Systemwalker
Software Configuration Manager

Operation Guide

Windows/Linux

B1X1-0128-03ENZ0(00)
July 2012

Preface

Purpose of this Document

This document explains how to use the different features and functions required to operate Systemwalker Software Configuration Manager V15.1.0.

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) 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	Windows
Microsoft(R) Windows Server(R) 2008 R2 Standard Microsoft(R) Windows Server(R) 2008 R2 Enterprise	Windows Server 2008 R2	
Microsoft(R) Windows Server(R) 2003 R2, Standard Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition	Windows Server 2003 R2	
Red Hat(R) Enterprise Linux(R) (for x86)	RHEL (x86)	RHEL
Red Hat(R) Enterprise Linux(R) (for Intel64)	RHEL (Intel64)	

Export Restrictions

If this document is to be exported or provided overseas, confirm legal requirements for the Foreign Exchange and Foreign Trade Act as well as other laws and regulations, including U.S. Export Administration Regulations, and follow the required procedures.

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.
- 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)

Copyright

Editing Record

Additions and changes	Section	Manual code
Logs for the admin server for Linux have been added.	4.1 Log Output	B1X1-0128-03ENZ0(00) B1X1-0128-03ENZ2(00)
A procedure for changing the discovery schedule or configuration baseline creation schedule for Linux has been added.	4.4.3 Changing Discovery Schedules and Configuration Baseline Creation Schedules	
A method for Linux to check whether regular discovery is running correctly has been added.	4.5 Checking the Execution of Regular Discovery	
A method for Linux to check whether configuration baselines are being created correctly has been added.	4.6 Checking the Execution of Configuration Baseline Creation	

Contents

Chapter 1 Operation Overview

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

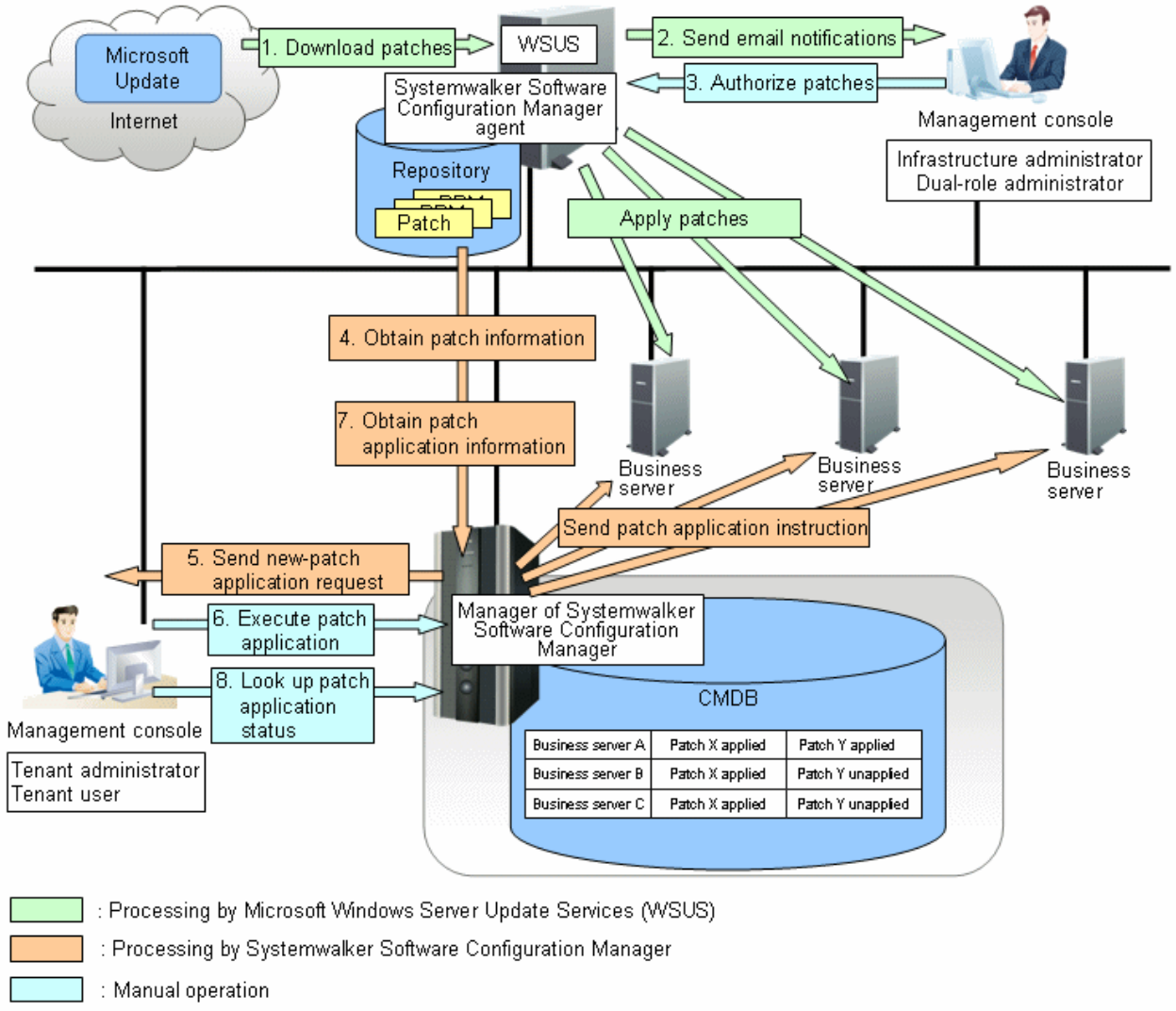
1.1 Operation Flow

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



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. This email is sent to the email addresses in the user information managed by ServerView Resource Orchestrator.

