FUJITSU

# FUJITSU Software Systemwalker Software Configuration Manager

# Technical Guide

Windows/Linux

B1X1-0126-08ENZ0(00)
August 2016

# Preface

## Purpose of this Document

This document explains the functions of Systemwalker Software Configuration Manager.

## 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<br>Microsoft(R) Windows Server(R) 2012 Standard | Windows Server 2012 | Windows |
| Microsoft(R) Windows Server(R) 2012 R2 Datacenter<br>Microsoft(R) Windows Server(R) 2012 R2 Standard | Windows Server 2012 R2 | |
| Microsoft(R) Windows Server(R) 2008 Standard<br>Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V<br>Microsoft(R) Windows Server(R) 2008 Enterprise<br>Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V | Windows Server 2008 | |
| Microsoft(R) Windows Server(R) 2008 R2 Standard<br>Microsoft(R) Windows Server(R) 2008 R2 Enterprise | Windows Server 2008 R2 | |
| Red Hat(R) Enterprise Linux(R) (for x86) | RHEL (x86) | RHEL |
| Red Hat(R) Enterprise Linux(R) (for Intel64) | RHEL (Intel64) | |
| Oracle Solaris | Solaris Operating System<br>Solaris OS | Solaris |

## Export Restrictions

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

## Trademarks

- Adobe, Adobe Reader, and Flash are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.
- Interstage, ServerView, 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.
- Oracle and Java are registered trademarks of Oracle and/or its affiliates in the United States and other countries. Company names and product names used in this document are registered trademarks or trademarks of those companies.
- VMware, the VMware "boxes" logo and design, Virtual SMP, and VMotion are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.
- Xen and XenSource are trademarks or registered trademarks of XenSource, Inc. in the United States and/or other countries.
- 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) |
| March 2014: Fourth edition | B1X1-0126-05ENZ0(00) / B1X1-0126-05ENZ2(00) |
| August 2014: Fifth edition | B1X1-0126-06ENZ0(00) / B1X1-0126-06ENZ2(00) |
| November 2015: Sixth edition | B1X1-0126-07ENZ0(00) / B1X1-0126-07ENZ2(00) |
| August 2016: Seventh Edition | B1X1-0126-08ENZ0(00) / B1X1-0126-08ENZ2(00) |

## Copyright

# Contents

# Chapter 1 Overview

This chapter provides 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 centrally manages the configuration information of an entire system including hardware, OS, and middleware.

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 centrally manage the information of the hardware and the information of the resources that have been dynamically deployed via the cloud. Moreover, the ability to install software, manage software parameters and the status of patch applications to servers, enables the workload of system administrators to be reduced.

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

- Sets up and maintains Systemwalker Software Configuration Manager.
- Defines the managed servers managed by Systemwalker Software Configuration Manager.
- Defines policies for managing Windows patches, releases the patches obtained from Microsoft Windows Server Update Services (WSUS), and determines classification levels.
- Obtains Linux patches and registers them with Yellowdog Updater Modified (yum) repository servers.
- Obtains software patches and registers them with Systemwalker Software Configuration Manager.
- Defines the information collection sources from which information about software and patches are collected. The information collection source for Fujitsu middleware is already defined.
- Defines the parameters to be collected from the software and the parameters to be configured in it.
- Uses the management console to reference the patch application status, software parameter setting values, and hardware and software configuration information for all the servers in the center.

Dual-role administrator

- Acts as both an infrastructure administrator and a tenant administrator.

Tenant administrator

- Uses the management console to apply patches to servers within their tenancy.
- Uses the management console to install software on the servers within their tenancy.
- Uses the management console to configure parameters in software on servers within their tenancy.
- Uses the management console to reference the patch application status, software parameter setting values, and software configuration information for the servers within their tenancy.

Tenant user

- Uses the management console to apply patches to the servers they manage themselves.
- Uses the management console to install software on servers they manage themselves.

- Uses the management console to configure parameters in software on servers they manage themselves.
- Uses the management console to reference the patch application status, software parameter setting values, and software configuration information for the servers they manage themselves.

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

1. Download patches

   This step involves downloading patches for the operating system and software from vendor web sites 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 software 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 managed 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 software and apply these patches by registering scripts.

