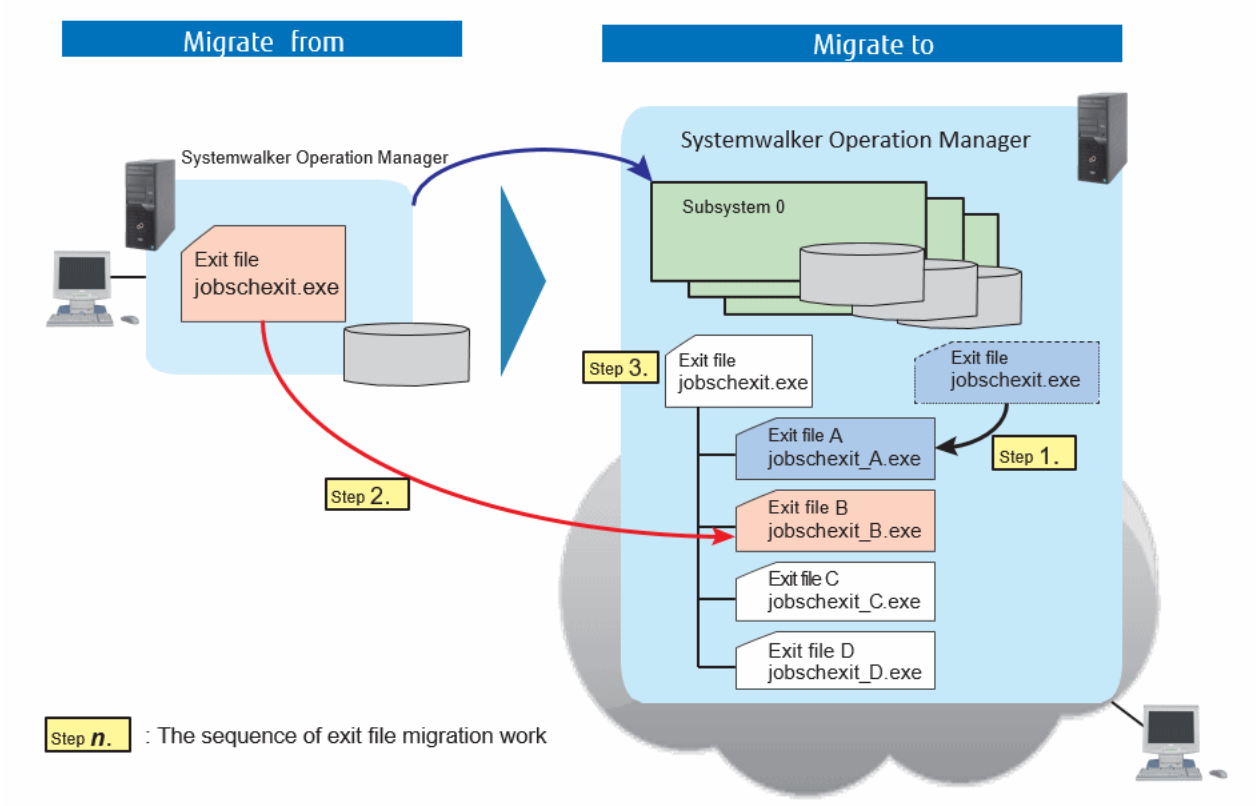
1. Execute the jobschprint command with the -v option to output a list of the calendar names.
2. Execute the jobschprint command with the -rh option for all calendars that you output in step 1 to output the result (holiday information control statement) to a file. Save the output result in a different file for each calendar.
3. Transfer the file that you created in step 1 to the migration destination server.

On the migration destination server

1. Specify the file that contains the output result and execute the jobschsethol comment with the -ent option.
2. Perform step 1 for all files that you transferred from the migration source.

2) Migrating the exit file [migration source/migration destination]

The following figure illustrates migration of the exit file:



Perform the following procedure to migrate the exit file:

1. On the migration destination server, change the name of the exit file that has the same name as the exit file to be migrated from the migration source server (example: jobschexit.exe).

   Example: Change jobschexit.exe to jobschexit_A.exe.

2. Copy the exit file from the migration source server to the exit file storage location (*1) on the migration destination server. Change the name of the exit file when copying it.

