FUJITSU Software
Systemwalker
Software Configuration Manager

Operation Guide

Windows/Linux

B1X1-0128-07ENZ0(00)
November 2015

Preface

Purpose of this Document

This document explains how to use the different features and functions required to operate Systemwalker Software Configuration Manager.

Intended Readers

This document is intended for those who want to understand the operating procedures of Systemwalker Software Configuration Manager.

It is assumed that readers of this document already have the following knowledge:

- Basic knowledge of the operating system being used

Structure of this Document

The structure of this document is as follows:

Chapter 1 Operation Overview

This chapter explains the operator tasks and workflow for Systemwalker Software Configuration Manager.

Chapter 2 Operation Setup

This chapter explains how to set up Systemwalker Software Configuration Manager operations.

Chapter 3 Starting and Stopping Systemwalker Software Configuration Manager

This chapter explains how to start and stop Systemwalker Software Configuration Manager.

Chapter 4 Maintenance

This chapter explains relevant maintenance information (such as log output and backup/restore).

Conventions Used in this Document

Refer to the *Documentation Road Map* for information on the names, abbreviations, and symbols used in this manual.

Abbreviations and Generic Terms Used for Operating Systems

This document uses the following abbreviations and generic terms to indicate operating systems.

Official name	Abbreviation	
Microsoft(R) Windows Server(R) 2012 Datacenter Microsoft(R) Windows Server(R) 2012 Standard	Windows Server 2012	Windows
Microsoft(R) Windows Server(R) 2012 R2 Datacenter Microsoft(R) Windows Server(R) 2012 R2 Standard	Windows Server 2012 R2	
Microsoft(R) Windows Server(R) 2008 Standard Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V Microsoft(R) Windows Server(R) 2008 Enterprise Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V	Windows Server 2008	
Microsoft(R) Windows Server(R) 2008 R2 Standard Microsoft(R) Windows Server(R) 2008 R2 Enterprise	Windows Server 2008 R2	
Red Hat(R) Enterprise Linux(R) (for x86)	RHEL (x86)	RHEL
Red Hat(R) Enterprise Linux(R) (for Intel64)	RHEL (Intel64)	
Oracle Solaris	Solaris Operating System Solaris OS	Solaris

Export Restrictions

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

- Adobe, Adobe Reader, and Flash are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.
- Interstage, ServerView, Symfoware, and Systemwalker are registered trademarks of Fujitsu Limited. "lix"
- Linux is a registered trademark of Linus Torvalds.
- Red Hat, RPM, and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc. in the United States and other countries.
- Oracle and Java are registered trademarks of Oracle and/or its affiliates in the United States and other countries. Company names and product names used in this document are registered trademarks or trademarks of those companies.
- VMware, the VMware "boxes" logo and design, Virtual SMP, and VMotion are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.
- Xen, and XenSource are trademarks or registered trademarks of XenSource, Inc. in the United States and/or other countries.
- Other company names and product names are trademarks or registered trademarks of their respective owners.

Note that system names and product names in this document are not accompanied by trademark symbols such as (TM) or (R).

Publication Date and Version

Version	Manual code
July 2012: First edition	B1X1-0128-02ENZ0(00) / B1X1-0128-02ENZ2(00)
July 2012: Second edition	B1X1-0128-03ENZ0(00) / B1X1-0128-03ENZ2(00)
January 2013: Third edition	B1X1-0128-04ENZ0(00) / B1X1-0128-04ENZ2(00)
March 2014: Fourth edition	B1X1-0128-05ENZ0(00) / B1X1-0128-05ENZ2(00)
August 2014: Fifth edition	B1X1-0128-06ENZ0(00) / B1X1-0128-06ENZ2(00)
November 2015: Sixth edition	B1X1-0128-07ENZ0(00) / B1X1-0128-07ENZ2(00)

Copyright

Contents

Chapter 1 Operation Overview

This chapter presents an overview of Systemwalker Software Configuration Manager operations.

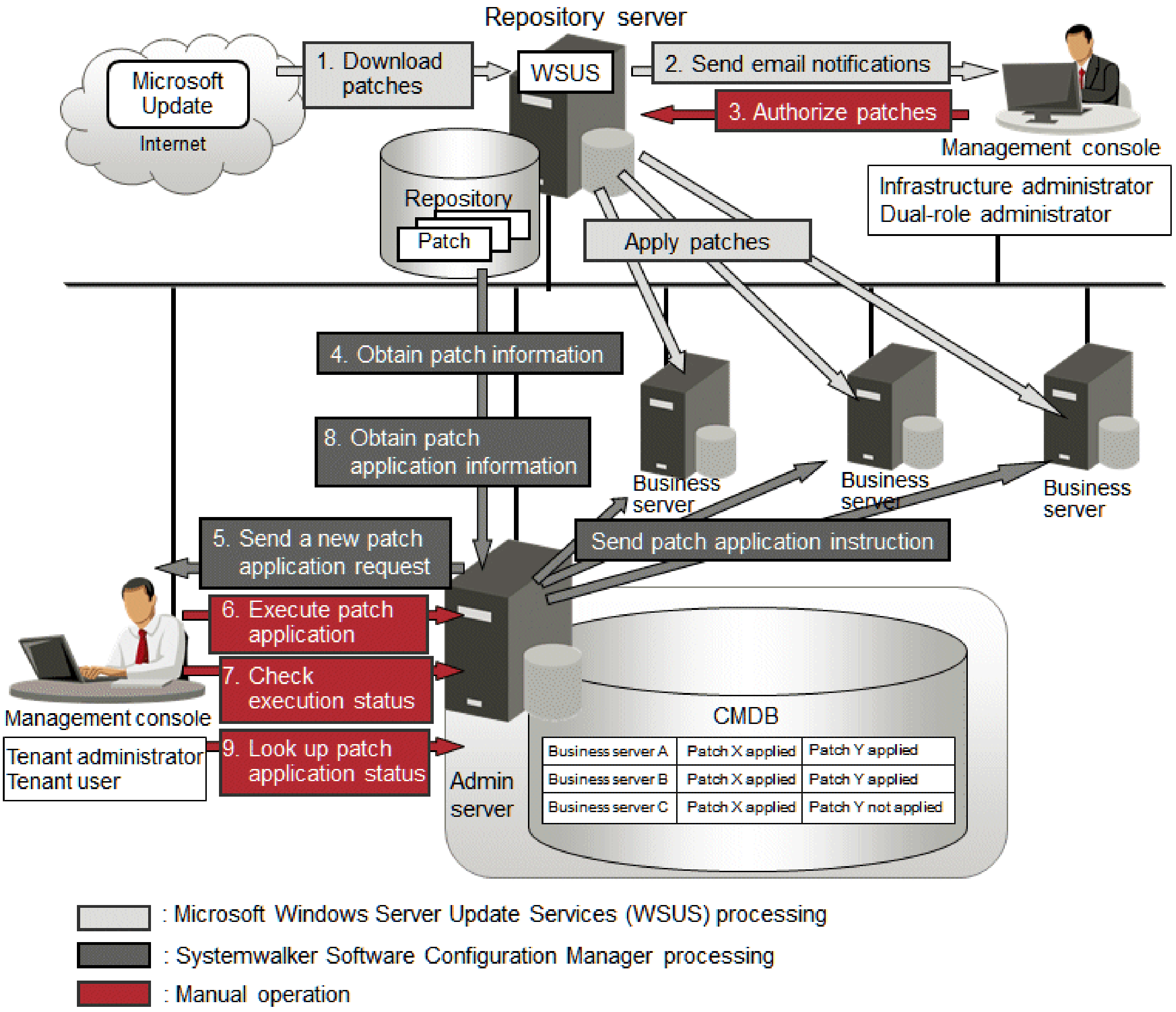
1.1 Operation Flow

This section explains the operation flow for each role.

1.1.1 Windows Patch Management

Windows patches are managed by linking to WSUS. The following diagram shows the overall flow of Windows patch management.

Figure 1.1 Overview of Windows patch management


Repository server
Microsoft Update
Internet
1. Download patches
WSUS
2. Send email notifications
3. Authorize patches
Management console
Infrastructure administrator
Dual-role administrator
Repository
Patch
Apply patches
4. Obtain patch information
8. Obtain patch application information
Business server
Business server
Business server
5. Send a new patch application request
Send patch application instruction
6. Execute patch application
7. Check execution status
9. Look up patch application status
Management console
Tenant administrator
Tenant user
Admin server
CMDB
▭ : Microsoft Windows Server Update Services (WSUS) processing
■ : Systemwalker Software Configuration Manager processing
🟥 : Manual operation

Business server A	Patch X applied	Patch Y applied
Business server B	Patch X applied	Patch Y applied
Business server C	Patch X applied	Patch Y not applied

1. Download patches **[processing by WSUS]**

   Use the WSUS function to synchronize with the Microsoft Update site and obtain the latest patch information.

2. Send email notifications to the infrastructure administrator **[processing by WSUS]**

   By setting up the WSUS email notification function, a synchronized message about new patches will be sent to the infrastructure administrator from WSUS via email.

3. Authorize new patches **[operation by the infrastructure administrator]**

   The infrastructure administrator performs authorization processing for the new patches using WSUS.

4. Obtain patch information **[processing by Systemwalker Software Configuration Manager]**

   Systemwalker Software Configuration Manager extracts information about new patches from WSUS and the management information on WSUS, and stores both sets of information in the CMDB.
   Patch information can be acquired either automatically or manually (using a command).

5. Send a new patch application request **[processing by Systemwalker Software Configuration Manager]**

   When a new patch is authorized on WSUS, an email is automatically sent to each tenant user and each tenant administrator requesting that they apply the new patch.

6. Execute patch application **[operation by the infrastructure administrator, the tenant user or the tenant administrator]**

   Either the tenant user or the tenant administrator logs in to the management console and applies the new patch.

   The infrastructure administrator can perform the patch application using the command on the admin server.

   Point

   - Patches are distributed by WSUS. Once patch application completes, application information is sent to WSUS.
   - Even if a new patch is displayed in the management console, a notification about the new patch may not have been sent to business servers, or the patch may not have been downloaded to business servers, depending on the schedule settings for WSUS. Check the schedule settings for WSUS.

7. Check execution status **[operation by the infrastructure administrator, the tenant administrator, or the tenant user]**

   Check the patch application status using the management console or the command on the admin server.

8. Obtain patch application information **[processing by Systemwalker Software Configuration Manager]**

   Systemwalker Software Configuration Manager extracts patch application information from WSUS and stores it in the CMDB.

9. Look up patch application status

   The infrastructure administrator, tenant administrator, and tenant user log in to the management console and check the patch application status. The infrastructure administrator can also check the patch application status using the command on the admin server.

The following table explains the operation flow for each role:

	Operation flow	User roles				Reference
		Infrastructure administrator	Dual-role administrator	Tenant administrator	Tenant user	
1	Download patches	Y	Y	-	-	Refer to the WSUS manuals.
2	Send email notifications to infrastructure administrators	-	-	-	-	Refer to the WSUS manuals.
3	Authorize new patches	Y	Y	-	-	Refer to the WSUS manuals.
4	Obtain patch information	Y	Y	-	-	"Patch Information Update Command" in the *Reference Guide*
5	Send new patch application requests	-	-	-	-	An email is sent automatically when a new patch is acquired.

	Operation flow	User roles				Reference
		Infrastructure administrator	Dual-role administrator	Tenant administrator	Tenant user	
						If email transmission fails, either an infrastructure administrator or a dual-role administrator must resend the email using the email resend command as described in the *Reference Guide*.
6	Execute patch application	Y(*1)	Y	Y (*2)	Y (*2)	"Patch Application Wizard" under "Patch Management" in the *Operator's Guide* "Patch Application Command" in the *Reference Guide*
7	Check execution status	Y	Y	Y(*2)	Y(*2)	"Job Management" in the *Operator's Guide* "Job Information Management Command" in the *Reference Guide*
8	Obtain patch application information	Y	Y	-	-	"Patch Information Update Command" in the *Reference Guide*
9	Reference patch application status	Y	Y	Y(*2)	Y(*2)	"Patch Management" in the *Operator's Guide* "Patch Information Output Command" in the *Reference Guide*

Y: Implement the task.

-: Do not implement the task

*1: Only the command can be operated.

*2: Only the management console can be operated.

Note

Notes on linking to WSUS

- Immediately after WSUS linkage is set up on a business server

  To perform patch management, register the business servers subject to patch management as the computers managed by WSUS. WSUS can only start managing a business server once it has been notified of the software configuration information from the business server. If discovery is performed before WSUS is notified about the business server information, it will not be possible for WSUS to collect information for that business server because information about the business server has not yet been registered with WSUS. If the business server is displayed in the **All Computers** group in the **WSUS console** window and a time is displayed in the **Last Status Report** column, the software configuration information for the business server has finished being notified to WSUS. Do not perform discovery until the software configuration information for the business server has been notified to WSUS. Perform discovery by executing the swcfmg_patch_updateinfo command.

  If this command is not executed, discovery will be executed at the next scheduled regular discovery.

  Example:

  ```
  swcfmg_patch_updateinfo.exe -repository
  ```

- If a business server has been added or removed as the computer managed by WSUS

  If a business server has been added or removed as the computer managed by WSUS, or if a business server that is already under the management of one WSUS service is moved to a location under the management of another WSUS service, do not perform discovery until the changes to the WSUS operation environment have completed and the software configuration information for the business server has been notified to WSUS. (If the business server is displayed in the **All Computers** group in the **WSUS console** window and a time is displayed in the **Last Status Report** column, the software configuration information for the business server has finished being notified to WSUS). Perform discovery by executing the swcfmg_patch_updateinfo command.

  If this command is not executed, discovery will be executed at the next scheduled regular discovery.

  Example:

  ```
  swcfmg_patch_updateinfo.exe -repository
  ```

- If WSUS server cleanup has been performed

  If the disk used by the WSUS service is full, redundant patches and patch information managed by WSUS can be deleted using a WSUS server cleanup. If a server cleanup has been performed, execute the swcfmg_patch_updateinfo command with the "-cleanup" option specified.

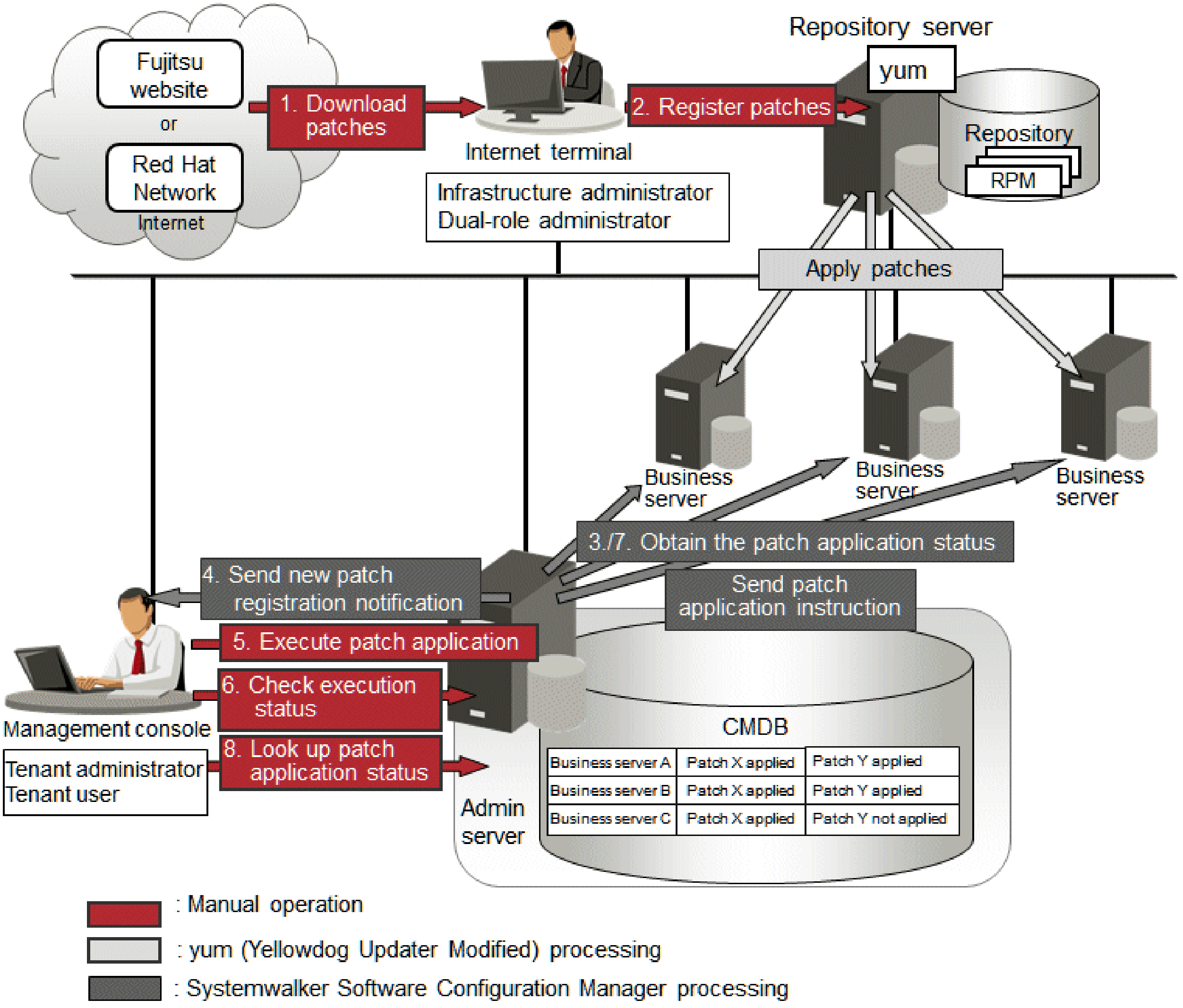
  Example:

  ```
  swcfmg_patch_updateinfo.exe -repository -cleanup
  ```

1.1.2 Linux Patch Management

Linux patches are managed by linking to Yellowdog Updater Modified (yum). The following diagram shows the overall flow of Linux patch management:

Figure 1.2 Overview of Linux patch management


Fujitsu website
or
Red Hat Network
Internet
1. Download patches
Internet terminal
Infrastructure administrator
Dual-role administrator
2. Register patches
Repository server
yum
Repository
RPM
Apply patches
Business server
Business server
Business server
3./7. Obtain the patch application status
Send patch application instruction
4. Send new patch registration notification
5. Execute patch application
6. Check execution status
8. Look up patch application status
Management console
Tenant administrator
Tenant user
Admin server
CMDB
: Manual operation
: yum (Yellowdog Updater Modified) processing
: Systemwalker Software Configuration Manager processing

Business server A	Patch X applied	Patch Y applied
Business server B	Patch X applied	Patch Y applied
Business server C	Patch X applied	Patch Y not applied

Point

When the linkage servers have internet access, work performed using Internet terminals can be performed on the linkage servers.

1. Download patches [operation by the infrastructure administrator]

   The infrastructure administrator uses the Internet terminal to download the latest patches (RPM packages) from either the Fujitsu website or the Red Hat Network.

2. Register patches **[operation by the infrastructure administrator]**

   The infrastructure administrator registers the patches (RPM packages) with the yum repository server. The infrastructure administrator then defines these patches as part of the Linux patch management target.
   If patches have been added to or removed from the yum repository server, define the Linux patch management target again and then execute the yum cache cleanup notification command.

3. Obtain the patch application status **[processing by Systemwalker Software Configuration Manager]**

   Systemwalker Software Configuration Manager extracts information about which RPM packages have been applied or can be applied from each server, and then registers this information in the CMDB.

   RPM package information can be obtained either automatically or manually (using a command).

4. Send new patch registration notifications **[processing by Systemwalker Software Configuration Manager]**

   When Systemwalker Software Configuration Manager detects a new patch, an email is automatically sent to each tenant user and each tenant administrator, notifying them that the new patch has been registered.

5. Execute patch application **[operation by the infrastructure administrator, the tenant user or the tenant administrator]**

   Either the tenant user or the tenant administrator logs in to the management console and applies the new patch.

   The infrastructure administrator can perform the patch application using the command on the admin server.

6. Check execution status **[operation by the infrastructure administrator, the tenant administrator. or the tenant user]**

   Check the patch application status using the management console or the command on the admin server.

7. Obtain patch application information **[processing by Systemwalker Software Configuration Manager]**

   Systemwalker Software Configuration Manager extracts patch application information from each server and stores it in the CMDB.

8. Look up patch application status

   The infrastructure administrator, tenant administrator, and tenant user log in to the management console and check the patch application status. The infrastructure administrator can also check the patch application status using the command on the admin server.

The following table explains the operation flow for each role.

	Operation flow	User roles				Reference
		Infrastructure administrator	Dual-role administrator	Tenant administrator	Tenant user	
1	Download patches	Y	Y	-	-	Refer to the yum manuals.
2	Register patches	Y	Y	-	-	Refer to the yum manuals for information on how to register patches (RPM packages). Refer to "2.8.2 Defining the Linux Patch Management Target" for information on how to define the Linux patch management target. Refer to "yum Cache Cleanup Notification Command" in the *Reference Guide* for information on the yum cache cleanup notification command.
3	Obtain patch application status	Y	Y	-	-	"Patch Information Update Command" in the *Reference Guide*
4	Send new patch registration notification	-	-	-	-	An email is sent automatically when a new patch is registered. If email transmission fails, either an infrastructure administrator or a dual-role administrator must resend the email using the email resend command as described in the *Reference Guide*.
5	Execute patch application	Y(*1)	Y	Y(*2)	Y(*2)	"Patch Application Wizard" under "Patch Management" in the *Operator's Guide*

	Operation flow	User roles				Reference
		Infrastructure administrator	Dual-role administrator	Tenant administrator	Tenant user	
						"Patch Application Command" in the *Reference Guide*
6	Check execution status	Y	Y	Y(*2)	Y(*2)	"Job Management" in the *Operator's Guide* "Job Information Management Command" in the *Reference Guide*
7	Obtain patch application status	Y	Y	-	-	"Patch Information Update Command" in the *Reference Guide*
8	Reference patch application status	Y	Y	Y(*2)	Y(*2)	"Patch Management" in the *Operator's Guide* "Patch Information Output Command" in the *Reference Guide*

Y: Implement the task.

-: Do not implement the task

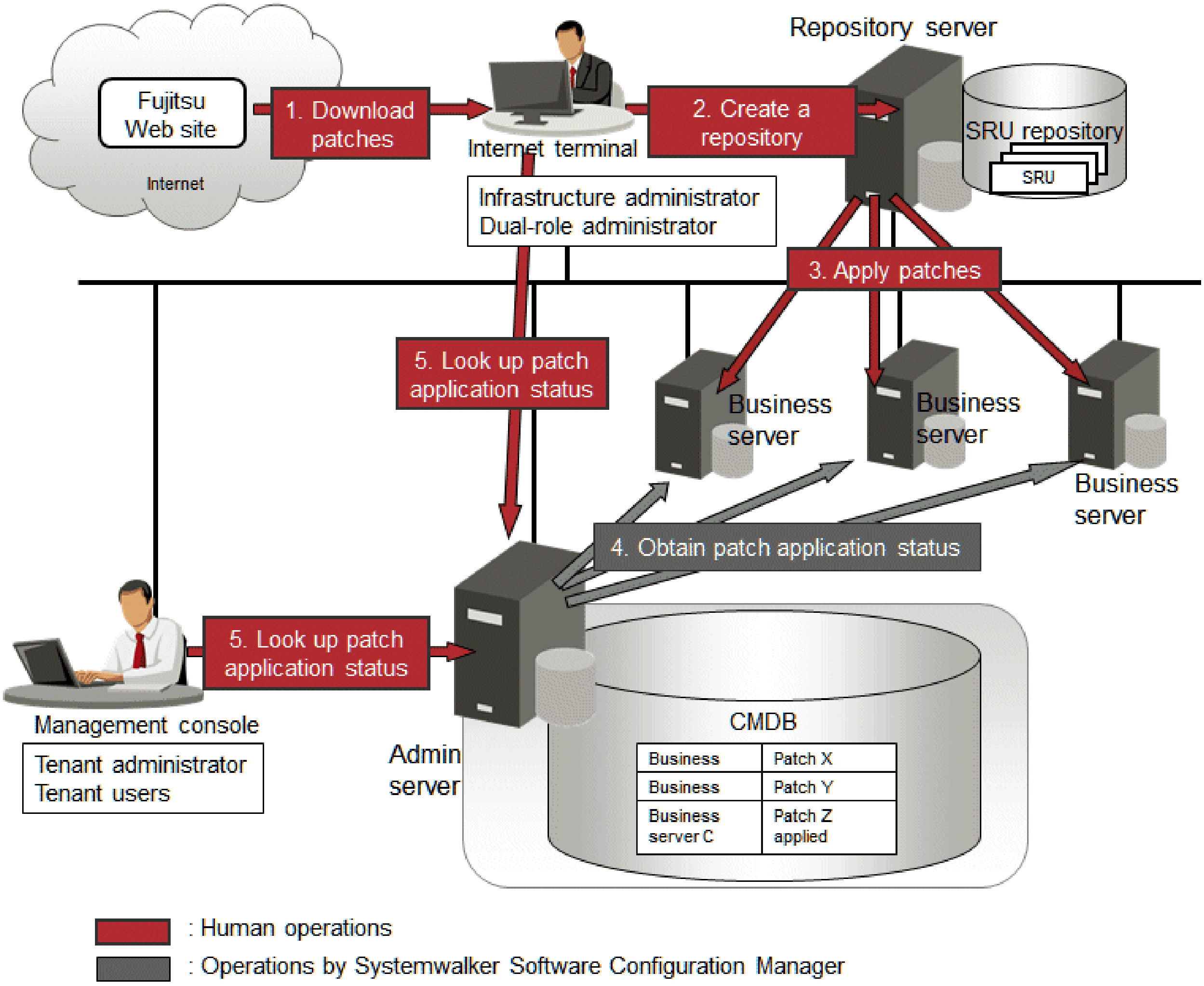
*1: Only the command can be operated.

*2: Only the management console can be operated.

1.1.3 Solaris Patch Management

Patch management for Solaris OS (Solaris 11) is performed using the standard pkg command. The following diagram shows the overall flow of Solaris OS patch management:

Figure 1.3 Overview of Solaris OS Patch Management



1. Download patches **[operation by the infrastructure administrator]**

   The infrastructure administrator uses the Internet terminal to download the latest patches (SRU) from the Fujitsu website.

2. Create a repository **[operation by the infrastructure administrator]**

   The infrastructure administrator creates a repository server using the patch (SRU).

   The tenant user/tenant administrator can also obtain the latest patch (SRU) from the Fujitsu website directly and store it on the business server without creating a repository. It is also possible to create a repository on each business server.

3. Apply patches **[operation by the tenant user or the tenant administrator]**

   Either the tenant user or the tenant administrator logs in to the business server and applies the new patch.

4. Obtain the patch application status **[processing by Systemwalker Software Configuration Manager]**

   Systemwalker Software Configuration Manager extracts applied SRU information from each server and stores it in the CMDB.

   SRU patch application status can be acquired either automatically or manually (using a command).

5. Look up patch application status

   The infrastructure administrator, tenant administrator, and tenant user log in to the management console and check the patch application status. The infrastructure administrator can also check the patch application status using the command on the admin server.

The following table explains the operation flow for each role.

	Operation flow	User roles				Reference
		Infrastructure administrator	Dual-role administrator	Tenant administrator	Tenant user	
1	Download patches	Y	Y	Y	Y	Refer to the email notifications from FSC-NEWS (SupportDesk customer notifications) and the information available from the UpdateSite (the Fujitsu SupportDesk website).
2	Create a repository	Y	Y	Y	Y	Refer to Oracle Solaris manuals.
3	Apply patches	-	-	Y	Y	Refer to Oracle Solaris manuals.
4	Obtain patch application status	Y	Y	-	-	"Patch Information Update Command" in the *Reference Guide*
5	Look up patch application status	Y	Y	Y(*1)	Y(*1)	"Server Details" under "Configuration Managementt" in the *Operator's Guide* "Pach Information Management Command" in the *Reference Guide*

Y: Implement the task.