3. Install software

   Install software on the managed servers according to the instructions from the tenant user.

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

4. Configure software parameters, and run scripts

   Configure parameters for the software on the managed servers based on instructions from the tenant user. Scripts can also be run on managed servers.

   The infrastructure administrator defines in advance parameters that can be configured in the software.

5. Perform discovery

   This step involves periodically and automatically collecting the patch application status, software parameter setting values, and hardware and software configuration information from managed servers and linkage servers, and then storing this information in the configuration management database (CMDB).

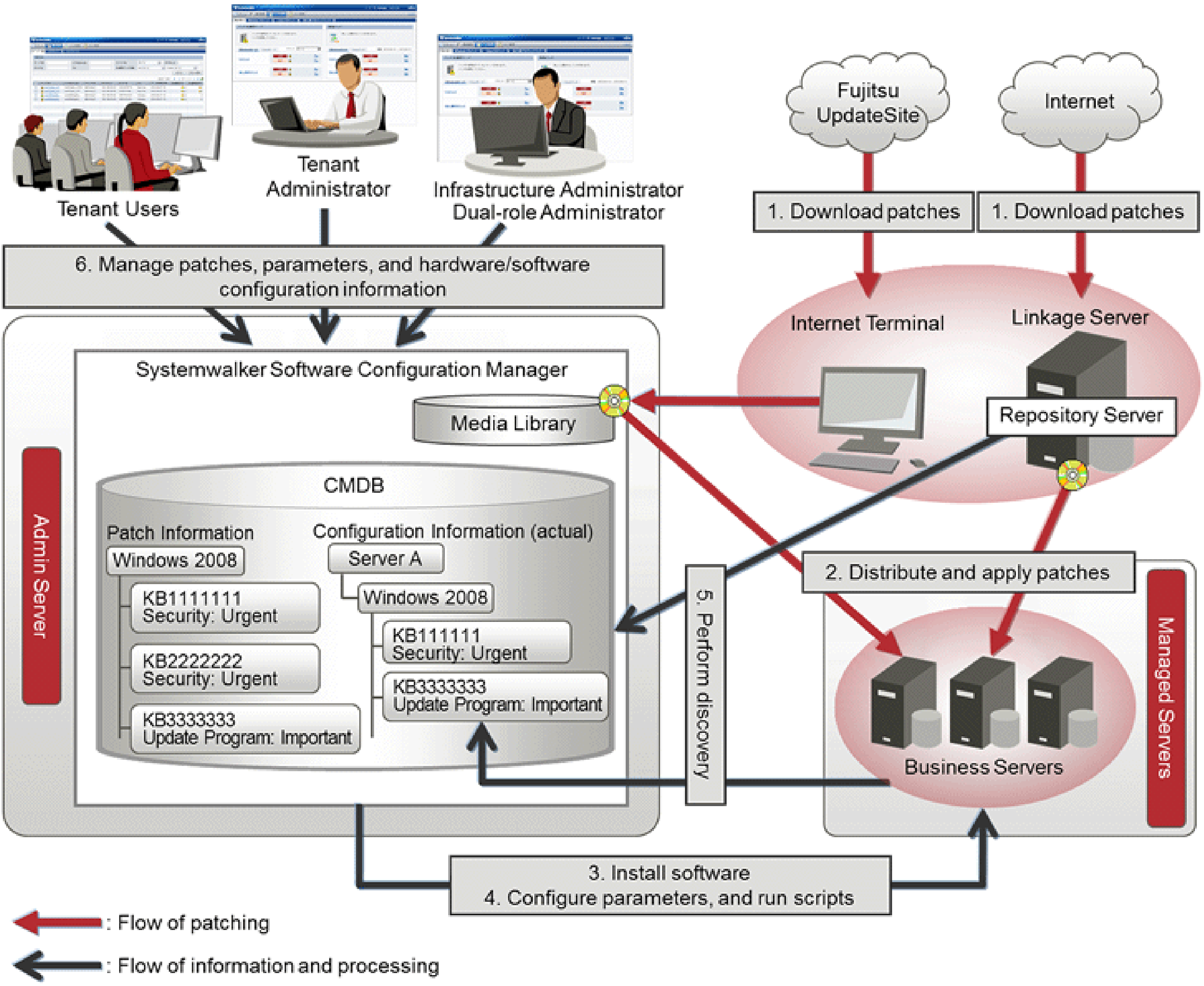
6. Manage configuration information, patches, and parameters

   Infrastructure administrators and dual-role administrators can check hardware and software configuration information for all the servers in the data center by logging in to the management console for Systemwalker Software Configuration Manager. They can also check the patch application status and software parameter setting values discovered from managed servers and linkage servers.