   Example: Change jobschexit.exe to jobschexit_B.exe.

3. Create an exit program for the migration destination server. (*2)

   The file name of the exit program on the migration destination server must be the same as the target exit file (example: jobschexit.exe). In addition, configure the exit program so that, when it is called, it checks the subsystem number that is passed by the argument and determines whether to call the exit file from step 1 or the exit file from step 2. (Refer to the program example below.)

4. Store the exit program in the exit file storage location (*1) on the migration destination server.

***1:**

Refer to the *Systemwalker Operation Manager Reference Guide* for details.

***2:**

If an exit program has already been created and stored, modify the processing so that the exit file in step 2 is called from the exit program.

The example below shows the program for a job net abnormal termination exit file (jobschexit.exe or jobsch.exit) that internally calls another exit file.

[Windows]

```
@ECHO OFF

SET bin_path="C:\Systemwalker\MPWALKER.JM\bin"
```

```
SET common_bat="%bin_path%\jobschexit_common.bat"
SET common_exe="%bin_path%\jobschexit_common.exe"
SET subsystem_bat="%bin_path%\jobschexit_subsys%7.bat"
SET subsystem_exe="%bin_path%\jobschexit_subsys%7.exe"

IF EXIST %subsystem_bat% (GOTO SUBSYS_BAT_EXEC)
IF EXIST %subsystem_exe% (GOTO SUBSYS_EXE_EXEC)
IF EXIST %common_bat% (GOTO COMMON_BAT_EXEC)
IF EXIST %common_exe% (GOTO COMMON_EXE_EXEC) ELSE GOTO BAT_END

:SUBSYS_BAT_EXEC
%subsystem_bat% %*
GOTO BAT_END

:SUBSYS_EXE_EXEC
%subsystem_exe% %*
GOTO BAT_END

:COMMON_BAT_EXEC
%common_bat% %*
GOTO BAT_END

:COMMON_EXE_EXEC
%common_exe% %*
GOTO BAT_END

:BAT_END
exit /b 0
```

[UNIX]

```
#!/bin/sh

bin_path="/opt/FJSVJOBSC/bin"

common_exit="$bin_path/jobsch_common.exit"
subsystem_exit="$bin_path/jobsch_subsys$7.exit"

echo $common_exit
echo $subsystem_exit

if [ -f $subsystem_exit ]; then
        `$subsystem_exit $*`
elif [ -f $common_exit ]; then
        `$common_exit $*`
fi

exit 0
```

Note

- Migrate the exit file while it is not running (for example, when no jobs are being scheduled if it is a job termination exit).
- If you change the exit file name, the exit file will not be subject to backup and restore, so you will have to back it up and restore it separately.

3) Setting the day change time [migration destination]

If the migration source server and migration destination server have different day change times, set the subsystem day change time at the migration destination to match the day change time of the migration source server.

2.3.4 Migrating Assets by Extracting and Distributing Policy Data [Tasks at the Migration Source/Migration Destination] (Schedule Server)

Using the function for extracting and distributing policy data, migrate the assets of the migration source server to the migration destination server.

Refer to the *Systemwalker Operation Manager Installation Guide* for details.

1) Extracting policy data on the migration source server [migration source]

Extract the assets of the migration source server by connecting the **Systemwalker Operation Manager Environment Setup** client to the migration source server and extracting the policy data.

Definition items that should not be extracted

You must take care when extracting policy data.

Distributing all the Systemwalker Operation Manager definitions and information listed below at the migration destination overwrites them on the migration destination server. Therefore, exclude these definitions and information as policy extraction targets.

Definitions to be excluded from extraction

- **Environment definition** of the **Extract Policy** window

  Common

  - **Monitored host**
  - **Shared parameter** (UNIX)

  Jobscheduler

  - **Monitoring permission host**

  Master schedule management

  - **Environment setup**

  Action control

  - **Action** (Windows)

- **Registration information** of the **Extract Policy** window

  Common

  - **Operation Manager user**

  Calendar

  - **Calendar**

  Jobscheduler

  - **Exit file**

  Service/application execution

  - **Service/application execution**

  Event monitoring

  - **Event monitoring condition** (Windows)

If you need to migrate this information, do so manually (by defining them on the migration destination server).