-: Do not implement the task

*1: Only the management console can be operated.

Information

For Solaris servers, only the following information can be checked.

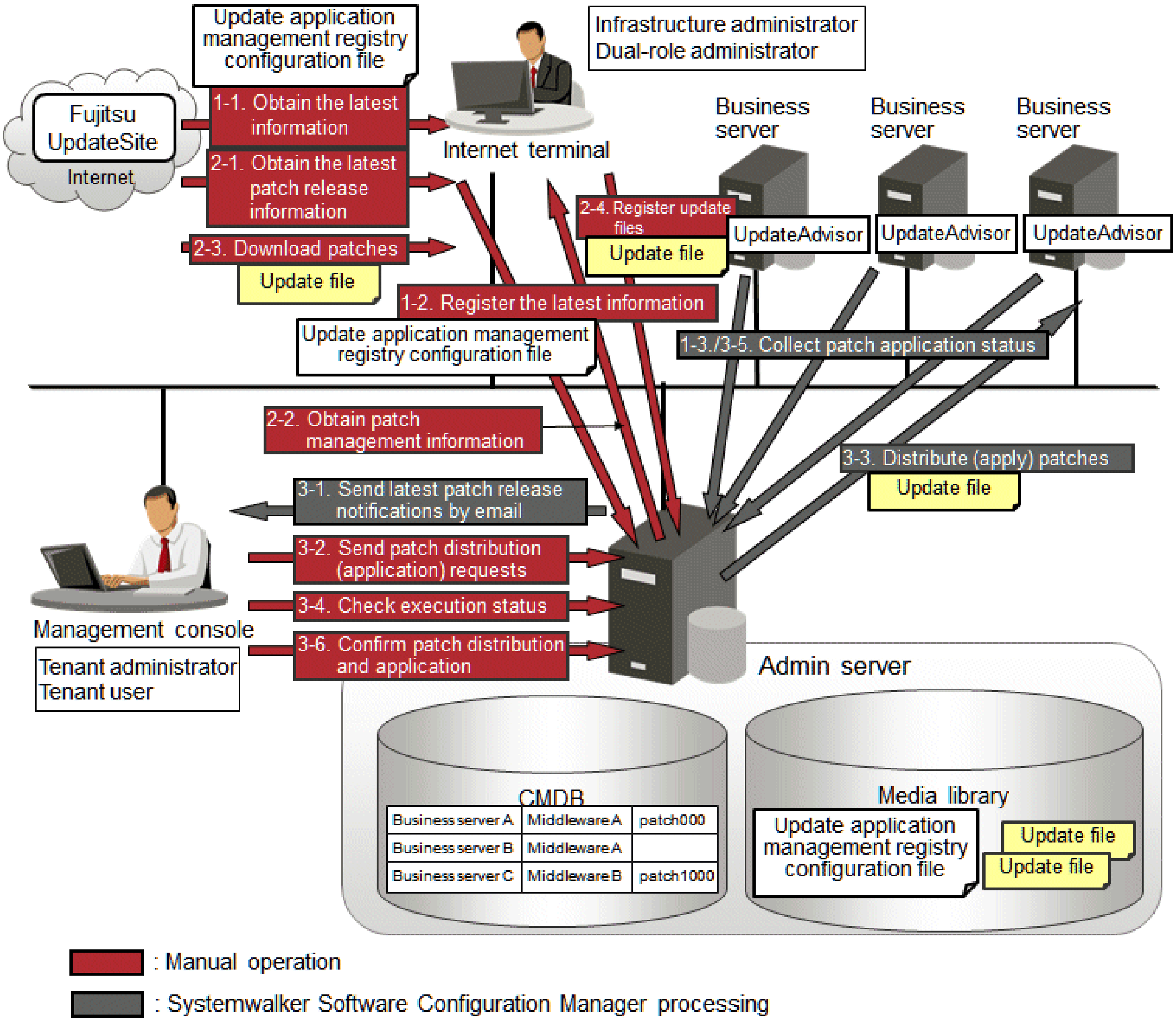
- Applied OS patches (SRU information)
- Installed Fujitsu middleware
- Application status of Fujitsu middleware patches

It is not possible to perform patch application, parameter setting, or script execution on Solaris servers.

1.1.4 Fujitsu Middleware Patch Management

Fujitsu middleware patches are managed by linking to the UpdateAdvisor (middleware). The following diagram shows the overall flow of Fujitsu middleware patch management:

Figure 1.4 Overview of Fujitsu middleware patch management


Update application management registry configuration file
Infrastructure administrator
Dual-role administrator
Fujitsu UpdateSite
Internet
1-1. Obtain the latest information
Internet terminal
2-1. Obtain the latest patch release information
2-3. Download patches
Update file
2-4. Register update files
Update file
Business server
Business server
Business server
UpdateAdvisor
UpdateAdvisor
UpdateAdvisor
1-2. Register the latest information
Update application management registry configuration file
1-3./3-5. Collect patch application status
2-2. Obtain patch management information
3-1. Send latest patch release notifications by email
3-2. Send patch distribution (application) requests
3-4. Check execution status
3-6. Confirm patch distribution and application
3-3. Distribute (apply) patches
Update file
Management console
Tenant administrator
Tenant user
Admin server
CMDB
Business server A | Middleware A | patch000
Business server B | Middleware A |
Business server C | Middleware B | patch1000
Media library
Update application management registry configuration file
Update file
Update file
🟥 : Manual operation
⬛ : Systemwalker Software Configuration Manager processing

Point

When the admin server has internet access, work performed using Internet terminals can be performed on the admin server.

1. Obtain Fujitsu middleware information, and perform discovery

   Obtain the update application management registry configuration file from the UpdateSite and collect the latest patch application status. The update application management registry configuration file must be updated to collect the latest patch application status. During operation, also obtain the latest application management registry configuration file from the UpdateSite.

   1. Obtain the latest information (the update application management registry configuration file) **[operation by the infrastructure administrator]**

      The infrastructure administrator uses the Internet terminal to download the latest update application management registry configuration file from the UpdateSite.

   2. Register the latest information (the update application management registry configuration file) **[operation by the infrastructure administrator]**

      The infrastructure administrator uses the UpdateAdvisor asset registration command on the admin server to store the latest update application management registry configuration file in the media library.

   3. Collect patch application status information **[processing by Systemwalker Software Configuration Manager]**

      Systemwalker Software Configuration Manager uses the update application management registry configuration file (that has been registered) to collect patch application status information from each business server.

2. Obtain Fujitsu middleware patches

   Obtain Fujitsu middleware patches from the UpdateSite and store in the media library. Patches stored in the media library can be distributed (applied) to the business servers.

   1. Obtain the latest patch release information [operation by the infrastructure administrator]

      The infrastructure administrator looks up email notifications from FSC-NEWS (SupportDesk customer notifications) and the UpdateSite (the website for the Fujitsu SupportDesk) to obtain information about the latest patches that have been released.

   2. Obtain patch management information **[operation by the infrastructure administrator]**

      The infrastructure administrator uses the patch management information acquisition command on the admin server to obtain the patch management information.

      The infrastructure administrator copies the patch management information and released patch acquisition tool obtained from the admin server to the Internet terminal.

   3. Download patches **[operation by the infrastructure administrator]**

      The infrastructure administrator uses the released patch acquisition tool on the Internet terminal to download newly released patches from the UpdateSite.

   4. Register update files **[operation by the infrastructure administrator]**

      The infrastructure administrator uses the Fujitsu middleware patch registration command on the admin server to store the downloaded files in the media library.

3. Check the distribution and application of Fujitsu middleware patches

   Distribute (apply) the Fujitsu middleware patches that were stored in the media library.

   However, patch distribution and application to managed Solaris servers is not supported.

   1. Send latest patch release notifications by email **[processing by Systemwalker Software Configuration Manager]**

      The tenant administrator and tenant user receive an email notification from Systemwalker Software Configuration Manager informing them that the latest patches have been released.

   2. Send patch distribution/application requests **[operation by the infrastructure administrator, the tenant user or the tenant administrator]**

      Either the tenant user or the tenant administrator uses the management console to distribute the latest patches to business servers.

      The infrastructure administrator can perform the patch application using the command on the admin server.

      Also, to apply Fujitsu middleware patches, a script specifying the application processing must be created and then registered as a post-execution script.

   3. Distribute/apply patches **[processing by Systemwalker Software Configuration Manager]**

      Systemwalker Software Configuration Manager distributes the specified patches to the specified business servers.

      If an application script has been registered, Systemwalker Software Configuration Manager also applies the patches by executing the application script. If an application script has not been registered, log on directly to the business server and apply the patches manually..

   4. Check execution status **[operation by the infrastructure administrator, the tenant administrator, or the tenant user]**

      Check the patch application status using the management console or the command on the admin server.

   5. Collect patch application status information **[processing by Systemwalker Software Configuration Manager]**

      Systemwalker Software Configuration Manager uses the update application management registry configuration file (that has been registered) to collect patch application status information from each business server.

6. Confirm patch distribution/application

   The infrastructure administrator, tenant administrator, and tenant user log in to the management console and check the patch application status. The infrastructure administrator can also check the patch application status using the command on the admin server.

The following table explains the operation flow for each role.

		Operation flow	User roles				Reference
			Infrastructure administrator	Dual-role administrator	Tenant administrator	Tenant user	
1	1	Obtain the latest information (the update application management registry configuration file)	Y	Y	-	-	Refer to the UpdateAdvisor (middleware) manuals.
	2	Register the latest information (the update application management registry configuration file)	Y	Y	-	-	Refer to "UpdateAdvisor Asset Registration Command" in the *Reference Guide*.
	3	Collect patch application status information	Y	Y	-	-	"Patch Information Update Command" in the *Reference Guide*
2	1	Obtain the latest patch release information	Y	Y	-	-	Refer to the email notifications from FSC-NEWS (SupportDesk customer notifications) and the information available from the UpdateSite (the Fujitsu SupportDesk website).
	2	Obtain patch management information	Y	Y	-	-	Refer to "Patch Management Information Acquisition Command" in the *Reference Guide*.
	3	Download the latest patches	Y	Y	-	-	Refer to "Released Patch Acquisition Tool" in the *Reference Guide*.
	4	Register update files	Y	Y	-	-	Refer to "Fujitsu Middleware Patch Registration Command" in the *Reference Guide*.
3	1	Send latest patch release notifications by email	-	-	-	-	An email is sent automatically when a new patch is acquired. If email transmission fails, either an infrastructure administrator or a dual-role administrator must resend the email using the email resend command as described in the *Reference Guide*.
	2	Send patch distribution/ application) requests	Y(*1)	Y	Y(*2)	Y(*2)	"Patch Application Wizard" under "Patch Management" in the *Operator's Guide*

		Operation flow	User roles				Reference
			Infrastructure administrator	Dual-role administrator	Tenant administrator	Tenant user	
							For details on how to apply patches, refer to "2.10 Fujitsu Middleware Patch Application". "Patch Application Command" in the *Reference Guide*
	3	Distribute/apply patches	-	-	-	-	-
	4	Check execution status	Y	Y	Y(*2)	Y(*2)	"Job Management" in the *Operator's Guide* "Job Information Management Command" in the *Reference Guide*
	5	Collect patch application status information	Y	Y	-	-	"Patch Information Update Command" in the *Reference Guide*
	6	Confirm patch distribution/application	Y	Y	Y(*2)	Y(*2)	"Patch Management" in the *Operator's Guide* "Patch Information Output Command" in the *Reference Guide*

Y: Implement the task.

-: Do not implement the task

*1: Only the command can be operated.

*2: Only the management console can be operated.

1.1.5 Software Installation

Perform installation of software on managed servers. Use configuration modification to perform software installation. Only software that can be installed in silent mode can be installed.

Configuration modification

Configuration modification is the function used for modifying software configuration information by executing pre-defined combinations of different operations such as command execution and file distribution on managed servers. This enables software installation. In addition, the following functions let you standardize and automate changes made to software configuration information.

- The configuration modification template standardizes the processes necessary for changing software configuration information
- The media library that manages files necessary for configuration modification as assets

The software installation flow is as shown below.

1. Register the software information [operation by the infrastructure administrator]

   When installing software that is not compatible with UpdateAdvisor (middleware), use commands to register the software information.

2. Register assets [infrastructure administrator]

   The infrastructure administrator registers the files necessary for installing the software as assets in the media library in advance.

3. Create a configuration modification template [infrastructure administrator/tenant administrator/tenant user]

   Either the tenant administrator or the tenant user logs in to the management console and creates a configuration modification template. Define the processes, parameters, and assets necessary for installing the software in the configuration modification template. Create the configuration modification template according to the manuals or other information provided by the software vendor.

4. Request configuration modification [infrastructure administrator/tenant administrator/tenant user]

   Either the tenant administrator or the tenant user logs in to the management console and requests configuration modification. Notifications that this request has been received, completed, or has ended in an error, are received by email.

   The infrastructure administrator can request configuration modification using the command on the admin server.

5. Install the software [performed using Systemwalker Software Configuration Manager]

   Systemwalker Software Configuration Manager installs software on managed servers according to the processes defined in the configuration modification template.

6. Check execution status [infrastructure administrator/tenant administrator/tenant user]

   Check the execution status of configuration modification using the management console or the commands on the admin server.

7. Collect software information [infrastructure administrator/tenant administrator/tenant user]

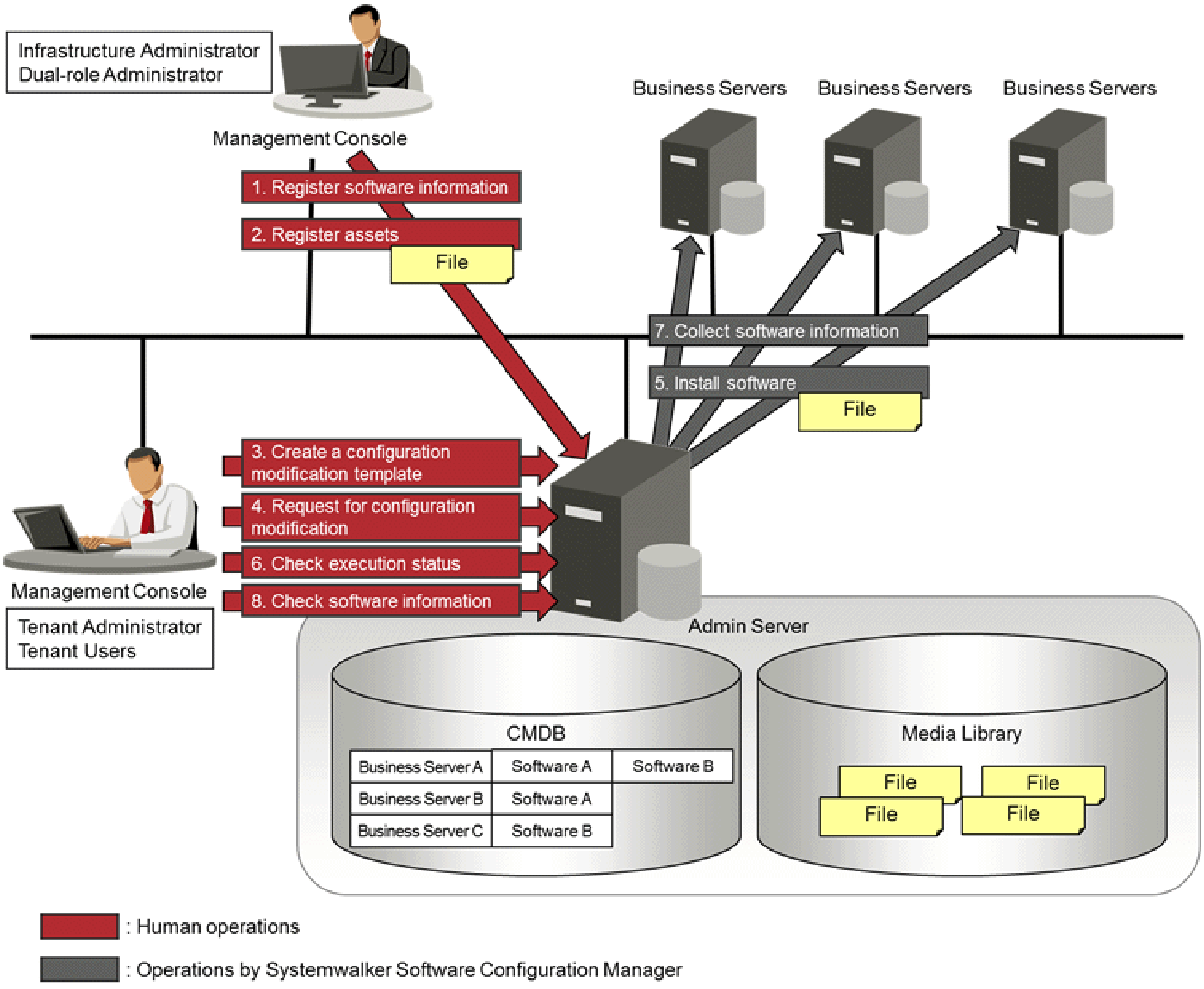
   Check the information about the software installed on the managed servers.

   For Fujitsu middleware information, perform discovery and collect the information using UpdateAdvisor (middleware).

   For the information about software that is not compatible with UpdateAdvisor (middleware), log into the managed server and check the information. After confirming the information about the software installed on the managed servers, register the information using commands.

8. Check the software information [infrastructure administrator/tenant administrator/tenant user]

   Infrastructure administrators, tenant users, and tenant administrators log in to the management console to check the software information. The infrastructure administrator can also check the software information using the command on the admin server.



The following table explains the operation flow for each role.

	Operation Flow	User Roles				Reference
		Infrastructure Administrator	Dual-role Administrator	Tenant Administrator	Tenant User	
1	Register software information	Y	Y	-	-	"Definition of Software Information" in the *Developer's Guide* "Software Information Management Command" in the *Developer's Guide*
2	Register assets	Y	Y	-	-	"Asset Information Management Command" in the *Reference Guide*
3	Create a configuration modification template	Y	Y	Y (*2)	Y (*2)	"Configuration Modification Template Wizard" in the *Operator's Guide* "Configuration Modification Template Information Management Command" in the *Reference Guide*
4	Request configuration modification	Y (*1)	Y	Y (*2)	Y (*2)	"Configuration Modification Wizard" in the *Operator's Guide*

	Operation Flow	User Roles				Reference
		Infrastructure Administrator	Dual-role Administrator	Tenant Administrator	Tenant User	
						"Configuration Modification Command" in the *Reference Guide*
5	Install software	-	-	-	-	-
6	Check execution status	Y	Y	Y (*2)	Y (*2)	"Job Management" in the *Operator's Guide* "Job Information Management Command" in the *Reference Guide*
7	Collect software information	Y	Y	-	-	"Patch Information Update Command" in the *Reference Guide* "Installed Software Information Management Command" in the *Developer's Guide*
8	Check the software information	Y	Y	Y (*2)	Y (*2)	"Configuration Management" in the *Operator's Guide* "Installed Software Information Management Command" in the *Developer's Guide*

Y: Implement the task

-: Do not implement the task

*1: Only commands can be executed.

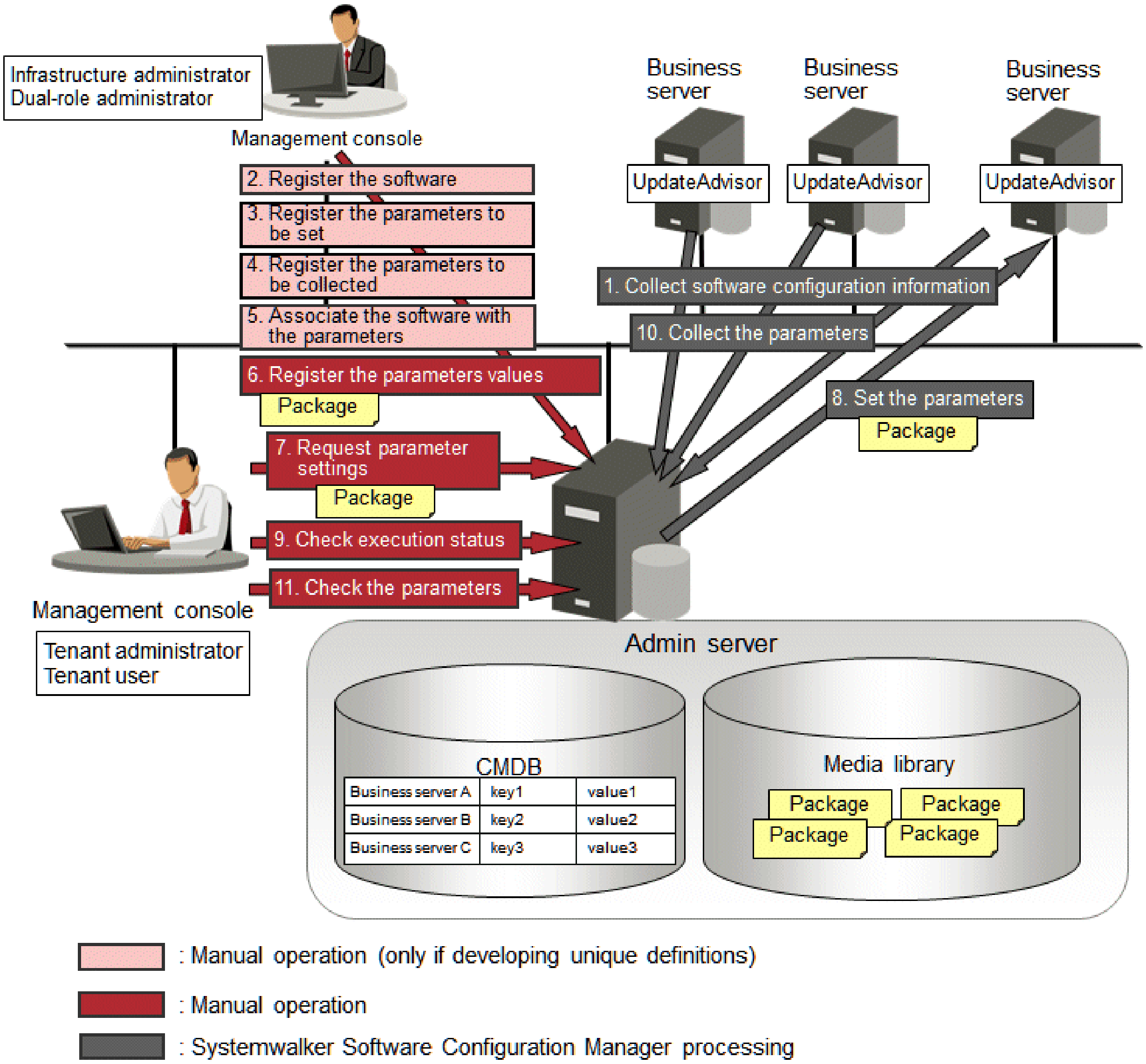
*2: Only the management console can be operated.

1.1.6 Software Parameter Management

The following diagram shows the overall flow of software parameters management.

Collect information on installed Fujitsu middleware using UpdateAdvisor (middleware).

However, parameter setting and collection for managed Solaris servers is not supported.


Infrastructure administrator
Dual-role administrator
Management console
2. Register the software
3. Register the parameters to be set
4. Register the parameters to be collected
5. Associate the software with the parameters
6. Register the parameters values
Package
7. Request parameter settings
Package
9. Check execution status
11. Check the parameters
Management console
Tenant administrator
Tenant user
Business server
Business server
Business server
UpdateAdvisor
UpdateAdvisor
UpdateAdvisor
1. Collect software configuration information
10. Collect the parameters
8. Set the parameters
Package
Admin server
CMDB
Media library
Package
Package
Package
Package
🟥 : Manual operation (only if developing unique definitions)
🟥 : Manual operation
⬛ : Systemwalker Software Configuration Manager processing

Business server A	key1	value1
Business server B	key2	value2
Business server C	key3	value3

1. Collect software configuration information **[Systemwalker Software Configuration Manager]**

   Perform discovery on the managed servers to collect information on installed Fujitsu middleware. Fujitsu middleware information is collected by UpdateAdvisor (middleware).

2. Register the software **[operation by the infrastructure administrator]**

   If managing software that is not compatible with UpdateAdvisor (middleware), use commands to register information about the software installed on the managed servers.

3. Register the parameters to set **[operation by the infrastructure administrator]**

   The infrastructure administrator defines the parameters to set in the software. Specify the list of parameters, and the scripts to set the parameters, using the parameter setting definition. Use commands to register the parameter setting definition.

   This step is not required if using the parameter setting definition pre-registered in this product.

4. Register the parameters to be collected **[operation by the infrastructure administrator]**

   The infrastructure administrator defines the parameters to be collected from the software. Specify the list of parameters, and the scripts to collect the parameters, using the parameter collection definition. Use commands to register the parameter collection definition.

   This step is not required if using the parameter collection definition pre-registered in this product.

5. Associate the software with the parameters **[operation by the infrastructure administrator]**

   The infrastructure administrator associates the parameter setting definition and the parameter collection definition with the software. The software is associated with the parameters using commands.

   This step is not required if using the software definition pre-registered in this product.

6. Register the parameters values **[operation by the infrastructure administrator]**

   The infrastructure administrator can define the values to be set in the parameters as predefined parameters. Predefined parameters are convenient to use when the user needs to configure the same value numerous times, or when a set of values to configure has been predetermined. Files, as well as values, can be specified in parameters. Use commands to register predefined parameters. Note that files can also be registered as packages.

7. Request parameter settings **[operation by the infrastructure administrator, the tenant administrator or the tenant user]**

   Either the tenant administrator or the tenant user logs in to the management console and requests parameter settings. Notifications that a request has been received, completed, or has ended in an error, are received by email.

   The infrastructure administrator can request the setting of parameters using the command on the admin server.

8. Set the parameters **[processing by Systemwalker Software Configuration Manager]**

   Systemwalker Software Configuration Manager configures the specified parameters in the managed servers.

9. Check execution status **[operation by the infrastructure administrator, the tenant administrator, or the tenant user]**

   Check the parameter setting status using the management console or the command on the admin server.

10. Collect the parameters **[processing by Systemwalker Software Configuration Manager]**

    Perform discovery on the managed servers to collect the software parameters. Files, as well as parameter values, can be collected.

11. Check the parameters **[operation by the infrastructure administrator, tenant administrator or the tenant user]**

    Infrastructure administrators, tenant users, and tenant administrators log in to the management console to check the parameters. The infrastructure administrator can check parameter values using the command on the admin server.

The following table explains the operation flow for each role.

	Operation flow	User roles				Reference
		Infrastructure administrator	Dual-role administrator	Tenant administrator	Tenant user	
1	Collect software configuration information	Y	Y	-	-	1.1.4 Fujitsu Middleware Patch Management
2	Register the software	Y	Y	-	-	"Definition of Software Information" in the *Developer's Guide* "Software Information Management Command" in the *Developer's Guide*
3	Register the parameters to set	Y	Y	-	-	"Definition of Parameters to be Set" under "Definition of Parameter Information" in the *Developer's Guide* "Parameter Settings Definition Management Command" in the *Developer's Guide*
4	Register the parameters to be collected	Y	Y	-	-	"Definition of Parameters to be Collected" under "Definition of Parameter Information" in the *Developer's Guide*

	Operation flow	User roles				Reference
		Infrastructure administrator	Dual-role administrator	Tenant administrator	Tenant user	
						"Parameter Collection Definition Management Command" in the *Developer's Guide*
5	Associate the software with the parameters	Y	Y	-	-	"Association with the Software" under " Definition of Parameter Information" in the *Developer's Guide* "Command to Associate Software and Parameter Definitions" in the *Developer's Guide*
6	Register the parameters values	Y	Y	-	-	2.11 Parameter Value Settings "Predefined Parameter Management Command" in the *Reference Guide*
7	Request parameter settings	Y(*1)	Y	Y (*2)	Y (*2)	"Parameter Settings Wizard" under "Configuration Management" in the *Operator's Guide* "Parameter Setting Command " in the *Reference Guide*
8	Set the parameters	-	-	-	-	-
9	Check execution status	Y	Y	Y(*2)	Y(*2)	"Job Management" in the *Operator's Guide* "Job Information Management Command" in the *Reference Guide*
10	Collect the parameters	Y	Y	-	-	"Parameter Information Update Command" in the *Reference Guide*
11	Check the parameters	Y	Y	Y(*2)	Y(*2)	"Configuration Management" in the *Operator's Guide* "Parameter Export Command" in the *Reference Guide*

Y: Implement the task.

