Systemwalker

Systemwalker
Software Configuration Manager

Technical Guide

Windows/Linux

B1X1-0126-04ENZ0(00)
January 2013

Preface

Purpose of this Document

This document explains the functions of Systemwalker Software Configuration Manager V15.1.1.

Intended Readers

This document is intended for those who are considering installing or want to understand the functions 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 Overview

This chapter provides an overview of Systemwalker Software Configuration Manager.

Chapter 2 Function Explanation

This chapter provides an overview of the functions of Systemwalker Software Configuration Manager.

Chapter 3 Operating Environment

This chapter provides an overview of the operating environment of Systemwalker Software Configuration Manager.

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) 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	
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, and Systemwalker are registered trademarks of Fujitsu Limited.

- 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.

- Microsoft, Internet Explorer, Hyper-V, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation 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).

Issue Date and Version

Version	Manual code
July 2012: First edition	B1X1-0126-02ENZ0(00) / B1X1-0126-02ENZ2(00)
July 2012: Second edition	B1X1-0126-03ENZ0(00) / B1X1-0126-03ENZ2(00)
January 2013: Third edition	B1X1-0126-04ENZ0(00) / B1X1-0126-04ENZ2(00)

Copyright

Contents

Chapter 1 Overview

This chapter presents an overview of the Systemwalker Software Configuration Manager product.

1.1 What is Systemwalker Software Configuration Manager?

Systemwalker Software Configuration Manager is a software product that manages software configuration information and patches for server software.

In recent years there has been a growing trend for the ICT department of a company to use virtualization to consolidate corporate servers in data centers, in order to improve cost competitiveness. However, the workload on system administrators is increasing, as it is no longer possible to keep up with dynamic changes or increasing server resources (such as IP addresses, operating systems, and middleware).

Systemwalker Software Configuration Manager makes it possible to automatically collect and manage information about resources that have been dynamically deployed to the cloud. Moreover, information about the status of the application of patches to servers can be managed centrally, thereby making it possible to reduce the workload for system administrators.

It is also possible to limit the range of which software configuration information is visible and which operations can be performed according to the tenancy that the administrator belongs to and the privileges of that administrator, thereby making it possible to prevent operation mistakes and reduce security risks.

🅿 Point

User roles

When explaining this product it is assumed that the user roles can be classified as follows:

Infrastructure administrator

- Infrastructure administrators set up and maintain Systemwalker Software Configuration Manager.

- Infrastructure administrators define policies for managing Windows patches, release the patches obtained from Microsoft Windows Server Update Services (WSUS), and determine classification levels.

- Infrastructure administrators obtain Linux patches and register them with Yellowdog Updater Modified (yum) repository servers.

- Infrastructure administrators obtain patches for Fujitsu middleware and register them with Systemwalker Software Configuration Manager.

- Infrastructure administrators can use the management console to look up patch application status and software configuration information for all the servers in the center.

Dual-role administrator

- Dual-role administrators act as both an infrastructure administrator and a tenant administrator.

Tenant administrator

- Tenant administrators can use the management console to look up patch application status and software configuration information for the servers within the tenancy that they belong to.

- Tenant administrators use the management console to apply patches to the servers within the tenancy that they belong to.

Tenant user

- Tenant users use the management console to apply patches to the servers that they manage.

- Tenant users can use the management console to look up patch application status and software configuration information for the servers that they manage.

Systemwalker Software Configuration Manager uses the following flow to manage patches and software configurations for servers:

1. Download patches

   This step involves downloading patches for the operating system and Fujitsu middleware from the vendor's website and the UpdateSite respectively.

   Patches for Windows operating systems are downloaded using Microsoft Windows Server Update Services (WSUS).

   Patches for Linux operating systems are downloaded and registered with Yellowdog Updater Modified (yum) repository servers by the infrastructure administrator.

   Patches for Fujitsu middleware are downloaded and registered with Systemwalker Software Configuration Manager by the infrastructure administrator.

2. Distribute and apply patches

   This step involves distributing and applying patches to business servers based on an instruction from the tenant user.

   Patches for Windows operating systems are distributed and applied by linking to Microsoft Windows Server Update Services (WSUS) based on a Systemwalker Software Configuration Manager operation.

   Patches for Linux operating systems are distributed and applied by linking to Yellowdog Updater Modified (yum) based on a Systemwalker Software Configuration Manager operation.

   Systemwalker Software Configuration Manager can also be used to distribute patches for Fujitsu middleware and apply these patches by registering scripts.

3. Perform discovery

   This step involves periodically and automatically collecting the patch application status and software configuration information for business servers from linkage servers, business servers and ServerView Resource Orchestrator, and then storing this information in the configuration management database (CMDB).

4. Monitor patch application and manage software configuration information

   This step involves checking the patch application status information that is discovered from linkage servers and business servers.

   Infrastructure administrators and dual-role administrators can check the patch application status and software configuration information for all the servers in the data center by logging in to the management console for Systemwalker Software Configuration Manager.

   Tenant administrators can check information for all the servers within their tenancy, whereas tenant users can check information for the servers that they manage themselves.

Figure 1.1 Overview of Systemwalker Software Configuration Manager
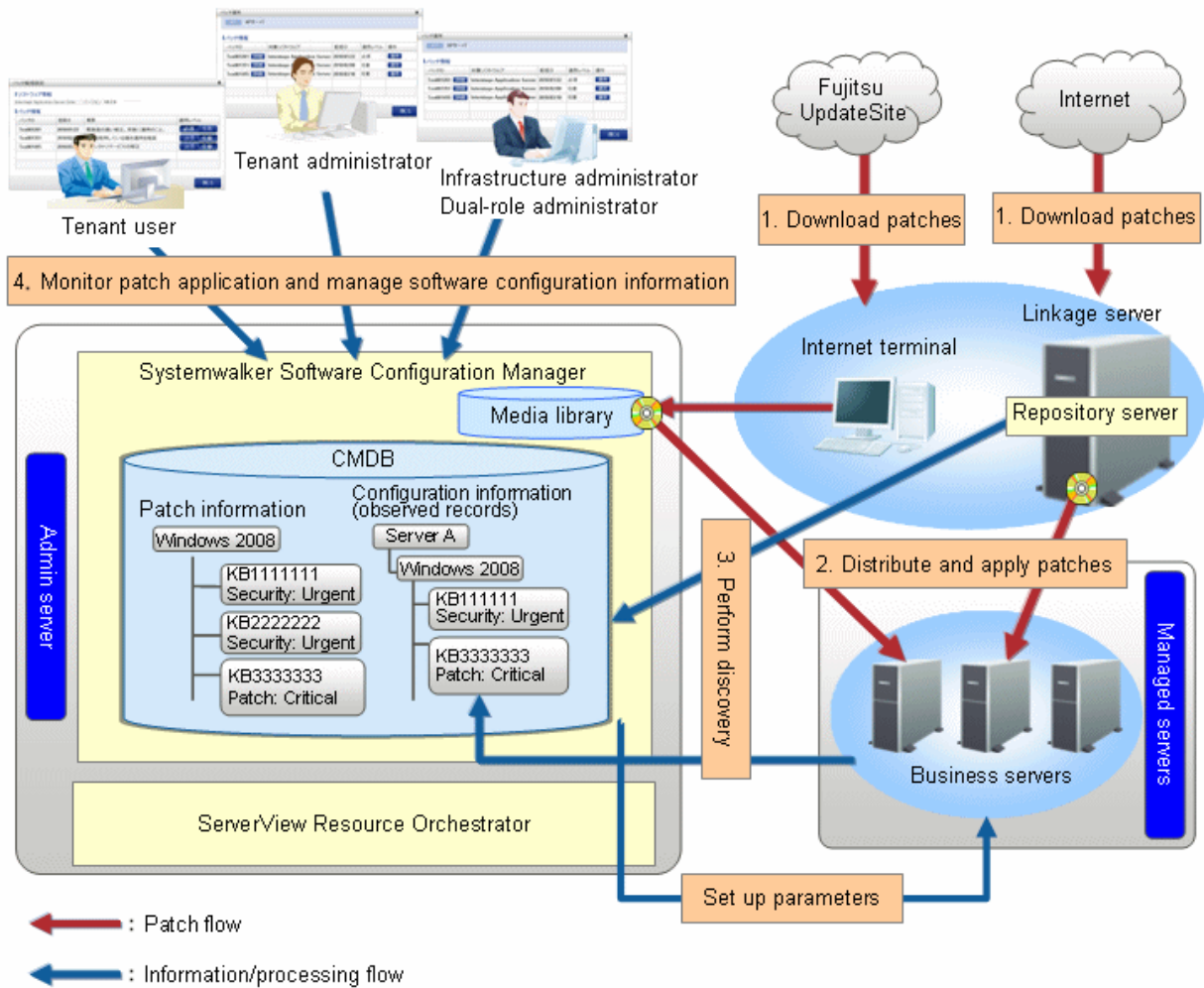
Information

ServerView Resource Orchestrator is a software product that automatically deploys physical and virtual servers.
Systemwalker Software Configuration Manager manages physical and virtual servers that have been deployed by ServerView Resource Orchestrator.

1.2 Features of Systemwalker Software Configuration Manager

Systemwalker Software Configuration Manager has the following features:

- **Discovery**

  Systemwalker Software Configuration Manager can collect and obtain patch application status and software configuration information for business servers.

- **Patch management**

  Systemwalker Software Configuration Manager can manage the patch application status of patches for Windows operating systems, Linux operating systems and Fujitsu middleware for business servers.

- **Configuration management**

  Systemwalker Software Configuration Manager can manage software configuration information for business servers using a configuration management database (CMDB).

- **Reporting**

   Systemwalker Software Configuration Manager can output various types of information in CSV format, including the results of applying patches to business servers and a list of servers with unapplied patches.

- **Software parameter settings**

   Systemwalker Software Configuration Manager can set up parameters for the software on an L-Platform when the L-Platform is deployed using ServerView Resource Orchestrator.

1.3 System Configuration

This section explains the system configuration for Systemwalker Software Configuration Manager.