Refer to "2.3.3 Migrating Assets Manually [Tasks at the Migration Source/Migration Destination] (Schedule Server)" for information on migrating **Calendar** and **Exit file**.

Refer to "Migrating Assets Manually [Tasks at the Migration Source/Migration Destination (Schedule Server)" in the *Systemwalker Operation Manager Installation Guide* for information on how to set other information.

2) Distributing policy data to the migration destination server [from the migration source to the migration destination]

Migrate assets to the migration destination server by specifying the migration destination server as the distribution destination and distributing policy data.

In the **Specify Distribution Subsystem** window, specify the subsystem number on the migration destination server. Click **OK**. In the **Apply Policy** window that is displayed, select **Apply at the next service startup** or **Apply at the next daemon startup**.

2.3.5 Migration Tasks on the Execution Server [Tasks at the Migration Source/Migration Destination]

To aggregate the execution server in the same way as the schedule server in an environment where the schedule server and execution server are being run as separate servers, you must migrate the execution server. This section describes how to migrate the execution server.

1) Changing a trust host definition [migration source]

If the schedule server to be aggregated has been specified as a trust host, you must change the trust host definition. On the migration source execution server, perform the following procedure to change the trust host definition:

1. Delete the trust host from the migration source schedule server.
2. Add the trust host to the migration destination schedule server.

Refer to "Defining a Trust Host" in the *Systemwalker Operation Manager Installation Guide* for details.

2) Migrating the execution server assets [migration source to migration destination]

Using the function for extracting and distributing policy data, migrate the assets of the migration source server to the migration destination server.

Extract the following policy data from the migration source execution server and distribute it to the migration destination server:

- **Environment definition** of the **Extract Policy** window

  Job control

  - **Operation information**
  - **Trust host**
  - **Job owner**
  - **Node name definition file**

- **Registration information** of the **Extract Policy** window

  Job control

  - **Job folder**

In the **Apply Policy** window that is displayed when you distribute policy data, select **Apply at the next service startup** or **Apply at the next daemon startup**.

Refer to the *Systemwalker Operation Manager Installation Guide* for details.

3) Creating an execution subsystem name definition file (schedule server)

On the schedule server that will use the migration destination execution server, create an execution subsystem name definition file to ensure that jobs are executed normally on the migration destination execution server.

Refer to "Defining an Execution Subsystem Name" in the *Systemwalker Operation Manager Installation Guide* for details.

2.3.6 Post-Migration Tasks [Tasks at the Migration Destination]

This section describes the tasks to be performed on the migration destination server after migration.

1) Restarting the migration destination subsystem service/daemon (schedule server/execution server)

When you restart the migration destination subsystem service/daemon on the migration destination server, the distributed policy data is applied.

2) Enabling job nets/groups (schedule server)

Job nets and groups of all projects are in a disabled state immediately after migration.

To start operation on the migration destination server, enable the job nets and groups as required using the procedure below:

Implementing on the client

1. Select the target job net or group in the job selection tree of the Systemwalker Operation Manager client.
2. In the **File** menu, select **Schedule Operation**, and then select **Enable** to enable the job net or group.

Implementing on the server

For job nets, execute the jobschcontrol command with the job net name and the "enable" option.

For groups, execute the jobschctlgrp command with the group name and the "enable" option.

2.4 Procedure for Migration in a Cluster Environment

Follow the procedure below to migrate the Systemwalker Operation Manager version in a cluster environment.

Procedure

1. For the tasks that are described in "Uninstalling Systemwalker Operation Manager from a Cluster System" in the *Systemwalker Operation Manager Cluster Setup Guide for Windows*, perform only the tasks that are not related to uninstallation of Systemwalker Operation Manager.
2. Perform upgrade tasks by referencing to the *Systemwalker Operation Manager Upgrade Guide*.
3. Perform installation tasks by referencing the *Systemwalker Operation Manager Cluster Setup Guide*.

2.5 Migrating Certificate/Key Management Environment

This section describes how to migrate certificate from Systemwalker Operation Manager V13.8.0 and earlier.