   Tenant administrators can check the software configuration information and patch application status, and software parameter settings, for all servers in the data center.

   Tenant users can check the software configuration information, patch application status, and software parameter settings of the servers that they themselves manage.

Figure 1.1 Overview of Systemwalker Software Configuration Manager



## What is an admin server?

Admin server is the server that operates Systemwalker Software Configuration Manager. It is used to manage the patch application status and software parameters, and to collect hardware and software configuration information.

## What is a managed server?

A general term for servers managed by Systemwalker Software Configuration Manager. It refers to the servers from which the hardware and software configuration information is collected as well as the target servers of patch management, software installation, and software parameter management. Systemwalker Software Configuration Manager can manage the admin server and linkage servers.

### When linked to ServerView Resource Orchestrator

ServerView Resource Orchestrator is a software product that automatically deploys physical and virtual servers.

By linking to ServerView Resource Orchestrator, Systemwalker Software Configuration Manager can manage patches on servers deployed by ServerView Resource Orchestrator, software parameters, and software configuration information.

### When coordinating with OpenStack

OpenStack is a software product that automatically deploys virtual servers.

Through coordination with OpenStack, Systemwalker Software Configuration Manager can manage patches on servers deployed by OpenStack, and server software parameters and configuration information.

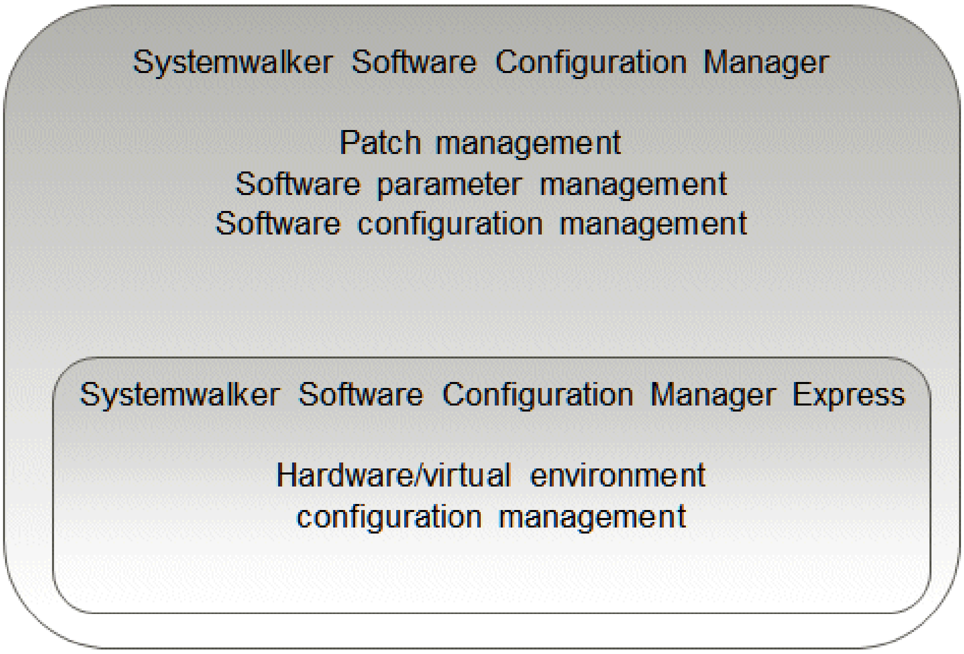
## 1.2 Product Road Map

As an edition of Systemwalker Software Configuration Manager, the following product provides only the configuration management function for hardware/virtual environments.