1.3.1 System Configuration for Performing Patch Management and Configuration Management

The following diagram illustrates the system configuration for performing patch management and configuration management:

Figure 1.2 System configuration for performing patch management and configuration management
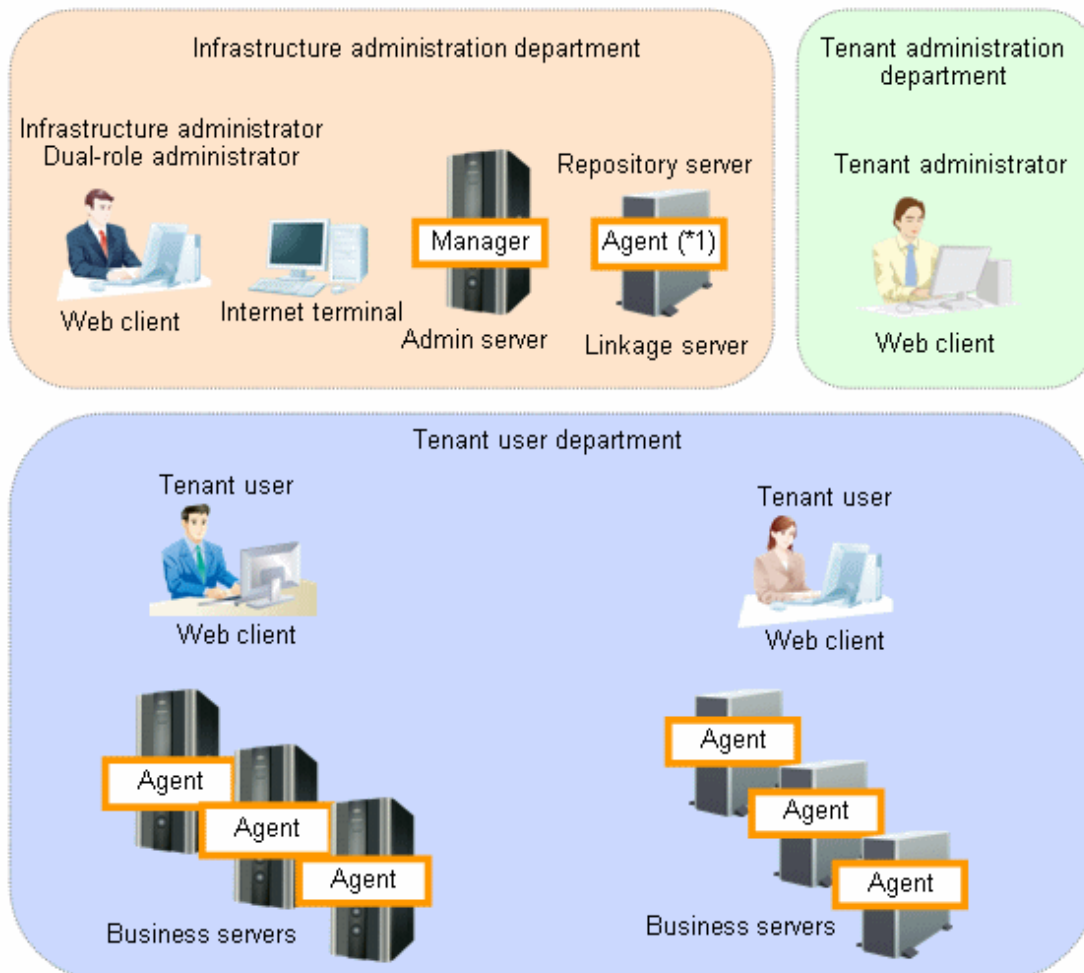
*1: A Systemwalker Software Configuration Manager agent must be installed when the repository server is using WSUS.

Admin server

This is the server where the manager of Systemwalker Software Configuration Manager runs. The admin server is used to obtain patch application status information, and to collect and manage software configuration information.

The manager of Systemwalker Software Configuration Manager is installed on the admin server.

The manager is a Systemwalker Software Configuration Manager program that runs on the admin server.

Linkage server

With Systemwalker Software Configuration Manager, the following servers are defined as linkage servers:

Repository server

A repository server is used to download patches from vendor websites, and store, distribute and apply these patches. This server is required to manage OS patches.

Microsoft Windows Server Update Services (WSUS) repository server

This server is used to download, distribute and apply Windows patches. This server can also manage the application status of Windows patches. This server is required to manage Windows patches.

A Systemwalker Software Configuration Manager agent is installed on WSUS servers.

An agent is a Systemwalker Software Configuration Manager program that runs on linkage servers and business servers.

Yellowdog Updater Modified (yum) repository server

A yum repository server is used to store, distribute and apply Linux patches (RPM packages). This server is required to manage Linux patches.

There is no need to install a Systemwalker Software Configuration Manager agent on yum repository servers.

Business server

This is a server from which software configuration information is collected and to which patches are applied.

Systemwalker Software Configuration Manager manages servers that have been deployed by ServerView Resource Orchestrator.

A Systemwalker Software Configuration Manager agent is installed on business servers.

An agent is a Systemwalker Software Configuration Manager program that runs on linkage servers and business servers.

Internet terminal

This is a terminal that is used to download the latest patches from the UpdateSite or vendor websites.

An Internet terminal is required to manage Linux patches and Fujitsu middleware patches.

Web client

This is a client for operating the Systemwalker Software Configuration Manager admin server. The management console is used in a web browser.

1.3.2 System Configuration for Setting up Software Parameters

The system configuration for setting up software parameters is the same as the system configuration for ServerView Resource Orchestrator, except that L-Servers must be connected to the admin server via an admin LAN.

Figure 1.3 System configuration for setting up software parameters
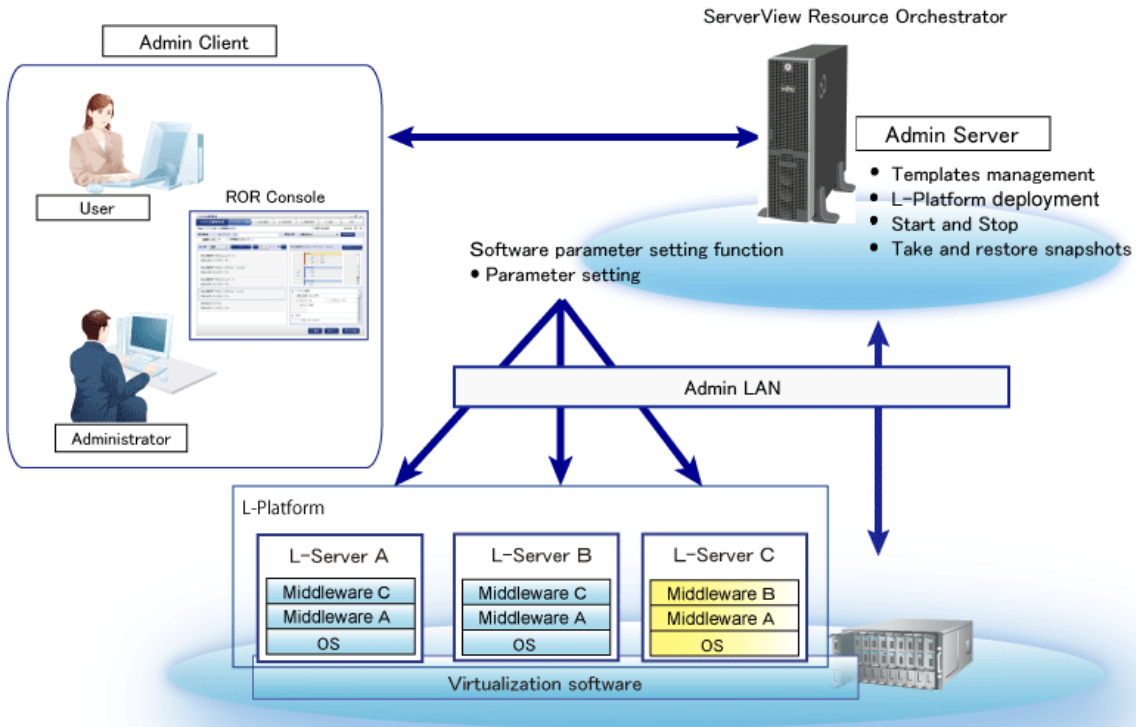
Admin server

This is the server where ServerView Resource Orchestrator runs. The software parameter settings function also runs on the admin server. This server is used to manage templates, deploy L-Platforms, and take and restore snapshots.

Admin client

This is a client for operating the ServerView Resource Orchestrator admin server.

Managed server

A managed server is used to operate server virtualization software such as VMware or Hyper-V. Managed servers are managed by the admin server.

L-Platform

An L-Platform is a resource that operates and manages an entire system that consists of multiple L-Servers, storage devices and network devices, such as in multi-tier systems (made up of web servers, application servers, and database servers).
L-Platforms are deployed on the server virtualization software for managed servers.

L-Server (business server)

An L-Server is a resource that defines the logical specifications (such as the number of CPUs, memory capacity, disk capacity, and the number of NICs) for a server, and for the storage and network devices connected to the server.

The software parameter settings function communicates with L-Servers that have been deployed in order to set up parameters for the software on the L-Servers. These communications take place via the admin LAN.

Admin LAN

The admin LAN is used to manage the managed servers and L-Servers from the admin server.

The admin LAN is set up separately from the public LAN that the managed servers and L-Servers use to perform operations.

To use the software parameter settings function, the admin server must be connected to L-Servers via an admin LAN.

1.4 Benefits of Installation

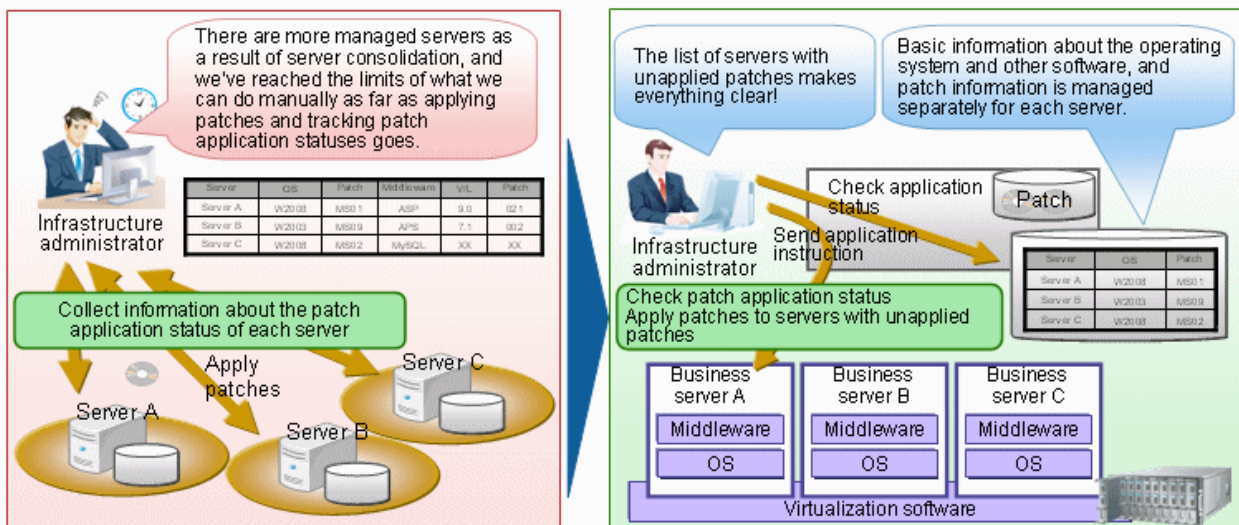Installing Systemwalker Software Configuration Manager provides the following benefits:

- Keep server patches up to date

- Automatically collect and visualize information about resources that have been automatically deployed to the cloud

- Ability to visualize software configuration information according to the tenant that the administrator belongs to and the privileges of that administrator

- Reduce system construction times and human error by using the software parameter settings function

Keep server patches up to date

Individual system administrators have to keep track of the software stack (operating systems, middleware and applications) and patch application status using Excel spreadsheets and other methods, and so it takes a long time to investigate the effects of making changes to software (such as applying security patches). As the number of systems increases, there is also the risk of systems that should be checked being missed. For an administrator to apply patches individually to each separate machine also requires a huge amount of work.