Emigration from the certificate/key management environment

To migrate, emigrate(retrieve) the PKCS#12 data file from migration source environment.

To retrieve the resource, execute cmmkpfx command in the migration source environment.

- The cmmkpfx command retrieves EE certificate (Include certificates in the route) and private key and, creates PKCS#12(PFX) data file.
- When outputting PKCS#12(PFX) data file, specify a nickname for site certificate.

[Windows]

Under the following conditions:

Operation management directory: d:\sslenv\sslcert

Slot ID in which the emigration target for certificate and key is present: 1

Nickname for site certificate: MySiteCert

File files that are stored PKCS#12(PFX) data: d:\sslenv\my_site_pfx.pfx

```
cmmkpfx d:\sslenv\my_site_pfx.pfx -ed d:\sslenv\sslcert -sn 1 -nn MySiteCert
```

[UNIX]

Under the following conditions:

Operation management directory: /export/home/sslcert

Slot ID in which the emigration target for certificate and key is present: 1

Nickname for site certificate: MySiteCert,

File files that are stored PKCS#12(PFX) data: /export/home/my_site_pfx.pfx

```
# cmmkpfx /export/home/my_site_pfx.pfx -ed /export/home/sslcert -sn 1 -nn MySiteCert
```

For the details of command, refer to the "cmmkpfx " of the "*Systemwalker Operation Manager Reference Guide*" in the migration source environment.

Populating the certificate

Retrieve each file from PKCS#12(PFX) data file which emigrated. Use the openssl pkcs12 command to retrieve each file as below.

1. Retrieve "Private Key" from PKCS#12(PFX) data file.

   [Windows]

   Systemwalker Operation Manager installation directory\MPWALKER.JM\mpahs\bin\openssl.exe pkcs12 -in <PKCS#12(PFX) *data file name*> -nocerts -out d:\mpahso\sslcert\<*private key file name* >

   [UNIX]

   /opt/FJSVftlo/mpahs/oss/openssl/bin/openssl pkcs12 -in <PKCS#12(PFX) *data file name*> -nocerts -out /export/home/mpahso/sslcert/< *private key file name* >

2. Retrieve "Site Certificate" from PKCS#12(PFX) data file.

   [Windows]

   Systemwalker Operation Manager installation directory\MPWALKER.JM\mpahs\bin\openssl.exe pkcs12 -in <PKCS#12(PFX) *data file name*> -clcerts -nokeys -out d:\mpahso\sslcert\cert\<*Site Certificate file name*>

   [UNIX]

   /opt/FJSVftlo/mpahs/oss/openssl/bin/openssl pkcs12 -in <PKCS#12(PFX) *data file name*> -clcerts -nokeys -out /export/home/mpahso/sslcert/cert/< *Site Certificate file name*>

3. Retrieve "Certificate Authority certificates" from PKCS#12(PFX) data file.

   [Windows]

   Systemwalker Operation Manager installation directory\MPWALKER.JM\mpahs\bin\openssl.exe pkcs12 -in <PKCS#12(PFX) *data file name*> -cacerts -nokeys -out d:\mpahso\sslcert\cert\< *Certificate Authority certificates file name*>

   [UNIX]

```
/opt/FJSVftlo/mpahs/oss/openssl/bin/openssl pkcs12 -in <PKCS#12(PFX) data file name> -cacerts -nokeys -out /export/home/mpahso/sslcert/cert/<Certificate Authority certificates file name>
```

The certificate authority certificate contains the root CA certificate, but it may contain one or more intermediate CA certificates, not just the root CA certificate depending on PKCS#12 data. In this case, the root CA certificate is listed first, followed by the intermediate CA certificate.

Here is an example of a certificate authority certificate, when including a root CA certificate and an intermediate CA certificate, and when a root CA certificate only as below.