6. Execute patch application **[operation by 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.

   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. 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.

8. Look up the patch application status

   The infrastructure administrator, dual-role administrator, tenant administrator and tenant user log in to the management console and check the patch application status.

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. If email transmission fails, either an infrastructure administrator or a dual-role administrator must resend the email using the email resend

	Operation flow	User roles				Reference
		Infrastructure administrator	Dual-role administrator	Tenant administrator	Tenant user	
						command as described in the *Reference Guide*.
6	Execute patch application	-	Y	Y	Y	"Patch Management" in the *Operator's Guide*
7	Obtain patch application information	Y	Y	-	-	"Patch Information Update Command" in the *Reference Guide*
8	Look up the patch application status	Y	Y	Y	Y	"Patch Management" in the *Operator's Guide*

Y: Implement the task.

-: Do not implement the task

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.

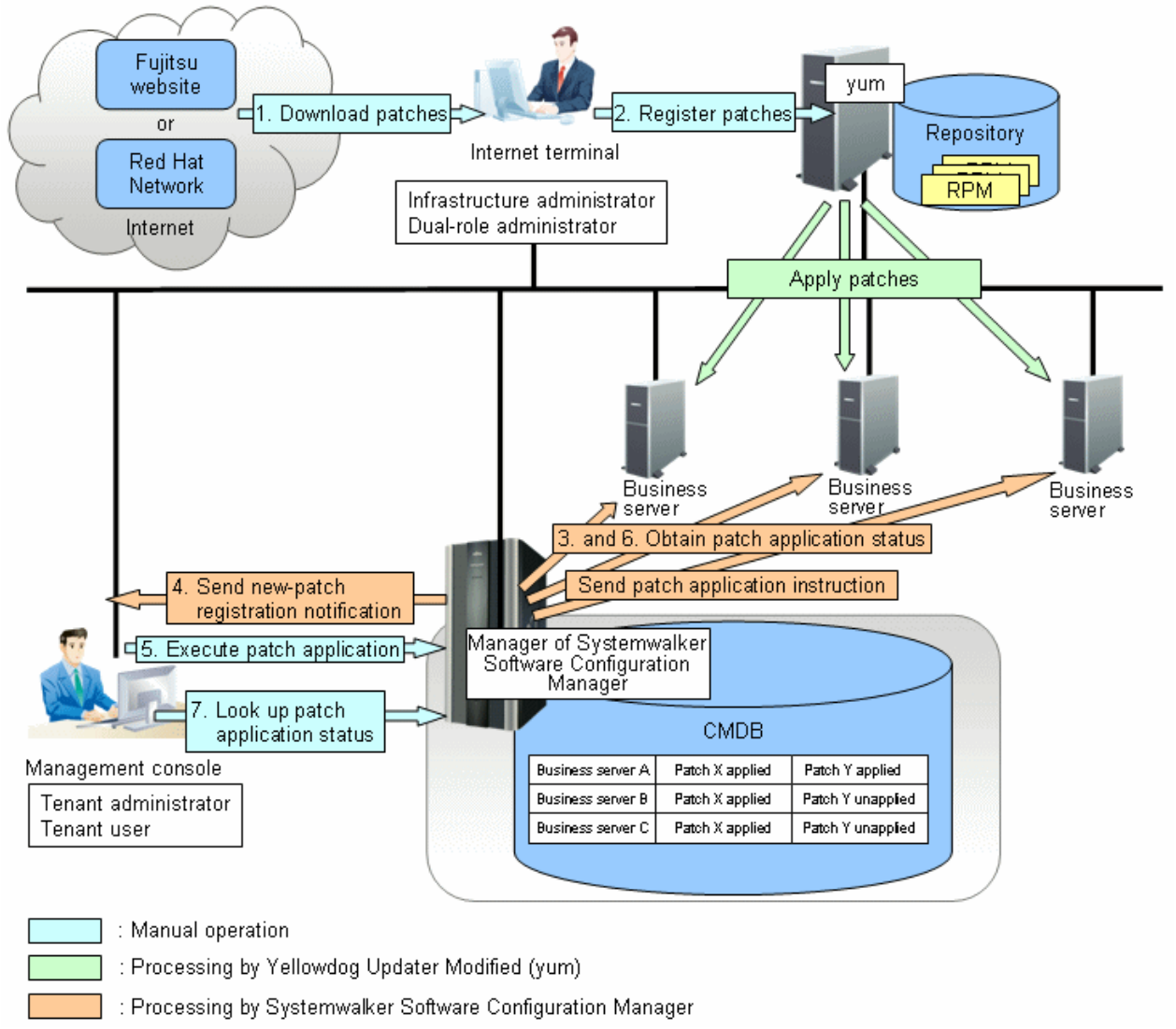
  Example:

```
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



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 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.

6. 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.

7. Look up the patch application status

   The infrastructure administrator, dual-role administrator, tenant administrator and tenant user log in to the management console and check the patch application status.

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 "2.1.2 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	Y	Y	"Patch Management" in the *Operator's Guide*
6	Obtain patch application status	Y	Y	-	-	"Patch Information Update Command" in the *Reference Guide*

	Operation flow	User roles				Reference
		Infrastructure administrator	Dual-role administrator	Tenant administrator	Tenant user	
7	Look up patch application status	Y	Y	Y	Y	"Patch Management" in the *Operator's Guide*

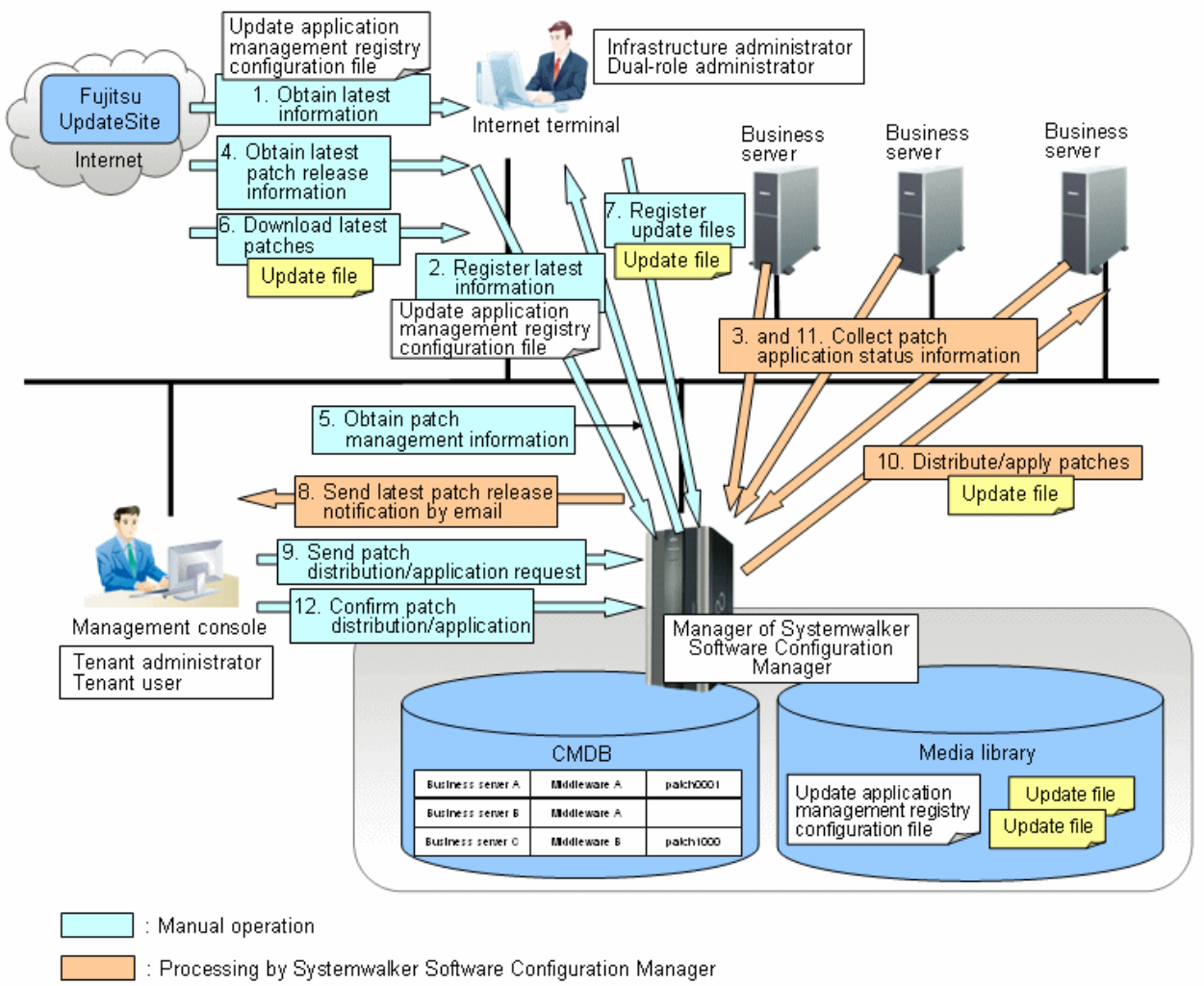
Y: Implement the task.

-: Do not implement the task

1.1.3 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 1.3 Overview of Fujitsu middleware patch management



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.

4. 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.

5. 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.

6. Download the latest 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.

7. 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.

8. 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.

9. Send patch distribution/application requests **[operation by 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.

   If the patches are to be applied as well, the tenant administrator or tenant user registers an application script.

10. 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 specified, Systemwalker Software Configuration Manager also applies the patches by executing the application script.

11. 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.

12. Confirm patch distribution/application

    The infrastructure administrator, dual-role administrator, tenant administrator and tenant user log in to the management console to check the patch application status.

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	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*
4	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).
5	Obtain patch management information	Y	Y	-	-	Refer to "Patch Management Information Acquisition Command" in the *Reference Guide*.
6	Download the latest patches	Y	Y	-	-	Refer to "Released Patch Acquisition Tool" in the *Reference Guide*.
7	Register update files	Y	Y	-	-	Refer to "Fujitsu Middleware Patch Registration Command" in the *Reference Guide*.
8	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*.
9	Send patch distribution/ application) requests	-	Y	Y	Y	"Patch Management" in the *Operator's Guide*
10	Distribute/apply patches	-	-	-	-	-
11	Collect patch application status information	Y	Y	-	-	"Patch Information Update Command" in the *Reference Guide*