Installing Systemwalker Software Configuration Manager makes it possible to centrally manage software configuration information (including patch information) and display a list of servers with unapplied patches. For servers with unapplied patches, notification emails can be sent to tenant users instructing them to apply the patches.

Figure 1.4 Benefit 1 (Keeping server patches up to date)

Automatically collecting and visualizing information about resources that have been automatically deployed to the cloud

For resources that have been deployed to the cloud, such as servers and IP addresses, information changes dynamically, which means that checking all systems manually is monotonous and time-consuming, and the workload has a tendency to increase. It is also difficult to keep track of the status of resources in an accurate and timely manner, this can be due to patch application or cancellation of deployed resources.

By installing Systemwalker Software Configuration Manager, system information can be automatically "discovered" (detected and collected). This enables infrastructure administrators to keep track of software configuration information effectively, even for resources that have been deployed to cloud environments.

Figure 1.5 Benefit 2 (Automatically collecting and visualizing information about resources that have been automatically deployed to the cloud)
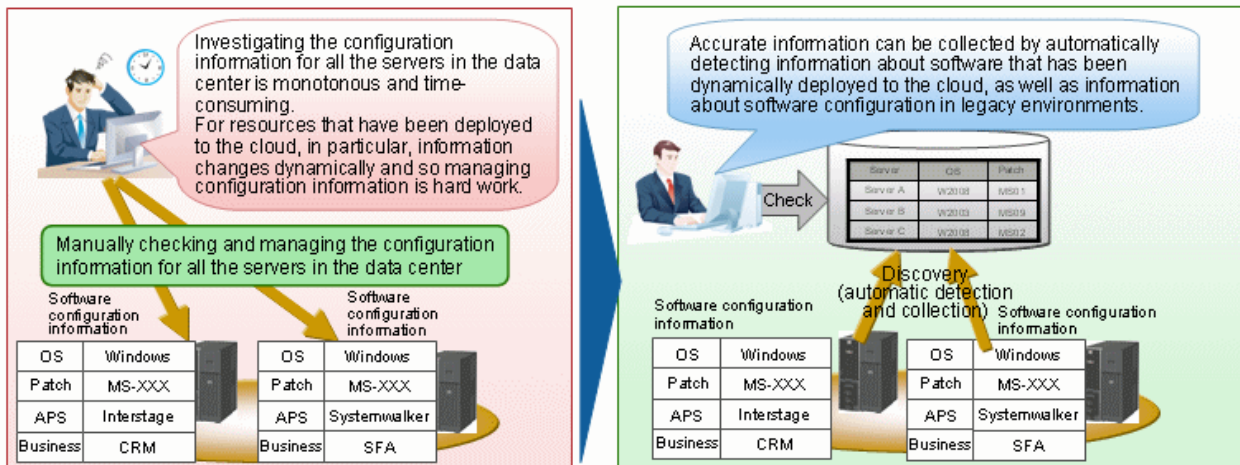
Visualizing software configuration information based on tenant and administrator privileges

Configuration management involves the collection of massive amounts of data, such as information about the systems in a data center. If an administrator can see and manipulate all the information in the configuration management system, there is a risk of operation mistakes resulting from the fact that administrators can perform operations beyond their area of responsibility, as well as information security risks due to information being made available without proper controls.

By installing Systemwalker Software Configuration Manager, both the range of information that can be viewed and the range of operations that can be performed can be limited according to tenant and administrator privileges. This can prevent operation mistakes and reduce security risk. Moreover, workloads can be reduced by having each person only handle the information that they are responsible for operating and maintaining.

Figure 1.6 Benefit 3 (Visualizing software configuration information based on tenant and administrator privileges)
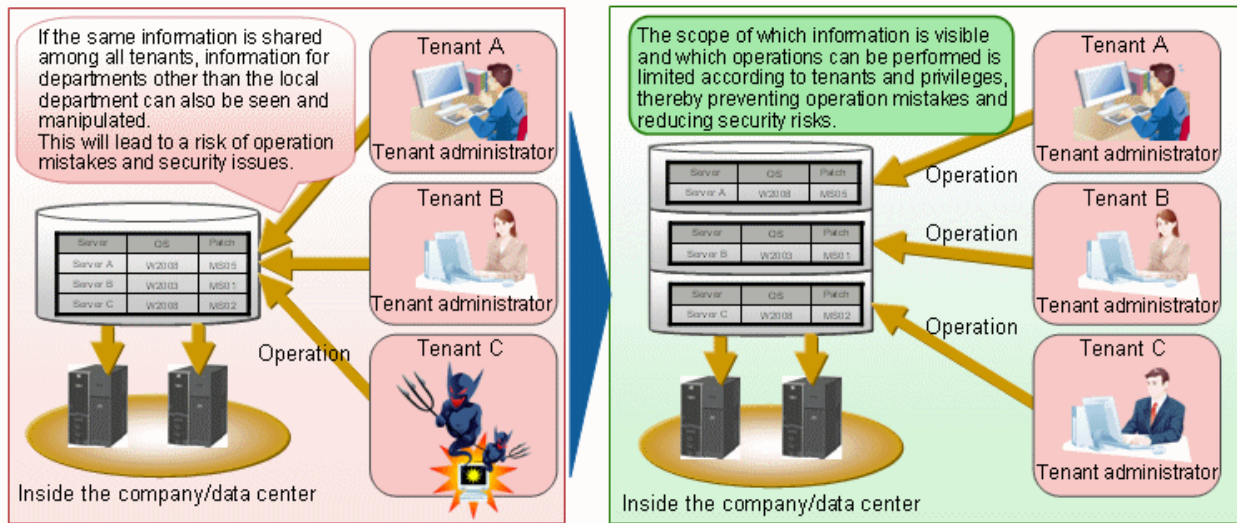

Reducing system construction times and human error by using the software parameter settings function

In systems where ICT resources have simply been consolidated in a private cloud, each department uses a different combination of operating systems, middleware and applications with different versions and levels, and so creating a cloud system involves a lot of work. Creating systems manually also introduces the possibility of human error.

The software parameter settings function is used to set up software parameters on an L-Platform (*1) when the L-Platform is deployed using ServerView Resource Orchestrator. Administrators can define software parameters as templates in advance. Then, when an L-Platform is deployed, the software parameters can be assigned automatically by simply selecting an appropriate template. This makes it possible to reduce the workload for infrastructure administrators and tenant administrators. Moreover, parameter information for multiple software programs can be defined for cloning images, reducing both the number of cloning images and the cost of managing them. Furthermore, software parameter information that has been defined for different L-Server usages can be automatically assigned when L-Platforms are deployed, so that tenant users can use L-Servers immediately.

*1: With ServerView Resource Orchestrator, logical platforms made up of multiple virtual servers, physical servers, storage devices, and network devices are referred to as "L-Platforms", whereas logical servers are referred to as "L-Servers".

Figure 1.7 Benefit 4 (Reducing system construction times and human error by using the software parameter settings function)
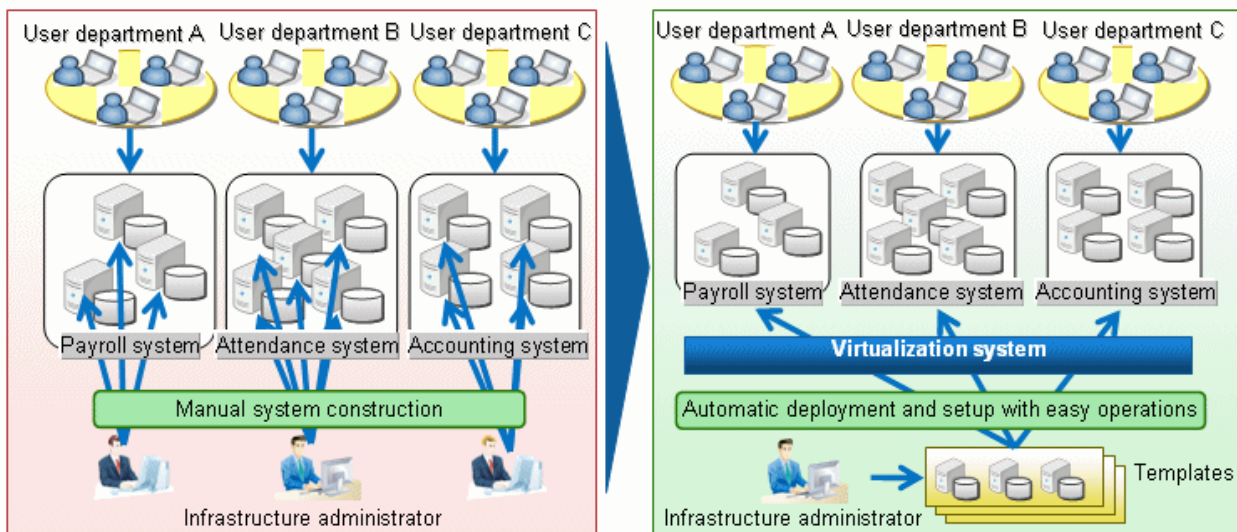
Chapter 2 Function Explanation

This product provides the following functions:

- Discovery

- Patch management

- Configuration management

- Software parameter settings

2.1 Discovery

"Discovery" is a function that collects software configuration information for business servers and registers it in the configuration management database (CMDB).

The software configuration information collected by the discovery function is registered in the CMDB as configuration items (CI).