- Certificate authority certificate file (When including a root CA certificate and an intermediate CA certificate)

```
Bag Attributes
    friendlyName:
subject=...
issuer=...
-----BEGIN CERTIFICATE-----
   (Root CA certificate data)
-----END CERTIFICATE-----
Bag Attributes
    friendlyName:
subject=...
issuer=...
-----BEGIN CERTIFICATE-----
   (Intermediate CA certificate 1 data)
-----END CERTIFICATE-----
Bag Attributes
    friendlyName:
subject=...
issuer=...
-----BEGIN CERTIFICATE-----
   (Intermediate CA certificate 2 data)
-----END CERTIFICATE-----
```

- Certificate authority certificate file (When a root CA certificate only)

```
Bag Attributes
    friendlyName:
subject=...
issuer=...
-----BEGIN CERTIFICATE-----
   (Root CA certificate data)
-----END CERTIFICATE-----
```

4. Divide the Certificate authority certificate file which retrieved in the procedure 3 into the root CA certificate and the intermediate CA certificate.

   If the retrieved CA certificate contains only one certificate (root CA certificate), this procedure is unnecessary. Go to the procedure 6.

   Here is example, the certificate authority certificate contains two intermediate CA certificates.

   Divide the retrieved certificate authority certificate into the root CA certificate, intermediate CA certificate 1, and intermediate CA certificate 2 with using text editor, etc.

   - Root CA certificate file

```
Bag Attributes
    friendlyName:
subject=...
issuer=...
-----BEGIN CERTIFICATE-----
```

```
   (Root CA certificate data)
-----END CERTIFICATE-----
```

- Intermediate CA certificate 1 file

```
Bag Attributes
    friendlyName:
subject=...
issuer=...
-----BEGIN CERTIFICATE-----
   (Intermediate CA certificate 1 data)
-----END CERTIFICATE-----
```

- Intermediate CA certificate 2 file

```
Bag Attributes
    friendlyName:
subject=...
issuer=...
-----BEGIN CERTIFICATE-----
   (Intermediate CA certificate 2 data)
-----END CERTIFICATE-----
```

5. Merge intermediate CA certificate file which divided in the procedure 4 to the site certificate in the sequence Intermediate CA certificate 2, intermediate CA certificate 1.

   [Windows]

```
type <Intermediate CA certificate 2 file name> >> d:\mpahso\sslcert\cert\<Site
certificate file name>
type <Intermediate CA certificate 1 file name> >> d:\mpahso\sslcert\cert\<Site
certificate file name>
```

   [UNIX]

```
# cat <Intermediate CA certificate 2 file name> >> /export/home/mpahso/sslcert/cert/
<Site certificate file name>
# cat <Intermediate CA certificate 1 file name> >> /export/home/mpahso/sslcert/cert/
<Site certificate file name>
```

6. Merge the root CA certificate to the site certificate.

   - If the certificate authority certificate contains an intermediate CA certificate:

     Merge the root CA certificate which divided in the procedure 4 to the site certificate.

     [Windows]

```
type <Root CA certificate file name> >> d:\mpahso\sslcert\cert\<Site certificate
file name>
```

     [UNIX]

```
# cat <Root CA certificate file name> >> /export/home/mpahso/sslcert/cert/<Site
certificate file name>
```

   - If the certificate authority certificate contains only the root CA certificate:

     [Windows]

```
type <Certificate authority certificate file name> >> d:\mpahso\sslcert\cert\<Site
certificate file name>
```

     [UNIX]

```
# cat <Certificate authority certificate file name> >> /export/home/mpahso/sslcert/
cert/<Site certificate file name>
```

7. Set the output file in the following directive of the httpd.conf.

   [Windows]

```
# Private key file of the site
SSLCertificateKeyFile  d:\mpahso\sslcert\<Private key file name>

# Site certificate file
SSLCertificateFile d:\mpahso\sslcert\cert\<Site certificate file name>
```

   [UNIX]