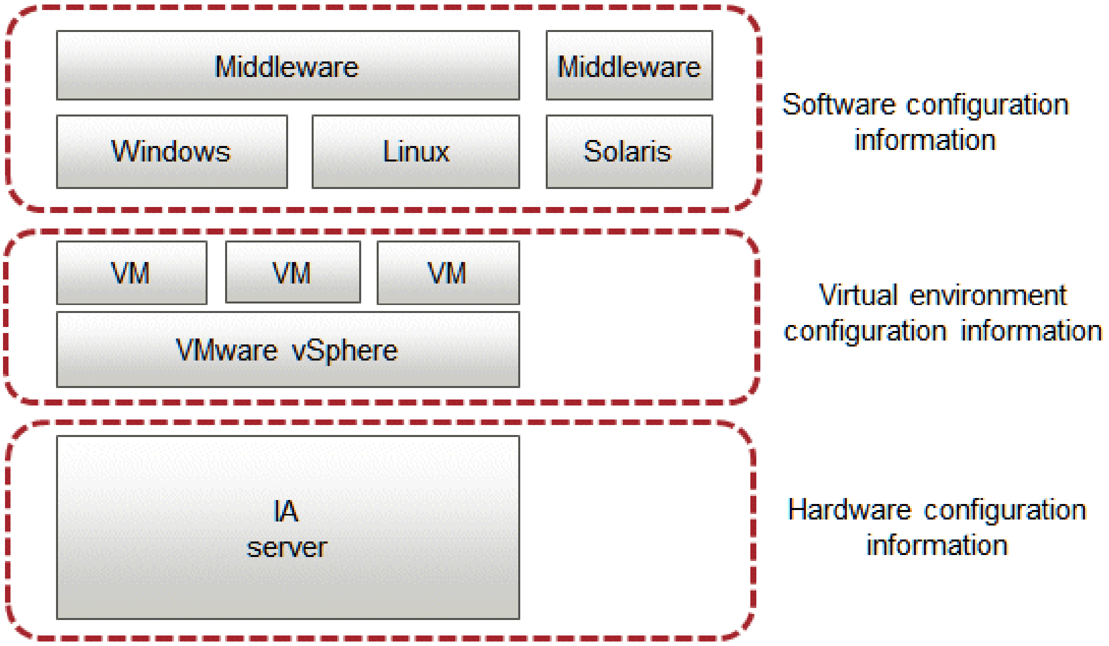
- Systemwalker Software Configuration Manager Express

  Automatically collects configuration information of hardware (chassis/servers) and virtual environments (hypervisor/guest OS) and store it in the CMDB for management.

The functions provided by Systemwalker Software Configuration Manager Express are shown below.


Systemwalker Software Configuration Manager
Patch management
Software parameter management
Software configuration management
Systemwalker Software Configuration Manager Express
Hardware/virtual environment
configuration management

Relationships between hardware configuration information, virtual environment configuration information, and software configuration information are shown below.


Middleware
Middleware
Windows
Linux
Solaris
Software configuration information
VM
VM
VM
VMware vSphere
Virtual environment configuration information
IA server
Hardware configuration information

See

For the overview, installation, management, and operation of Systemwalker Software Configuration Manager, refer to the *Express User's Guide*.

## 1.3 Features of Systemwalker Software Configuration Manager

Systemwalker Software Configuration Manager has the following features:

- **Discovery**

  Collects and obtain patch application statuses, software parameter setting values, hardware/virtual environment configuration information, and software configuration information for managed servers.

- **Patch management**

  Applies patches and manages the application status of patches for Windows operating systems, Linux operating systems, and software on managed servers.

- **Software installation**

  Software can be installed on the managed servers.

- **Software parameter management**

  Configures parameters in software on managed servers and manage the configured values.

- **Resource management**

  Manages hardware/virtual environment configuration information, and software configuration information for managed servers using the configuration management database (CMDB).

- **Reporting**

  Defining views enables easy reporting on collected configuration information. Defining policies makes it possible to determine whether configuration information is appropriate.

  In addition, various types of information, including the results of applying patches to managed servers, a list of servers with unapplied patches, and software parameter setting values, can be output in CSV format.