Figure 2.1 Overview of the discovery function
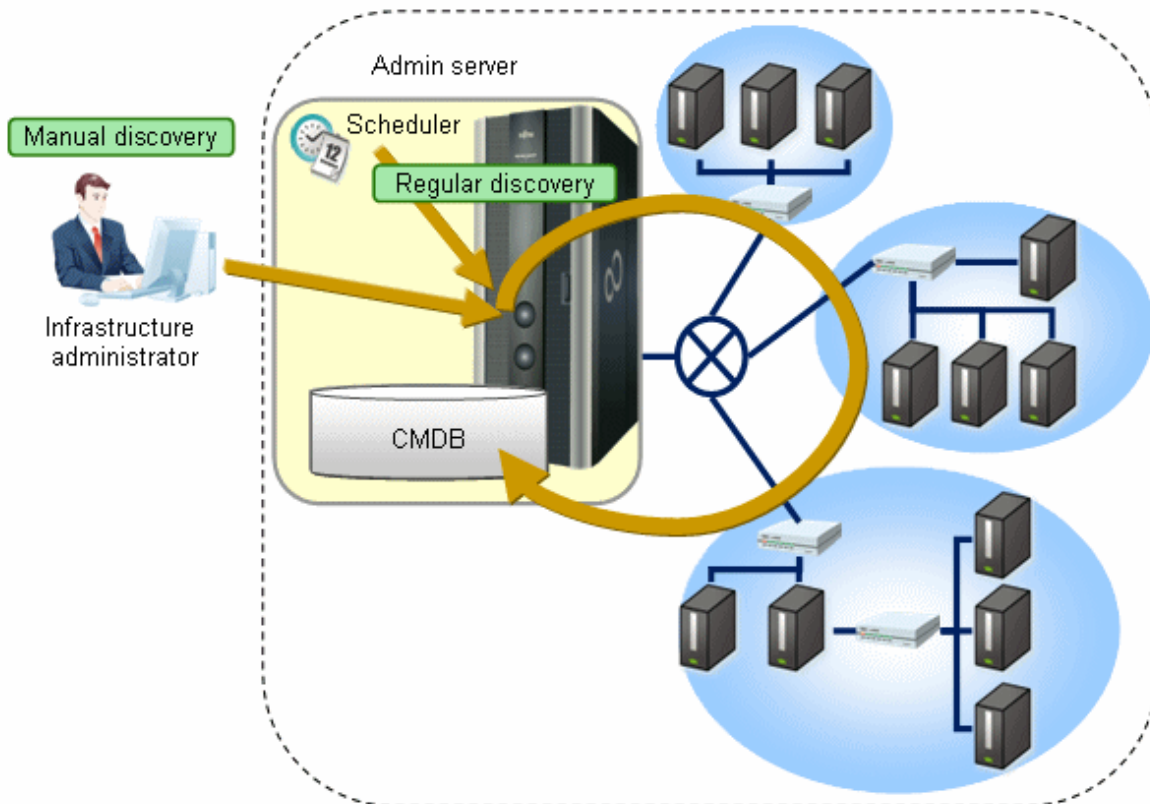
Software configuration information collected

The following software configuration information can be collected using the discovery function:

Table 2.1 Software configuration information collected by the discovery function

Resource				Required product	Linkage product/linkage function		
				ServerView Resource Orchestrator	Microsoft Windows Server Update Services (WSUS)	yum(Yellowdog Updater Modified)	UpdateAdvisor (middleware)
System configuration information	Resource information for the physical or virtual servers that make up the system (IP addresses and operating system information only)			Y	Y (*1)	Y (*1)	Y (*1)
	Tenant information			Y	-	-	-
	L-Platform information			Y	-	-	-
Patch information	Windows patches	Information about Windows patches released by Microsoft	OS patch information	-	Y	-	-
			Physical / virtual Windows servers where the patches can be applied	-	Y	-	-
		Information about the OS patches that have already been applied to the physical/virtual Windows servers that make up the system		-	Y	-	-
	Linux patches	Information about Linux patches (RPM packages) released by the Red Hat Network or the Fujitsu website	Information about OS patches (RPM packages)	-	-	Y	-
			Physical/ virtual Linux servers where the patches can be applied	-	-	Y	-
		Information about the OS patches (RPM packages) that have already been applied to the physical/ virtual Linux servers that make up the system		-	-	Y	-
	Middleware patches	Fujitsu middleware patches released on	Fujitsu middleware patches	-	-	-	- (*2)

Resource			Required product	Linkage product/linkage function			
			ServerView Resource Orchestrator	Microsoft Windows Server Update Services (WSUS)	yum(Yellowdog Updater Modified)	UpdateAdvisor (middleware)
		the UpdateSite	Physical/ virtual servers where the patches can be applied	-	-	-	- (*3)
		Information about the Fujitsu middleware patches that have already been applied to the physical/ virtual servers that make up the system		-	-	-	Y
Software information		Information about the Fujitsu middleware products that have already been installed on the physical/virtual servers that make up the system	-	-	-	Y

Y: Can be collected.

-: Cannot be collected.

*1: IP addresses only

*2: This information is not collected by the swcfmg_patch_updateinfo command. Information about Fujitsu middleware patches is registered in the CMDB by executing the swcfmg_fjmwpatch_update command (the Fujitsu middleware patch registration command). Refer to the *Reference Guide* for more details.

*3: This information is not collected by the swcfmg_patch_updateinfo command. If a tenant user or tenant administrator makes a patch distribution/application request, authorization information for the physical or virtual servers to which the patch can be applied will be registered in the CMDB. Refer to "Patch Management" in the *Operation Guide* for information on how to make patch distribution/ application requests.

The timing of discovery

Discovery is performed at the following times:

- Regular discovery

  Discovery is executed periodically according to a schedule.

- Manual discovery

  Discovery is manually performed by the infrastructure administrator executing a command.

Regular discovery

With regular discovery, the latest software configuration information is collected according to a schedule that the infrastructure administrator has defined in advance. The operating system's scheduler function is used for the schedule definition.

Figure 2.2 Regular discovery
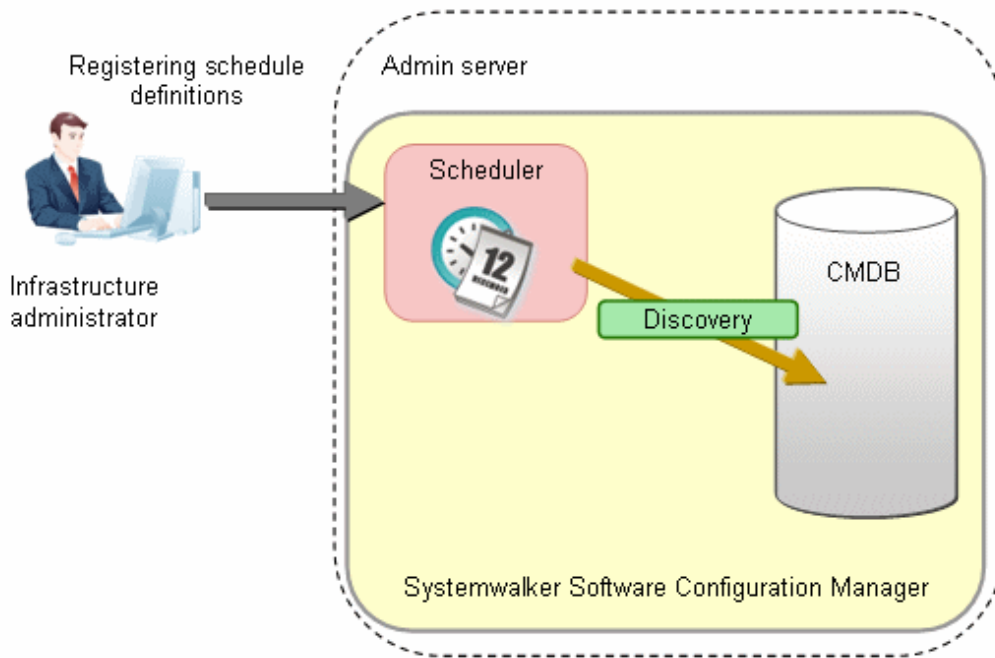
Manual discovery

With manual discovery, the infrastructure administrator collects the latest software configuration information by executing the swcfmg_patch_updateinfo command to perform discovery.

Figure 2.3 Manual discovery
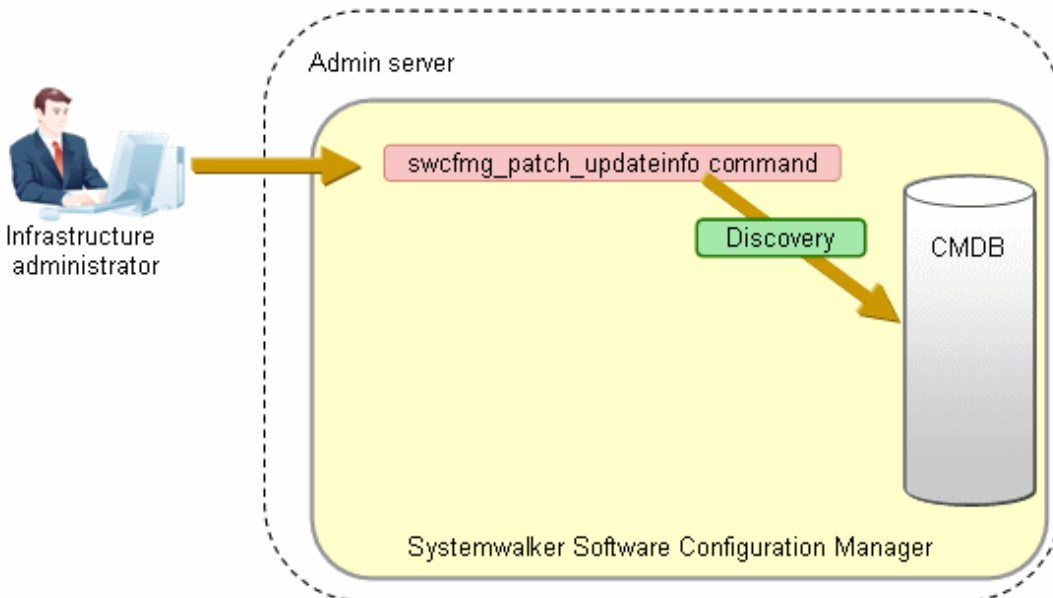
2.2 Patch Management

Systemwalker Software Configuration Manager manages the patch application status of each of the servers on the L-Platforms managed by ServerView Resource Orchestrator V3.

Systemwalker Software Configuration Manager manages the following patches:

- Windows patches

- Linux patches

- Fujitsu middleware patches

Windows patches

Windows patches are managed by linking to a WSUS repository server provided by Microsoft.

Acquisition of the latest patches and management of patch application status is performed via WSUS, while Systemwalker Software Configuration Manager automatically collects and manages information about patches and patch application statuses from WSUS.

It is also possible to apply patches to business servers remotely via the management console for Systemwalker Software Configuration Manager.

Linux patches

Linux patches are managed by linking to yum repository servers supported by Red Hat.

Acquisition of the latest patches and registration of the patches (RPM packages) with the yum repository server is performed by the infrastructure administrator, while Systemwalker Software Configuration Manager collects and manages patch application status information from each business server.

It is also possible to apply patches to business servers remotely via the management console for Systemwalker Software Configuration Manager.

Fujitsu middleware patches

Patch management for Fujitsu middleware is performed by linking to the UpdateSite and UpdateAdvisor (middleware) provided by Fujitsu.