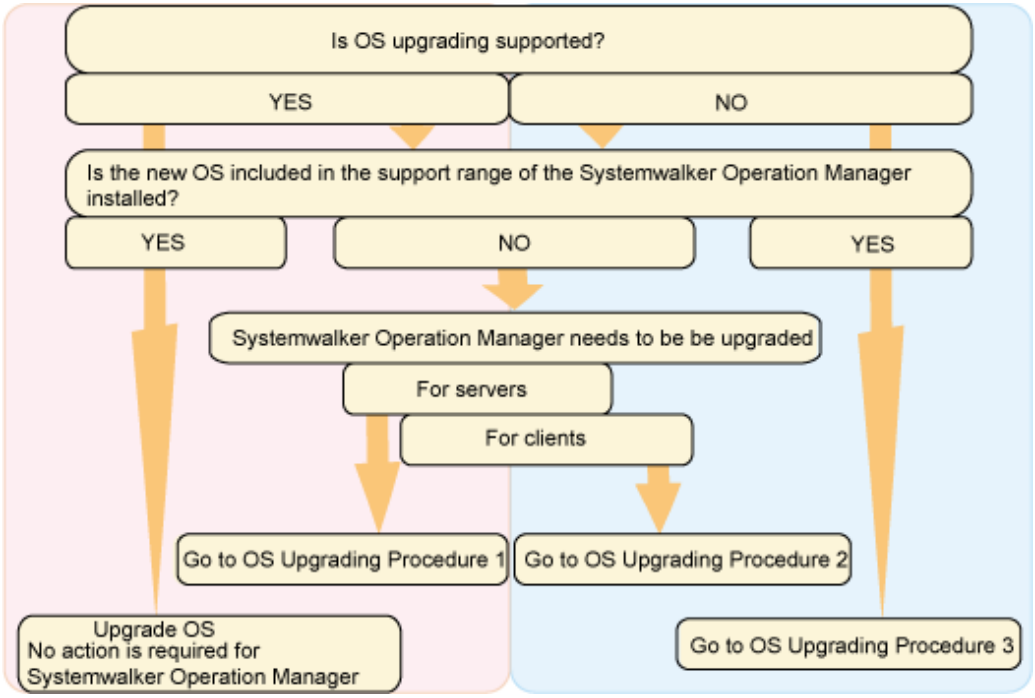
```
# Private key file of the site
SSLCertificateKeyFile  /export/home/mpahso/sslcert/<Private key file name>

# Site certificate file
SSLCertificateFile /export/home/mpahso/sslcert/cert/<Site certificate file name>
```

Chapter 3 OS Upgrading

This chapter describes upgrading of the OS (Windows(R)) in an environment in which Systemwalker Operation Manager is installed.

The pattern of upgrading the OS is shown below



The following sections explain each procedure.

When OS upgrading is supported, visit the Microsoft website to confirm the possible combination of upgrading OS.

In addition, the available installation type and edition varies depending on OS. For details, see the *Systemwalker Operation Manager Technical Guide*.

3.1 OS Upgrading Procedure 1 (Upgrading Operation Manager Servers)

Use the policy information extraction/distribution functions when upgrading a Systemwalker Operation Manager server at the same time as the OS. The upgrading procedure is as follows.

1. Prepare the machine for use as the client.

   Apart from the upgrade target machine, prepare a machine for use as the Systemwalker Operation Manager client and install the Systemwalker Operation Manager client function of this version in it.

2. Extracting policy information

   Connect the Systemwalker Operation Manager client of this version to the upgrading target machine and extract the policy information.

   For details on the policy information extraction procedure, see "Definitions when Constructing the Existing Environment on Another Server" in the *Systemwalker Operation Manager Installation Guide*.

   Note

   If Systemwalker Centric Manager has been installed, be sure to eliminate the following settings from the policy extraction target.

- **Extract Policy** window - **Environment definition** sheet: **Action** checkbox under **Action Control**
- **Extract Policy** window - **Registration information** sheet: **Event monitoring condition** checkbox under **Event monitoring**

3. Delete the environment.

   Uninstall Systemwalker Operation Manager. For the procedure, see "Uninstallation" in the *Systemwalker Operation Manager Installation Guide*.

4. Upgrade the OS.

5. Install Systemwalker Operation Manager.

   Install Systemwalker Operation Manager that supports new operating systems. Pay attention to the followings for installation.

   - The installation directory should be identical to that used before upgrading.
   - If the "shutdown process job net" has been defined in Jobscheduler, it becomes necessary to make settings again for the shutdown process job net. Refer to "Shutting Down the System at Optional Times [Windows version]" in the *Systemwalker Operation Manager User's Guide* for details on "shutdown process job net".
   - Register the user ID that has been used as the project owner and the user ID that has been used for setting up the project access rights.
   - When migrating an environment operating multiple subsystems, you must build the same multi-subsystem environment in advance.