-: Do not implement the task

*1: Only the command can be operated.

*2: Only the management console can be operated.

1.1.7 Hardware/Virtual Environment Configuration Management

Perform discovery of hardware configuration information to collect serial numbers of chassis, blade servers, and rack mount servers, firmware versions, CPU/memory, and other hardware information.

Perform discovery of virtual environment configuration information to collect the host OS version, guest OS, IP address, CPU/memory and other information in VMware vSphere environments.

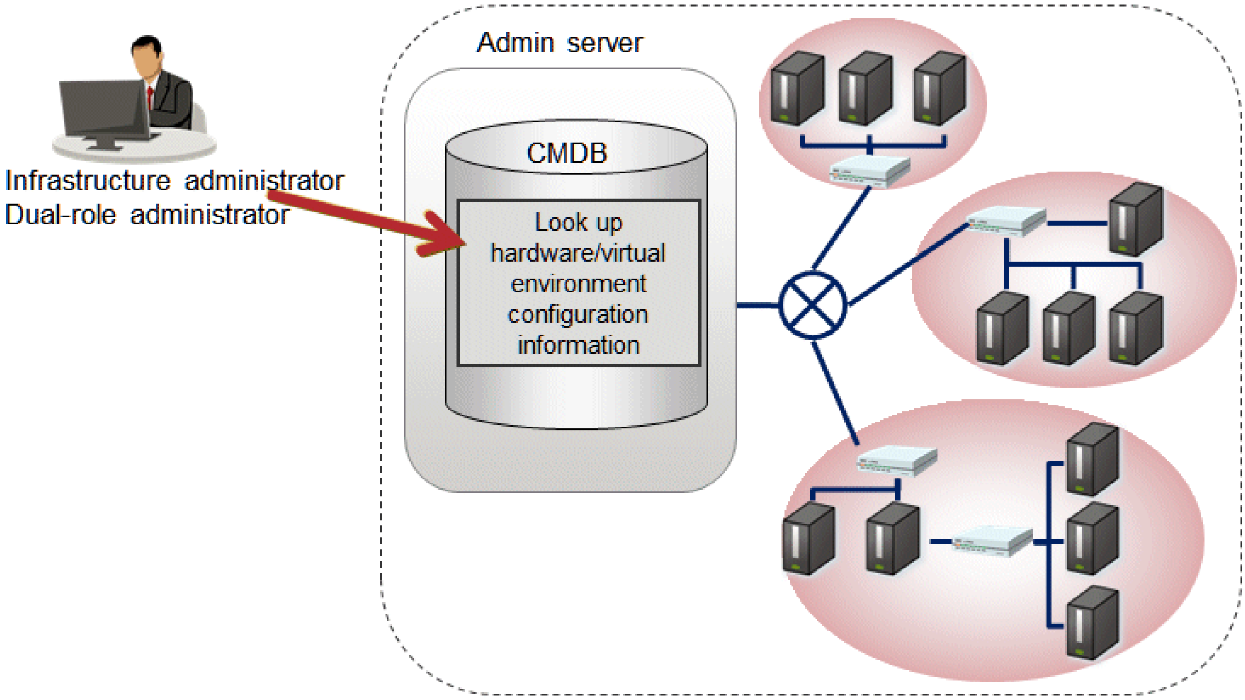
To manage configuration information of hardware and virtual environments, perform the following operations.

- Look up hardware/virtual environment configuration information

  The servers for which information has been collected by the discovery function can be displayed as a list, and detailed information about each individual server can be looked up. It is also possible to display information that has been filtered by specifying particular conditions.

The usage scope of hardware and virtual environment configuration management is as follows.

Figure 1.5 Overview of Hardware/Virtual Environment Configuration Management


Infrastructure administrator
Dual-role administrator
Admin server
CMDB
Look up hardware/virtual environment configuration information

The following table explains the operation flow for each role.

	Operation flow	User roles				Reference
		Infrastructure administrator	Dual-role administrator	Tenant administrator	Tenant user	
1	Look up hardware virtual environment configuration information	Y	Y	-	-	"Configuration Management" in the *Operator's Guide*

Y: Implement the task.

-: Do not implement the task

1.1.8 Software Configuration Management

To manage server information such as the server names, tenant names, host names, and IP addresses of various servers collected by performing discovery, as well as software configuration information such as information about installed software and applied patches, perform the following tasks from the **Configuration Management** window.

- Looking up software configuration information

  The servers for which information has been collected by the discovery function can be displayed as a list, and detailed information about each individual server can be looked up, including the patch application status for each server. It is also possible to display information that has been filtered by specifying particular conditions.

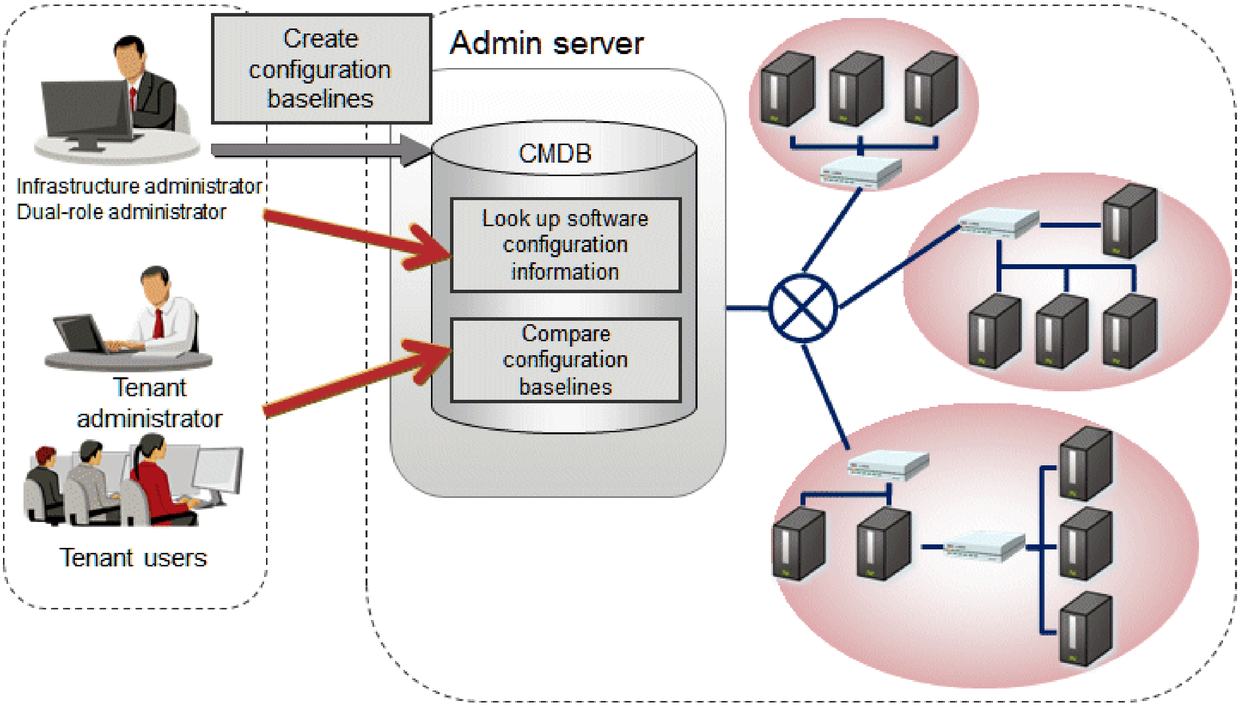
- Comparing configuration baselines

  A configuration baseline is a snapshot of the information collected by the discovery function at a certain moment in time.

  If a problem occurs with a server, it is possible to check which patches have been applied since the server was last running correctly by comparing the current configuration baseline with the configuration baseline at the time when the server was running correctly.

  Configuration baselines are created periodically according to a schedule. Configuration baselines can also be created by the infrastructure administrator.

Figure 1.6 Overview of Software Configuration Management


Create configuration baselines
Admin server
CMDB
Infrastructure administrator
Dual-role administrator
Look up software configuration information
Compare configuration baselines
Tenant administrator
Tenant users

The following table explains the operation flow for each role:

	Operation flow	User roles				Reference
		Infrastructure administrator	Dual-role administrator	Tenant administrator	Tenant user	
1	Create configuration baselines	Y	Y	-	-	"Configuration Baseline Creation Command" in the *Reference Guide*
2	Reference software configuration information	Y	Y	Y	Y	"Configuration Management" in the *Operator's Guide*
3	Compare configuration baselines	Y	Y	Y	Y	"Configuration Management" in the *Operator's Guide*

Y: Implement the task.

-: Do not implement the task

1.1.9 Automating Setup of the Infrastructure Environment

Use cloning images to automate the setup operation of an infrastructure environment, including server deployment, software installation, and software configuration. Infrastructure environment setup is performed in coordination with the following software that performs server deployment using cloning images. Deploy the server using the server management software to coordinate with, and then configure the OS and middleware using the operation commands of this product.

- Server management software such as ServerView Resource Orchestrator, OpenStack, or VMware vCenter Server

The flow of the installation environment setup is as shown below.

1. Collect cloning images [Performed using the server management software]

   Collect cloning images. Install agents of this product on the server from which cloning images are to be collected, in advance. Collect cloning images according to the information in the manuals or other documentation provided by the coordinated server management software.

2. Register servers [operation by the infrastructure administrator]

   Register the server for which the OS and middleware are configured with this product.

   - If coordinating with ServerView Resource Orchestrator Cloud Edition, this operation is not necessary because server registration is performed automatically.

   - If coordinating with OpenStack, this procedure is not necessary, because after step 3-1 the server is registered by performing discovery of the OpenStack information.

3. Set up the infrastructure environment [Performed using the server management software/Systemwalker Software Configuration Manager]

   Deploy the server and then configure the OS and middleware to set up the infrastructure environment. Infrastructure environment setup can be automated by including the processes to be executed for the following "server deployment/OS customization" and "OS and middleware configuration" in an executable program such as a script beforehand. When coordinating with ServerView Resource Orchestrator Cloud Edition or OpenStack, also refer to the "Information" section that follows.

   1. Server deployment and OS customization [Performed using the server management software]

      Deploy the server using the collected cloning image. After deployment, customize the OS and configure the machine-specific network information, such as the host name and the IP address. Perform server deployment and OS customization according to the information in the manuals or other documentation provided by the server management software to coordinate with.

      When coordinating with OpenStack, after server deployment, register the server by performing discovery of the OpenStack information.

   2. Configure the OS and middleware [performed using Systemwalker Software Configuration Manager]

      Configure the following settings for the OS and middleware. Use the operation commands provided by this product to do so.

Setting	Operation Command	Remarks
Windows OS patch application	swcfmg_patch_apply (Patch Application command)	- Specify the "-wait" option. - Specify the "-force" option. - When configuring immediately after server deployment, specify a sufficient monitoring period for the "-monitor" option.
Linux OS patch application		
Fujitsu Middleware patch application		
Software parameter configuration	swcfmg_param_startsetting (Parameter Configuration command)	
Software installation	swcfmg_configuration_change (Configuration Modification Command)	- Specify the "-wait" option. - When configuring immediately after the server deployment, define server operation check as the first process to execute in the configuration modification template and specify the monitoring time.
Settings other than the above		

      - When performing multiple configurations in succession, specify the "-wait" option for all of the above commands and then execute the commands in succession.

- When performing application of Windows OS patches, Linux OS patches, or Fujitsu middleware patches, or configuration of software parameters, execute the commands with the "-force" option specified.
- When performing configuration operations immediately after the server is deployed, it is necessary to perform the server operation check first to confirm that the OS customization is complete. Perform the following operations.

  - Application of Windows OS patches, Linux OS patches, or Fujitsu middleware patches, or configuration of software parameters

  Specify a sufficient monitoring period for the "-monitor" option.

  - Software installation

  Define server operation check as the first process to execute in the configuration modification template and specify the monitoring period.

4. Check execution status [operation by the infrastructure administrator]

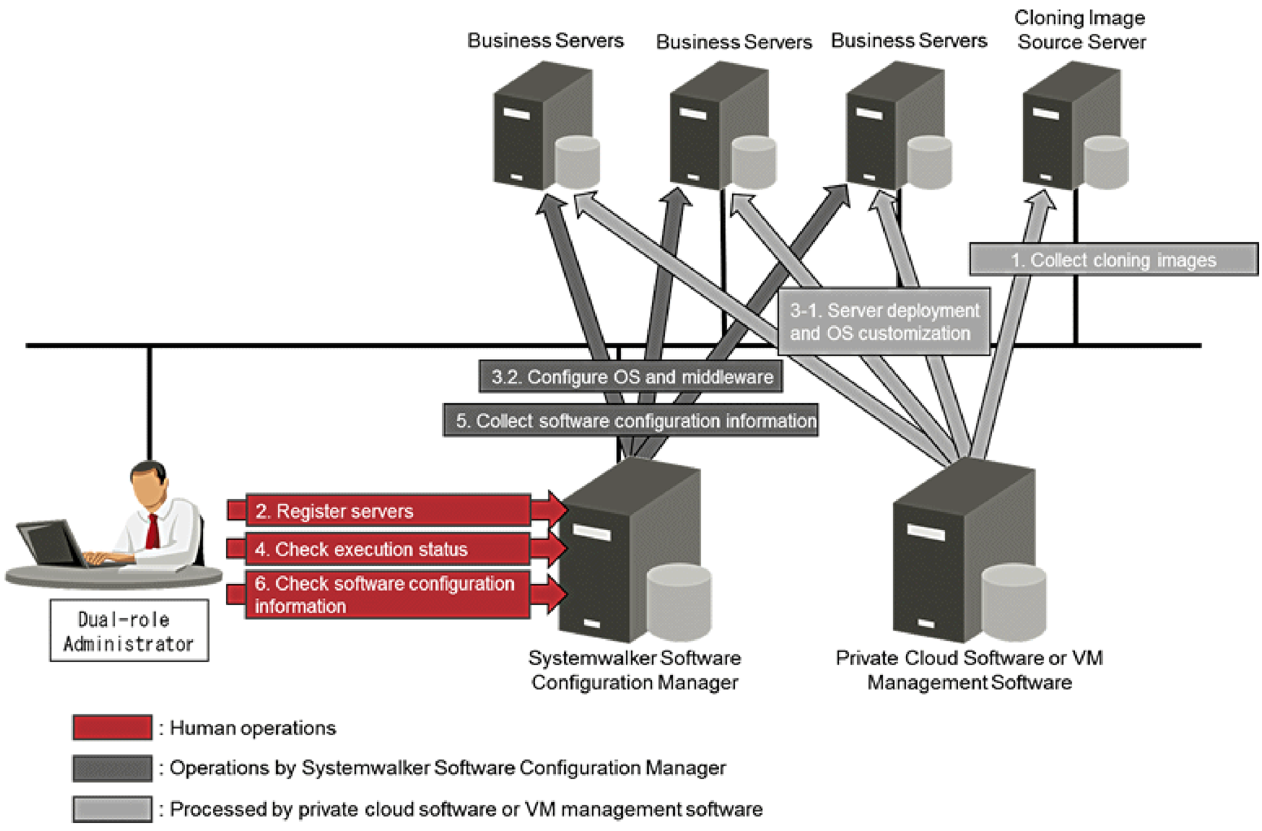
   Check the execution status of patch application, parameter configuration, or configuration modification using the management console or the commands on the admin server.

5. Collect software configuration information [performed using Systemwalker Software Configuration Manager]

   Systemwalker Software Configuration Manager collects the software configuration information of the business server.

6. Check the software configuration information [operation by the infrastructure administrator]

   Infrastructure administrators log in to the management console to check the software configuration information.


Business Servers
Business Servers
Business Servers
Cloning Image Source Server
1. Collect cloning images
3-1. Server deployment and OS customization
3.2. Configure OS and middleware
5. Collect software configuration information
2. Register servers
4. Check execution status
6. Check software configuration information
Dual-role Administrator
Systemwalker Software Configuration Manager
Private Cloud Software or VM Management Software
: Human operations
: Operations by Systemwalker Software Configuration Manager
: Processed by private cloud software or VM management software

	Operation Flow	User roles				Reference
		Infrastructure Administrator	Dual-role Administrator	Tenant Administrator	Tenant User	
1	Collection of cloning images	-	-	-	-	Manuals of server management software

		Operation Flow	User roles				Reference
			Infrastructure Administrator	Dual-role Administrator	Tenant Administrator	Tenant User	
2		Server registration	Y	Y	-	-	"Server Information Management Command" in the *Reference Guide*
3	1	Server deployment and OS customization	-	-	-	-	Manuals of server management software "OpenStack Information Update Command" in the Reference Guide
	2	OS and middleware configuration	Y (*1)	Y	-	-	"Patch Application Command" in the *Reference Guide* "Parameter Setting Command" in the *Reference Guide* "Configuration Modification Command" in the *Reference Guide*
4		Check execution status	Y	Y	-	-	"Job Management" in the *Operator's Guide* "Job Information Management Command" in the *Reference Guide*
5		Collect software configuration information	-	-	-	-	"Patch Information Update Command" in the *Reference Guide* "Parameter Information Update Command" in the *Reference Guide*
6		Check the software configuration information	Y	Y	-	-	"Configuration Management" in the *Operator's Guide* "Patch Management" in the *Operator's Guide*

Y: Implement the task.

-: Do not implement the task

*1: Only operation using commands is possible.

Information

When linked to ServerView Resource Orchestrator Cloud Edition

When performing set up of an infrastructure environment in coordination with ServerView Resource Orchestrator Cloud Edition, execute the scripts that are created and placed by the user before or after the operation of ServerView Resource Orchestrator. Create the scripts that configure the OS and middleware and register them with ServerView Resource Orchestrator in advance so that the OS and middleware can be configured automatically after the L-Platform is deployed. As the scripts for configuring the OS and middleware need to be executed asynchronously from the script registered directly with ServerView Resource Orchestrator, it is necessary to create the following two scripts: This section explains how to create and register scripts.

- Script to be registered with ServerView Resource Orchestrator
- Script for configuring the OS and middleware

Creating Scripts

The processes to be included in the script are shown below.

Script to be registered with ServerView Resource Orchestrator

The script to be registered directly with ServerView Resource Orchestrator. This script acquires the information necessary for configuring the OS and middleware from ServerView Resource Orchestrator and then executes the scripts for configuring the OS and middleware asynchronously.

1. Obtain L-Platform IDs and tenant names

   The script obtains the L-Platform IDs and tenant names specified for the arguments. For details on the script arguments, refer to "Script Execution when Operating L-Platforms or L-Servers" in the *ServerView Resource Orchestrator Cloud Edition Reference Guide (Command/XML)*. Obtained L-Platform IDs and tenant names are specified when executing the GetLPlatformConfiguration command in the script for configuring the OS and middleware.

2. Execute the script for configuring the OS and middleware

   Execute the script for configuring the OS and middleware asynchronously.

Script for configuring the OS and middleware

The script for configuring OS and middleware. This script obtains the information necessary for configuring the OS and middleware from ServerView Resource Orchestrator and then configures the OS and middleware.

1. Obtain the IP address

   Execute the GetLPlatformConfiguration command provided by ServerView Resource Orchestrator to obtain the IP address of the server for which the OS and middleware are to be configured. The IP address must be the one that is configured for the control NIC. Obtain the IP address of the NIC with the management tag set to "1".

   If necessary, obtain the template ID, cloning image ID, and L-Server name. For details on the GetLPlatformConfiguration command, refer to "GetLPlatformConfiguration (Gets Configuration Information for an LPlatform)" in the *ServerView Resource Orchestrator Cloud Edition Reference Guide (Command/XML)*.

2. OS and middleware configuration

   Execute the operation commands provided by this product to configure the OS and middleware.

Registering Scripts

Register the created scripts with ServerView Resource Orchestrator so that they are executed after L-Platform deployment is completed. For details on the registration procedure, refer to "Script Execution when Operating L-Platforms or L-Servers" in the *ServerView Resource Orchestrator Cloud Edition Reference Guide (Command/XML)*.

When coordinating with OpenStack

The following is an execution example of OS and middleware configuration for the instances in the stack, which is performed in step 3.

1. Deploy stacks

   Deploy stacks using the OpenStack APIs. Obtain the ID of the deployed stack from the API response.

2. Discover OpenStack patches

   Perform discovery of the OpenStack information, and register the deployed stacks and instances with this product. Specify the ID and monitoring time of the stack using swcfmg_openstack_updateinfo (OpenStack Information Update command).

3. Obtain the server ID

   Obtain the server ID of the server for which the OS and middleware are to be configured. Using the list display of swcfmg_server (Server Information Management command), specify the site ID, server group ID, and server name to obtain the server information of the configuration target. The server ID, server group ID, and server group name can be obtained from the following information beforehand. Specifying the -getserverid option outputs only the server ID.

   Site ID: "OpenStack"

Server group ID: Stack ID + "@OpenStack"

Server name: Instance name defined in the Heat template

4. OS and middleware configuration

   Use the operation commands provided by this product to configure the OS and middleware. For details, refer to "step 3-2". Specify the server of the operation target using its server ID.

1.2 Job Management

A job refers to an operation requested to Systemwalker Software Configuration Manager.

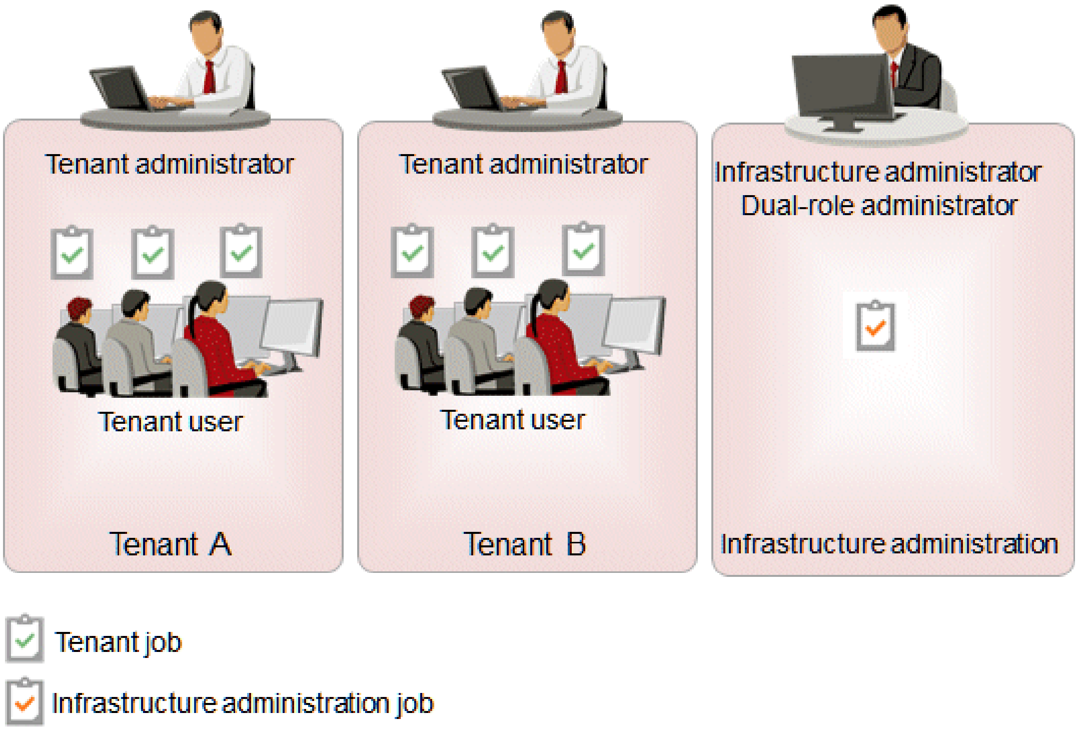
Operations such as patch distribution, patch application, parameter setting, and script execution are executed as a series of jobs. Managing these operations as jobs enables visualization of the process execution status and facilitates confirmation of the progress status. If a decision from the user is required, such as when an error occurs during job execution, the user can take the required action, such as retrying or canceling the job. Jobs can be managed using the management console or the Job Information Management command.

This section explains how to manage jobs.

Job Administrator

The user requesting a job is allocated as the administrator of that job. The job administrator can manage the job referencing the job and executing actions.

Figure 1.7 Tenant Jobs/Infrastructure Administration Jobs



Job Types

Jobs are categorized into the following two types:

- Tenant Job

  A tenant job is the job managed based on the tenant. Any job requested by a tenant user or a tenant administrator is regarded as a job owned by the tenant that they belong to, and is managed by the user of that tenant.

- Infrastructure Administration Job

  Any job requested by a dual-role administrator is regarded as a job owned by the infrastructure administration department, and is managed by the dual-role administrator or infrastructure administrator.

Job Management Scope by Role

Job management scope by user role is as follows.

- Tenant users can manage the jobs which they are assigned as the administrator (the jobs requested by themselves).
- Tenant administrators can manage all jobs owned by the managed tenant.
- Infrastructure administrators can manage all jobs owned by the infrastructure administration department. They can also look up tenant jobs.
- Dual-role administrators can manage all jobs owned by the infrastructure department and all tenants.

Table 1.1 Job Management Scope by Role

User role	Tenant job	Infrastructure administration job
Infrastructure administrator	N (*1)	Y
Dual-role administrator	Y	Y
Tenant administrator	Y	-
Tenant user	N (*2)	-

Y: Manageable

-: Not manageable

N: Conditional or restricted.

*1: Reference only.

*2: Only the jobs which that user is assigned as the administrator can be managed.

1.3 Configuration Modification Template Management

Configuration modification templates are a standardized set of the processes necessary for changing software configuration information. This section explains how to manage configuration modification templates.

Configuration modification template administrator

The user who created a configuration modification template is assigned as the administrator of that template. The template administrator can update and delete the template.

Scope of the configuration modification template

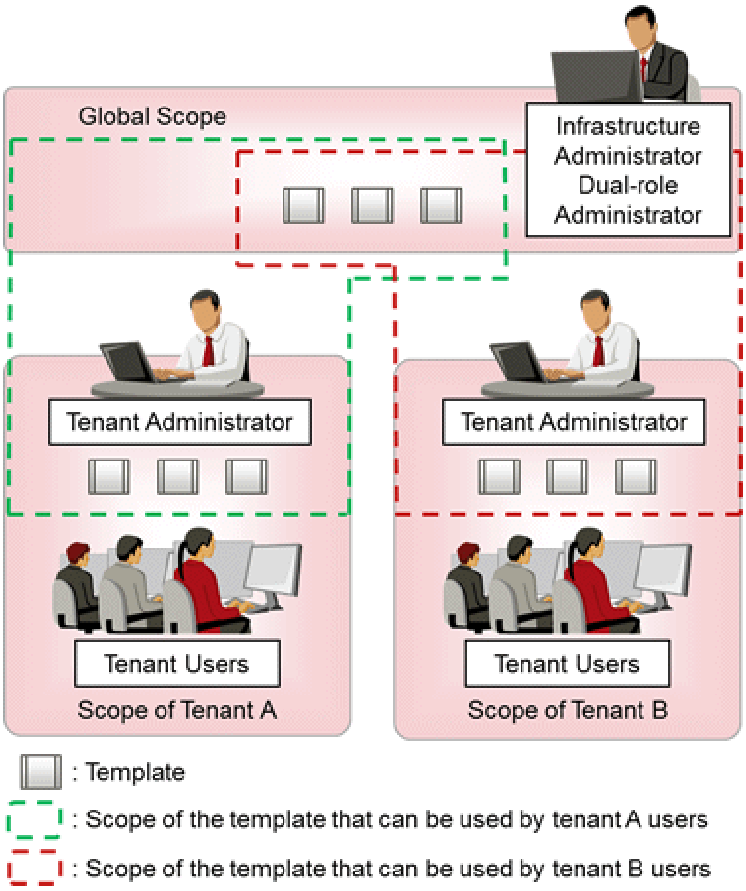
Setting a scope enables limiting of the users of the configuration modification template. There are two following types of scopes:

- Tenant

  The users belonging to a particular tenant are only allowed to use the configuration modification template.