Acquisition of the latest patches from the UpdateSite and registration of the latest patches with Systemwalker Software Configuration Manager is performed by the infrastructure administrator, while Systemwalker Software Configuration Manager collects and manages patch application status information from the UpdateAdvisor (middleware) on each business server.

It is also possible to distribute and apply update files to business servers remotely from the management console for Systemwalker Software Configuration Manager.

2.2.1 Windows Patch Management

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

Figure 2.4 Overview of Windows patch management

- : Processing by Microsoft Windows Server Update Services (WSUS)
- : Processing by Systemwalker Software Configuration Manager
- : Manual operation
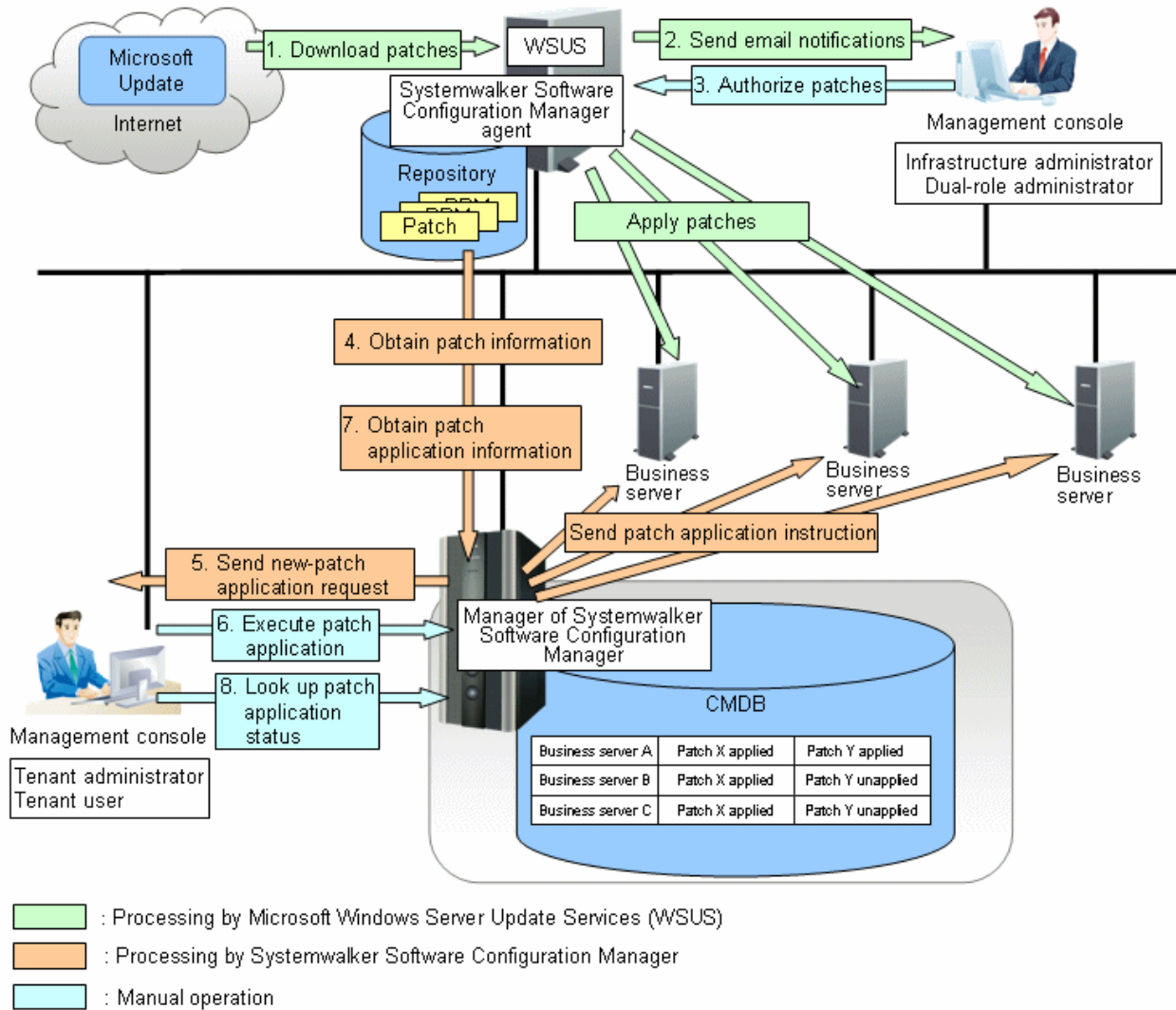
1. Download patches **[processing by WSUS]**

   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, an email will be sent from WSUS to the infrastructure administrator, informing him or her that a new patch has been downloaded from the Microsoft Update site.

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 obtained 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.

2.2.2 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 2.5 Overview of Linux patch management
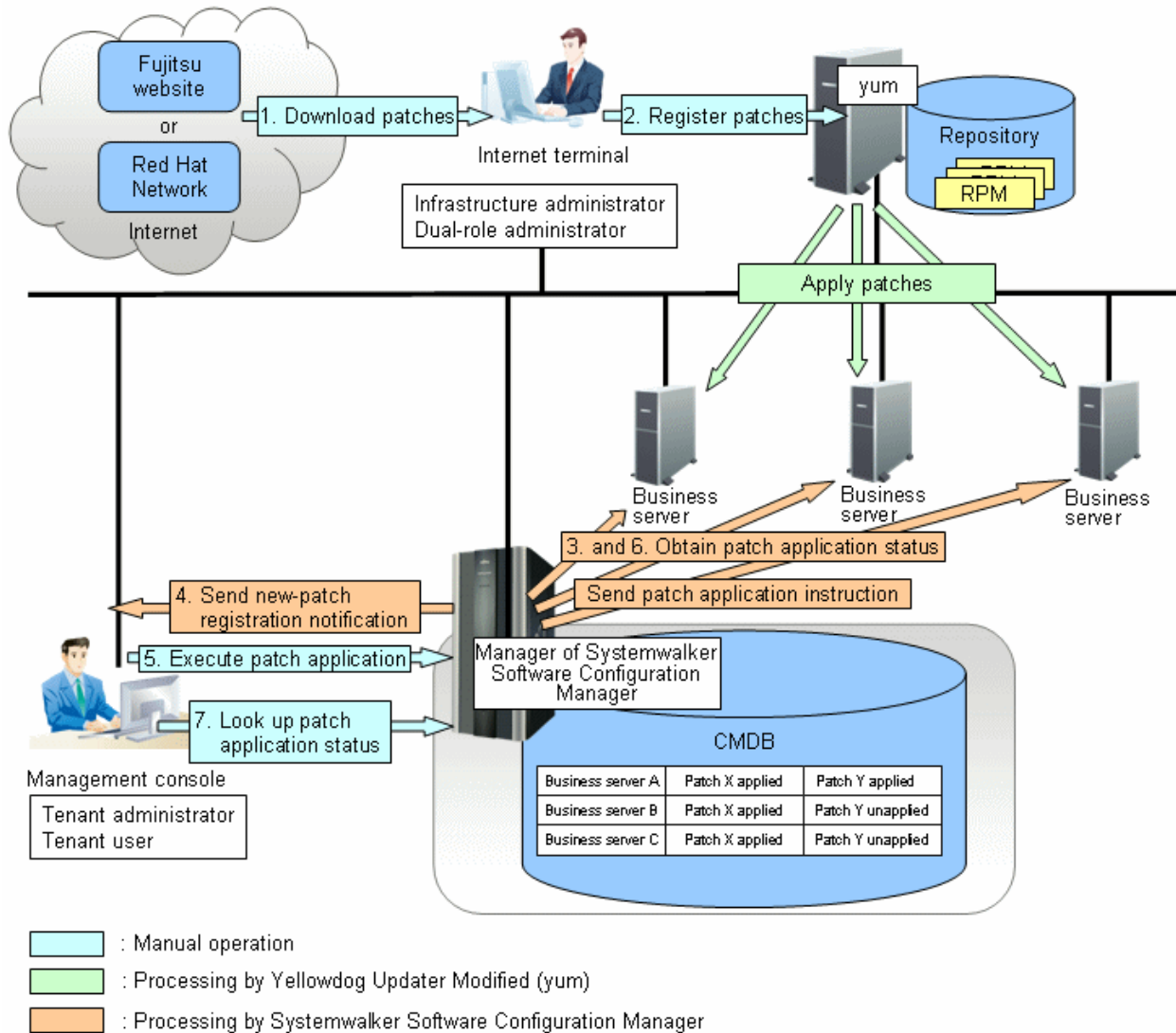
1. Download patches **[operation by the infrastructure administrator]**

   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 notification **[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.

2.2.3 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 2.6 Overview of Fujitsu middleware patch management
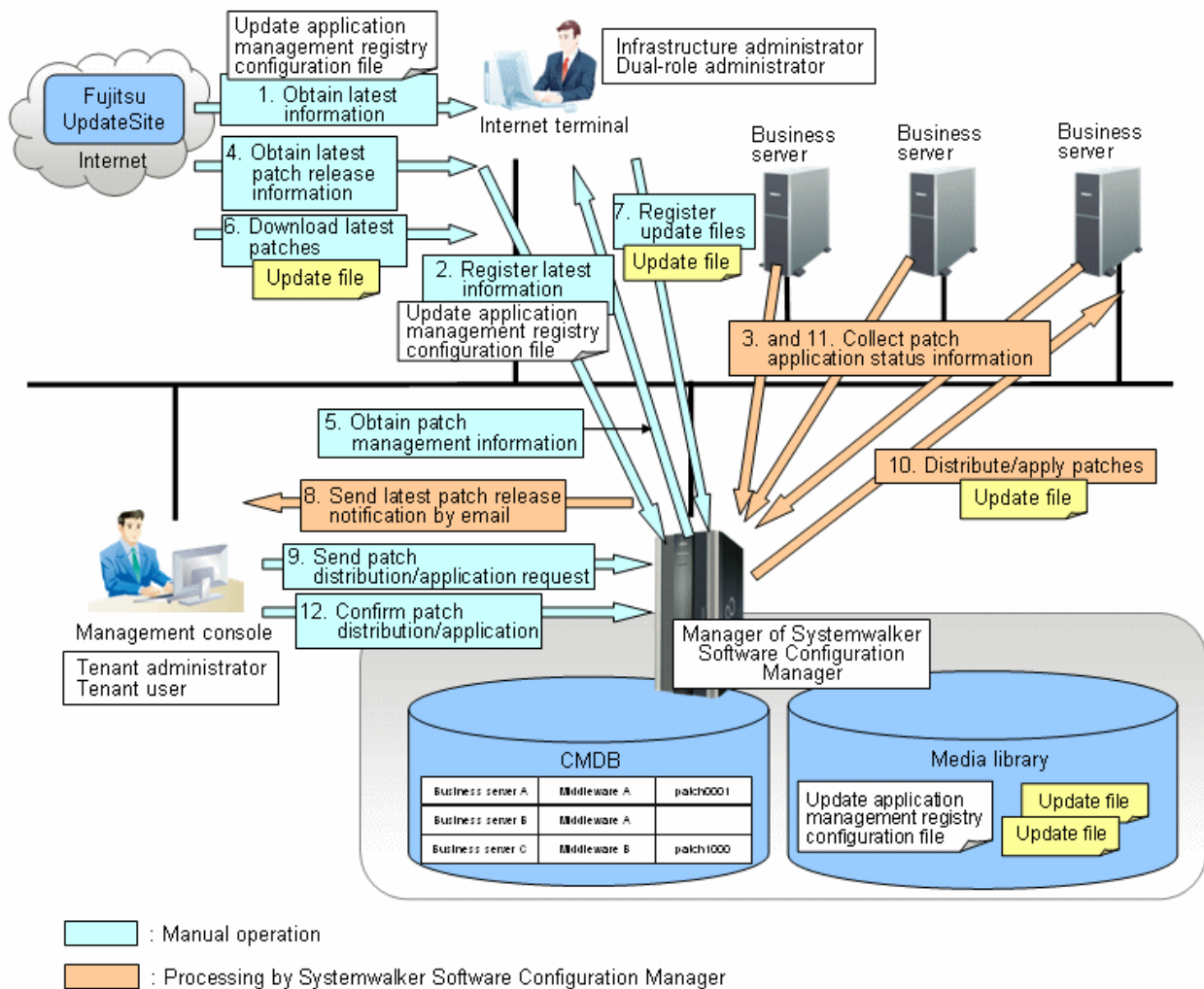
1. Obtain the latest information (update application management registry configuration file) **[operation by the infrastructure administrator]**