   For more information on the installation procedure and environment settings, see the *Systemwalker Operation Manager Installation Guide*.

6. Distributing policy information

   Connect the Systemwalker Operation Manager client of this version to the upgrading target machine and distribute the policy information extracted in step 2. Distribution of the policy information copies the assets.

   For details on the policy information distribution procedure, see "Definitions when Constructing the Existing Environment on Another Server" in the *Systemwalker Operation Manager Installation Guide*.

7. Define user restrictions

   If the **Operation Manager user restrictions** checkbox has been disabled in the **Define Operation Manager Shared Parameter** window before upgrading, disable the **Operation Manager user restrictions** check box on the upgraded machine.

   The **Define Operation Manager Shared Parameter** window can be displayed by clicking the **Shared parameter** button in the **Systemwalker Operation Manager Environment Setup** window.

Note

- When the job owner information has been defined, redefine the job owner information. For how to set it, see "Defining the Job Owner Information [Windows version]" in the *Systemwalker Operation Manager Installation Guide*.
- The job execution history information and the operation record information are not migrated. If this information needs to be migrated, perform migration by transferring files between servers. Note that information files for the day of migration itself must not be copied by overwriting. To reference pre-migration information on the day of migration, refer to the copy source files.
- If a directory under <*Systemwalker installation directory*>\MPWALKER.JM\mpmjessv\mjespool is specified as **Saved Directory** under **Save job execution history information**, or as **Saved Directory** under **Save operation results data**, in the **Logging** sheet of the **Define Operating Information** window, it must be changed to a directory other than the one in <*Systemwalker installation directory*>\MPWALKER.JM\mpmjessv\mjespool after policy application.
- When the Process Monitoring definition information has been changed, re-set it. For the setting procedure, see "Defining the Process Monitoring function" in the *Systemwalker Operation Manager Installation Guide*.

3.2 OS Upgrading Procedure 2 (Upgrading Operation Manager Clients)

When upgrading a Systemwalker Operation Manager client at the same time as the OS, perform the following procedure.

1. Uninstall Systemwalker Operation Manager.

   For the procedure, see "Uninstallation" in the *Systemwalker Operation Manager Installation Guide*.

2. Upgrade the OS.

3. Install Systemwalker Operation Manager.

   Install Systemwalker Operation Manager that supports new operating systems. For the procedure, see "Uninstallation" in the *Systemwalker Operation Manager Installation Guide*.

3.3 OS Upgrading Procedure 3 (Reinstalling Systemwalker Operation Manager)

When OS upgrading is not supported, it is required to back up the assets of Systemwalker Operation Manager and reinstall Systemwalker Operation Manager after upgrading. The OS upgrading procedure is as follows.

1. Back up the assets.

   Back up the assets of Systemwalker Operation Manager. For the procedure, see "Backup" in the *Systemwalker Operation Manager Installation Guide*.

2. Delete the environment.

   Uninstall Systemwalker Operation Manager. For the procedure, see "Uninstallation" in the *Systemwalker Operation Manager Installation Guide*.

3. Upgrade the OS.

4. Install Systemwalker.

   Reinstall this version. Pay attention to the followings for installation.

   - The installation directory should be identical to that used before upgrading.
   - If the "shutdown process job net" has been defined in Jobscheduler, it becomes necessary to make settings again for the shutdown process job net. Refer to "Shutting Down the System at Optional Times [Windows version]" in the *Systemwalker Operation Manager User's Guide* for details on "shutdown process job net".
   - Register the user ID that has been used as the project owner and the user ID that has been used for setting up the project access rights.
   - When migrating an environment operating multiple subsystems, you must build the same multi-subsystem environment in advance.

   For more information on the installation procedure and environment settings, see the *Systemwalker Operation Manager Installation Guide*.

5. Restore the assets.

   Restore the assets of Systemwalker Operation Manager. For the procedure, see "Restore" in the *Systemwalker Operation Manager Installation Guide*.

Note

- When the job owner information has been defined, redefine the job owner information. For how to set it, see "Defining the Job Owner Information [Windows]" in the *Systemwalker Operation Manager Installation Guide*.