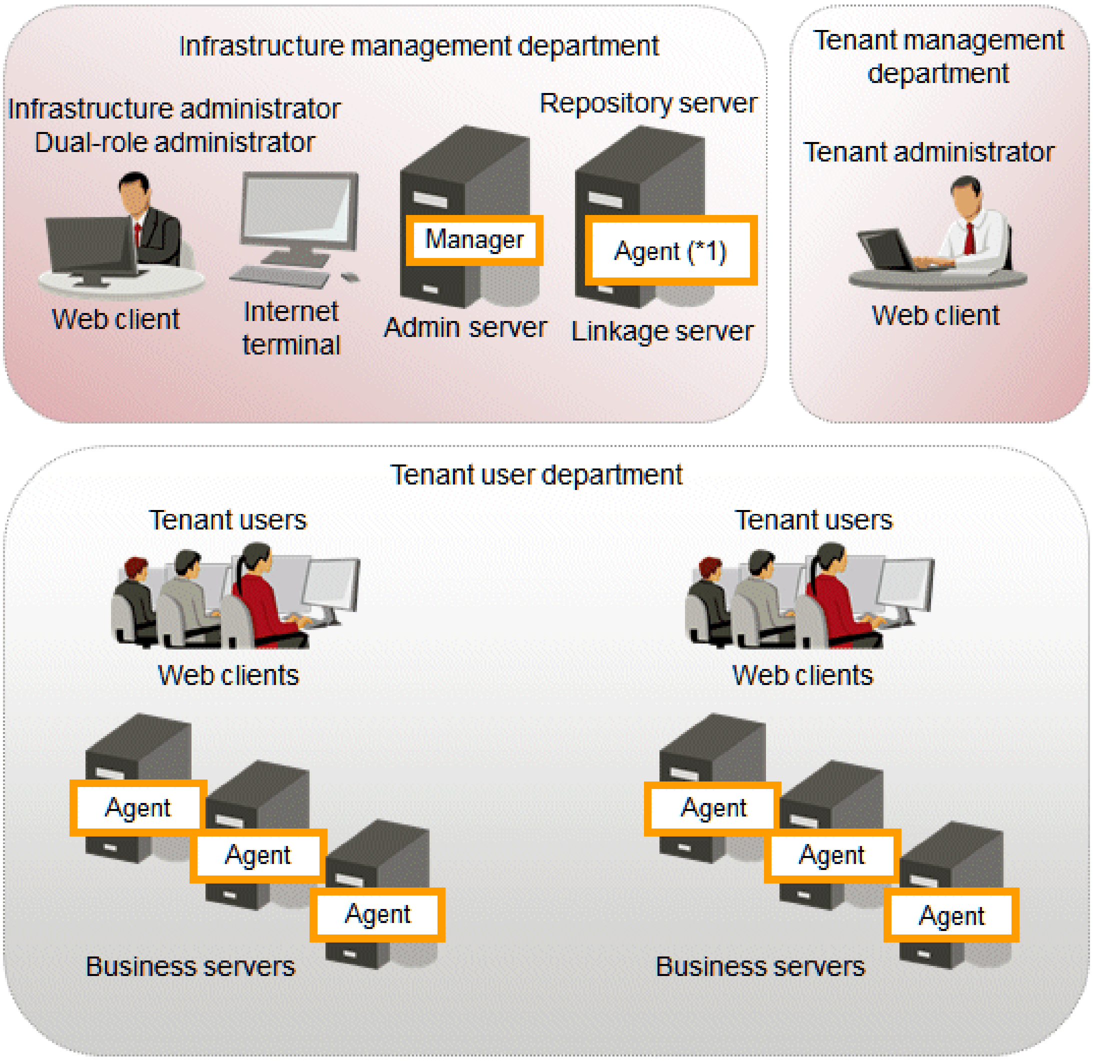
## 1.4 System Configuration

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

### 1.4.1 System configuration for managing patches and software configuration

The following diagram illustrates the system configuration for management of patches and software configuration.

Figure 1.2 System configuration for managing patches and software configuration



*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

A server 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 which are not managed by Systemwalker Software Configuration Manager.

#### Business server

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

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

#### Internet terminal

A terminal used to download the latest patches from the UpdateSite or vendor websites.

An internet terminal is required for the management of Linux OS patches, Solaris OS patches, and patches for software such as Fujitsu middleware.