12	Confirm patch distribution/ application	Y	Y	Y	Y	"Patch Management" in the *Operator's Guide*

Y: Implement the task.

-: Do not implement the task

1.1.4 Configuration Management

The software configuration information that has been collected by the discovery function (such as the server name, tenant name, host name and IP address of each server) can be viewed in 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.

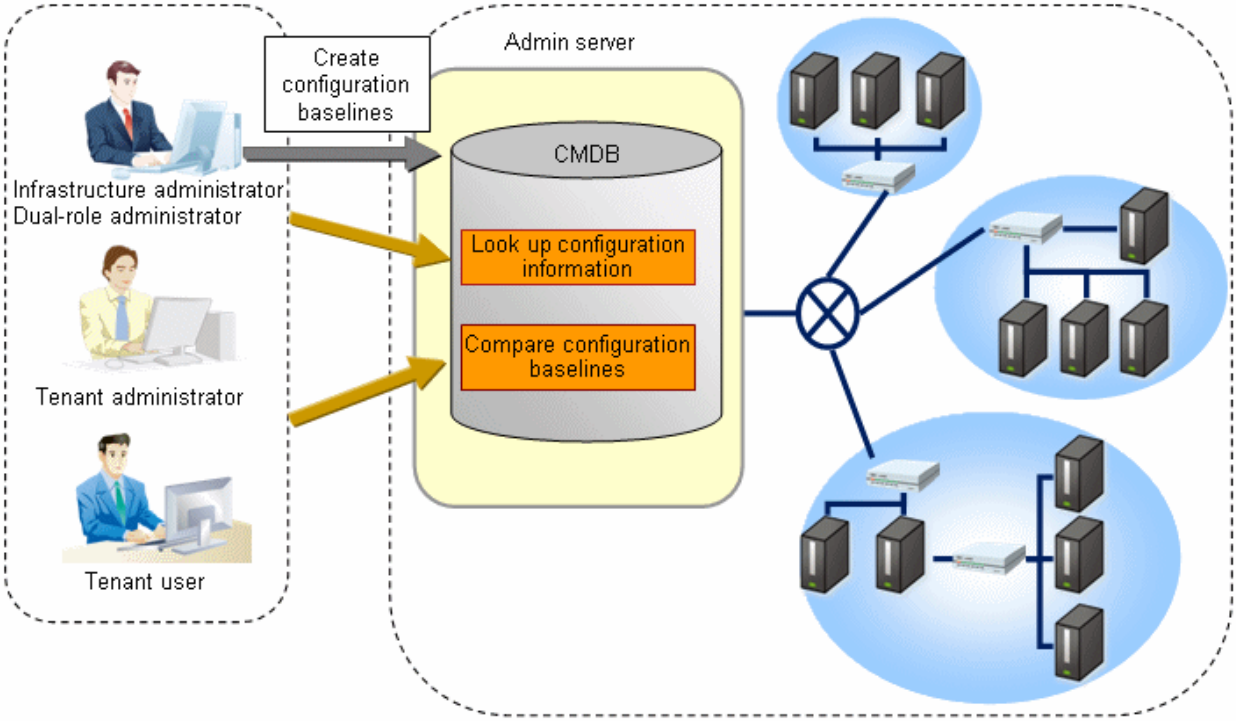
- Comparing configuration baselines

  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 1.4 Overview of configuration management



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	Looking up 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

Chapter 2 Operation Setup

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

2.1 Setup for Patch Management

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

2.1.1 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]

/opt/FJSVswcfmg/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. 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 that the infrastructure administrator recommends applying, but for which a tenant user can cancel the application if they judge that it may 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

Item	Description
	- 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

2.1.2 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.

2.2 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 patch distribution/application)

2.2.1 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.

2.2.2 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.

2.2.3 Email Template Files (for Patch Distribution/Application)

If an event has occurred during patch distribution or application processing, an email will be sent to the user for whom the patch has been distributed or applied.

Table 2.1 The emails that are sent with patch distribution/application processing, and their triggers

Email subject	Email description	Trigger for the email to be sent
Notification of failure to start the automated operation process for patch distribution and application	Indicates that patch distribution or application has failed.	When patch distribution/application is requested

Email subject	Email description	Trigger for the email to be sent
Notification of acceptance for patch distribution requests	Indicates that a patch distribution request has been received, and processing has started.	After the request is issued
Notification of acceptance for patch application requests	Indicates that a patch application request has been received, and processing has started.	After the request is issued
Schedule cancelation notification	Indicates that the schedule has been canceled, and processing has terminated.	After schedule cancelation is executed
Server error notification	Indicates that the server to which the patch is to be distributed or applied is in an abnormal state.	When server operations are found to be abnormal
Pre-execution script error notification	Indicates that the pre-execution script processing has failed.	When the pre-application script is executed
Patch distribution/application failure notification	Indicates that patch distribution or application has failed.	When patch distribution/application processing is executed
Post-execution script error notification	Indicates that the post-execution script processing has failed.	When the post-application script is executed
Restart failure notification	Indicates that restart has failed after patch distribution or application.	When patch distribution and application is followed by restart processing failure
Post-processing failure notification	Indicates that post-processing has failed.	When post-processing is performed
Notification of patch distribution completion	Indicates that patch distribution has completed.	When patch distribution has completed
Notification of patch application completion	Indicates that patch application has completed.	When patch application has completed
Notification of patch distribution/ application cancellation	Indicates that either patch distribution/ application processing has been canceled, or a timeout has occurred.	When "cancel" is selected by the user, or a timeout occurs