   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 (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 this update application management registry configuration file 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 (Fujitsu SupportDeskWeb) 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 and check the patch application status.

2.3 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 software configuration 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.

The following table shows the range within which each role can use configuration management:

Role	Usage range of software configuration information
Infrastructure administrator	Can look up software configuration information for all servers.
Dual-role administrator	Can look up software configuration information for all servers.
Tenant administrator	Can look up software configuration information for the servers associated with the tenancy (organization) to which the tenant administrator belongs.
Tenant user	Can look up software configuration information for the servers that the tenant user manages.

Figure 2.7 Overview of configuration management
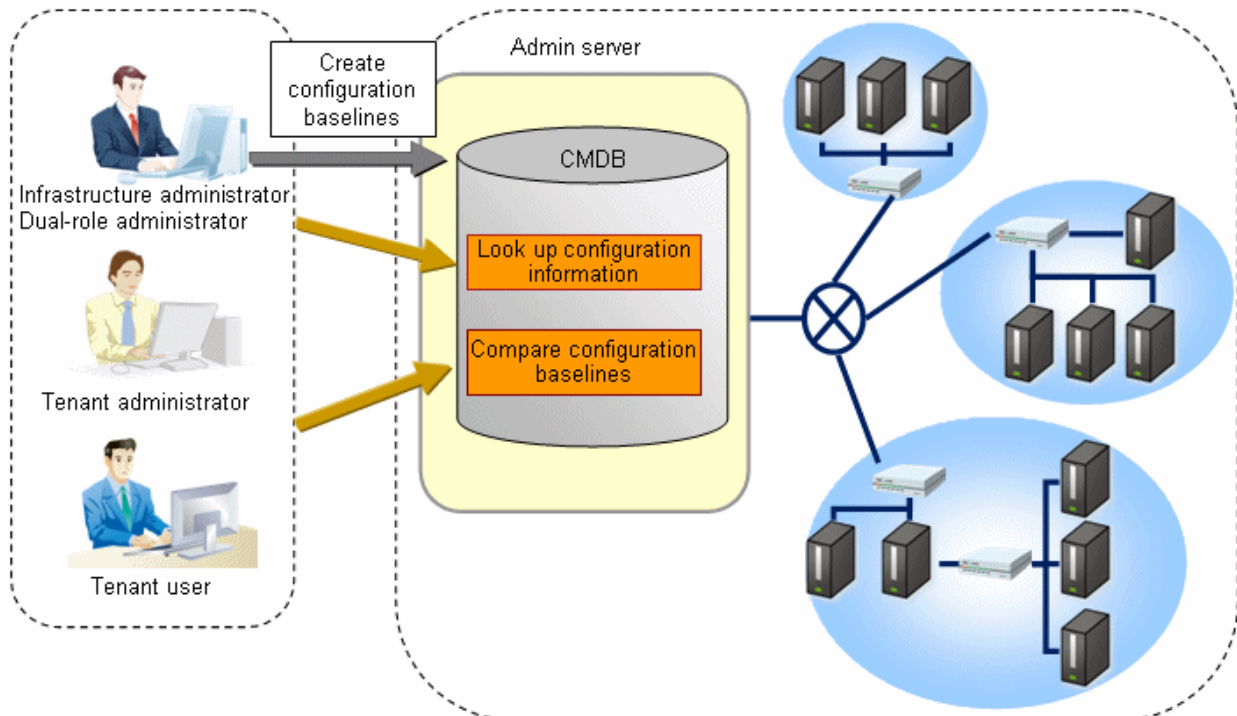
2.4 Software Parameter Settings

The software parameter settings function is used to set up parameters for the software on an L-Platform when the L-Platform is deployed using ServerView Resource Orchestrator. Automating software parameter settings reduces the workload for infrastructure administrators and tenant administrators. Moreover, parameter information for multiple software programs can be defined for cloning images, reducing both the number of cloning images and the cost of managing them. Furthermore, software parameter information that has been defined for different L-Server usages can be automatically assigned when L-Platforms are deployed, so that tenant users can use L-Servers immediately.

The software parameter settings function is provided as an additional function for ServerView Resource Orchestrator. In order to enable this function, the settings for ServerView Resource Orchestrator must be changed.

Also, to create cloning images, a procedure specific to this function must be followed. The rest of this section explains this additional function for ServerView Resource Orchestrator, and the procedures for using this function.

L-Platform management

In order to assign software parameters when L-Platforms are deployed, a function is added to the ROR console as part of L-Platform management.

- **Selecting the values for the parameters to be assigned**

    If an application to use an L-Platform is submitted using the **L-Platform** tab, the values of the parameters can be selected using the **Reconfigure** page. The parameter values and options can be defined using L-Platform templates.
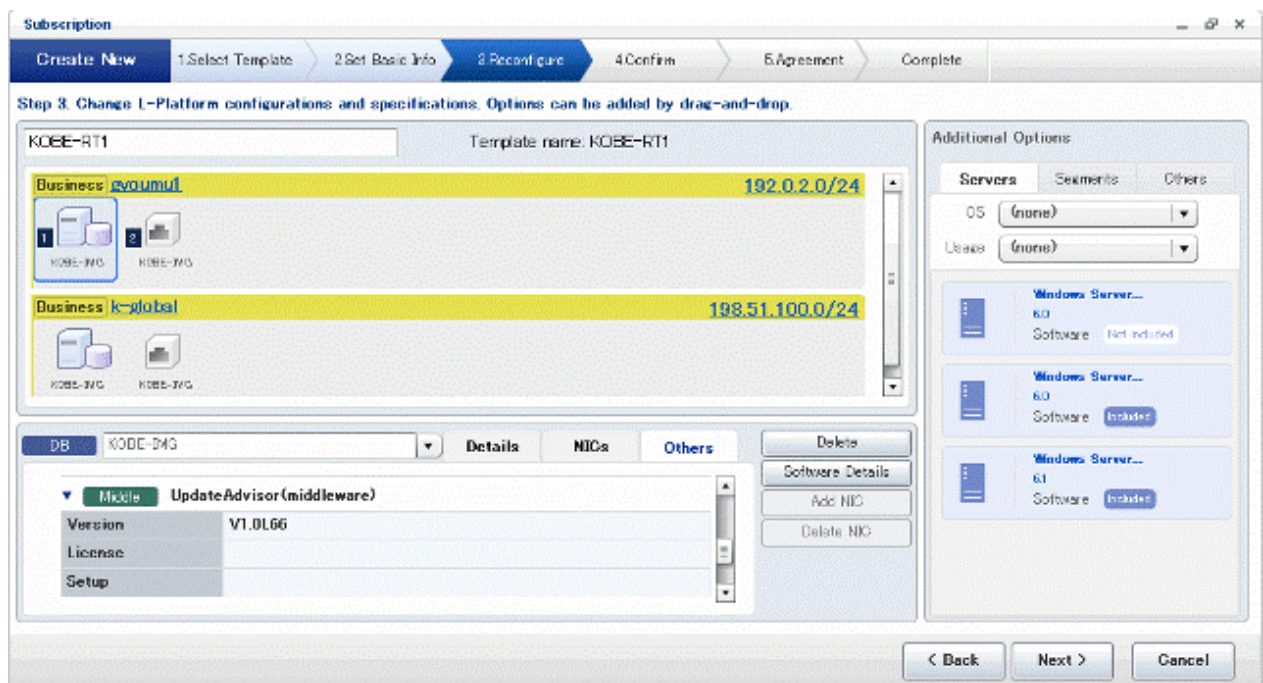
- **Setting up parameters when L-Platforms are deployed**

    When an application to use an L-Platform is submitted using the **L-Platform** tab, the parameters for the software on the L-Servers that are deployed as part of the L-Platform are assigned. At this point, the admin server communicates to the L-Servers that have been deployed in order to assign the parameters for the software.