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

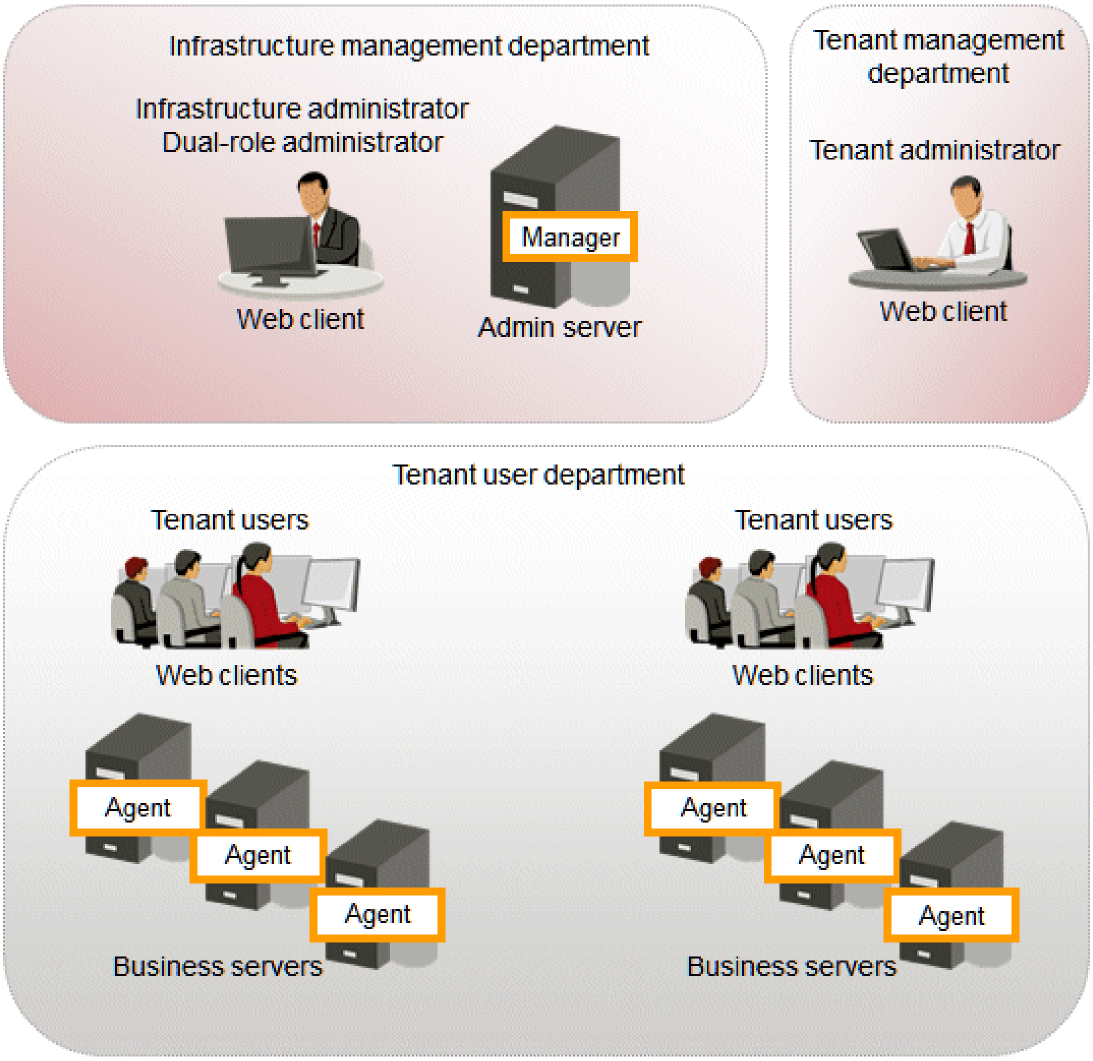
#### Web client

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

## 1.4.2 System Configuration for Software Installation and Software Parameter Management

The system configuration for software installation and software parameter management is shown below.

Figure 1.3 System configuration for performing software installation and software parameter management



### Admin server

Admin server is the server that operates Systemwalker Software Configuration Manager. The admin server installs software on business servers. It also collects parameters and configures the parameters of the installed software.

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.