- Global

  All users are allowed to use the configuration modification template.


Global Scope
Infrastructure Administrator
Dual-role Administrator
Tenant Administrator
Tenant Administrator
Tenant Users
Scope of Tenant A
Tenant Users
Scope of Tenant B
: Template
: Scope of the template that can be used by tenant A users
: Scope of the template that can be used by tenant B users

Management scope by role

Template management scope by user role is as follows.

- Tenant users can update and delete the templates that they have created. The created template will be within the scope of the tenant that the creator belongs to.
- Tenant administrators can update and delete the templates within the scope of each tenant that they manage. The created template will be within the scope of the tenant that the creator belongs to.
- Infrastructure administrators can create, update, and delete the templates within the scope of all tenants and also the templates within the global scope.
- Dual-role administrators can create, update, and delete the templates within the scope of all tenants and also the templates within the global scope.

Table 1.2 Template operation scope by user role

User Role	Tenant Scope				Global Scope			
	Use	Creation	Updating	Deletion	Use	Creation	Updating	Deletion
Infrastructure administrator	N	Y	Y	Y	N	Y	Y	Y
Dual-role administrator	Y	Y	Y	Y	Y	Y	Y	Y
Tenant administrator	Y (*1)	Y (*1)	Y (*1)	Y (*1)	Y	N	N	N
Tenant User	Y (*1)	Y (*1)	Y (*2)	Y (*2)	Y	N	N	N

Y: Operable.

N: Not operable.

Y (*): Conditional or restricted.

*1: Only the templates within the scope of the tenant that they belong to are operable.

*2: Only the templates that they created are operable.

1.4 Asset Management

Assets refers to the files stored in the media library. By managing files as assets, it is possible to perform version management and file distribution to managed servers using Systemwalker Software Configuration Manager.

Asset scope

Setting a scope enables limiting of the users of assets. There are two following types of scopes:

- Tenant

  The users belonging to a particular tenant are only allowed to use the configuration modification template.

- Global

  All users are allowed to use the configuration modification template.

Chapter 2 Operation Setup

This chapter explains how to set up Systemwalker Software Configuration Manager operations.

2.1 User Management

This section explains the following items with regard to managing users:

- Registering a user
- Changing the password
- Updating a user
- Moving a user
- Deleting a user

When linked to ServerView Resource Orchestrator

When linked to ServerView Resource Orchestrator, tasks such as registering a user or changing the password, as well as updating, moving, or deleting a user, should be performed from ServerView Resource Orchestrator. Refer to the following manuals for information on how to perform these tasks using ServerView Resource Orchestrator:

- "Tenant" in the *ServerView Resource Orchestrator Cloud Edition User's Guide for Infrastructure Administrators*
- "Tenant" in the *ServerView Resource Orchestrator Cloud Edition User's Guide for Tenant Administrators*

Refer to "Login Users" in the *Operator's Guide* for information on the correspondences between the roles of users registered with ServerView Resource Orchestrator and the roles for Systemwalker Software Configuration Manager.

Note

If a server group owner is deleted

If a server group owner is deleted when coordinating with ServerView Resource Orchestrator, the following emails will no longer be delivered to that owner:

- Latest patch release notification emails
- Event notification emails regarding patch application, patch distribution, parameter settings, script execution, and configuration modification

In addition, the following messages will be output to the event log/system log and to the standard output:

Event log/system log

```
CFMGD10003 Unable to send an email to [user:{userId (*1)}]. [Details:{details}]
```

```
CFMGD10004 Unable to send an email because the user ID for the administrator cannot be acquired from the managed server.
[Server ID:{serverID (*2)}] [IP address:{ipAddress (*3)}]
```

Standard output

```
CFMGC00126 Unable to send an email to [user:{userId (*1)}]. [Details:{details}]
```

Details

The following message IDs will be output in the details of "CFMGD10003" and "CFMGC00126".

```
CFMGM20004 User information could not be found. User ID = {userId (*1)}
```

```
CFMGM20006 Unable to send email because an email address has not been set. User ID = {userId (*1)}
```

*1: The user ID of the corresponding user

*2: Server ID of the relevant server

*3: IP address of the relevant server

Change the relevant server group owner to another existing user. For details on how to change the server group owner, refer to "2.3.4 Changing a Server Group Owner".

2.1.1 Registering a User

The following kinds of information can be specified when registering a user with the swcfmg_account command (refer to "swcfmg_account (User Information Management Command)" in the *Reference Guide* for details):

Information	Description
User ID	An ID that uniquely identifies the user.
Password	User password.
Tenant	Tenant to whom the user belongs.
Role	Role of the user.
Email address	Email address of the user.
Surname	Name of the user. Registration of middle names is optional.
Middle name(s)	
Given name	
Telephone number	Registration of the user's telephone number is optional.
Company or organization name	Name of the company or organization to which the user belongs. Registration is optional.

2.1.2 Changing the Password

Use swcfmg_account to change the user password (refer to "swcfmg_account (User Information Management Command)" in the *Reference Guide* for details).

2.1.3 Updating a User

Use swcfmg_account to update user information (refer to "swcfmg_account (User Information Management Command)" in the *Reference Guide* for details).

2.1.4 Moving a User

The tenant to which the user belongs can be changed by moving the user with swcfmg_account.

Moving of users is performed using the User Information Management command. Refer to "swcfmg_account (User Information Management Command)" in the Reference Guide for details.

If the user is a server group owner, the tenants that belong to that the server group will not change. One of the actions below must be performed when moving a user:

- Before moving the user, change the ownership of their server group to one of the current tenants.

  For details on how to modify the server group owner, refer to "2.3.4 Changing a Server Group Owner".

- After moving the user, move the server group owned by that user to a tenant at the destination.

  For details on how to move the server group, refer to "2.3.3 Moving a Server Group".

Note

When moving a tenant user, ensure that none of the jobs managed by that user are in the "Running", "Selecting (abnormal)", or "Waiting" state. Once the user is moved, that user will not be able to operate those jobs. To check if a job is in the "Running", "Selecting (abnormal)", or "Waiting" state, use the **Job Management** window or the list display option of the job information management command. If the user is moved leaving the jobs managed by that user in the above states, those jobs should be operated by the tenant administrator.

2.1.5 Deleting a User

Use swcfmg_account to delete a user (refer to "swcfmg_account (User Information Management Command)" in the *Reference Guide* for details).

When deleting a user, use the Server Group Information Management command with the -list option to ensure that the user does not own the server group. If the user does own the server group, perform either of the following operations.

- Change ownership of the server group to one of the current tenants

  For details on how to modify the server group owner, refer to "2.3.4 Changing a Server Group Owner".

- Delete the server group

  For details on how to delete server groups, refer to "2.3.5 Deleting a Server Group".

2.2 Tenant Management

A tenant is a unit of management for segmenting and isolating the management and operation of resources, based on an organization or business. This section describes the following operations for managing tenants:

- Registering a tenant
- Updating a tenant
- Deleting a tenant

Default tenant

When installing this product, the following default tenant is automatically registered. The default tenant cannot be deleted. When linked with ServerView Resource Orchestrator, the L-Platform cannot be deployed to the default tenant from ServerView Resource Orchestrator, and users cannot be created.

Tenant ID	Display name
__DEFAULT__	Default Tenant

When linked to ServerView Resource Orchestrator

When linked to ServerView Resource Orchestrator, tasks such as registering, updating, or deleting a tenant should be performed from that product. Refer to the following manuals for information on how to perform these tasks using ServerView Resource Orchestrator:

- "Tenant" in the *ServerView Resource Orchestrator Cloud Edition User's Guide for Infrastructure Administrators*
- "Tenant" in the *ServerView Resource Orchestrator Cloud Edition User's Guide for Tenant Administrators*

Note

When deleting a tenant using ServerView Resource Orchestrator, use the Server Group Information Management command with the -list option to ensure that the server group does not belong to the tenant.

If a tenant with a server group is inadvertently deleted, move the server group to a currently existing tenant.

The Server Group Information Management command can be used with the -list option to confirm the server groups that do not belong to a tenant.

2.2.1 Registering a Tenant

The following kinds of information can be specified when registering a tenant with the swcfmg_tenant command (refer to "swcfmg_tenant (Tenant Information Management Command)" in the *Reference Guide* for details):

Information	Description
Tenant ID	A name that uniquely identifies the tenant.
Display name	Display name of the tenant. Only limited characters can be used for the 'tenant name', so a name that easily identifies the tenant can be configured here if needed.

2.2.2 Updating a Tenant

Use swcfmg_tenant to update tenant information. Refer to "swcfmg_tenant (Tenant Information Management Command)" in the *Reference Guide* for details.

2.2.3 Deleting a Tenant

Use swcfmg_tenant to delete a tenant. Refer to "swcfmg_tenant (Tenant Information Management Command)" in the *Reference Guide* for details.

Confirm the following before deleting a tenant:

- Confirm that no users or server groups exist within the tenant by executing the User Group Information Management command with the -list option or with the Server Group Information Management command with the -list option. If a user or a server group exists, perform one of the steps below before deleting the tenant.

  - Move the user or server group to another tenant

    Refer to "2.1.4 Moving a User" for details on how to move a user. For details on how to move server groups, refer to "2.3.3 Moving a Server Group".

  - Delete the user or the server group.

    For details on how to delete a user, refer to "2.1.5 Deleting a User". For details on how to delete server groups, refer to "2.3.5 Deleting a Server Group".

- Execute the Asset Information Management command with the -list option or the Configuration Modification Template Information Management command with the -list option and confirm that there are no assets or configuration modification templates within the tenant scope. If the corresponding asset or configuration modification template exists, perform one of the steps below before deleting the tenant.

  - Change the scope of the asset or configuration modification template

    For details on how to change the scope of an asset, refer to "2.7.2 Updating an Asset". For details on how to change the scope of the configuration modification template, refer to "2.6.2 Updating a Configuration Modification Template".

  - Delete the asset or configuration modification template

    For details on how to delete an asset, refer to "2.7.3 Deleting an Asset". For details on how to delete a configuration modification template, refer to "2.6.3 Deleting a Configuration Modification Template".

2.3 Server Group Management

A server group is a management unit to perform grouping of servers depending on the system for operations. The methods to manage server groups differ depending on the site. This section explains the following operations for methods to manage the server group for each site:

- Registering a Server Group
- Updating a Server Group
- Moving a Server Group
- Changing a Server Group Owner
- Deleting a Server Group

2.3.1 Registering a Server Group

This section explains how to register server groups.

Manual registration

Use the Server Group Information Management command to manually register the server group. When registering a server group, the following information can be registered: Refer to "swcfmg_servergroup/swcfmg_lplatform (Server Group Information Management Command)" in the Reference Guide.

Information	Description
Server group name	Name of the server group. A name can be assigned to the server group for management purposes.
Tenant	Tenant to which the server group belongs.
Owner	Owner of the server group.

ServerView Resource Orchestrator

To register a server group of ServerView Resource Orchestrator, it is necessary to create an L-Platform using ServerView Resource Orchestrator. Refer to the following manuals for information on how to create an L-Platform: The created L-Platform is automatically registered as a server group. L-Platforms created before installing this product are automatically registered as server groups after installation.

- "L-Platform" in the *ServerView Resource Orchestrator Cloud Edition User's Guide for Tenant Administrators*
- "L-Platform" in the *ServerView Resource Orchestrator Cloud Edition User's Guide for Tenant Users*
- "Importing to L-Platform" in the *ServerView Resource Orchestrator Cloud Edition Operation Guide*

OpenStack

To register server groups of OpenStack, it is necessary to perform discovery of the OpenStack information. The stacks of OpenStack are registered as server groups after discovery.

2.3.2 Updating a Server Group

This section explains how to update server group information.

Manual registration

Use the Server Group Information Management command to update the manually registered server information Refer to "swcfmg_servergroup/swcfmg_lplatform (Server Group Information Management Command)" in the *Reference Guide.*

ServerView Resource Orchestrator

Update the L-Platform information using ServerView Resource Orchestrator to update the server group information. Refer to the following manuals for details:

- "L-Platform" in the *ServerView Resource Orchestrator Cloud Edition User's Guide for Tenant Administrators*
- "L-Platform" in the *ServerView Resource Orchestrator Cloud Edition User's Guide for Tenant Users*

OpenStack

Update the stack information of OpenStack to update the server group information. When discovery of OpenStack information is performed after update, the server group information is updated.

2.3.3 Moving a Server Group

This section explains how to move server groups.

The tenant to which a server group belongs can be changed by moving the server group.

If moving a server group, one of the actions below must be performed to ensure that the server group owner will become a user in a tenant at the destination:

- Before moving a server group, move the server group owner to a tenant at the destination.

  Refer to "2.1.4 Moving a User" for details on how to move a user.

- After moving a server group, change the server group owner to a user in a tenant at the destination.

  For details on how to modify the server group owner, refer to "2.3.4 Changing a Server Group Owner".

Note

When moving a server group, ensure that none of the jobs for the servers in the server group are in the "Running", "Selecting (abnormal)", or "Waiting" state. Once that a server group is moved, jobs which were in the "Running", "Selecting (abnormal)", or "Waiting" state during moving of the server group may be operated by the user of the tenant that the server group belonged to. To check if a job is in the "Running", "Selecting (abnormal)", or "Waiting" state, use the **Job Management** window or the list display option of the job information management command.

Manual registration

Use the Server Group Information Management command to move manually registered server groups. Refer to "swcfmg_servergroup/swcfmg_lplatform (Server Group Information Management Command)" in the *Reference Guide*.

ServerView Resource Orchestrator

Move server groups of ServerView Resource Orchestrator using ServerView Resource Orchestrator. Refer to the following manuals for details:

- "Tenant" in the *ServerView Resource Orchestrator Cloud Edition User's Guide for Infrastructure Administrators*
- "Tenant" in the *ServerView Resource Orchestrator Cloud Edition User's Guide for Tenant Administrators*

OpenStack

Server groups of OpenStack cannot be moved.

2.3.4 Changing a Server Group Owner

This section explains how to change server group owners.

Ensure that the server group owner is a user in the tenant to which the server group belongs.

Manual registration

Use the Server Group Information Management command to change manually registered server group owners. Refer to "swcfmg_servergroup/swcfmg_lplatform (Server Group Information Management Command)" in the Reference Guide.

ServerView Resource Orchestrator

Change server group owners of ServerView Resource Orchestrator using ServerView Resource Orchestrator. Refer to the following manuals for details:

- "Tenant" in the *ServerView Resource Orchestrator Cloud Edition User's Guide for Infrastructure Administrators*

- "Tenant" in the *ServerView Resource Orchestrator Cloud Edition User's Guide for Tenant Administrators*

OpenStack

Server group owners of OpenStack cannot be changed.

2.3.5 Deleting a Server Group

This section explains how to delete server groups.

Manual registration

Use the Server Group Information Management command to delete manually registered server groups. Refer to "swcfmg_servergroup/swcfmg_lplatform (Server Group Information Management Command)" in the Reference Guide.

Before deleting a server group, use the Server Information Management command with the -list option to ensure that there are no servers in the server group. If a server is found, delete it before deleting the server group.

ServerView Resource Orchestrator

To delete a server group of ServerView Resource Orchestrator, it is necessary to delete the L-Platform using ServerView Resource Orchestrator. Refer to the following manuals for information on how to delete an L-Platform:

- "L-Platform" in the *ServerView Resource Orchestrator Cloud Edition User's Guide for Tenant Administrators*

- "L-Platform" in the *ServerView Resource Orchestrator Cloud Edition User's Guide for Tenant Users*

OpenStack

To delete a server group of OpenStack, the stack must be deleted using OpenStack. When discovery of OpenStack information is performed after deletion, the server group is deleted.

2.4 Hardware/Virtual Environment Management

The following hardware can be managed using this product.

- Blade server chassis

- Blade server server blades

- Single servers (rack mount or tower)

- The following virtual environments can be managed:

- VMware vSphere 5.1 or later

This section describes the following operations for managing hardware:

- Registering hardware

- Updating hardware

- Deleting hardware

Note

Ensure that the IP addresses of physical servers, hypervisors, and OSs managed using Systemwalker Software Configuration Manager are unique.

2.4.1 Registering Hardware/Virtual Environment

Register hardware to enable chassis, server blades, and single servers to be managed by Systemwalker Software Configuration Manager. VMware vSphere can also be managed.

The following kinds of information can be registered when registering hardware. Use the hardware information management command to register hardware. For details, refer to "swcfmg_hardware (Hardware Information Management Command)" in the Reference Guide.

To manage a server blade as the management target, it is also necessary to register the chassis on which the server blade is mounted as a management target.

Item	Description
ipaddress	The admin IP address.
serial-number	The serial number.
hardware-type	The hardware type.
vendor-classification-name	Indicates the vendor. Specify FUJITSU, IBM, or HP.
model-group-name	Leave this field blank in this version.
hardware-name	The hardware name. A name can be assigned to the hardware for management purposes.
asset-number	The asset number.
description	A memo about the hardware.
snmp-community-name	The SNMP community name of the chassis.
hardware-user-id	A user ID used for iRMC connections.
hardware-password	A user password used for iRMC connections.
os-ipaddress	The OS IP address.
hypervisor-type	Type of Hypervisor. When managing VMware vSphere, specify VMware.
hypervisor-user-id	The user ID for the user for connection to the hypervisor.
hypervisor-password	The password for the user for connection to the hypervisor.

2.4.2 Updating Hardware

Use the hardware information management command to update the hardware information. For details, refer to "swcfmg_hardware (Hardware Information Management Command)" in the Reference Guide.

2.4.3 Deleting Hardware

To stop hardware from being managed by Systemwalker Software Configuration Manager, delete it.

Use the hardware information management command to delete the hardware. For details, refer to "swcfmg_hardware (Hardware Information Management Command)" in the Reference Guide.

2.5 Server Management

The methods to manage servers differ depending on the site. This section describes the following operations for managing servers depending on the site:

- Registering a server
- Updating a Server
- Deleting a server
- Managing a server managed by Systemwalker Runbook Automation

Note

Ensure that the IP addresses of servers managed using Systemwalker Software Configuration Manager are unique.

If linking to ServerView Resource Orchestrator or OpenStack, ensure that all IP addresses are unique, including those of ROR and OpenStack servers.

2.5.1 Registering a Server

This section explains how to register servers.

Register a server to enable it to be managed by Systemwalker Software Configuration Manager.

Manual registration

Use the Server Information Management command to manually register servers. The kinds of information listed below can be specified when registering a server with the swcfmg_server command Refer to "swcfmg_server (Server Information Management Command)" in the Reference Guide for details.

Perform a connection test whenever you register a server (refer to "swcfmg_connectiontest (Connection Test Command)" in the *Reference Guide* for details).

Item	Description
IP address	The IP address connected to the admin LAN.
Server name	Name of the server. A name can be assigned to the server for management purposes.
Server group	Server group to which the server belongs.
Host name	Host name of the server.
Operating system type	Type of operating system.
OS architecture	Architecture of the operating system.
Operating system name	Name of the operating system.

ServerView Resource Orchestrator

To register a server of ServerView Resource Orchestrator, it is necessary for the L-Server to belong to the L-Platform in ServerView Resource Orchestrator. Perform the operations below using ServerView Resource Orchestrator:

- Create an L-Platform
- Reconfigure the L-Platform and add the L-Server
- Import the L-Server to the L-Platform.

Refer to the following manuals for details: L-Servers that already belong to the L-Platform before installing this product are automatically registered as servers after installation.

- "L-Platform" in the *ServerView Resource Orchestrator Cloud Edition User's Guide for Tenant Administrators*
- "L-Platform" in the *ServerView Resource Orchestrator Cloud Edition User's Guide for Tenant Users*
- "Importing to L-Platform" in the *ServerView Resource Orchestrator Cloud Edition Operation Guide*

OpenStack

To register servers of OpenStack it is necessary to perform discovery of the OpenStack information. The instances of OpenStack are registered as servers after discovery. When the following instances are found during discovery, a server group is automatically created for each instance. The instance is registered as a server that belongs to the automatically created server group.

- Instances which are not configured for the stack

- Instances created using resource_type with a value other than "OS::Nova::Server" using the Heat template.

The server group name and the server group ID of the automatically created server group are as given below.

Server group name	Server group ID
No stack (instance ID)	NoStack_instance ID

2.5.2 Updating a Server

This section explains how to update server information.

Manual registration

Use the Server Information Management command to update the manually registered server information Refer to "swcfmg_server (Server Information Management Command)" in the *Reference Guide* for details.

ServerView Resource Orchestrator

To delete a server of ServerView Resource Orchestrator, the server must be deleted using ServerView Resource Orchestrator. Refer to the following manuals for information on how to delete an L-Server:

- "L-Platform" in the *ServerView Resource Orchestrator Cloud Edition User's Guide for Tenant Administrators*
- "L-Platform" in the *ServerView Resource Orchestrator Cloud Edition User's Guide for Tenant Users*

OpenStack

Update the instance information of OpenStack to update the server information. When discovery of OpenStack information is performed after update, the server information is updated.

2.5.3 Deleting a Server

This section explains how to delete servers.

Delete a server to stop it from being managed by Systemwalker Software Configuration Manager.

Manual registration

Use the Server Information Management command to delete manually registered servers. Refer to "swcfmg_server (Server Information Management Command)" in the *Reference Guide* for details.

ServerView Resource Orchestrator

To delete a server of ServerView Resource Orchestrator, the server must be deleted using ServerView Resource Orchestrator. Refer to the following manuals for information on how to delete an L-Server:

- "L-Platform" in the *ServerView Resource Orchestrator Cloud Edition User's Guide for Tenant Administrators*
- "L-Platform" in the *ServerView Resource Orchestrator Cloud Edition User's Guide for Tenant Users*

OpenStack

To delete a server of OpenStack, the instance must be deleted using OpenStack. When discovery of OpenStack information is performed after deletion, the server is deleted.

2.5.4 Hypervisor and OS Management

It is necessary to register a hypervisor or an OS as a managed server of Systemwalker Software Configuration Manager to perform patch management or software parameter management for a hypervisor or the OS of a server blade or single server. This section explains how to manage a hypervisor or an OS as a managed server.

Registering a Server

To register a guest OS or a hypervisor as a managed server of Systemwalker Software Configuration Manager, it is necessary to perform both of the following operations: Specify an IP address for the OS, when registering hardware. Specify the same value as specified for the IP address of an OS when registering hardware as the value for the IP address when registering a server.

- Register a server using the Server Information Management command
- Register hardware using the hardware information management command

Updating a Server

Use the server information management command to update the server information. <=Delete=>

Deleting a Server

To configure a hypervisor or an OS to no longer be managed by this product, delete it using the Server Information Management command.

2.5.5 Guest OS Management

To perform patch management or software parameter management for the guest OS, it is necessary to register a guest OS as a managed server of Systemwalker Software Configuration Manager. This section explains how to manage a hypervisor or an OS as a managed server.

Registering a Server

To register a guest OS as a managed server of Systemwalker Software Configuration Manager, it is necessary to perform both of the following operations:

- Register a server using the Server Information Management command
- Collect the configuration information of the guest OS by performing discovery of the virtual environment configuration information

Updating a Server

Use the server information management command to update the server information. <=Delete=>

Deleting a Server

To configure a guest OS to no longer be managed by this product, delete it using the Server Information Management command

2.6 Configuration Modification Template Management

This section explains the following items with regard to managing configuration modification templates.

- Creating a configuration modification template
- Updating a configuration modification template
- Deleting a configuration modification template

2.6.1 Creating a Configuration Modification Template

When creating a configuration modification template, register the following information.

Use the management console or the Configuration Modification Template Information Management command to create a configuration modification template. For details, refer to "Configuration Modification Template List" in the *Operator's Guide* or "swcfmg_changetemplate (Configuration Modification Template Information Management command)" in the "*Reference Guide*".

Information	Description
Template name	The name of the configuration modification template.
Template ID	The unique ID for identifying the configuration modification template. When omitted, the ID is automatically assigned.

Information	Description
Description	The description of the configuration modification template.
Scope	The scope of the configuration modification template.
Administrator	The administrator of the configuration modification template.
Processes	The configuration modification processes executed from the configuration modification template.
Parameters	The parameters of the configuration modification template.

2.6.2 Updating a Configuration Modification Template

Use the management console or the Configuration Modification Template Information Management command to update a configuration modification template. For details, refer to "Configuration Modification Template Details" in the *Operator's Guide* or "swcfmg_changetemplate (Configuration Modification Template Information Management Command)" in the "*Reference Guide*". The content of the configuration modification jobs being executed cannot be changed even if the configuration modification template is updated.

2.6.3 Deleting a Configuration Modification Template

Use the management console or the Configuration Modification Template Information Management command to delete a configuration modification template. For details, refer to "Configuration Modification Template Details" in the *Operator's Guide* or "swcfmg_changetemplate (Configuration Modification Template Information Management Command)" in the "*Reference Guide*".

2.7 Asset Management

This section explains the following items with regard to asset management:

- Registering an asset
- Updating an asset
- Deleting an asset
- Uploading an asset
- Downloading an asset

2.7.1 Registering an Asset

When registering an asset, the following information can be registered:

Use the Asset Information Management command to register an asset. For details, refer to "swcfmg_repository (Asset Information Management Command)" in the *Reference Guide*. To use assets for configuration modification, register and upload the assets.

Information	Description
Asset name	The name of the asset.
Asset ID	An ID that uniquely identifies the asset. When omitted, the ID is automatically assigned.
Description	The description of the asset.
Scope	The scope of the asset.
Administrator	The administrator of the asset.

2.7.2 Updating an Asset

Use the Asset Information Management command to update assets. For details, refer to "swcfmg_repository (Asset Information Management Command)" in the *Reference Guide*.

2.7.3 Deleting an Asset

Use the Asset Information Management command to delete assets. For details, refer to "swcfmg_repository (Asset Information Management Command)" in the *Reference Guide*.

When deleting assets, note the following:

- The assets being used for file collection and script execution performed by the configuration modification job cannot be deleted. Wait until the corresponding job is completed and the job status changes to "Complete", "Complete (error)", or "Cancel" before deleting the assets.
- The assets used in the configuration modification template cannot be deleted. Delete the corresponding configuration modification template first and then delete the assets.

2.7.4 Uploading an Asset

Use the Asset Information Management command to upload an asset. When an asset is uploaded, the version number of that asset is incremented. For details, refer to "swcfmg_repository (Asset Information Management Command)" in the *Reference Guide*. The maximum size of files that can be uploaded is 5 GB.

2.7.5 Downloading an Asset

Use the Asset Information Management command to download an asset. For details, refer to "swcfmg_repository (Asset Information Management Command)" in the *Reference Guide*.

2.8 Setup for Patch Management

This section explains how to configure settings for patch management and changes these settings.

2.8.1 Setting up Patch Management Policies for Windows Operating Systems and Fujitsu Middleware

The patch management policies for Windows operating systems and Fujitsu middleware are set up when Systemwalker Software Configuration Manager is set up. To change this policy, edit the patch management policy definition file.

Refer to the *Reference Guide* for information on the patch management policy definition file.

[Windows]

```
<Systemwalker Software Configuration Manager installation directory>\SWCFMGM\config\patch_management_policy.xml
```

[Linux]

```
/etc/opt/FJSVcfmgm/config/patch_management_policy.xml
```

Setting up the patch management policy for Windows operating systems

This section explains how to set up the patch management policy for Windows operating systems.

Setting up the patch management policy allows infrastructure administrators to set the patch types (the classification of updates, which represent the WSUS update program types) for application status monitoring, as well as the patch types to be applied to all servers without fail.