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

2.3 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]

/opt/FJSVswcfmg/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

2012-07-15, There will be maintenance for related networks over the weekend. 2012-07-10, A new patch has been released. 2012-07-02, 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. Check that ServerView Resource Orchestrator is running.

   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.

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.

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 log 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	This log contains audit logs.	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	This log contains trace logs for the management console.	10 MB	10 generations (*1)
cfmgbase_trace_log	This log contains trace logs for the manager itself.		
cfmgdiscovery_trace_log	This log contains trace logs for the discovery function.		
cfmgcommand_trace_log	This log contains trace logs for the following commands: - Status display command - Start command - Stop command - Email resend command - Backup command - Restore command - Problem investigation data collection command		
cfmgcommand_discovery_trace_log	This log contains the following trace logs: - Information that is output when all information is collected using the patch information update command		
cfmgcommand_discovery_wsus_trace_log	This log contains the following trace logs: - Information that is output when only WSUS information is collected using the patch information update command		
cfmgcommand_discovery_yum_trace_log	This log contains the following trace logs:		

Log name	Description	Size	Number of generations
	- Information that is output when only yum information is collected using the patch information update command		
cfmgcommand_discovery_fjmw_trace_log	This log contains the following trace logs: - Information that is output when only Fujitsu middleware information is collected using the patch information update command		
Event log (Windows)	This log contains information such as information about errors that occurs while patch application status information for deployed servers is being collected.	-	-
Syslog (Linux)	This log 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 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

Item	Description
Operation result	"SUCCESS" if the operation was successful and "FAILURE" if the operation failed

Operation type

Operation type	Description
/managerview/login.json	Login
/managerview/logout.json	Logout
/managerview/userInfo.json	Acquiring user information
/managerview/org/list.json	Acquiring a list of tenants
/managerview/ls/list.json	Acquiring a list of servers
/managerview/ls/map.json	Acquiring the map of unapplied patches
/managerview/ls/copy.json	Copying a list of servers
/managerview/ls.json	Acquiring server details
/managerview/info/list.json	Acquiring notifications
/managerview/windows.csv	Outputting Windows patch information to a CSV file
/managerview/patch/windows/list.json	Acquiring a list of Windows patches
/managerview/patch/windows/map.json	Acquiring the map of servers with unapplied Windows patches
/managerview/windows.json	Acquiring Windows patch details
/managerview/patch/copy.json	Copying a list of Windows patches
/managerview/patch/linux.csv	Outputting Linux patch information to a CSV file
/managerview/patch/linux/list.json	Acquiring a list of Linux patches
/managerview/patch/linux/map.json	Acquiring the map of servers with unapplied Linux patches
/managerview/patch/linux.json	Acquiring Linux patch details
/managerview/wsus.json	Refresh
/managerview/patchType/list.json	Acquiring a list of patch types
/managerview/patchSummary/list.json	Acquiring a summary of patches
/managerview/midPatch.csv	Outputting Fujitsu middleware patch information to CSV file
/managerview/midPatch/list.json	Acquiring a list of Fujitsu middleware patches
/managerview/midPatch/map.json	Acquiring the map of servers with unapplied Fujitsu middleware patches
/managerview/midPatch.json	Acquiring details on Fujitsu middleware patches