L-Platform template management

The software parameters and the values set for these parameters are defined as part of the L-Platform template. To do this, a function is added to the ROR console and commands as part of L-Platform template management.
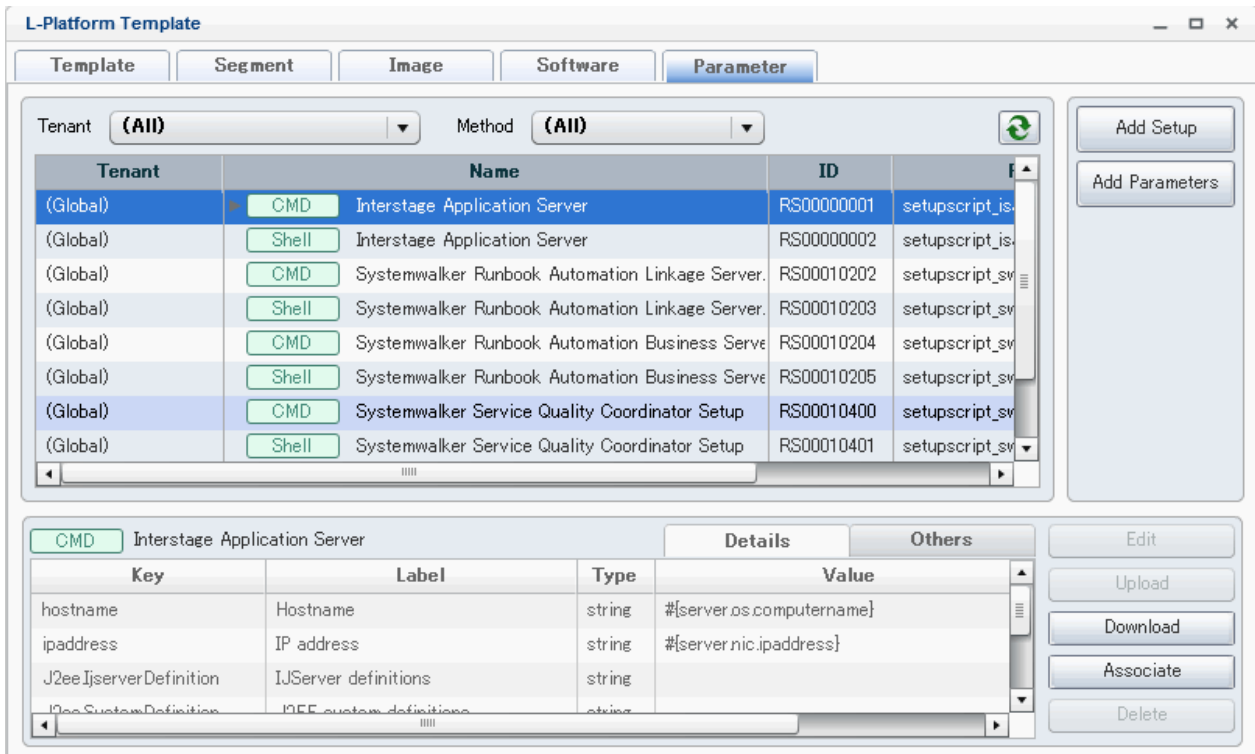
The following section explains the L-Platform templates associated with the software parameter settings function.

- **Software setup information**

    It is possible to define a list of the parameters that can be set for the software, as well as the method for setting these parameters. However, software setup information only defines the parameters. This means that it must be associated with the corresponding software information. For some middleware, the associations between software setup information and software information have been registered.

- **Parameter information**

    For parameters defined by software setup information, the values to be set can be defined. To specify parameter values using the GUI, select values from the combo boxes. Parameter information defines one of these options.

- **Template information**

    Template information defines the configuration of the L-Platform, such as the network devices, L-Servers and disks. Within the template information, options for the values to be set for software parameters can also be defined. The values to be set for parameters are specified using parameter information. Parameter values on the screen are selected using combo boxes. These options can be defined.

The following diagram shows the mutual relationships between the various types of information that make up an L-Platform template.

Figure 2.8 Mutual relationships between the various types of information that make up an L-Platform template
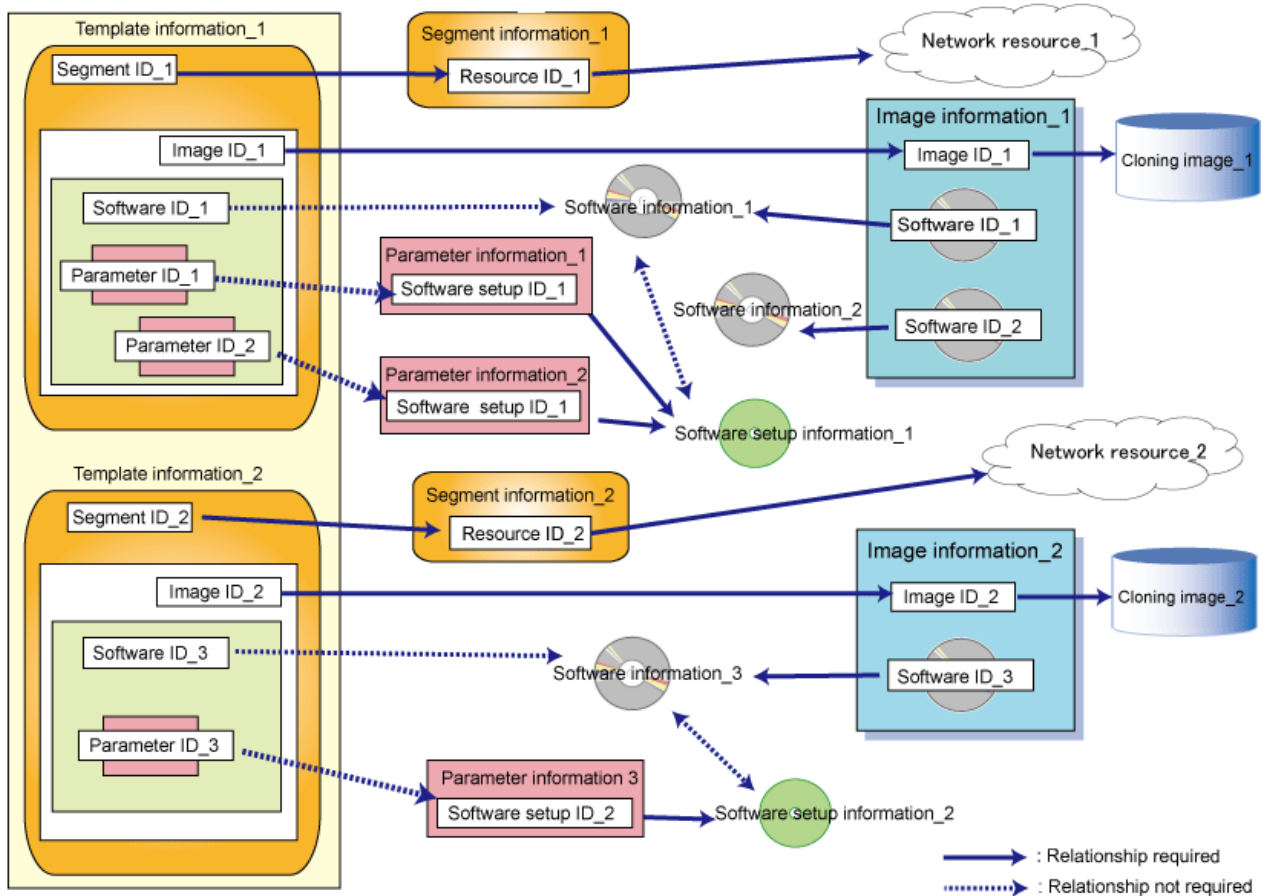
Creating cloning images

To create cloning images, the following procedure specific to this function must be followed:

1. Installing an agent on the L-Servers

   To set parameters for software, it is necessary to communicate from the admin server to the L-Servers that have been deployed. This means that a Systemwalker Software Configuration Manager agent must be installed on L-Servers.

2. Installing the middleware for which software information has been registered

   The middleware for which software information has been registered must be installed in accordance with the installation procedure. If the middleware is installed using this procedure, the middleware will run correctly after it is deployed. For middleware that will be affected if the IP address or host name of the operating system is changed, use the software parameter settings function to assign the new IP address or host name after deployment.

Chapter 3 Operating Environment

This chapter explains the operating environment for this product.

3.1 Required Hardware

This section explains the hardware resources that are required to install and operate this product, separately for admin servers, linkage servers, and business servers.

3.1.1 Recommended Hardware Resources

Admin server

Type of hardware	Requirements
Supported model	PRIMERGY, PRIMEQUEST 1000 series
CPU	Intel(R) Xeon(R) 3GHz or higher
Memory capacity (excluding the operating system)	At least 3.0 GB

Linkage server

Type of hardware	Requirements
Supported model	PRIMERGY, PRIMEQUEST 1000 series
CPU	Intel(R) Pentium 4 equivalent or higher
Memory capacity (excluding the operating system)	At least 1 GB

Business server

Type of hardware	Requirements
Supported model	PRIMERGY, PRIMEQUEST 1000 series
CPU	Intel(R) Pentium 4 equivalent or higher
Memory capacity (excluding the operating system)	At least 500 MB

3.1.2 Disk Capacity

Admin server

Static disk capacity

[Windows]

Product name	Disk space required for installation
Systemwalker Software Configuration Manager	Installation directory: 3 GB

Note: In addition to the disk space requirements above, the following disk space is required to manage and uninstall the software:

- %SYSTEMDRIVE%\FujitsuF4CR: 150 MB

[Linux]

Product name	Location	Disk space required for installation
Systemwalker Software Configuration Manager	/opt	1.0 GB or more
	/etc	0.5 GB or more
	/var	1.5 GB or more

Dynamic disk capacity

Database and memory space for the CMDB manager

The amount of database and memory space for the CMDB manager increases as the number of managed business servers increases. Estimate the amount of database and memory space based on the following table:

Number of business servers	Total amount of disk space used	Total amount of memory space used
500	Approx. 1.5 GB (*1)	Approx. 2.5 GB (*1)
1,000	Approx. 2.6 GB (*1)	Approx. 3.6 GB (*1)
1,500	Approx. 3.7 GB (*1)	Approx. 4.8 GB (*1)

*1: Assuming that ten patches per month are applied to each business server, if a business server is used for five years then these figures will increase by approximately 2GB.

Linkage server

Static disk capacity

[Windows]

Product name	Disk space required for installation
Systemwalker Software Configuration Manager	Installation directory: 800 MB

Business server

Static disk capacity

[Windows]

Product name	Disk space required for installation
Systemwalker Software Configuration Manager	Installation directory: 300 MB

Note: In addition to the disk space requirements above, the following disk space is required to manage and uninstall the software:

- %SYSTEMDRIVE%\FujitsuF4CR: 150 MB

[Linux]

Product name	Location	Disk space required for installation
Systemwalker Software Configuration Manager	/opt	240 MB or more
	/etc	10 MB or more
	/var	16 MB or more

3.2 Required Software

This section explains the software resources that are required to install this product.

3.2.1 Operating Systems for Performing Patch Management and Configuration Management

This section presents the operating systems for performing patch management and configuration management.