This enables tenant users to distinguish which patches are mandatory and which patches are optional when they apply patches.

Item	Description
Classification level specification for the updates for WSUS	Specify the classification level for the update programs acquired from WSUS. Classification levels classify the importance of a patch in terms of patch management by Systemwalker Software Configuration Manager, and can be specified as either "Required" or "Recommended" for each classification of update.

Item	Description
	The classification levels are as follows: - "Required": A patch that must be applied uniformly to all servers according to the decision that the infrastructure administrator has made - "Recommended": A patch recommended for application by the infrastructure administrator that can be canceled by a tenant user if they determine it will affect business activities. "Required" or "Recommended" can be specified for each classification of update. By default, the classification levels are as follows: [Required] - Security Updates - Critical Updates [Recommended] - Feature Packs - Service Packs - Tools - Drivers - Updates - Update Rollups - Definition Updates

Setting up the patch management policy for Fujitsu middleware

This section explains how to set up the patch management policy for Fujitsu middleware.

Setting up the patch management policy allows infrastructure administrators to set which types of patches they want to classify.

This enables tenant users to distinguish which patches should be applied based on their importance when they apply patches.

The infrastructure administrator sets up the following item in the property file during installation. This item can be changed even during operations.

Item	Description
Classification level specification based on the importance level of update files	Specify the classification level based on the importance level that has been set in the update file: The classification levels are as follows: - "Required" (patches that must be applied) - "Recommended" (patches for which application is recommended) Set either "Required" or "Recommended" for each individual importance level for update files. By default, the classification levels are as follows: [Required] - Security - Important [Recommended] - Recommended

2.8.2 Defining the Linux Patch Management Target

RPM packages subject to Linux patch management are not defined during setup. This means that RPM packages subject to Linux patch management must be defined manually.

To define RPM packages subject to Linux patch management or change the definitions, use the following procedure to edit the Linux patch management target configuration file, and then use a command to register the definitions with Systemwalker Software Configuration Manager:

1. Export the existing Linux patch management target configuration file.

   This step is not required when defining RPM packages subject to Linux patch management for the first time.

   [Windows]

   ```
   swcfmg_patch_exportrpmpolicy.exe -f C:\work\linuxpatchpolicy.csv
   ```

   [Linux]

   ```
   swcfmg_patch_exportrpmpolicy -f /tmp/linuxpatchpolicy.csv
   ```

   Refer to the *Reference Guide* for information on the swcfmg_patch_exportrpmpolicy command.

2. Edit the Linux patch management target configuration file.

   Refer to the *Reference Guide* for information on how to edit the Linux patch management target configuration file.

3. Import the Linux patch management target configuration file edited in Step 2 above.

   [Windows]

   ```
   swcfmg_patch_importrpmpolicy.exe -f C:\work\linuxpatchpolicy.csv
   ```

   [Linux]

   ```
   swcfmg_patch_importrpmpolicy -f /tmp/linuxpatchpolicy.csv
   ```

   Refer to the *Reference Guide* for information on the swcfmg_patch_importrpmpolicy command.

Note

To manage Linux patches, RPM packages subject to Linux patch management must be defined. If RPM packages subject to Linux patch management have not been defined, patch information for Linux operating systems will not be displayed in the management console.

2.9 Creating Scripts/Specifying Commands

When performing patch application, patch distribution, parameter setting, script execution, and configuration modification, it is possible to execute the following scripts or commands on business servers.

- Pre-execution/post-execution scripts for patch application, patch distribution, and parameter setting operations
- Script execution scripts
- Script or command execution for configuration modification

Advisory notes for these scripts and commands are shown below.

Advisory notes when creating scripts and specifying commands

- Valid return values for use in scripts and commands

  It is recommended to create the script so that it returns "0" when successfully completed, or another value when an error occurs - Note that values from 159 to 240 cannot be used as return values.

- Script file names

  The file name for a script must be composed of 155 or less characters, using alphanumeric characters, spaces, and the following symbols:
  ~ _ - . ( )
  If a script with a file name exceeding 155 characters is specified, an error may occur when the script is executed.

  In Windows, ".bat" or ".cmd" should be used for the script extensions. Shell scripts created using PowerShell cannot be executed.

- Notes on creating scripts for use across different platforms

  When creating scripts for use across different platforms, the line feed code must be converted to suit the operating system:

  - In Windows, use CR/LF (carriage return followed by line feed).

  - In Linux, use LF (line feed).

- Commands that cannot be used with a script

  Do not execute the following commands from a script or a command. Executing these commands may cause the script to enter standby status on the business server and the script process may not be completed.

  - Commands that require interaction **[Windows/Linux/Solaris]**

  - Commands that require restarting or stopping of the OS **[Windows/Linux/Solaris]**

  - Commands for which a window opens during execution **[Windows]**

  - AT commands **[Windows]**

  - Commands that run in full-screen mode **[Linux/Solaris]**

- User

  Scripts and commands are executed as the following user according to the OS on the business server:

  [Windows] LocalSystem account

  [Linux/Solaris] root

- Single-user mode [Linux/Solaris]

  - When executing scripts or commands in single-user mode, the service called FJSVsglcf is automatically registered. Execute scripts or commands after checking that the FJSVsglcf service is not registered. After execution of scripts or commands, the FJSVsglcf service is automatically deleted.

  - The following files for single-user mode are automatically generated when switching to single-user mode. The original file is backed up with "_FJSVsglcf" appended to the file name, and then the file backed up after executing scripts or commands is restored. For this reason, do not delete the backed up file created when executing scripts or commands while using single-user mode.

    [Linux]

    - For Red Hat Enterprise Linux 5 or Red Hat Enterprise Linux 6

      ```
      /etc/inittab
      ```

    - For Red Hat Enterprise Linux 7

      ```
      /etc/systemd/system/default.target
      ```

  - The OS is restarted when switching to and from single-user mode. Note the following:

    - When executing the post-execution script of patch deployment using single-user mode, as the OS is restarted using the post-execution script, it is not necessary to specify restarting of the OS when requesting the job.

    - When executing scripts or commands for the global zone using single-user mode, non-global zones are stopped or restarted by restarting of the OS of the global zone. [Solaris]

  - The jobs including execution of scripts or commands of the target server with single-user mode are, "Waiting", "Running", or "Selecting (abnormal)". New jobs including execution or commands using single-user mode cannot be requested.

- When scripts or commands executed using single-user mode do not finish within one hour, an error will occur and the job will be aborted. When executing scripts or commands using single-user mode, specify scripts or commands which can be completed within an hour.

Example of log output when an error occurs

One of the following can be specified as the error judgment method of scripts and commands. For script execution and command execution for configuration modification, a return value for normal executions can be specified.

- "0" is considered a normal execution while any other value is considered an error.
- All return values are considered a normal execution.

When a script or a command is considered an error, the job status becomes "Selecting (abnormal)". In the Process details section of the **Job Management** window, the return value, standard output, and standard error of the script and command are displayed. Review the script and command referring to this value.

Corrective action when a timeout occurs

When a script or command process is not completed due to hang-up or other reasons, or when a business server stops during processing, a timeout error occurs when 12 hours have elapsed since the start of the process and the following message is displayed in the **Process details** window. In addition, the job status becomes "Selecting (abnormal)". Review the script and command, and perform retry, continuation, or cancellation of operations.

CFMGP20008 An error has occurred during command execution. [Return value:{0}][Command: The specified script or command][Details: The operation component was successful.]Example of script attachments

The registered script can be downloaded from the Process details section of the **Job Management** window on the management console.

An example is shown below.

Script	script.cmd

2.10 Fujitsu Middleware Patch Application

Fujitsu Middleware patches are only distributed to the target servers. This section explains the method to apply Fujitsu Middleware patches.

Fujitsu middleware patch distribution destination

Fujitsu Middleware patches are distributed using the following path on the target server.

When executing distribution of Fujitsu middleware patches, a directory with a name including the job ID and the date is created in the path as the standard distribution destination.

- Business server

  [Windows]

  %SWCFMGA_DISTRIBUTE%\<*job_ID*>_<*yyyy-MM-dd_HH-mm-ss*>

  The default environment variable is as follows:

  Systemwalker Software Configuration Manager installation directory\SWCFMGB\var\distribute

  [Linux]

  /var/opt/FJSVcfmgb/distribute/<*job_ID*>_<*yyyy-MM-dd_HH-mm-ss*>

- Linkage server

  [Windows]

  %SWCFMGA_DISTRIBUTE%\<*job_ID*>_<*yyyy-MM-dd_HH-mm-ss*>

The default environment variable is as follows:

Systemwalker Software Configuration Manager installation directory\SWCFMGA\var\distribute

[Linux]

```
/var/opt/FJSVcfmga/distribute/<job_ID>_<yyyy-MM-dd_HH-mm-ss>
```

Method to Change the Path for the Standard Distribution Destination

To change the path for the standard distribution destination, edit the values in the following system environment variables or files on the business server:

- Business server

  [Windows]

  The system environment variable "SWCFMGA_DISTRIBUTE" contains the distribution directory - to change it, simply edit the system environment variable.

  [Linux]

  ```
  /etc/opt/FJSVcfmgb/config/distribute.properties
  ```

  The distribution destination directory path is defined in the "distribute_dir" item.

  Example: distribute_dir=/var/opt/FJSVcfmgb/distribute

- Linkage server

  [Windows]

  The system environment variable "SWCFMGA_DISTRIBUTE" contains the distribution directory - to change it, simply edit the system environment variable.

  [Linux]

  ```
  /etc/opt/FJSVcfmga/config/distribute.properties
  ```

  The distribution destination directory path is defined in the "distribute_dir" item in the configuration file.

  Example: distribute_dir=/var/opt/FJSVcfmga/distribute

Method to Apply Fujitsu Middleware Patches

The revision information file (text file) and the update file are distributed to the patch distribution destination. For details on the patch application conditions and the application methods, check the revision information file. Use UpdateAdvisor (middleware) to apply the update files.

Examples of using the UpdateAdvisor (middleware) command are as follow. Apply all patches in the patch distribution destination. For details, refer to "Applying Updates (Using uam add)" in the UpdateAdvisor (middleware) help.

Example:

[Windows]

```
"C:\Program Files (x86)\Fujitsu\UpdateAdvisor\UpdateAdvisorMW\uam" add -s -d <Patch distribution destination>
```

[Linux]

```
/opt/FJSVfupde/bin/uam add -s -d <Patch distribution destination>
```

Deleting the Distribution Destination

The patch distribution destination is not automatically deleted. After patch application, delete the directory with the directory name, "<*job_ID*>_<*yyyy-MM-dd_HH-mm-ss*>" in the distribution destination. If the directory containing the distribution destination is wrongly deleted, an error will occur when Fujitsu middleware patches are distributed. In that case, manually create the directory with the path of the standard distribution destination.

2.10.1 Creating a Fujitsu Middleware Patch Application Script

When distributing Fujitsu middleware patches, after execution register the scripts to apply the patches. This section explains the method to describe the scripts.

Fujitsu middleware patch distribution destination

The distribution destination of Fujitsu middleware patches is configured in the script environment variable, "DISTRIBUTE_PATCH_PATH". Describe the patch application process using this environment variable.

Example of creating a script to apply Fujitsu middleware patches

Execute the UpdateAdvisor (middleware) command to apply Fujitsu middleware patches. An example of creating a script to apply Fujitsu middleware patches is shown below.

Execute the UpdateAdvisor (middleware) command to apply Fujitsu middleware patches. It is recommended to delete the distribution destination directory after patch application.

An example of creating a script to apply Fujitsu middleware patches and delete the distribution destination directory after patch application is shown below.

All patches distributed to directories included in the path specified in the "DISTRIBUTE_PATCH_PATH" environment variable will be applied.

Example:

[Windows]

```
"C:\Program Files (x86)\Fujitsu\UpdateAdvisor\UpdateAdvisorMW\uam" add -s -d %DISTRIBUTE_PATCH_PATH%
rd /s /q %DISTRIBUTE_PATCH_PATH%
```

[Linux]

```
/opt/FJSVfupde/bin/uam add -s -d $DISTRIBUTE_PATCH_PATH
rm -rf $DISTRIBUTE_PATCH_PATH
```

A sample script for applying Fujitsu middleware patches is stored in the directory below.

Extract this script and revise if necessary before using.

Note that the admin server stores scripts for both Windows and Linux, while the business server stores only the scripts that match the operating system.

Storage location

- Admin server

  [Windows]

  ```
  cfmgInstallDir\SWCFMGM\sample
  ```

  [Linux]

  ```
  /opt/FJSVcfmgm/sample
  ```

- Business server

  [Windows]

  ```
  cfmgInstallDir\SWCFMGB\sample
  ```

[Linux]

```
/opt/FJSVcfmgb/sample
```

File name

- Windows: win_mw_patch.bat
- Linux: lin_mw_patch.sh

Notes on creating a Fujitsu middleware patch application script

Notes on creating a Fujitsu middleware patch application script are shown below (for general notes on scripts, refer to "Advisory notes when creating scripts and specifying commands"):

- Checking the conditions and methods for applying Fujitsu middleware patches

  Before creating a script to apply Fujitsu middleware patches, check the application conditions and methods described in the revision information file.

  Note that revisions which cannot be performed by script alone cannot be applied in Systemwalker Software Configuration Manager. In this situation, log on to the managed server and apply the patches manually.

2.11 Parameter Value Settings

To configure values in software parameters, specify values and parameter packages in parameters that have been defined in the parameter settings definition. Note that sets of values to be configured in parameters can also be created as predefined parameters. Use the **Parameter Settings** wizard of the management console to set values for software parameters. Use the predefined parameter management command (swcfmg_param_predef) to create predefined parameters. Refer to the *Operator's Guide* for information on the management console. Refer to the *Reference Guide* for information on commands.

The knowledge required for these steps is explained below:

- Variables that can be specified as values

  It is possible to specify variables as values. Refer to "Variables that can be Specified as Values" under "Definition of Parameter Information" in the *Developer's Guide* for details.

- Package files

  Parameter packages can be specified as parameters. Refer to "Package Files" under "Definition of Parameter Information" in the Developer's Guide for details.

- Predefined parameters

  Sets of values to be configured in the parameters can be defined as predefined parameters using parameter information.

2.11.1 Predefined Parameters

Predefined parameters are parameters in which sets of values have been defined in advance using parameter information.

In the parameter information, specify the keys and values to be configured in the values of the parameters contained in the parameter settings definition. A parameter package can also be specified (a parameter package is a package file containing the parameter settings script file attachment compressed in ZIP format).

Required information

An explanation of details to be specified in the parameter information is shown below.

Tag name	Allowable range	Description	Mandatory	Settings
name	256 characters or less	Specifies parameter information name.	Y	

Tag name		Allowable range	Description	Mandatory	Settings
description		256 characters or less	Specifies the parameter information description.	N	
parameters		0 or more	Specifies multiple parameters that can be configured in the software.	N	
	key	1 to 256 bytes	Specifies the parameter key.	Y	Only the key contained in the parameter settings definition can be specified.
	value	4096 characters or less	Specifies the parameter value.	Y	Values that can be specified are determined by 'type'. The string "__EMPTY__" (prefixed and suffixed by 2 underscores) cannot be specified. Variables can be specified as values by prefixing them with # (to specify # or \ as part of the value, prefix them with the \ escape character). Refer to "Variables that can be Specified as Values" under "Definition of Parameter Information" in the *Developer's Guide* for details.
Parameter package		2 MB or less	Specifies the package file containing the parameter settings script compressed in ZIP format.	Y	For details on parameter settings scripts, refer to "Parameter Settings Scripts" under "Definition of Parameter Information" in the *Developer's Guide*. For details on package files, refer to "Package Files" under "Definition of Parameter Information" in the *Developer's Guide*.

2.12 Editing Email Template Files

This section explains how to edit the following email template files:

- Email template files (for OS patches)
- Email template files (for Fujitsu middleware patches)
- Email template files (for Job Management)

2.12.1 Email Template Files (for OS Patches)

When a new OS patch is released on the repository server (or registered with yum), an email is sent to tenant administrators and tenant users informing them that a new patch has been released, and prompting them to apply it.

Refer to the *Reference Guide* for information on the email template files.

2.12.2 Email Template Files (for Fujitsu Middleware Patches)

When a new patch for Fujitsu middleware is registered with Systemwalker Software Configuration Manager, an email is sent to tenant administrators and tenant users informing them that a new patch has been released, and prompting them to apply it.

Refer to the *Reference Guide* for information on the email template files.

2.12.3 Email Template Files (for Job Management)

If an event occurs during any of the following jobs when executed using a management console wizard, an email notification will be sent to the administrator of that job.

- Patch distribution
- Patch application
- Parameter settings
- Script execution

Email subject	Trigger	Email description
Job request acceptance notification	When the job is requested	Indicates that a job request has been received.
Schedule cancelation notification	After the schedule is canceled	Indicates that the schedule has been canceled, and the job has been terminated.
Server error notification	When server operations are checked and found to be abnormal	Indicates that an error has occurred on the server.
Pre-execution script error notification	When the pre-execution script is executed	Indicates that the pre-script processing has failed.
Processing failure notification	When executing patch distribution, patch application, parameter settings, or script execution	Indicates that patch distribution, patch application, parameter settings, or script execution failed.
Post-execution script error notification	When the post-execution script is executed	Indicates that the post-script processing has failed.
Restart failure notification	When the restart process fails	Indicates that restart has failed.
Job completion notification	When the job is complete	Indicates that the job is complete.
Processing cancelation notification	When **Cancel** is selected or a timeout occurs	Indicates that either the job has been canceled or a timeout has occurred.
Script execution	When executing a script	Means that the script execution process has failed during configuration modification.
Command execution	When executing a command	Means that the command execution process has failed during configuration modification.
File distribution	When distributing files	Means that the file distribution process has failed during configuration modification.
File collection	File collection	Means that the file collection process has failed during configuration modification.

The notification details for each job are shown below:

Email subject	Patch distribution	Patch application	Parameter settings	Script execution	Configuration Modification
Job request acceptance notification	Y	Y	Y	Y	Y
Schedule cancelation notification	Y	Y	Y	Y	Y

Email subject	Patch distribution	Patch application	Parameter settings	Script execution	Configuration Modification
Server error notification	Y	Y	Y	Y	Y
Pre-execution script error notification	Y	Y	Y	N	N
Processing failure notification	Y	Y	Y	Y	N
Post-execution script error notification	Y	Y	Y	N	N
Restart failure notification	Y	Y	Y	Y	Y
Job completion notification	Y	Y	Y	Y	Y
Job cancelation notification	Y	Y	Y	Y	Y
Script execution	N	N	N	N	Y
Command execution	N	N	N	N	Y
File distribution	N	N	N	N	Y
File collection	N	N	N	N	Y

Y: Email notification is sent

N: Email notification is not sent

Refer to the *Reference Guide* for details on the email template files.

2.13 Notification Settings in the Management Console

When a user logs in to the management console, the **Home** window is displayed. Notifications (such as maintenance information) can be sent from the system to tenant administrators and tenant users.

How to edit notifications

This section explains how to edit the notifications that are displayed in the bottom part of the **Home** window.

Edit notifications by editing the following text file. Data that has been changed is applied immediately.

[Windows]

```
<Systemwalker Software Configuration Manager installation directory>\SWCFMGM\config\information_mes.txt
```

[Linux]

```
/etc/opt/FJSVcfmgm/config/information_mes.txt
```

Note

If the text file does not exist, no notifications will be displayed.

Settings

Enter each message on separate lines using the following format:

```
date,message
```

- There is no set format for the date.

- Use UTF-8 as the character encoding for the text file.
- The text file contains "YYYY-MM-DD,XXXX" as the default value. If necessary, edit this default value.

Settings example

```
2013-07-15, There will be maintenance for related networks over the weekend.
2013-07-10, A new patch has been released.
2013-07-02, An urgent security patch has been released.
```

Chapter 3 Starting and Stopping Systemwalker Software Configuration Manager

This chapter explains how to start and stop the Systemwalker Software Configuration Manager admin server.

3.1 Starting Systemwalker Software Configuration Manager

This section explains how to start Systemwalker Software Configuration Manager.

1. Ensure that ServerView Resource Orchestrator is running if you want to use it to manage servers deployed by the tool.

   Refer to the ServerView Resource Orchestrator manuals for more information.

2. Execute the following command on the admin server:

   [Windows]

   Select **Run as administrator** to execute the command:

   ```
   <Systemwalker Software Configuration Manager installation directory>\SWCFMGM\bin\swcfmg_start
   ```

   [Linux]

   Execute the command as a superuser:

   ```
   /opt/FJSVcfmgm/bin/swcfmg_start
   ```

3. If Systemwalker Software Configuration Manager starts successfully, the following message will be output:

   ```
   Startup processing for Systemwalker Software Configuration Manager will start.
   The startup processing for Systemwalker Software Configuration Manager has completed normally.
   ```

See

Refer to the *Reference Guide* for information on this command.

Information

As the Systemwalker Software Configuration Manager agent installed on the business server or the linkage server is automatically started, startup and stop operations are not provided.

When it is necessary to stop or start the Systemwalker Software Configuration Manage agent installed on the business server or the linkage server for some reason, perform the following operation:

Starting Systemwalker Software Configuration Manager

[Windows]

Start the "Systemwalker File Transfer Library Control(SWCFMG)" service.

[Linux]

Execute the following command:

```
service FJSVlnkcf start
```

[Solaris]

Execute the following command:

```
/etc/init.d/FJSVlnkcf start
```

3.2 Stopping Systemwalker Software Configuration Manager

This section explains how to stop Systemwalker Software Configuration Manager.

1. Execute the following command on the admin server:

   [Windows]

   Select **Run as administrator** to execute the command:

   ```
   <Systemwalker Software Configuration Manager installation directory>\SWCFMGM\bin\swcfmg_stop
   ```

   [Linux]

   Execute the command as a superuser:

   ```
   /opt/FJSVcfmgm/bin/swcfmg_stop
   ```

2. If Systemwalker Software Configuration Manager stops successfully, the following message will be output:

   ```
   Stop processing for Systemwalker Software Configuration Manager will start.
   The stop processing for Systemwalker Software Configuration Manager has completed normally.
   ```

See

Refer to the *Reference Guide* for information on this command.

Information

As the Systemwalker Software Configuration Manager agent installed on the business server or the linkage server is automatically started, startup and stop operations are not provided.

When stopping the Systemwalker Software Configuration Manager agent installed on the business server or the linkage server for some reason, perform the following operation:

Stopping Systemwalker Software Configuration Manager

[Windows]

Stop the "Systemwalker File Transfer Library Control(SWCFMG)" service.

[Linux]

Execute the following command:

```
service FJSVlnkcf stop
```

[Solaris]

Execute the following command:

```
/etc/init.d/FJSVlnkcf stop
```

3.3 Checking the Status of Systemwalker Software Configuration Manager

Use the status display command to check the setup status and startup status of Systemwalker Software Configuration Manager. The following statuses can be checked:

- Systemwalker Software Configuration Manager has not been set up.
- Systemwalker Software Configuration Manager is running.
- Systemwalker Software Configuration Manager is not running.

Use the following procedure to check the status of Systemwalker Software Configuration Manager:

1. Execute the following command on the admin server:

   [Windows]

   Select **Run as administrator** to execute the command:

   ```
   <Systemwalker Software Configuration Manager installation directory>\SWCFMGM\bin\swcfmg_status
   ```

   [Linux]

   Execute the command as a superuser:

   ```
   /opt/FJSVcfmgm/bin/swcfmg_status
   ```

2. The following messages are output according to the status of Systemwalker Software Configuration Manager:

   - If Systemwalker Software Configuration Manager has not been set up:

     ```
     Systemwalker Software Configuration Manager has not been set up.
     ```

   - If Systemwalker Software Configuration Manager is running:

     ```
     Systemwalker Software Configuration Manager is running.
     ```

   - If Systemwalker Software Configuration Manager is not running:

     ```
     Systemwalker Software Configuration Manager is not running.
     ```

See

Refer to the *Reference Guide* for information on this command.

Chapter 4 Maintenance

This chapter explains topics relating to maintenance, such as the logs that are output when Systemwalker Software Configuration Manager is used, and how to back up and restore the admin server.

4.1 Log Output

This section explains the logs output by Systemwalker Software Configuration Manager.

4.1.1 Logs Output on the Admin Server

The types of logs that are output on the admin server are shown in the tables below.

Audit logs

Log name	Description	Size	Number of generations
cfmg_audit_log	Audit log.	10 MB	10 generations (*1)

*1: If this number is exceeded, previous generations will be deleted, starting with the oldest.

Investigation logs

Log name	Description	Size	Number of generations
managerview_trace_log	Trace log for the management console.	10 MB	10 generations (*1)
cfmgcommand_trace_log	Trace log for commands. -		
cfmgcommand_discovery_trace_log	Trace log with the following: - Information that is output when all information is collected using the patch information update command - Information that is output when parameter information is collected using the parameter information update command.		
cfmgcommand_discovery_wsus_trace_log	Trace log with the following: - Information that is output when only WSUS information is collected using the patch information update command		
cfmgcommand_discovery_yum_trace_log	Trace log with the following: - Information that is output when only yum information is collected using the patch information update command		
cfmgcommand_discovery_sol_trace_log	A trace log with the following is output: - Information that is output when only Solaris information is collected using the patch information update command.		
cfmgcommand_discovery_fjmw_trace_log	Trace log with the following:		

Log name	Description	Size	Number of generations
	- Information that is output when only Fujitsu middleware information is collected using the patch information update command		
mdr_cfmg_srv.log	A trace log with the following is output: - Information that is output when hardware/virtual environment information is collected using cmdbrefresh (Observed Record Collection Request Command).		
Event log (Windows)	Contains information such as information about errors that occurs while patch application status information for deployed servers is being collected.	-	-
Syslog (Linux)	Contains information such as information about errors that occurred while patch application status information for deployed servers was being collected.	-	-

*1: If this number is exceeded, previous generations will be deleted, starting with the oldest.

4.1.1.1 Log Output Destination

The output destination for mdr_cfmg_srv.log is shown below.

[Windows]

Output folder	Output file
<Systemwalker Software Configuration Manager installation directory>\CMDB\FJSVcmdbm\var\log	Same as the log name.

[Linux]

Output folder	Output file
/opt/FJSVcfmgm/CMDB/FJSVcmdbm/var/log	Same as the log name.

The output destination for other logs is shown below.

[Windows]

Output folder	Output file
<Systemwalker Software Configuration Manager installation directory> \SWCFMGM\logs	Same as the log name.

[Linux]

Output folder	Output file
/var/opt/FJSVcfmgm/logs	Same as the log name.

4.1.1.2 Output Format for Audit Logs

The output format for audit logs is as shown below. It is possible to change the output destination for audit logs, the file size, and the number of generations held.