/managerview/baseLine/list.json	Acquiring a list of configuration baselines
/managerview/baseLine/patchComp.json	Comparing Windows patches
/managerview/baseLine/linux/patchComp.json	Comparing Linux patches
/managerview/baseLine/midPatchComp.json	Comparing Fujitsu middleware patches
/managerview/software/list.json	Acquiring a list of software programs
/managerview/software.json	Acquiring software details
/managerview/appliedPatch.csv	Outputting patch application information to a CSV file
/managerview/appliedPatch.do	Applying patches

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="C:\ProgramData \Fujitsu\SystemwalkerCF\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 "MGRV". - The prefix for cfmgbase_trace_log is "BASE". - The prefix for cfmgdiscovery_trace_log is "DISCOVERY".	
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="C:\ProgramData\Fujitsu\SystemwalkerCF\logs\managerview_trace_log" /> element under the <appender name="managerviewtrace" class="org.apache.log4j.RollingFileAppender"> element
cfmgbase_trace_log		The <param name="File" value="C:\ProgramData\Fujitsu\SystemwalkerCF\logs\cfmgbase_trace_log" /> element under the <appender name="cfmgbasetrace" class="org.apache.log4j.RollingFileAppender"> element
cfmgdiscovery_trace_log		The <param name="File" value="C:\ProgramData\Fujitsu\SystemwalkerCF\logs\cfmgdiscovery_trace_log" /> element under the <appender name="cfmgdiscoverytrace" class="org.apache.log4j.RollingFileAppender"> element
cfmgcommand_discovery_trace_log	<*Systemwalker Software Configuration Manager installation directory*>\SWCFMGM\config\manager_log4j.xml	The <param name="File" value="C:\ProgramData\Fujitsu\SystemwalkerCF\logs\cfmgcommand_discovery_trace_log" /> element under the <appender name="cfmgbasetrace" class="org.apache.log4j.RollingFileAppender"> element
cfmgcommand_trace_log		The <param name="File" value="C:\ProgramData\Fujitsu\SystemwalkerCF\logs\cfmgcommand_trace_log" /> element under the <appender name="cfmgcommandtrace" class="org.apache.log4j.RollingFileAppender"> element
cfmgcommand_base_trace_log		The <param name="File" value="C:\ProgramData\Fujitsu\SystemwalkerCF\logs\cfmgcommand_base_trace_log" /> element under the <appender name="cfmgbasetrace" class="org.apache.log4j.RollingFileAppender"> element
cfmgcommand_discovery_trace_log	<*Systemwalker Software Configuration Manager installation directory*>\SWCFMGM\config\manager_discovery_log4j.xml	The <param name="File" value="C:\ProgramData\Fujitsu\SystemwalkerCF\logs\cfmgcommand_discovery_trace_log" /> element under the <appender name="cfmgbasetrace"class="org.apache.log4j.RollingFileAppender"> element
cfmgcommand_discovery_wsus_trace_log	<*Systemwalker Software Configuration Manager installation directory*>\SWCFMGM\config\manager_discovery_wsus_log4j.xml	The <param name="File" value="C:\ProgramData\Fujitsu\SystemwalkerCF\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="C:\ProgramData\Fujitsu\SystemwalkerCF\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_fjmw_trace_log	<*Systemwalker Software Configuration Manager installation directory*>\SWCFMGM\config\manager_discovery_fjmw_log4j.xml	The <param name="File" value="C:\ProgramData\Fujitsu\SystemwalkerCF\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
cfmgbase_trace_log		The <param name="File"value="/var/opt/FJSVcfmgm/logs/cfmgbase_trace_log" /> element under the <appender name="cfmgbasetrace"class="org.apache.log4j.RollingFileAppender"> element
cfmgdiscovery_trace_log		The <param name="File"value="/var/opt/FJSVcfmgm/logs/cfmgdiscovery_trace_log" /> element under the <appender name="cfmgdiscoverytrace"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_base_trace_log		The <param name="File"value="/var/opt/FJSVcfmgm/logs/cfmgcommand_base_trace_log" /> element under the <appender name="cfmgbasetrace"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
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.

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 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]

<*ServerView Resource Orchestrator installation directory*>\SVROR\\SWRBAM\CMDB\\FJSVcmdbm\var\log\audit\audit.log

[Linux]

/opt/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","",""
```