Admin server

- Windows Server 2012 (for x64) (*1)

- Windows Server 2008 (for x86)

- Windows Server 2008 (for x64) (*1)

- Windows Server 2008 R2 (*1)

- Red Hat Enterprise Linux 5 (for x86)

- Red Hat Enterprise Linux 5 (for Intel 64) (*2)

- Red Hat Enterprise Linux 6 (for x86)

- Red Hat Enterprise Linux 6 (for Intel 64) (*2)

Linkage server (32-bit agent)

- Windows Server 2012 (for x64) (*1)

- Windows Server 2008 (for x86)

- Windows Server 2008 (for x64) (*1)

- Windows Server 2008 R2 (*1)

Linkage server (64-bit agent)

- Windows Server 2012 (for x64)

- Windows Server 2008 (for x64)

- Windows Server 2008 R2

Business server (32-bit agent)

- Windows Server 2012 (for x64) (*1)

- Windows Server 2008 (for x86)

- Windows Server 2008 (for x64) (*1)

- Windows Server 2008 R2 (*1)

- Windows Server 2003 R2 (for x86) (Service Pack 2 or later)

- Windows Server 2003 R2 (for x64) (Service Pack 2 or later) (*1)

- Red Hat Enterprise Linux 5 (for x86)

- Red Hat Enterprise Linux 5 (for Intel 64) (*2)

- Red Hat Enterprise Linux 6 (for x86)

- Red Hat Enterprise Linux 6 (for Intel 64) (*2)

Business server (64-bit agent)

- Windows Server 2012 (for x64)

- Windows Server 2008 (for x64)

- Windows Server 2008 R2

- Windows Server 2003 R2 (for x64) (Service Pack 2 or later)

- Red Hat Enterprise Linux 5 (for Intel64)

- Red Hat Enterprise Linux 6 (for Intel64)

*1: Runs as a 32-bit application on the WOW64 (Windows 32-bit On Windows 64-bit) subsystem

*2: Runs in 32-bit compatibility mode

3.2.2 Operating Systems for Performing Software Parameter Settings

This section presents the operating systems for performing software parameter settings.

Admin server

The operating systems for the admin server are the same as the operating systems for ServerView Resource Orchestrator V3 Cloud Edition.

Managed server

- VMware

- Hyper-V

- Windows

- Linux

L-Server (business server: 32-bit agent)

- Windows Server 2012 (for x64) (*1)

- Windows Server 2008 (for x86)

- Windows Server 2008 (for x64) (*1)

- Windows Server 2008 R2 (*1)

- Windows Server 2003 R2 (for x86) (Service Pack 2 or later)

- Windows Server 2003 R2 (for x64) (Service Pack 2 or later) (*1)

- Red Hat Enterprise Linux 5 (for x86)

- Red Hat Enterprise Linux 5 (for Intel 64) (*2)

- Red Hat Enterprise Linux 6 (for x86)

- Red Hat Enterprise Linux 6 (for Intel 64) (*2)

L-Server (business server: 64-bit agent)

- Windows Server 2012 (for x64)

- Windows Server 2008 (for x64)

- Windows Server 2008 R2

- Windows Server 2003 R2 (for x64) (Service Pack 2 or later)

- Red Hat Enterprise Linux 5 (for Intel64)

- Red Hat Enterprise Linux 6 (for Intel64)

*1: Runs as a 32-bit application on the WOW64 (Windows 32-bit On Windows 64-bit) subsystem

*2: Runs in 32-bit compatibility mode

Note
....
Software parameter settings are not supported if a managed server uses Hyper-V as the server virtualization software and the operating system of the L-Servers is Red Hat Enterprise Linux.
....

3.2.3 Mandatory Software

This section presents mandatory software.

3.2.3.1 Mandatory Software for Performing Patch Management and Configuration Management

This section presents the mandatory software for performing patch management and configuration management.

Admin server

- ServerView Resource Orchestrator V3.1.1 Cloud Edition

Web client

- Internet Explorer 8, 9 or 10

- Adobe Reader X (required to view PDF manuals)

Note
....
The recommended display size (screen resolution) for the management console is 1024x768 pixels.
....

3.2.3.2 Mandatory Software for Performing Software Parameter Settings

This section presents the mandatory software for performing software parameter settings.

Admin server

- ServerView Resource Orchestrator V3.1.1 Cloud Edition

3.2.3.3 Mandatory Software for Linux

Admin server

The following software, which comes with the operating system, is required.

- redhat-lsb package

- The elfutils package (*1)

  Red Hat Enterprise Linux 5.2 or earlier

  elfutils-libelf-0.125-3.el5.i386.rpm (*1)

  Red Hat Enterprise Linux 5.3 or later

  elfutils-libelf-0.137-3.el5.i386.rpm (*1)

  Red Hat Enterprise Linux 6.0 or later

  elfutils-libelf-0.148-1.el6.i686.rpm (*1)

  *1: The 32-bit version is required even for 64-bit versions of Linux.

Red Hat Enterprise Linux or later, in addition to the above, the following software, which comes with the operating system, is required.

Red Hat Enterprise Linux 6.0 (for x86) or later

- alsa-lib pack package (32-bit versions)

- cloog-ppl package (32-bit versions)

- compat-readline5 package (32-bit versions)

- compat-libtermcap package (32-bit versions)

- cpp package (32-bit versions)

- file package (32-bit versions)

- gcc package (32-bit versions)

- gcc-c++ package (32-bit versions)

- gdb package (32-bit versions)

- glibc-devel package (32-bit versions)

- glibc-headers package (32-bit versions)

- kernel-headers package (32-bit versions)

- libICE package (32-bit versions)

- libSM package (32-bit versions)

- libX11 package (32-bit versions)

- libX11-common package

- libXau package (32-bit versions)

- libXext package (32-bit versions)

- libXi package (32-bit versions)

- libXp package (32-bit versions)

- libXt package (32-bit versions)

- libXtst package (32-bit versions)

- libgomp package (32-bit versions)

- libstdc++-devel package (32-bit versions)

- libtool-ltdl package (32-bit versions)

- libxcb package (32-bit versions)

- make package (32-bit versions)

- mpfr package (32-bit versions)

- nss-softokn-freebl package (32-bit versions)

- perl package (32-bit versions)

- perl-Module-Pluggable package (32-bit versions)

- perl-Pod-Escapes package (32-bit versions)

- perl-Pod-Simple package (32-bit versions)

- perl-libs package (32-bit versions)

- perl-version package (32-bit versions)

- ppl package (32-bit versions)

- strace package (32-bit versions)

- tcsh package (32-bit versions)

- unixODBC package (32-bit versions)

Red Hat Enterprise Linux 6.0 (for Intel64) or later

- alsa-lib package (32-bit versions)

- audit-libs package (32-bit versions)

- cloog-ppl package (64-bit versions)

- compat-readline5 package (32-bit versions)

- compat-libtermcap package (32-bit versions)

- cpp package (64-bit versions)

- cracklib package (32-bit versions)

- db4 package (32-bit versions)

- expat package (32-bit versions)

- file package (64-bit versions)

- gcc package (64-bit versions)

- gcc-c++ package (64-bit versions)

- glibc package (32-bit versions)

- glibc-devel package (32-bit versions)

- glibc-headers package (64-bit versions)

- kernel-headers package (64-bit versions)

- libICE package (32-bit versions)

- libSM package (32-bit versions)

- libX11 package (32-bit versions)

- libX11-common package

- libXau package (32-bit versions)

- libXext package (32-bit versions)

- libXi package (32-bit versions)

- libXp package (32-bit versions)

- libXt package (32-bit versions)

- libXtst package (32-bit versions)

- libattr package (32-bit versions)

- libcap package (32-bit versions)

- libgcc package (32-bit versions)

- libgomp package (64-bit versions)

- libselinux package (32-bit versions)

- libstdc++ package (32-bit versions)

- libstdc++-devel package (64-bit versions)

- libtool-ltdl package (32-bit versions)

- libuuid package (32-bit versions)

- libxcb package (32-bit versions)

- make package (64-bit versions)

- mpfr package (64-bit versions)

- ncurses-libs package (32-bit versions)

- nss-softokn-freebl package (32-bit versions)

- pam package (32-bit versions)

- perl package (64-bit versions)

- perl-Module-Pluggable package (64-bit versions)

- perl-Pod-Escapes package (64-bit versions)

- perl-Pod-Simple package (64-bit versions)

- perl-libs package (64-bit versions)

- perl-version package (64-bit versions)

- ppl package (64-bit versions)

- readline package (32-bit versions)

- tcsh package (64-bit versions)

- unixODBC package (32-bit versions)

- zlib package (32-bit versions)

Business server

The following software, which comes with the operating system, is required.

- redhat-lsb package

For installations in Red Hat Enterprise Linux 6 (for Intel64) environments, the 32-bit version of the following software, which is provided with the operating system, will be required:

- expat package

- glibc package

- libattr package

- libcap package

- libgcc package

- libstdc++ package

- nss-softokn-freebl package

- zlib package

3.2.4 Related Software

This section presents related software programs that are required for this product.

Linkage server

- Microsoft Windows Server Update Services (WSUS) 3.0 SP2

  This software is required to manage Windows patches.

  Note that a Client Access License (CAL) agreement must be concluded according to the number of target machines for which patches are to be applied by WSUS.

  There is no need to create WSUS servers if they have already been created.

P Point

For Systemwalker Software Configuration Manager, it is recommended that each WSUS server only manage up to 500 business servers in order to balance the load on the WSUS servers.

Number of business servers	Number of WSUS servers
500	1
1,000	2
1,500	3

- Yellowdog Updater Modified (yum) repository server

  This server is required to manage Linux patches.

  The following versions/levels of yum are supported:

  - RHEL6.2: yum-3.2.29-22.el6.noarch.rpm

  - RHEL6.1: yum-3.2.29-17.el6.noarch.rpm

  - RHEL6.0: yum-3.2.27-14.el6.noarch.rpm

  - RHEL5.7: yum-3.2.22-37.el5.noarch.rpm

  - RHEL5.6: yum-3.2.22-33.el5.noarch.rpm

  - RHEL5.5: yum-3.2.22-26.el5.noarch.rpm

  - RHEL5.4: yum-3.2.22-20.el5.noarch.rpm

  - RHEL5.3: yum-3.2.19-18.el5.noarch.rpm

  - RHEL5.2: yum-3.2.8-9.el5.noarch.rpm

- RHEL5.1: yum-3.0.1-5.el5.noarch.rpm

- RHEL5.0: yum-3.0.1-5.el5.noarch.rpm

There is no need to create yum repository servers if they have already been created.

Business server

- yum and rpm commands

These commands are required to manage Linux patches.

The yum and rpm commands are installed as part of the standard installation from RHEL5 and onwards.

The yum and rpm commands are used for the following purposes:

- Obtaining information about the RPM packages that have been applied to business servers

- Obtaining information about the RPM packages that can be applied to business servers (for the yum command only)

- UpdateAdvisor (middleware)

The UpdateAdvisor (middleware) is required to manage patches and software for Fujitsu middleware.

The UpdateAdvisor (middleware) is used for the following purposes:

- Obtaining information about the patches for Fujitsu middleware that have been applied to business servers

- Obtaining information about the Fujitsu middleware that has been installed on business servers

Note that a paid subscription to the support service is required to connect to the UpdateSite. It is also necessary to obtain and install the UpdateAdvisor (middleware).

Internet terminal

In order to manage patches for Linux operating systems or Fujitsu middleware, or to collect software information, prepare an "Internet terminal" (a terminal that can connect to the Internet).

Use Windows(R) XP, Windows Vista, Windows 7 or Windows 8 as the operating system for the Internet terminal.