Output format for audit logs

Output format
<Operation date/time>,*<User ID>*,*<Tenant name>*,*<Operation type>*,*<Parameters>*,*<Operation result>*

Item	Description
Operation date/time	YYYY-MM-DD HH:MM:SS.sss (local time)
User ID	The user ID of the user that executed the operation
Tenant name	The tenant name of the user that executed the operation Note: For operations performed by infrastructure administrators, "admin" is output.
Operation type	A string indicating the content of the operation
Parameters	The parameters specified by the request
Operation result	"SUCCESS" if the operation was successful and "FAILURE" if the operation failed

Operation type

Operation type	Description
/managerview/login.json	Performs login
/managerview/logout.json	Performs logout
/managerview/userInfo.json	Acquires user information
/managerview/org/list.json	Acquires a list of tenants
/managerview/ls/list.json	Acquires a list of servers
/managerview/ls/map.json	Acquires the map of unapplied patches
/managerview/ls/copy.json	Copies a list of servers
/managerview/ls.json	Acquires server details
/managerview/info/list.json	Acquires notifications
/managerview/windows.csv	Outputs Windows patch information to a CSV file
/managerview/patch/windows/list.json	Acquires a list of Windows patches
/managerview/patch/windows/map.json	Acquires the map of servers with unapplied Windows patches
/managerview/windows.json	Acquires Windows patch details
/managerview/patch/copy.json	Copies a list of Windows patches
/managerview/patch/linux.csv	Outputs Linux patch information to a CSV file
/managerview/patch/linux/list.json	Acquires a list of Linux patches
/managerview/patch/linux/map.json	Acquires the map of servers with unapplied Linux patches
/managerview/patch/linux.json	Acquires Linux patch details
/managerview/wsus.json	Refreshes
/managerview/patchType/list.json	Acquires a list of patch types
/managerview/patchSummary/list.json	Acquires a summary of patches
/managerview/midPatch.csv	Outputs Fujitsu middleware patch information to CSV file
/managerview/midPatch/list.json	Acquires a list of Fujitsu middleware patches
/managerview/midPatch/map.json	Acquires the map of servers with unapplied Fujitsu middleware patches
/managerview/midPatch.json	Acquires details on Fujitsu middleware patches
/managerview/baseLine/list.json	Acquires a list of configuration baselines

Operation type	Description
/managerview/baseLine/patchComp.json	Compares Windows patches
/managerview/baseLine/linux/patchComp.json	Compares Linux patches
/managerview/baseLine/midPatchComp.json	Compares Fujitsu middleware patches
/managerview/software/list.json	Acquires a list of software programs
/managerview/software.json	Acquires software details
/managerview/appliedPatch.csv	Outputs patch application information to a CSV file
/managerview/appliedPatch.do	Applies patches
/managerview/software/map.json	Acquires the map of servers for which software parameters can be configured
/managerview/lsParameter.json	Acquires parameter information
/managerview/lsParameter.csv	Outputs parameter information to CSV file
/managerview/parameterSettingDefinition.json	Acquires the parameter settings definition
/managerview/parameterDesignDefinition.json	Acquires parameter settings information
/managerview/parameterDefinition/list.json	Acquires a list of parameter settings information
/managerview/execParameter.csv	Outputs parameter settings information to CSV file
/managerview/execScript.csv	Outputs script execution information to CSV file

Procedure for changing the audit log output destination

Use the following procedure to change the audit log output destination:

1. Rewrite the configuration file.

   The following table shows the configuration file and the location to change:

   [Windows]

Log name	Configuration file	Location to change (one location)
cfmg_audit_log	<Systemwalker Software Configuration Manager installation directory>\SWCFMGM\config \manager_base_log4j.xml	The <param name="File" value="<*Systemwalker Software Configuration Manager installation directory*>/SWCFMGM/logs/cfmg_audit_log" /> element under the <appender name="cfmgaudit" class="org.apache.log4j.RollingFileAppender"> element

   [Linux]

Log name	Configuration file	Location to change (one location)
cfmg_audit_log	/etc/opt/FJSVcfmgm/config/ manager_base_log4j.xml	The <param name="File" value="/var/opt/ FJSVcfmgm/logs/cfmg_audit_log"/> element under the <appender name="cfmgaudit" class="org.apache.log4j.RollingFileAppender"> element

2. Restart Systemwalker Software Configuration Manager.

Procedure for changing the size of the audit log file

Use the following procedure to change the size of the audit log file:

1. Rewrite the configuration file.

   The location to change is shown below.

[Windows]

Log name	Configuration file	Location to change (one location)
cfmg_audit_log	<Systemwalker Software Configuration Manager Installation directory>\SWCFMGM\config\manager_base_log4j.xml	Change the underlined part of the <param name="MaxFileSize" value="*10MB*" /> element under the <appender name="cfmgaudit" class="org.apache.log4j.RollingFileAppender"> element to a desired value. Example: value="100MB" (to change the size of the audit log file to 100 MB)

[Linux]

Log name	Configuration file	Location to change (one location)
cfmg_audit_log	/etc/opt/FJSVcfmgm/config/manager_base_log4j.xml	Change the underlined part of the <param name="MaxFileSize" value="10MB" /> element under the <appender name="cfmgaudit"class="org.apache.log4j.RollingFileAppender"> element to a desired value. Example: value="100MB" (to change the size of the audit log file to 100 MB)

2. Restart Systemwalker Software Configuration Manager.

Procedure for changing the number of audit log generations to be held

Use the following procedure to change the number of generations to be held for each audit log.

1. Rewrite the configuration file.

   The location to change is shown below.

   [Windows]

Log name	Configuration file	Location to change (one location)
cfmg_audit_log	<*Systemwalker Software Configuration Manager Installation directory*>\SWCFMGM\config\manager_base_log4j.xml	Change the underlined part of the <param name="MaxBackupIndex" value="*9*" /> element under the <appender name="cfmgaudit" class="org.apache.log4j.RollingFileAppender"> element to a desired value. Example: value="100" (to change the number of generations to 100)

[Linux]

Log name	Configuration file	Location to change (one location)
cfmg_audit_log	/etc/opt/FJSVcfmgm/config/manager_base_log4j.xml	Change the underlined part of the <param name="MaxBackupIndex" value="9" /> element under the <appender name="cfmgaudit"class="org.apache.log4j.RollingFileAppender"> element to a desired value. Example: value="100" (to change the number of generations to 100)

2. Restart Systemwalker Software Configuration Manager.

4.1.1.3 Investigation Logs

The output format for investigation logs is as below. The output destination for investigation logs can be changed.

Output format for investigation logs

Output format
<*Date/time*> <*Log level*> <*Message ID*> <*Message text*>

Item	Description	
Date/time	YYYY-MM-DD HH:MM:SS.sss (local time)	
Log level	One of the following:	
	info	Information message
	warn	Warning message
	error	Error message
	fatal	Fatal message
Message ID	The prefix and message number - The prefix for managerview_trace_log is " CFMGV ". - The prefix for cfmgcommand_trace_log is "CFMGC" - The prefix for cfmgcommand_discovery_trace_log, cfmgcommand_discovery_wsus_trace_log, cfmgcommand_discovery_yum_trace_log, cfmgcommand_discovery_sol_trace_log, and cfmgcommand_discovery_fjmw_trace_log is "CFMGD"	
Message text	Body text of the message	

Procedure for changing the investigation log output destination

Use the following procedure to change the investigation log output destination:

1. Rewrite the configuration files corresponding to each log.

   The following table shows the configuration files and the locations to change:

   [Windows]

Log name	Configuration file	Location to change (one location)
managerview_trace_log	<*Systemwalker Software Configuration Manager installation directory*>\SWCFMGM\config\manager_base_log4j.xml	The <param name="File" value="<*Systemwalker Software Configuration Manager installation directory*>/SWCFMGM/logs/managerview_trace_log" /> element under the <appender name="managerviewtrace" class="org.apache.log4j.RollingFileAppender"> element
cfmgcommand_trace_log	<*Systemwalker Software Configuration Manager installation directory*>\SWCFMGM\config\manager_log4j.xml	<param name="File" value="<*Systemwalker Software Configuration Manager installation directory*>/SWCFMGM/logs/cfmgcommand_trace_log" /> under the element <appender name="cfmgcommandtrace" class="org.apache.log4j.RollingFileAppender">
cfmgcommand_discovery_trace_log	<*Systemwalker Software Configuration Manager installation directory*>\SWCFMGM\config\manager_discovery_log4j.xml	The <param name="File" value="<*Systemwalker Software Configuration Manager installation directory*>/SWCFMGM/logs/cfmgcommand_discovery_trace_log" /> element under the <appender name="cfmgbasetrace"class="org.apache.log4j.RollingFileAppender"> element

Log name	Configuration file	Location to change (one location)
cfmgcommand_discovery_wsus_trace_log	*<Systemwalker Software Configuration Manager installation directory>*\SWCFMGM\config\manager_discovery_wsus_log4j.xml	The <param name="File" value="<*Systemwalker Software Configuration Manager installation directory*>/SWCFMGM/logs/cfmgcommand_discovery_wsus_trace_log" /> element under the <appender name="cfmgdiscoverytrace" class="org.apache.log4j.RollingFileAppender"> element
cfmgcommand_discovery_yum_trace_log	*<Systemwalker Software Configuration Manager installation directory>*\SWCFMGM\config\manager_discovery_yum_log4j.xml	The <param name="File" value="<*Systemwalker Software Configuration Manager installation directory*>/SWCFMGM/logs/cfmgcommand_discovery_yum_trace_log" /> element under the <appender name="cfmgdiscoverytrace" class="org.apache.log4j.RollingFileAppender"> element
cfmgcommand_discovery_sol_trace_log	*<Systemwalker Software Configuration Manager installation directory>*\SWCFMGM\config\manager_discovery_sol_log4j.xml	<param name="File" value="<Systemwalker Software Configuration Manager installation directory>/SWCFMGM/logs/cfmgcommand_discovery_sol_trace_log" /> under the element <appender name="cfmgdiscoverytrace" class="org.apache.log4j.RollingFileAppender">
cfmgcommand_discovery_fjmw_trace_log	*<Systemwalker Software Configuration Manager installation directory>*\SWCFMGM\config\manager_discovery_fjmw_log4j.xml	The <param name="File" value="<*Systemwalker Software Configuration Manager installation directory*>/SWCFMGM/logs/cfmgcommand_discovery_fjmw_trace_log" /> element under the <appender name="cfmgdiscoverytrace" class="org.apache.log4j.RollingFileAppender"> element

[Linux]

Log name	Configuration file	Location to change (one location)
managerview_trace_log	/etc/opt/FJSVcfmgm/config/manager_base_log4j.xml	The <param name="File" value="/var/opt/FJSVcfmgm/logs/managerview_trace_log" /> element under the <appender name="managerviewtrace" class="org.apache.log4j.RollingFileAppender"> element
cfmgcommand_trace_log	/etc/opt/FJSVcfmgm/config/manager_log4j.xml	The <param name="File"value="/var/opt/FJSVcfmgm/logs/cfmgcommand_trace_log" /> element under the <appender name="cfmgcommandtrace"class="org.apache.log4j.RollingFileAppender"> element
cfmgcommand_discovery__trace_log	/etc/opt/FJSVcfmgm/config/manager_discovery_log4j.xml	The <param name="File"value="/var/opt/FJSVcfmgm/logs/cfmgcommand_discovery_trace_log" /> element under the <appender name="cfmgdiscoverytrace"class="org.apache.log4j.RollingFileAppender"> element
cfmgcommand_discovery_wsus_trace_log	/etc/opt/FJSVcfmgm/config/manager_discovery_wsus_log4j.xml	The <param name="File"value="/var/opt/FJSVcfmgm/logs/cfmgcommand_discovery_wsus_trace_log" /> element under the <appender name="cfmgdiscoverytrace"class="org.apache.log4j.RollingFileAppender"> element
cfmgcommand_discovery_yum_trace_log	/etc/opt/FJSVcfmgm/config/manager_discovery_yum_log4j.xml	The <param name="File"value="/var/opt/FJSVcfmgm/logs/cfmgcommand_discovery_yum_trace_log" /> element under the <appender name="cfmgdiscoverytrace"class="org.apache.log4j.RollingFileAppender"> element

Log name	Configuration file	Location to change (one location)
cfmgcommand_discovery_sol_trace_log	/etc/opt/FJSVcfmgm/config/manager_discovery_sol_log4j.xm	<param name="File" value="/var/opt/FJSVcfmgm/logs/cfmgcommand_discovery_sol_trace_log" /> under the element <appender name="cfmgdiscoverytrace" class="org.apache.log4j.RollingFileAppender">
cfmgcommand_discovery_fjmw_trace_log	/etc/opt/FJSVcfmgm/config/manager_discovery_fjmw_log4j.xml	The <param name="File"value="/var/opt/FJSVcfmgm/logs/cfmgcommand_discovery_fjmw_trace_log" /> element under the <appender name="cfmgdiscoverytrace"class="org.apache.log4j.RollingFileAppender"> element

2. Restart Systemwalker Software Configuration Manager.

Procedure for changing the size of the investigation log file

Use the following procedure to change the size of the investigation log file:

1. Rewrite the configuration file.

   The location to change is shown below.

Log Name	Configuration File	Location to Change (One location)
managerview_trace_log	<*Systemwalker Software Configuration Manager installation directory*>\SWCFMGM\config\manager_base_log4j.xml	<param name="MaxFileSize" value="10MB" /> under the element <appender name="managerviewtrace" class="org.apache.log4j.RollingFileAppender"> <=Delete=> Example: value="100MB" (to change the size of the audit log file to 100 MB)
cfmgcommand_trace_log	<*Systemwalker Software Configuration Manager installation directory*>\SWCFMGM\config\manager_log4j.xml	<param name="MaxFileSize" value="10MB" /> under the element <appender name="cfmgcommandtrace" class="org.apache.log4j.RollingFileAppender"> <=Delete=> Example: value="100MB" (to change the size of the audit log file to 100 MB)
cfmgcommand_discovery_trace_log	<*Systemwalker Software Configuration Manager installation directory*>\SWCFMGM\config\manager_discovery_log4j.xml	<param name="MaxFileSize" value="10MB" /> under the element <appender name="cfmgdiscoverytrace" class="org.apache.log4j.RollingFileAppender"> <=Delete=> Example: value="100MB" (to change the size of the audit log file to 100 MB)
cfmgcommand_discovery_wsus_trace_log	<*Systemwalker Software Configuration Manager installation directory*>\SWCFMGM\config\manager_discovery_wsus_log4j.xml	<param name="MaxFileSize" value="10MB" /> under the element <appender name="cfmgdiscoverytrace" class="org.apache.log4j.RollingFileAppender"> <=Delete=> Example: value="100MB" (to change the size of the audit log file to 100 MB)
cfmgcommand_discovery_yum_trace_log	<*Systemwalker Software Configuration Manager installation directory*>\SWCFMGM\config\manager_discovery_yum_log4j.xml	<param name="MaxFileSize" value="10MB" /> under the element <appender name="cfmgdiscoverytrace" class="org.apache.log4j.RollingFileAppender"> <=Delete=>

Log Name	Configuration File	Location to Change (One location)
		Example: value="100MB" (to change the size of the audit log file to 100 MB)
cfmgcommand_discovery_sol_trace_log	<*Systemwalker Software Configuration Manager installation directory*>\SWCFMGM\config\manager_discovery_sol_log4j.xml	<param name="MaxFileSize" value="10MB" /> under the element <appender name="cfmgdiscoverytrace" class="org.apache.log4j.RollingFileAppender"> <=Delete=> Example: value="100MB" (to change the size of the audit log file to 100 MB)
cfmgcommand_discovery_fjmw_trace_log	<*Systemwalker Software Configuration Manager installation directory*>\SWCFMGM\config\manager_discovery_fjmw_log4j.xml	<param name="MaxFileSize" value="10MB" /> under the element <appender name="cfmgdiscoverytrace" class="org.apache.log4j.RollingFileAppender"> <=Delete=> Example: value="100MB" (to change the size of the audit log file to 100 MB)

[Linux]

Log Name	Configuration File	Location to Change (One location)
managerview_trace_log	/etc/opt/FJSVcfmgm/config/manager _base_log4j.xml	<param name="MaxFileSize" value="10MB" /> under the element <appender name="managerviewtrace" class="org.apache.log4j.RollingFileAppender"> <=Delete=> Example: value="100MB" (to change the size of the audit log file to 100 MB)
cfmgcommand_trace_log	/etc/opt/FJSVcfmgm/config/manager_log4j.xml	<param name="MaxFileSize" value="10MB" /> under the element <appender name="cfmgcommandtrace" class="org.apache.log4j.RollingFileAppender"> <=Delete=> Example: value="100MB" (to change the size of the audit log file to 100 MB)
cfmgcommand_discovery__trace_log	/etc/opt/FJSVcfmgm/config/manager_discovery_log4j.xml	<param name="MaxFileSize" value="10MB" /> under the element <appender name="cfmgdiscoverytrace" class="org.apache.log4j.RollingFileAppender"> <=Delete=> Example: value="100MB" (to change the size of the audit log file to 100 MB)
cfmgcommand_discovery_wsus_trace_log	/etc/opt/FJSVcfmgm/config/manager_discovery_wsus_log4j.xml	<param name="MaxFileSize" value="10MB" /> under the element <appender name="cfmgdiscoverytrace" class="org.apache.log4j.RollingFileAppender"> <=Delete=> Example: value="100MB" (to change the size of the audit log file to 100 MB)
cfmgcommand_discovery_yum_trace_log	/etc/opt/FJSVcfmgm/config/manager_discovery_yum_log4j.xml	<param name="MaxFileSize" value="10MB" /> under the element <appender name="cfmgdiscoverytrace" class="org.apache.log4j.RollingFileAppender"> <=Delete=>

Log Name	Configuration File	Location to Change (One location)
		Example: value="100MB" (to change the size of the audit log file to 100 MB)
cfmgcommand_discovery_sol_trace_log	/etc/opt/FJSVcfmgm/config/manager_discovery_sol_log4j.xm	<param name="MaxFileSize" value="10MB" /> under the element <appender name="cfmgdiscoverytrace" class="org.apache.log4j.RollingFileAppender"> <=Delete=> Example: value="100MB" (to change the size of the audit log file to 100 MB)
cfmgcommand_discovery_fjmw_trace_log	/etc/opt/FJSVcfmgm/config/manager_discovery_fjmw_log4j.xml	<param name="MaxFileSize" value="10MB" /> under the element <appender name="cfmgdiscoverytrace" class="org.apache.log4j.RollingFileAppender"> <=Delete=> Example: value="100MB" (to change the size of the audit log file to 100 MB)

2. Restart Systemwalker Software Configuration Manager.

Procedure for changing the number of investigation log generations to be held

Use the following procedure to change the number of generations to be held for each investigation log.

1. Rewrite the configuration file.

   The location to change is shown below.

Log Name	Configuration file	Location to change (one location)
managerview_trace_log	<*Systemwalker Software Configuration Manager installation directory*>\SWCFMGM\config\manager_base_log4j.xml	<param name="MaxBackupIndex" value="9" /> under the element <appender name="managerviewtrace" class="org.apache.log4j.RollingFileAppender"> <=Delete=> Example: value="100" (to change the number of generations to 100)
cfmgcommand_trace_log	<*Systemwalker Software Configuration Manager installation directory*>\SWCFMGM\config\manager_log4j.xml	<param name="MaxBackupIndex" value="9" /> under the element <appender name="cfmgcommandtrace" class="org.apache.log4j.RollingFileAppender"> <=Delete=> Example: value="100" (to change the number of generations to 100)
cfmgcommand_discovery_trace_log	<*Systemwalker Software Configuration Manager installation directory*>\SWCFMGM\config\manager_discovery_log4j.xml	<param name="MaxBackupIndex" value="9" /> under the element <appender name="cfmgdiscoverytrace" class="org.apache.log4j.RollingFileAppender"> <=Delete=> Example: value="100" (to change the number of generations to 100)
cfmgcommand_discovery_wsus_trace_log	<*Systemwalker Software Configuration Manager installation directory*>\SWCFMGM\config\manager_discovery_wsus_log4j.xml	<param name="MaxBackupIndex" value="9" /> under the element <appender name="cfmgdiscoverytrace" class="org.apache.log4j.RollingFileAppender"> <=Delete=> Example: value="100" (to change the number of generations to 100)

Log Name	Configuration file	Location to change (one location)
cfmgcommand_discovery_yum_trace_log	<*Systemwalker Software Configuration Manager installation directory*>\SWCFMGM\config\manager_discovery_yum_log4j.xml	<param name="MaxBackupIndex" value="9" /> under the element <appender name="cfmgdiscoverytrace" class="org.apache.log4j.RollingFileAppender"> <=Delete=> Example: value="100" (to change the number of generations to 100)
cfmgcommand_discovery_sol_trace_log	<*Systemwalker Software Configuration Manager installation directory*>\SWCFMGM\config\manager_discovery_sol_log4j.xml	<param name="MaxBackupIndex" value="9" /> under the element <appender name="cfmgdiscoverytrace" class="org.apache.log4j.RollingFileAppender"> <=Delete=> Example: value="100" (to change the number of generations to 100)
cfmgcommand_discovery_fjmw_trace_log	<*Systemwalker Software Configuration Manager installation directory*>\SWCFMGM\config\manager_discovery_fjmw_log4j.xml	<param name="MaxBackupIndex" value="9" /> under the element <appender name="cfmgdiscoverytrace" class="org.apache.log4j.RollingFileAppender"> <=Delete=> Example: value="100" (to change the number of generations to 100)

[Linux]

Log Name	Configuration File	Location to Change (One location)
managerview_trace_log	/etc/opt/FJSVcfmgm/config/manager _base_log4j.xml	<param name="MaxBackupIndex" value="9" /> under the element <appender name="managerviewtrace" class="org.apache.log4j.RollingFileAppender"> <=Delete=> Example: value="100" (to change the number of generations to 100)
cfmgcommand_trace_log	/etc/opt/FJSVcfmgm/config/manager_log4j.xml	<param name="MaxBackupIndex" value="9" /> under the element <appender name="cfmgcommandtrace" class="org.apache.log4j.RollingFileAppender"> <=Delete=> Example: value="100" (to change the number of generations to 100)
cfmgcommand_discovery__trace_log	/etc/opt/FJSVcfmgm/config/manager_discovery_log4j.xml	<param name="MaxBackupIndex" value="9" /> under the element <appender name="cfmgdiscoverytrace" class="org.apache.log4j.RollingFileAppender"> <=Delete=> Example: value="100" (to change the number of generations to 100)
cfmgcommand_discovery_wsus_trace_log	/etc/opt/FJSVcfmgm/config/manager_discovery_wsus_log4j.xml	<param name="MaxBackupIndex" value="9" /> under the element <appender name="cfmgdiscoverytrace" class="org.apache.log4j.RollingFileAppender"> <=Delete=> Example: value="100" (to change the number of generations to 100)

Log Name	Configuration File	Location to Change (One location)
cfmgcommand_discovery_yum_trace_log	/etc/opt/FJSVcfmgm/config/manager_discovery_yum_log4j.xml	<param name="MaxBackupIndex" value="9" /> under the element <appender name="cfmgdiscoverytrace" class="org.apache.log4j.RollingFileAppender"> <=Delete=> Example: value="100" (to change the number of generations to 100)
cfmgcommand_discovery_sol_trace_log	/etc/opt/FJSVcfmgm/config/manager_discovery_sol_log4j.xm	<param name="MaxBackupIndex" value="9" /> under the element <appender name="cfmgdiscoverytrace" class="org.apache.log4j.RollingFileAppender"> <=Delete=> Example: value="100" (to change the number of generations to 100)
cfmgcommand_discovery_fjmw_trace_log	/etc/opt/FJSVcfmgm/config/manager_discovery_fjmw_log4j.xml	<param name="MaxBackupIndex" value="9" /> under the element <appender name="cfmgdiscoverytrace" class="org.apache.log4j.RollingFileAppender"> <=Delete=> Example: value="100" (to change the number of generations to 100)

2. Restart Systemwalker Software Configuration Manager.

4.1.1.4 Event Logs or syslogs

Output format for event logs [Windows]

Source	Description
Systemwalker Software Configuration Manager	Message ID and message content

Output format for syslogs [Linux]

Date/time	Host name	Package name	Description
Jun 11 01:01:01	Server	FJSVcfmgm	Message ID and message content

4.1.2 Logs Output on the Business Server

The types of logs that are output on the business server are shown in the table below.

Audit logs

Log name	Description	Size	Number of generations
swcfmga_param_setting_log	Contains the information generated when parameters are set.	10 MB	10 generations (*1)
swcfmga_param_collecting_log	Contains the information generated when the parameter information is collected.		

*1: If this number is exceeded, previous generations will be deleted, starting with the oldest.

4.1.2.1 Log Output Destination

The output destination for logs is shown below.

[Windows]

Output folder	Output file
<*Systemwalker Software Configuration Manager agent installation directory*>\SWCFMGB\logs	Same as the log name.

[Linux]

Output folder	Output file
/var/opt/FJSVcfmgb/logs	Same as the log name.

4.1.3 Audit Logs for CMDB

When operations are performed on the CMDB via agents, commands, or the **Maintenance** window (displayed from the **Configuration management** window on the management console), the content of the operation is output as an audit log.

Audit logs are output to the following file:

[Windows]

```
<Systemwalker Software Configuration Manager installation directory>\CMDB\FJSVcmdbm\var\log\audit\audit.log
```

[Linux]

```
/opt/FJSVcfmgm/CMDB/FJSVcmdbm/var/log/audit/audit.log
```

- Up to 10 generations of audit log files are kept, named "audit.log", "audit.log.1", "audit.log.2", and so on up to "audit.log.9". Each audit log is 5 MB. Once the maximum number of generations is exceeded, the oldest file (audit.log.9) is deleted.

Output format for audit logs

```
<Date/time>,<Operation location>,<Execution host>,<Operator>,<Operation type>,<Operation
target>,<Operation content>,<Execution result>,<Component>,<Additional information>,<Reserved area>
```

- *<Date/time>*: This item indicates the date and time in "date time time-difference" format.
- *<Operation location>*: This item indicates the IP address of the machine where the operation was performed
- *<Execution host>*: This item indicates the host name of the machine where the operation was performed (The machine hosting the CMDB manager).
- *<Operator>*: This item indicates information on the agent or command that performed the operation.
    - If the operation was performed by an agent, this item indicates the agent ID. However, if it is the first operation and the agent ID has not yet been set up, this item indicates the agent type name.
    - If the operation was performed by a command, this item indicates the OS user name for the user that executed the command.
- *<Operation type>*: This item indicates the operation name.
- *<Operation target>*: This item indicates the target and result of the operation in "name=value;" format.
- *<Operation content>*: This item indicates the content of the operation. If the execution result is operation failure, this item indicates error details.
- *<Execution result>*: This item indicates one of the following values:
    - S: Success
    - F: Failure
- *<Component>*: This item indicates "FSERV".
- *<Additional information>*: This item indicates any additional information for the operation in "name=value;" format.

- *<Reserved area>*: This item is not used. No value is set for this item.

Output example

```
"2012/05/10 15:29:37.009
+0900","192.168.1.10","Server1","mdr000000000005","addEntities","id=gid000000000086;
type=LogicalServer; record=observed; version=1;","updateEntity","S","FSERV","",""

"2012/05/10 15:44:21.878
+0900","192.168.1.10","Server1","Administrator","updateEntities","id=gid000000000714; type=Patch;
record=cataloged; version=3;","updateEntity","S","FSERV","",""

"2012/05/10 15:44:21.882
+0900","192.168.1.10","Server1","Administrator","updateEntities","id=gid000000000689; type=Patch;
record=cataloged; version=3;","updateEntity","S","FSERV","",""

"2012/05/10 15:53:24.214 +0900","192.168.1.10","Server1","SYSTEM","updateEntity","id=gid000000008583;
type=Server; record=observed; version=1;","addEntity","S","FSERV","",""

"2012/05/10 15:53:48.316 +0900","192.168.1.10","Server1","SYSTEM","updateEntity","id=gid000000008584;
type=Server; record=observed; version=1;","addEntity","S","FSERV","",""

"2012/05/10 15:54:27.822 +0900","192.168.1.10","Server1","SYSTEM","addEntity","id=gid000000008583;
type=Server; record=observed; version=1;","updateEntity","S","FSERV","",""

"2012/05/10 15:55:28.062 +0900","192.168.1.10","Server1","SYSTEM","addEntity","id=gid000000008583;
type=Server; record=observed; version=1;","updateEntity","S","FSERV","",""
```

4.1.4 Audit Logs for Job Management

The history of operations performed by a user is output to an audit log. This includes when one of the following operations is performed using a wizard on the management console or using a command, when an action is executed from the **Job Management** window, or using the job information management command.

- Patch distribution
- Patch application
- Parameter settings
- Script execution
- Configuration modification

Audit logs

Log name	Description	Size	Number of generations
swcfmg_job_audit_log	Outputs audit logs for patch distribution, patch application, parameter settings, and script execution.	10 MB	10 generations

Output destination

The output destination for logs is shown below.

[Windows]

Output folder	Description
<Systemwalker Software Configuration Manager installation directory> \SWCFMGM\logs	Same as the log name.