4.1.3 Audit Logs for Patch Distribution/Application Processing

When patch distribution and application processing is performed from the management console, the content of the operations performed in the **Task management** window is output as audit logs.

How to use audit logs

To collect audit logs for patch distribution and application processing, execute the process instance audit information acquisition command below.

[Windows]

```
<ServerView Resource Orchestrator installation directory>\SWRBAM\bin\swrba_audit
```

[Linux]

```
/opt/FJSVswrbam/bin/swrba_audit
```

The audit information that can be acquired for process instances is information about process instances that have completed since the last time the command was executed.

Privilege required/execution environment

[Windows]

- Administrator privileges are required. When using Windows Server 2008 operating system, run as an administrator.
- This command can be executed on the admin server.

[Linux]

- System administrator (superuser) privileges are required.
- This command can be executed on the admin server.

Output file

The following table shows the file name, file size and number of generations for audit logs:

Log name	Description	File size	Number of generations
swrba_audit.log	This log contains audit logs.	10 MB	10 generations (*1)

*1:

- The file switches to a new generation when the size of the file reaches 10 MB.
  Even if the swrba_audit command is executed multiple times, information will be output to the same file, so long as the size of the file is less than 10 MB.
- Once 10 generations (or 100 MB) are exceeded, the oldest file (swrba_audit9.log) is deleted.

Output destination

The output destination for logs is shown below.

[Windows]

Output destination	Output file
<*ServerView Resource Orchestrator installation directory*>\SWRBAM \var\audit	swrba_audit[n].log (where "n" is the number of generations)

[Linux]

Output destination	Output file
/opt/FJSVswrbam/var/audit	swrba_audit[n].log (where "n" is the number of generations)

Output format

Audit logs are CSV format files, with the following items output in the following order.

Information about a single process instance is displayed as a single record.

<Time when the process instance started>,<Person who started the process instance>,<Name of the process instance>,<Process instance state>,<Time when the process instance ended>,<Activity name>,<Task execution date/time>,<Person in charge>,<Status>,<Task processing>,...,<Task result>

Item	Description
Time when the process instance started	The time when the application was submitted
Person who started the process instance	The user ID of the person who submitted the application
Name of the process instance	Name of the process instance - Patch application request_xxx - Patch distribution request_xxx
Process instance state	State of the process instance closed: Indicates that the process instance has completed
Time when the process instance ended	Time when the process instance ended yyyy-mm-dd hh:mm:ss.sss
Activity name	Activity name - Patch application acceptance

Item	Description
	- Patch distribution acceptance - Schedule cancelation - Server check for normal operation - Server error check - Pre-execution script error check - Post-execution script error check - Patch application failure check - Patch distribution failure check - OS restart failure check - Pre-execution script transfer - Post-execution script transfer - OS patch application - OS restart - Patch application completion check - Directory creation - Directory deletion - Service/process start check
Task execution date/time	The date/time when the task was executed
Person in charge	The user ID of the user that executed the task
Status	The status of the task COMPLETED: Indicates that the task has completed
Task processing	Name of the button used to execute the activity - apply - distribute - Successful - Retry - Continue - Cancel - Distribution complete - Application complete - Normal operation - Running
Task result	The result of the submitted application - Exit - Successful - Failed - Patch applied successfully

Item	Description
	- Patch distributed successfully - Server operating normally - Server error

Output example

```
"2012-05-09 16:44:10.830","user1","Patch application
request_Server1(VZG0D8L02O0001)_143312","closed","2012-05-09 17:04:02.857","Patch application
acceptance","2012-05-0916:44:12.138","111004","COMPLETED","apply","Exit"
```

Point

By using the scheduling function provided by the operating system (such as Task Scheduler for Windows or cron for Linux) to set up a schedule so that the process instance audit information acquisition command is executed at regular intervals, the audit logs for the process instances that have executed in between the last time the command was executed and the current command execution will be collected.

4.2 Backing up the Admin Server

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

Systemwalker Software Configuration Manager must be stopped before backing up data.

4.2.1 Backing up the Resources for ServerView Resource Orchestrator

Back up the resources for ServerView Resource Orchestrator. To back up CMDB assets, perform an offline backup. CMDB assets are not backed up by online backups. Refer to "Backup and Restoration of Admin Servers" in the *ServerView Resource Orchestrator Cloud Edition Operation Guide* for details.

4.2.2 Backing up Various Configuration Files

To back up user assets, use the following command from a command prompt. Refer to "Command Reference" in the *Reference Guide* for information on this command.

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 Backing up the Media Library

The Systemwalker Software Configuration Manager repository stores assets associated with Fujitsu middleware patches.

To back up the media library, use the following command from a command prompt. Refer to "Command Reference" in the *Reference Guide* for information on this command.

Command name	Overview
swcfmg_repository_backup	This command backs up the media library.

Note

- User assets must be backed 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.

4.3 Restoring the Admin Server

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

Systemwalker Software Configuration Manager must be stopped before restoring data.

4.3.1 Restoring the Resources for ServerView Resource Orchestrator

Refer to "Backup and Restoration of Admin Servers" in the *ServerView Resource Orchestrator Cloud Edition Operation Guide* for information on how to restore the resources for ServerView Resource Orchestrator.

4.3.2 Restoring Various Configuration Files

To restore user assets, use the following command from a command prompt. Refer to "Command Reference" in the *Reference Guide* for information on this command.

Command name	Overview
swcfmg_restore	This command restores user assets.

Note

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

4.3.3 Restoring the Media Library

To restore the media library, use the following command from a command prompt. Refer to "Command Reference" in the *Reference Guide* for information on this command.

Command name	Overview
swcfmg_repository_restore	This command restores the media library.

Note

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

4.4 Changing the Systemwalker Software Configuration Manager Environment

4.4.1 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.

4.4.2 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 "2.1.2 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.

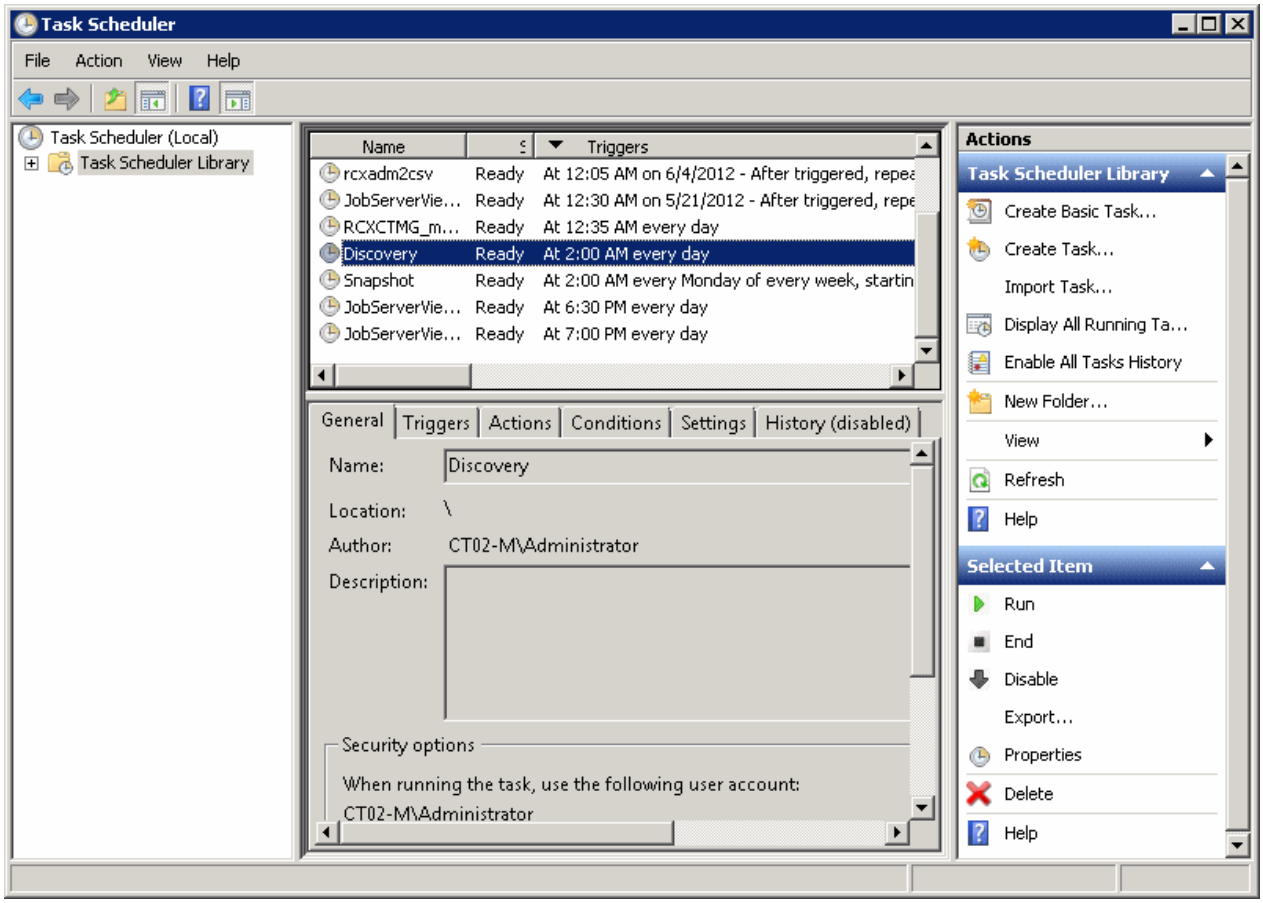
4.4.3 Changing Discovery Schedules and Configuration Baseline Creation Schedules