[Linux]

Output folder	Description
/var/opt/FJSVcfmgm/logs	Same as the log name.

Output format

The output format is shown below. It is possible to change the output destination for audit logs, the file size, and the number of generations held.

Output format
<Operation date/time>,*<User ID>*,*<Tenant name>*,*<Operation type>*,*<Parameters>*,*<Operation result>*

Item	Description
Operation date/time	YYYY-MM-DD HH:MM:SS.sss (local time)
User ID	The user ID of the user that executed the operation Note: When the operation is performed using the command, "#COMMAND" is output.
Tenant name	The tenant name of the user that executed the operation Note: For operations performed by infrastructure administrators, "admin" is output. It is not output when the operation is performed using the command.
Operation type	A string indicating the content of the operation
Parameters	The parameters specified by the request
Operation result	"SUCCESS" if the operation was successful and "FAILURE" if the operation failed

Operation type

Operation type	Description	Parameter
patchDistributionStart	Requests patch distribution from the **Patch Application** wizard or using the patch application command	jobid="*<job ID>*"&jobname="*<job name>*"
patchApplicationStart	Requests patch application from the **Patch Application** wizard or using the patch application command	jobid="*<job ID>*"&jobname="*<job name>*"
parameterSettingStart	Requests parameter settings from the **Parameter Settings** wizard or from the parameter settings command	jobid="*<job ID>*"&jobname="*<job name>*"
scriptExecutionStart	Request script execution from the **Script Execution** wizard or using the script execution command	jobid="*<job ID>*"&jobname="*<job name>*"
configurationChangeStart	Request configuration change from the configuration modification wizard or the configuration modification command	jobid="*job ID*"&jobname="*job name*"
patchDistributionAction	After requesting patch distribution, execute an action from the **Job Management** window or using the job information management command	jobid="*<job ID>*"&jobname="*<job name>*"&processname="*<process name>*"&processorder="*<process order>*"&processtype="*<process type>*"&action="*<action>*"

Operation type	Description	Parameter
patchApplicationAction	After requesting patch distribution, execute an action from the **Job Management** window or using the job information management command	jobid="*<job ID>*"&jobname="*<job name>*"&processname="*<process name>*"&processorder="*<process order>*"&processtype="*<process type>*"&action="*<action>*"
parameterSettingAction	After requesting parameter settings, execute an action from the **Job Management** window or using the job information management command	jobid="*<job ID>*"&jobname="*<job name>*"&processname="*<process name>*"&processorder="*<process order>*"&processtype="*<process type>*"&action="*<action>*"
scriptExecutionAction	After requesting script execution, execute an action from the **Job Management** window or using the job information management command	jobid="*<job ID>*"&jobname="*<job name>*"&processname="*<process name>*"&processorder="*<process order>*"&processtype="*<process type>*"&action="*<action>*"
configurationChangeAction	After requesting configuration modification, execute an action from the **Job Management** window or using the Job Information Management command	jobid="*job ID*"&jobname="*job name*"&processname="*process name*"&processorder="*process order*"&processtype="*process type*"&action="*action*"

4.2 Backing Up and Restoring the Admin Server

This section explains how to back up and restore the Systemwalker Software Configuration Manager admin server.

4.2.1 Notes on Backup and Restoration

This section provides notes regarding Systemwalker Software Configuration Manager backup and restore.

Advisory notes when coordinating with ServerView Resource Orchestrator

When coordinating with ServerView Resource Orchestrator, ServerView Resource Orchestrator and Systemwalker Software Configuration Manager share the CMDB. Backup and restore of the CMDB data are performed using ServerView Resource Orchestrator.

For details on backup and restore of ServerView Resource Orchestrator, refer to "Mechanism of Backup and Restoration" in the "ServerView Resource Orchestrator Cloud Edition Operation Guide" for details.

Notes on the environments where backups and restorations are performed

The backup and restoration environments must follow the criteria below:

- When OS are different in from backup and to restore

  However, execution will be possible if the operating system versions of the same vendor are different.

- When the product installation directories are different [Windows]
- When the host information (host name/IP address) is different
- When the code types are different
- When the CMDB database storage directories are different
- When the Web server (Interstage HTTP Server), message broker, and server function port numbers are different
-

Notes on the timing of backups and restorations

- When backup and restore are executed, it will be necessary to restart Systemwalker Software Configuration Manager. When linked to ServerView Resource Orchestrator, it will be necessary to restart Systemwalker Software Configuration Manager and ServerView Resource Orchestrator. For this reason, the operator should execute backup and restore in a time zone that does not use Systemwalker Software Configuration Manager and ServerView Resource Orchestrator.
- The statuses of patch application, patch distribution, parameter setting, and script execution that were in effect at the time of backup will be restored. If restore is performed using backup resources for which script execution is in progress, operation will be resumed. Before performing backup, confirm that patch application, patch distribution, parameter setting, and script execution are not running.

Handling backup resources

- When moving backup resources to the restoration target, move the directory specified as the backup directory and all its files.
- Do not delete the backup resources in the directory specified as the backup directory until the restoration completes.
- The backup command cannot be used to back up data to the following types of media:
    - Optical disks such as CD-Rs and DVD-Rs

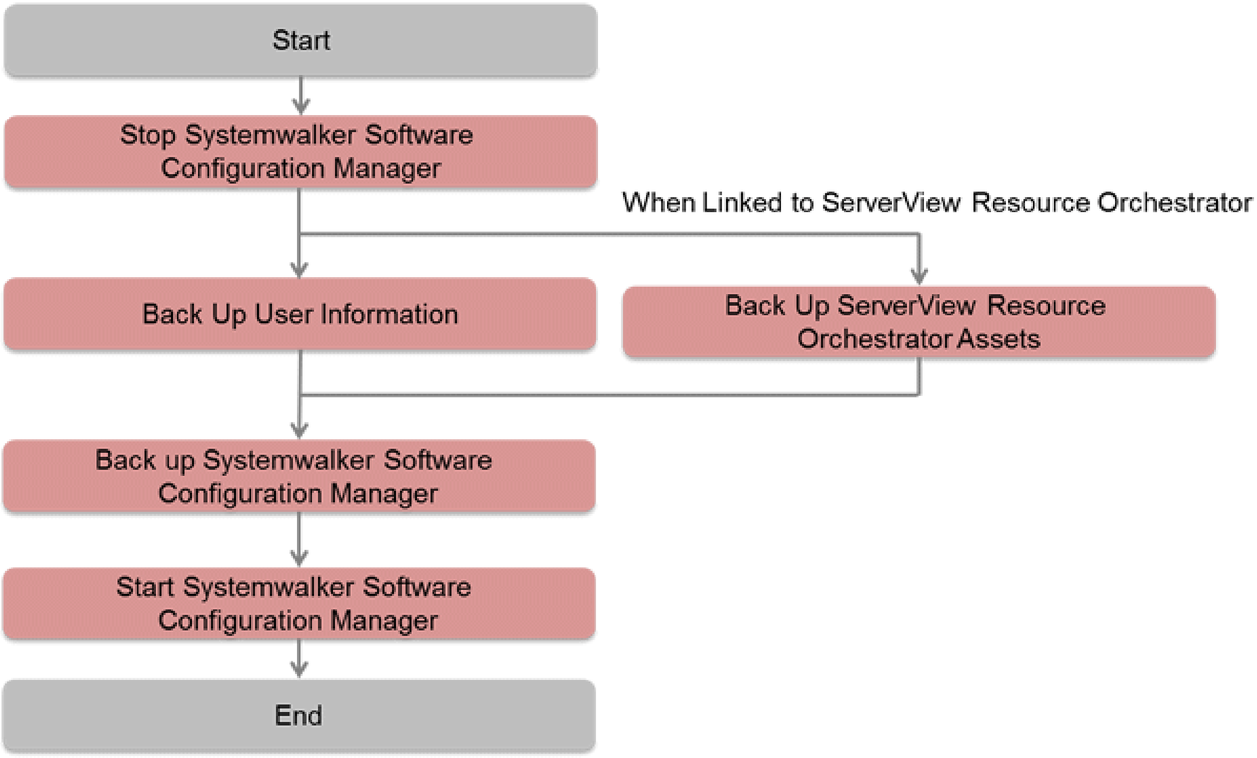
      To save user assets to optical disks, first back up the data to the local disk, and then, write it to the media using a dedicated optical disk writer, for example.
    - Network paths [Windows]
    - Directories whose pathnames include spaces

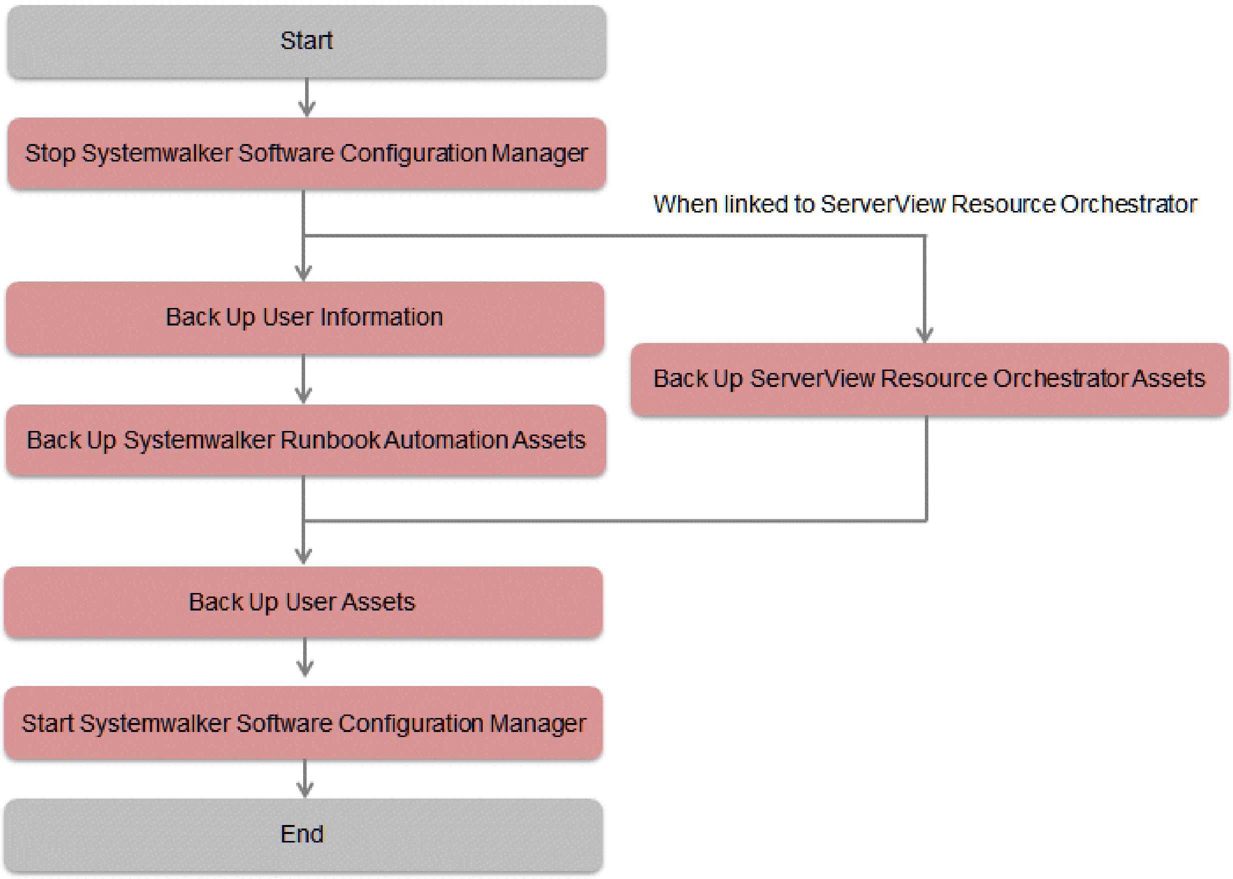
4.2.2 Backing Up the Admin Server

This section explains how to back up the Systemwalker Software Configuration Manager admin server.

Note that Systemwalker Software Configuration Manager must be stopped before performing backup.

For details on how to start and stop Systemwalker Software Configuration Manager, refer to "Chapter 3 Starting and Stopping Systemwalker Software Configuration Managerr".


Start
Stop Systemwalker Software Configuration Manager
When Linked to ServerView Resource Orchestrator
Back Up User Information
Back Up ServerView Resource Orchestrator Assets
Back up Systemwalker Software Configuration Manager
Start Systemwalker Software Configuration Manager
End


Start
Stop Systemwalker Software Configuration Manager
When linked to ServerView Resource Orchestrator
Back Up User Information
Back Up ServerView Resource Orchestrator Assets
Back Up Systemwalker Runbook Automation Assets
Back Up User Assets
Start Systemwalker Software Configuration Manager
End

-
- 4.2.2.2 Backing Up User Information
-
- 4.2.2.3 Backing Up ServerView Resource Orchestrator Assets (when Linked to ServerView Resource Orchestrator)
- 4.2.2.4 Backup of Systemwalker Software Configuration Manager

4.2.2.1 Required Disk Space for Backup

Before backing up Systemwalker Software Configuration Manager, estimate the amount of disk space required for each asset, as explained below:

Asset	Required disk space

Systemwalker Software Configuration Manager	**[Windows]**
	`Required disk space =`
	`+ Size of <media library directory> (*1)`
	`+ Size of <database directory of CMDB manager>\FJSVcmdbm\Shunsaku\directorData (*2)`
	`+ Size of <database directory of CMDB manager>\FJSVcmdbm\fcmdb\file (*2)`
	`+ Size of <Systemwalker Software Configuration Manager installation directory>\SWCFMGM\SWCFMGDB`
	`+ 100 MB`
	[Linux]
	`Required disk space =`
	`+ Size of <media library directory> (*1)`
	`+ Size of <database directory of CMDB`

Asset	Required disk space

	`manager>/FJSVcmdbm/Shunsaku/directorData (*2)`
	`+ Size of <database directory of CMDB manager>/FJSVcmdbm/fcmdb/file (*2)`
	`+ Size of /var/opt/FJSVcfmgm/SWCFMGMDB`
	`+ 100 MB`
	*1: Size specified for the "media library installation directory" during setup.
	*2: Size specified for the "CMDB Manager database directory" during setup.

ServerView Resource Orchestrator	Refer to "Mechanism of Backup and Restoration" in the *ServerView Resource Orchestrator Cloud Edition Operation Guide* for details.

4.2.2.2 Backing Up User Information

User information is backed up when the directory service is backed up. Refer to the relevant ServerView Operations Manager manual below for information on how to back up the directory service. If linked to ServerView Resource Orchestrator, then use it to back up user information.

[Windows]

- "Backing up and restoring OpenDJ data on Windows systems" in *User Management in ServerView*

[Linux]

- "Backing up and restoring OpenDJ data on Linux systems" in *User Management in ServerView*

4.2.2.3 Backing Up ServerView Resource Orchestrator Assets (when Linked to ServerView Resource Orchestrator)

Use offline backup to back up the ServerView Resource Orchestrator assets. CMDB assets are not backed up by online backups. Refer to "Offline Backup of the Admin Server" in the *ServerView Resource Orchestrator Cloud Edition Operation Guide* for details.

4.2.2.4 Backup of Systemwalker Software Configuration Manager

Execute the following command from the command prompt to execute backup of Systemwalker Software Configuration Manager. Refer to the Reference Guide for information on commands.

Command name	Overview
swcfmg_backup	This command backs up user assets.

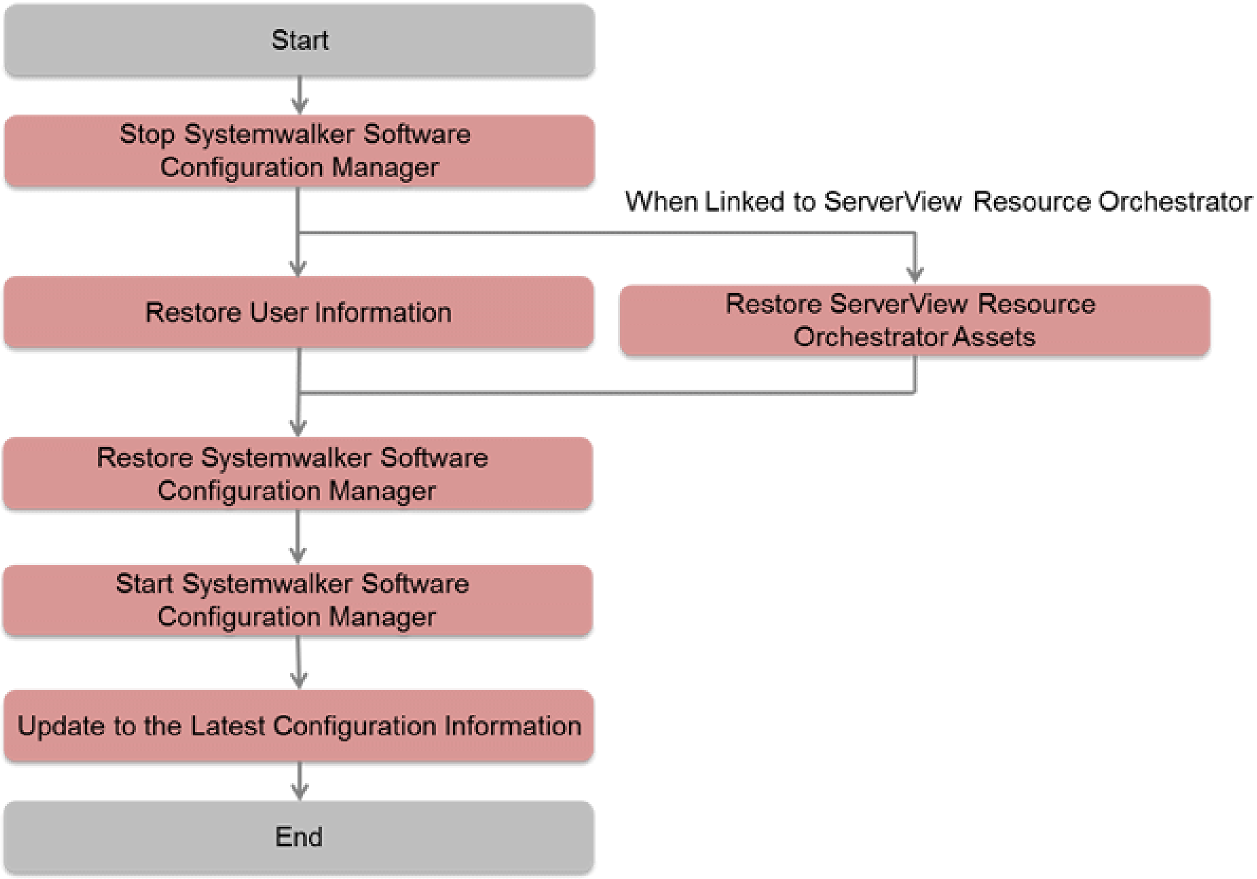
Note

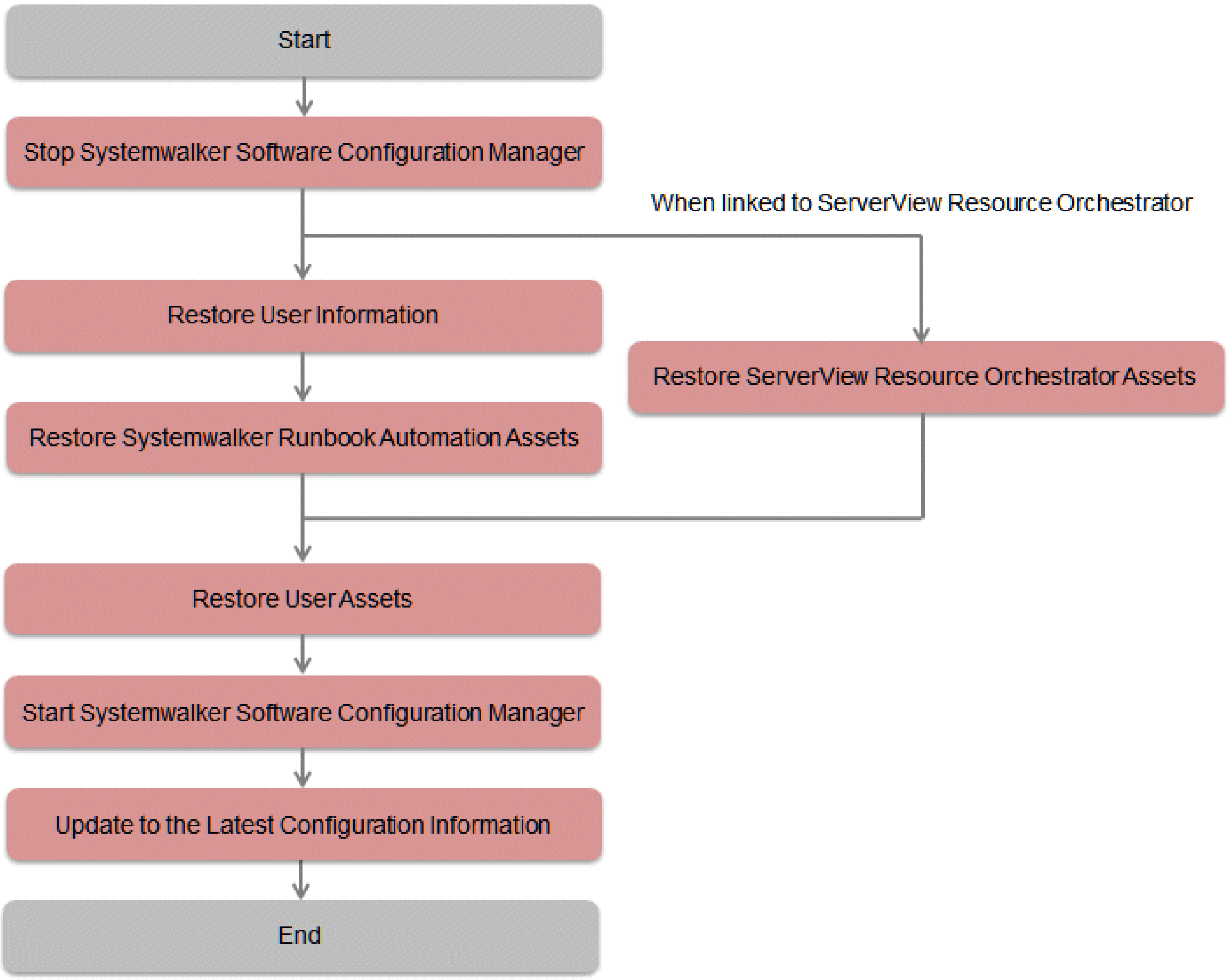
- User assets must be backed up using OS administrator privileges (administrator or root).
- For the backup destination, specify a directory with sufficient disk space.
- If the disk runs out of space during the backup, all of the data at the backup destination will be deleted.

4.2.3 Restoring the Admin Server

This section explains how to restore the Systemwalker Software Configuration Manager admin server.

Note that Systemwalker Software Configuration Manager must be stopped before restoring Note that after restoration, it is necessary to start Systemwalker Software Configuration Manager before updating to the latest configuration information.For details on how to start and stop Systemwalker Software Configuration Manager, refer to "Chapter 3 Starting and Stopping Systemwalker Software Configuration Managerr".


Start
Stop Systemwalker Software Configuration Manager
When Linked to ServerView Resource Orchestrator
Restore User Information
Restore ServerView Resource Orchestrator Assets
Restore Systemwalker Software Configuration Manager
Start Systemwalker Software Configuration Manager
Update to the Latest Configuration Information
End


Start
Stop Systemwalker Software Configuration Manager
When linked to ServerView Resource Orchestrator
Restore User Information
Restore ServerView Resource Orchestrator Assets
Restore Systemwalker Runbook Automation Assets
Restore User Assets
Start Systemwalker Software Configuration Manager
Update to the Latest Configuration Information
End

-

- 4.2.3.1 Restoring User Information
- 4.2.3.2 Restoring ServerView Resource Orchestrator Assets (when Linked to ServerView Resource Orchestrator)
- 4.2.3.3 Restoration of Systemwalker Software Configuration Manager
- 4.2.3.4 Updating to the Latest Configuration Information

4.2.3.1 Restoring User Information

Restore user information that was backed up at "Backing Up User Information" (refer to the relevant ServerView Operations Manager manual below for details). If linked to ServerView Resource Orchestrator, then use it to restore user information.

[Windows]

- "Backing up and restoring OpenDJ data on Windows systems" in *User Management in ServerView*

[Linux]

- "Backing up and restoring OpenDJ data on Linux systems" in *User Management in ServerView*

4.2.3.2 Restoring ServerView Resource Orchestrator Assets (when Linked to ServerView Resource Orchestrator)

Restore ServerView Resource Orchestrator assets backed up at "Backing Up ServerView Resource Orchestrator Assets (when Linked to ServerView Resource Orchestrator)" (refer to "Restoring the Admin Server" in the *ServerView Resource Orchestrator Cloud Edition Operation Guide* for details).

4.2.3.3 Restoration of Systemwalker Software Configuration Manager

Restore the assets collected in "Backup of Systemwalker Software Configuration Manager". Execute the following command from the command prompt to restore Systemwalker Software Configuration Manager. Refer to the Reference Guide for information on commands.

Command name	Overview
swcfmg_restore	This command restores user assets.

Note

User assets must be restored using OS administrator privileges (administrator or root).

4.2.3.4 Updating to the Latest Configuration Information

After restoring Systemwalker Software Configuration Manager, start Systemwalker Software Configuration Manager and then update to the latest configuration information.

The procedure for updating to the latest configuration information is described below:

1. Execute cmdbrefresh to update the CMDB information:

   [Windows]

   ```
   %SWCMDBINSTALLPATH%\CMDB\FJSVcmdbm\bin\cmdbrefresh.exe -a -q-
   ```

   [Linux]

   ```
   /opt/FJSVcfmgm/CMDB/FJSVcmdbm/bin/cmdbrefresh.sh -a -q
   ```

2. Perform discovery to update to the latest patch information and Fujitsu middleware product information:

   [Windows]

   ```
   <Systemwalker Software Configuration Manager installation directory>\SWCFMGM\bin
   \swcfmg_patch_updateinfo.exe -repository
   ```

   [Linux]

   ```
   /opt/FJSVcfmgm/bin/swcfmg_patch_updateinfo -repository
   ```

   To discover only particular information, execute the command below:

   - Windows patch information

     [Windows]

     ```
     <Systemwalker Software Configuration Manager installation directory>\SWCFMGM\bin
     \swcfmg_patch_updateinfo.exe -t windows -repository
     ```

     [Linux]

     ```
     /opt/FJSVcfmgm/bin/swcfmg_patch_updateinfo -t windows -repository
     ```

   - Linux patch information

     [Windows]

     ```
     <Systemwalker Software Configuration Manager installation directory>\SWCFMGM\bin
     \swcfmg_patch_updateinfo.exe -t linux
     ```

     [Linux]

```
/opt/FJSVcfmgm/bin/swcfmg_patch_updateinfo -t linux
```

- Fujitsu middleware patch information and Fujitsu middleware product information

  [Windows]

  ```
  <Systemwalker Software Configuration Manager installation directory>\SWCFMGM\bin
  \swcfmg_patch_updateinfo.exe -t middleware
  ```

  [Linux]

  ```
  /opt/FJSVcfmgm/bin/swcfmg_patch_updateinfo -t middleware
  ```

3. Perform discovery for the parameter information:

   [Windows]

   ```
   <Systemwalker Software Configuration Manager installation directory>\SWCFMGM\bin
   \swcfmg_param_updateinfo.exe
   ```

   [Linux]

   ```
   /opt/FJSVcfmgm/bin/swcfmg_param_updateinfo
   ```

4.3 Changing the Systemwalker Software Configuration Manager Environment

4.3.1 Changing the Operating Environment for WSUS

To change the operating environment for Microsoft Windows Server Update Services (WSUS), perform the following setup operation.

Adding a WSUS server

- Install a Systemwalker Software Configuration Manager agent on the WSUS server to be added.
- Implement changes to the configuration between WSUS servers by referring to the WSUS manuals.