[Windows]

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

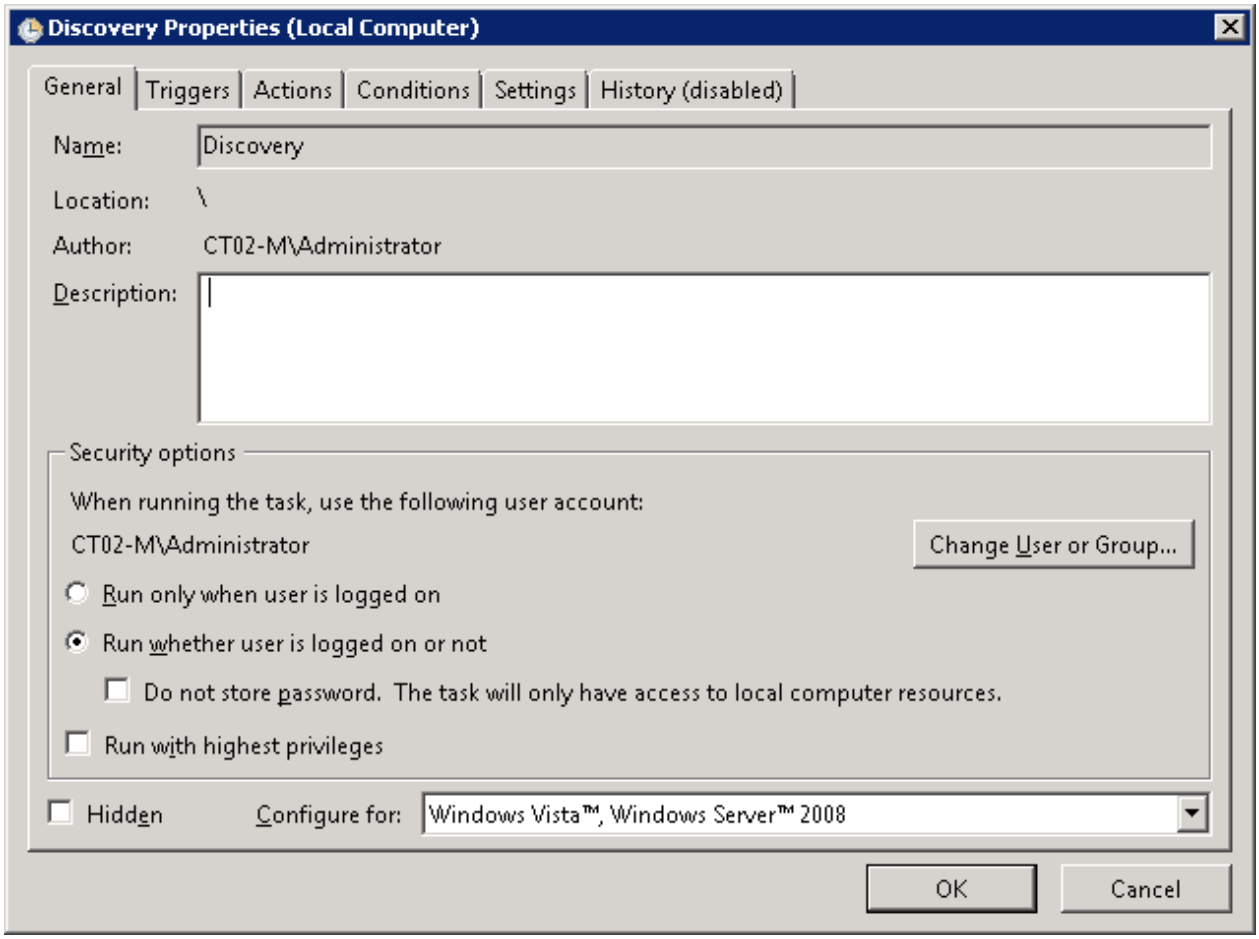
1. Log in to Windows using an account that belongs to the Administrators group.
2. Select **Start** >> **All Programs** >> **Administrative Tools** >> **Task Scheduler**.

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



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

   The properties of the task will be displayed.



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 everyday 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.

4.4.4 Moving 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, move the media library to resolve the disk space shortage.

The procedure for moving 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. Restart Systemwalker Software Configuration Manager.

   [Windows]

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

   [Linux]

   /opt/FJSVcfmgm/bin/swcfmg_start

4.5 Checking the Execution of Regular Discovery

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

Discovery for OS patches

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

For Linux, check whether 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.

4.6 Checking the Execution of Configuration Baseline Creation

Use the following method to check whether 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]

   ```
   %SWCMDB_INSTALL_PATH%\FJSVcmdbm\bin\snapview.exe -q num=all
   ```

   [Linux]

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

   [Execution example]

   [Windows]

   ```
   %SWCMDB_INSTALL_PATH%\FJSVcmdbm\bin\snapview.exe -q num=all
   Do you want to display the next? [y, n, all]
   all

   Snapshot Name             Create 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/FJSVcmdbm/bin/snapview.sh -q num=all
   Do you want to display the next? [y, n, all]
   all

   Snapshot Name             Create Date
   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. Check that the configuration baselines have been created exactly in accordance with the registered schedule.

   Check whether 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]

- The ServerView Resource Orchestrator service is not running.
- The Task Scheduler or cron are not running.

[Actions]

- Check that the ServerView Resource Orchestrator service is running.
- Review the schedule registration.