  (For example, changing upstream or downstream servers, migrating the managed computers, etc.)
- To take a business server that was being managed by an existing WSUS server and have it managed by an additional WSUS server, use the following procedure to migrate the managed computer:

  1. Delete the business server to be migrated from the list of computers managed by the existing WSUS server.
  2. Execute the connection destination repository server registration command (swcfmg_register_repsv) on the business server that has been migrated in order to register the additional WSUS server.

     Example:

     ```
     swcfmg_register_repsv.bat wsus -to 10.10.10.10
     ```

     Refer to the *Reference Guide* for information on the connection destination repository server registration command (swcfmg_patch_importrpmpolicy).

- Register the additional WSUS server on the admin server.

  Modify the discovery definition file.

  Example: Adding the WSUS server with IP address 11.11.11.11 to an environment where only the WSYS server with IP address 10.10.10.10 had been used

```
<?xml version="1.0" encoding="utf-8"?>
<Discovery>
  <RepositoryServers>
    <WSUS>
      <entry key="enable-wsus">true</entry>
      <entry key="ipaddress">10.10.10.10</entry>
    </WSUS>
    <WSUS>
      <entry key="enable-wsus">true</entry>
      <entry key="ipaddress">11.11.11.11</entry>
    </WSUS>
  </RepositoryServers>
</Discovery>
```

Refer to the *Reference Guide* for information on the discovery definition file.

There is no need to restart Systemwalker Software Configuration Manager.

Removing a WSUS server

- Uninstall the Systemwalker Software Configuration Manager agent from the WSUS server to be removed.
- Implement changes to the configuration between WSUS servers by referring to the WSUS manuals.

  (For example, changing upstream or downstream servers, migrating the managed computers, etc.)
- To take a business server that was being managed by the WSUS server to be removed and have it managed by another WSUS server, use the following procedure to migrate the managed computer:

  1. Execute the connection destination repository server registration command (swcfmg_register_repsv) on the business server that has been migrated.

     Example:

     ```
     swcfmg_register_repsv.bat wsus -to 10.10.10.10
     ```

     Refer to the *Reference Guide* for information on the connection destination repository server registration command (swcfmg_patch_importrpmpolicy).

- Delete the WSUS server to be removed from the management target for the admin server.

  Modify the discovery definition file.

  Example: Removing a WSUS server with IP address 10.10.10.10

```
<?xml version="1.0" encoding="utf-8"?>
<Discovery>
  <RepositoryServers>
    <WSUS>
      <entry key="enable-wsus">false</entry>
      <entry key="ipaddress">10.10.10.10</entry>
    </WSUS>
  </RepositoryServers>
</Discovery>
```

Note: Omitting the <WSUS> element has the same result.

Refer to the *Reference Guide* for information on the discovery definition file.

There is no need to restart Systemwalker Software Configuration Manager.

4.3.2 Changing the Configuration of the yum Repository Server

If the configuration of the yum repository server has been changed, the yum caches for Linux business servers (yum clients) must be cleared. If the yum cache needs to be cleared, execute the swcfmg_notify_yumcacheclean command (the yum cache cleanup notification command). Refer to the *Reference Guide* for information on the swcfmg_notify_yumcacheclean command (the yum cache cleanup notification command).

- Cases where the yum caches for Linux business servers (yum clients) must be cleared:
    - When a repository server has been added or removed
    - When a RPM package has been added or removed
    - When the storage destinations for RPM packages have been changed (added or removed)
    - When the communication protocols used between the repository server and yum clients have been changed (added or removed)

These operations are performed by infrastructure administrators.

Note

Do not decide whether to clear the yum caches for Linux business servers (yum clients) based on messages etc. The infrastructure administrator that manages the yum repository server must always execute the yum cache cleanup notification command whenever the configuration of the yum repository server is changed.

If the configuration of the yum repository server is changed but the yum cache cleanup notification command is not executed, then historic information will be displayed in the management console for the application status of Linux patches, even if discovery is performed.

If RPM packages have been registered with the yum repository server and set in the Linux patch management target definitions but the Linux patch information in the management console does not show the RPM packages that should have been registered with the yum repository server, then it is possible that the yum caches on Linux business servers have not been recreated. Perform discovery after executing the yum cache cleanup notification command. Refer to "2.8.2 Defining the Linux Patch Management Target" for information on how to define the Linux patch management target.

If the RPM packages registered with the yum repository server are still not displayed in the patch list in the management console, this means that no Linux business servers to which these RPM packages can be applied have been deployed at the moment.

4.3.3 Changing Discovery Schedules and Configuration Baseline Creation Schedules

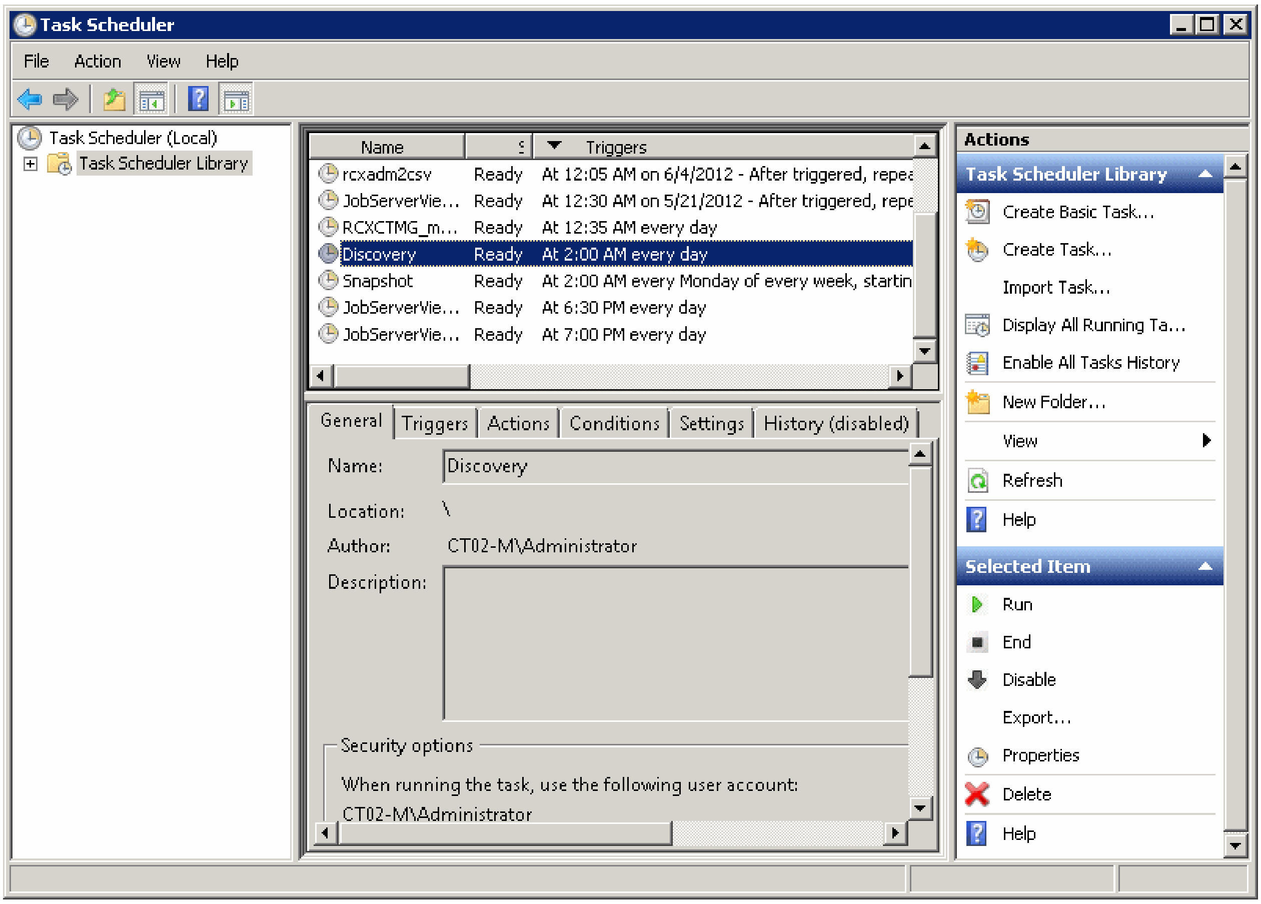
[Windows]

This section describes the procedure for changing the discovery schedule or configuration baseline creation schedule that has been registered with the Task Scheduler.

1. Log in to Windows using an account that belongs to the Administrators group.

2. Select **Start** >> **Administrative Tools** >> **Task Scheduler**.

   The **Task Scheduler** window will be displayed.



Name	S	Triggers
rcxadm2csv	Ready	At 12:05 AM on 6/4/2012 - After triggered, repea
JobServerVie...	Ready	At 12:30 AM on 5/21/2012 - After triggered, repe
RCXCTMG_m...	Ready	At 12:35 AM every day
Discovery	Ready	At 2:00 AM every day
Snapshot	Ready	At 2:00 AM every Monday of every week, startin
JobServerVie...	Ready	At 6:30 PM every day
JobServerVie...	Ready	At 7:00 PM every day

Name: Discovery

Location: \

Author: CT02-M\Administrator

Description:

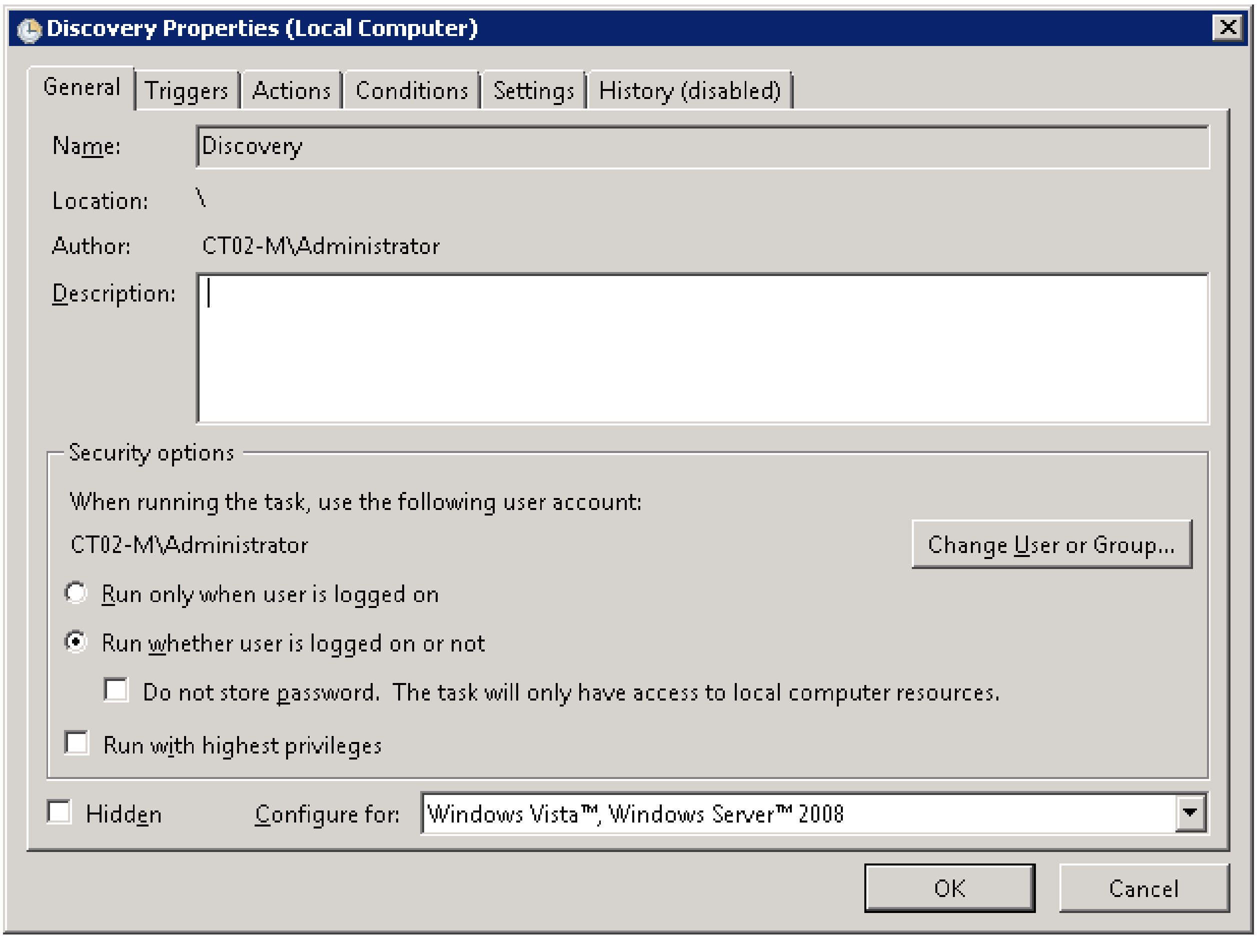
Security options

When running the task, use the following user account:

CT02-M\Administrator

3. Right-click on the task to be changed, and then select **Properties**.

   The properties of the task will be displayed.



Discovery Properties (Local Computer)

Name: Discovery

Location: \

Author: CT02-M\Administrator

Description:

Security options

When running the task, use the following user account:

CT02-M\Administrator

○ Run only when user is logged on

● Run whether user is logged on or not

□ Do not store password. The task will only have access to local computer resources.

□ Run with highest privileges

□ Hidden

Configure for: Windows Vista™, Windows Server™ 2008

4. Select the **Triggers** tab and change the schedule.

5. Click the **OK** button to close the window.

[Linux]

This section describes the procedure for changing the discovery schedule or configuration baseline creation schedule that has been registered with cron.

Perform the following procedure as the root user:

1. Execute the following command to edit the schedule definitions:

```
>crontab -e
```

   Executing the "crontab -e" command starts the vi editor. Refer to the vi editor manuals for information on the vi editor.

   Example: Discovering all information every day at 2:00

```
0 2 * * * /opt/FJSVcfmgm/bin/swcfmg_patch_updateinfo -repository > /dev/null 2>&1
```

   Example: Creating a configuration baseline every Monday at 6:00

```
0 6 * * 1 /opt/FJSVcmdbm/bin/snapcreate.sh -q > /dev/null 2>&1
```

   Refer to "Registering Discovery Schedules" and "Registering a Configuration Baseline Creation Schedule" in the *Installation Guide* for information on schedule definitions.

4.3.4 Migrating the Media Library

If there is not enough disk space for the media library, take the following actions:

- Delete unnecessary files from the disk for the media library
- Increase the amount of disk space available for the media library.

However, if these actions are difficult, migrate the media library to resolve the disk space shortage.

The procedure for migrating the media library is shown below.

1. Stop Systemwalker Software Configuration Manager.

   [Windows]

   ```
   <Systemwalker Software Configuration Manager installation directory>\SWCFMGM\bin\swcfmg_stop
   ```

   [Linux]

   ```
   /opt/FJSVcfmgm/bin/swcfmg_stop
   ```

2. Back up the media library. Refer to "Command Reference" in the *Reference Guide* for information on this command.

   [Windows]

   ```
   <Systemwalker Software Configuration Manager installation directory>\SWCFMGM\bin\swcfmg_repository_backup -d
   <Output path>
   ```

   [Linux]

   ```
   /opt/FJSVcfmgm/bin/swcfmg_repository_backup -d <Output path>
   ```

3. Restore the media library. For the "-to" option, specify the migration destination for the media library.

   For the migration destination, specify a directory with sufficient free space. Refer to "Command Reference" in the *Reference Guide* for information on this command.

   [Windows]

   ```
   <Systemwalker Software Configuration Manager installation directory>\SWCFMGM\bin\swcfmg_repository_restore -d <Path
   to the directory where the backup data is stored> -to <Path to the migration destination for the media library>
   ```

   [Linux]

   ```
   /opt/FJSVcfmgm/bin/swcfmg_repository_restore -d <Path to the directory where the backup data is stored> -to <Path to the
   migration destination for the media library>
   ```

4. When you migrate the media library, the definition file changes. For this reason, you must perform a backup again if various configuration files were backed up before migrating the media library. Refer to "4.2.2.4 Backup of Systemwalker Software Configuration Manager " for information on how to back up various configuration files.

5. Restart Systemwalker Software Configuration Manager.

   [Windows]

   ```
   <Systemwalker Software Configuration Manager installation directory>\SWCFMGM \bin\swcfmg_start
   ```

   [Linux]

   ```
   /opt/FJSVcfmgm/bin/swcfmg_start
   ```

Note

When starting operation of this product before performing backup and restore of the media library, inconsistency occurs between the backup data and other data of this product. Do not start and operate this product before performing backup and restore of the media library.

4.3.5 Changing Passwords of Users who Use this Product

This section explains how to change the passwords of users of the following directory services used with this product:

- User for process control
- LDAP administrator

4.3.5.1 Changing the Password of a User for Process Control

The procedure for changing the password of a user for process control is described below:

1. Stop Systemwalker Software Configuration Manager.

   Refer to "3.2 Stopping Systemwalker Software Configuration Manager" for details.

2. Change the password of the user for process control Execute the following command:

   [Windows]

   ```
   <Systemwalker Software Configuration Manager installation directory>\SWCFMGM\bin\swcfmg_environment -set -key
   job.process.controller.password -value <new password>
   ```

   [Linux]

   ```
   /opt/FJSVcfmgm/bin/swcfmg_environment -set -key job.process.controller.password -value <new password>
   ```

3. Restart Systemwalker Software Configuration Manager.

   Refer to "3.1 Starting Systemwalker Software Configuration Manager" for details.

4.3.5.2 Changing the Password of an LDAP Administrator DN

The procedure for changing the password of an LDAP administrator DN is described below

When coordinating with ServerView Resource Orchestrator, also change the password registered in ServerView Resource Orchestrator.

1. Stop Systemwalker Software Configuration Manager.

   Refer to "3.2 Stopping Systemwalker Software Configuration Manager" for details.

2. Change the LDAP administrator DN password. Change the password of svuser referring to manuals of ServerView Operations Manager.

   - "Defining / changing the password of svuser" in "User Management in ServerView"

3. When coordinating with ServerView Resource Orchestrator, configure the new password in ServerView Resource Orchestrator. - Refer to "Reconfiguring Single Sign-On" in the ServerView Resource Orchestrator Cloud Edition Operation Guide for details.

4. Execute the following command in the command prompt to set the new password for Systemwalker Software Configuration Manager:

   [Windows]

   ```
   <Systemwalker Software Configuration Manager installation directory>\SWCFMGM\bin\swcfmg_environment -set -key
   user.ldap.administrator.password -value <new password>
   ```

   [Linux]

   ```
   /opt/FJSVcfmgm/bin/swcfmg_environment -set -key user.ldap.administrator.password -value <new password>
   ```

5. Restart Systemwalker Software Configuration Manager. Refer to "3.1 Starting Systemwalker Software Configuration Manager" for details.

4.3.6 Changing Passwords of Operating System Users who Use this Product

The procedure for changing the passwords of the following users of operating systems used with this product is described below:

- swcfmgdb

4.3.6.1 Changing the Password for swcfmgdb

The procedure for changing the password for swcfmgdb is described below:

1. Stop Systemwalker Software Configuration Manager.

   Refer to "3.2 Stopping Systemwalker Software Configuration Manager" for details.

2. Change the password.

   If using Windows, execute the command below:

   ```
   net user swcfmgdb <new password>
   ```

3. If using Windows, change the password of the service startup account.

   The service below will be changed:

   - Systemwalker Software Configuration Manager DataBase Service

4. Set a new password for Systemwalker Software Configuration Manager. Execute the following command: For the new password, set the same value as the password specified in steps 2 and 3.

   [Windows]

   ```
   <Systemwalker Software Configuration Manager installation directory>\SWCFMGM\bin\swcfmg_environment -set -key
   database.user.password -value <new password>
   ```

   [Linux]

   ```
   /opt/FJSVcfmgm/bin/swcfmg_environment -set -key database.user.password -value <new password>
   ```

5. Restart Systemwalker Software Configuration Manager.

   Refer to "3.1 Starting Systemwalker Software Configuration Manager" for details.

4.3.7 Changing the Reference Directory for the Storage Location

This section explains how to change the reference directory for the storage location during the file collection process of the configuration modification function. The reference directory for the storage location is automatically configured using the following default value during setup of this product. To change the default value for the reference directory for the storage location, perform the following procedure. The change is reflected on the configuration modification jobs requested after the change. The change is not reflected on the configuration modification jobs requested prior to the change.

[Windows]

```
%ProgramData%/Fujitsu/SWCFMGM/storagedir
```

[Linux]

```
/var/opt/FJSVcfmgm/storagedir
```

1. Stop Systemwalker Software Configuration Manager. Refer to "3.2 Stopping Systemwalker Software Configuration Manager" for details.

2. Rewrite the configuration file.

   [Windows]

Configuration File	Location to Change (One location)
<*Systemwalker Software Configuration Manager installation directory*>\SWCFMGM\config\manager_config.xml	<entry key="standard-storage-dir">C:/ProgramData/Fujitsu/SWCFMGM/storagedir</entry> <=Delete=>

   [Linux]

Configuration File	Location to Change (One location)
/etc/opt/FJSVcfmgm/config/manager_config.xml	<entry key="standard-storage-dir">/var/opt/FJSVcfmgm/storagedir</entry> <=Delete=>

3. Restart Systemwalker Software Configuration Manager. Refer to "3.1 Starting Systemwalker Software Configuration Manager" for details.

4.4 Checking the Execution of Regular Discovery

Use the following method to check if regular discovery is running correctly.

Discovery for OS patches

For Windows, check if the following messages were output to the event log on the admin server at the times specified by the Task Scheduler.

For Linux, check if the following messages were output to the syslog on the admin server at the times specified by cron:

- CFMGD00006: The processing for updating patch information has started.

  If this message was not output, the Task Scheduler or cron may not be running. Check the settings for Task Scheduler or cron.

- CFMGD00005: Finished updating patch information.

  If this message was not output, discovery may have failed.

  Take the appropriate action by referring to the error messages output to the event log or syslog.

4.5 Checking the Execution of Configuration Baseline Creation

Use the following method to check if configuration baselines are being created correctly.

Configuration baselines are created according to the schedule that is registered using the procedure in "Registering a Configuration Baseline Creation Schedule" in the *Installation Guide*.

Check the "creation dates" for configuration baselines.

1. Execute the following command to display information about the configuration baselines that have been created:

   [Windows]

```
<Systemwalker Software Configuration Manager installation directory>\CMDB\FJSVcmdbm\bin
\snapview.exe -q num=all
```

   [Linux]

```
/opt/FJSVcmdbm/bin/snapview.sh -q num=all
```

   [Execution example]

   [Windows]

```
C:\Program Files (x86)\Fujitsu\SWCFMG\CMDB\FJSVcmdbm\bin\snapview.exe -q num=al
Do you want to display the next? [y, n, all]
all

Snapshot name        Created date
snap20120103020000        2012/01/03 02:00:00
snap20111227020000        2011/12/27 02:00:00
snap20111220020000        2011/12/20 02:00:00
snap20111213020000        2011/12/13 02:00:00
snap20111206020000        2011/12/06 02:00:00
```

[Linux]

```
[root@ct04-m ~]# /opt/FJSVcfmgm/CMDB/FJSVcmdbm/bin/snapview.sh -q num=all
Do you want to display the next? [y, n, all]
all

Snapshot name        Created name
snap20120705000001        2012/07/05 00:00:02
snap20120704100001        2012/07/04 10:00:01
snap20120704010002        2012/07/04 01:00:02
snap20120703010002        2012/07/03 01:00:02
```

2. Ensure that the configuration baselines have been created exactly in accordance with the registered schedule.

   Check if the "creation dates" for the configuration baselines obtained in Step 1 indicate that the configuration baselines have been created in accordance with the schedule registered using the procedure in "Registering a Configuration Baseline Creation Schedule" in the *Installation Guide*. If configuration baselines have been created as scheduled, the cause of the problem may either of the following.

   [Causes]

   - ServerView Resource Orchestrator is linked, but its service is not running.
   - The Task Scheduler or cron are not running.

   [Actions]

   - Ensure that the ServerView Resource Orchestrator service is running when the tool is linked.
   - Review the schedule registration.

4.6 Installing Updates on Systemwalker Software Configuration Manager

For stable and continuous operation of Systemwalker Software Configuration Manager, periodically check update information released by Fujitsu, and install released updates as soon as possible.

This section explains how to check update information for Systemwalker Software Configuration Manager, and how to install updates.

4.6.1 Installing Updates on the Admin Server

This section explains how to install updates on the admin server.

The procedure for installing updates is described below:

1. Stop Systemwalker Software Configuration Manager

   Execute the following command on the admin server:

   [Windows]

   Execute the command as a user with administrator privileges.

```
<Systemwalker Software Configuration Manager installation directory>\SWCFMGM\bin\swcfmg_stop
```

[Linux]

Execute the command as a superuser.

```
/opt/FJSVcfmgm/bin/swcfmg_stop
```

If Systemwalker Software Configuration Manager stops successfully, a stop completion message will be output.

```
Stop processing for Systemwalker Software Configuration Manager will start.
Stop processing for Systemwalker Software Configuration Manager has completed normally.
```

2. Install the updates

   Install the updates according to the explanations for the updates to be installed.

3. Start Systemwalker Software Configuration Manager

   Execute the following command on the admin server:

   [Windows]

   Execute the command as a user with administrator privileges.

   ```
   <Systemwalker Software Configuration Manager installation directory>\SWCFMGM\bin\swcfmg_start
   ```

   [Linux]

   Execute the command as a superuser.

   ```
   /opt/FJSVcfmgm/bin/swcfmg_start
   ```

   If Systemwalker Software Configuration Manager starts successfully, a startup completion message will be output.

   ```
   Start processing for Systemwalker Software Configuration Manager will start.
   Start processing for Systemwalker Software Configuration Manager has completed normally.
   ```

4.6.2 Installing Updates on the Linkage Server

This section explains how to install updates on the linkage server:

The procedure for installing updates is described below:

1. Stop the file transfer infrastructure

   Stop the file transfer infrastructure.

   [Windows]

   Use the services feature in Windows(R) to stop the file transfer infrastructure as a user with administrator privileges.

   a. Click **Control Panel** >> **Administrative Tools** >> **Services**.

   b. Select **Systemwalker File Transfer Library Control(SWCFMG)** and click the **Stop** button.

2. Install the updates

   Install the updates according to the explanations for the updates to be installed.

3. Start the file transfer infrastructure

   Start the file transfer infrastructure.

   [Windows]

   Use the services feature in Windows(R) to start the file transfer infrastructure as a user with administrator privileges.

   a. Click **Control Panel** >> **Administrative Tools** >> **Services**.

   b. Select **Systemwalker File Transfer Library Control(SWCFMG)** and click the **Start** button.

4.6.3 Installing Updates on the Business Server

This section explains how to install updates on the business server:

The procedure for installing updates is described below:

1. Stop the file transfer infrastructure

   Stop the file transfer infrastructure.

   [Windows]

   Using the Windows(R) Services function, stop the file transfer infrastructure as a user with administrator privileges:

   a. Click **Control Panel** >> **Administrative Tools** >> **Services**.

   b. Select **Systemwalker File Transfer Library Control(SWCFMG)**, and then click the **Stop** button.

   [Linux]

   Execute the following command:

   ```
   service FJSVlnkcf stop
   ```

   [Solaris]

   Execute the following command:

   ```
   /etc/init.d/FJSVlnkcf stop
   ```

2. Install the updates

   Install the required updates according to the instructions.

3. Start the file transfer infrastructure

   Start the file transfer infrastructure.

   [Windows]

   Use the services feature in Windows(R) to start the file transfer infrastructure as a user with administrator privileges.

   a. Click **Control Panel** >> **Administrative Tools** >> **Services**.

   b. Select Systemwalker File Transfer Library Control(SWCFMG) and click the Start button.

   [Linux]

   Execute the following command:

   ```
   service FJSVlnkcf start
   ```

   [Solaris]

   Execute the following command:

   ```
   /etc/init.d/FJSVlnkcf start
   ```