### Business server

The server on which software is installed. Parameters are collected and configured for the installed software. Systemwalker Software Configuration Manager agents are installed on business servers. An agent is a Systemwalker Software Configuration Manager program that runs on business servers.

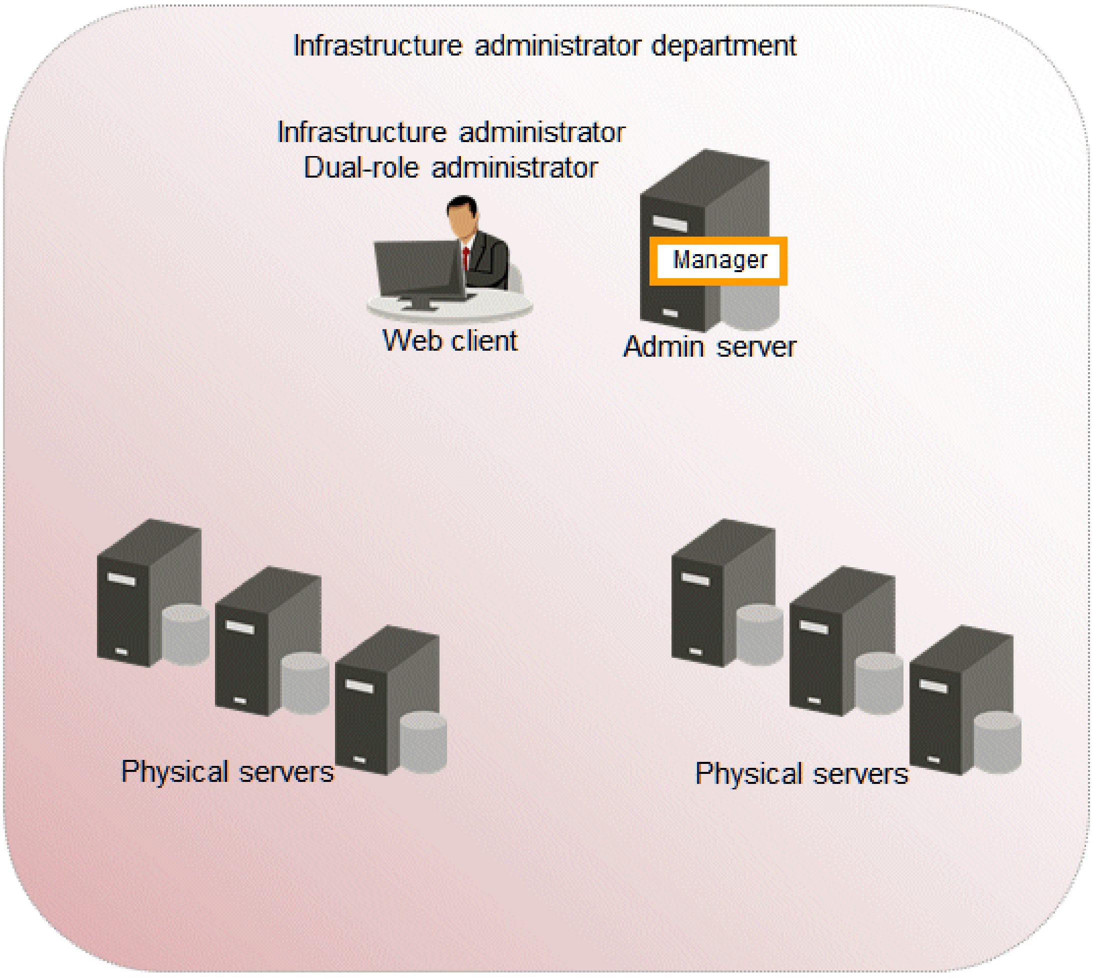
### Web client

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

## 1.4.3 System Configuration for Managing Hardware/Virtual Environment Configurations

The following diagram illustrates the system configuration for managing hardware and virtual environment configuration.

Figure 1.4 System Configuration for Managing Hardware/Virtual Environment Configurations



### Admin server

**The admin server is the server that operates Systemwalker Software Configuration Manager. The admin server collects the configuration information of physical server hardware and virtual environments.**

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.

### Physical server (business server)

A physical server managed by Systemwalker Software Configuration Manager.

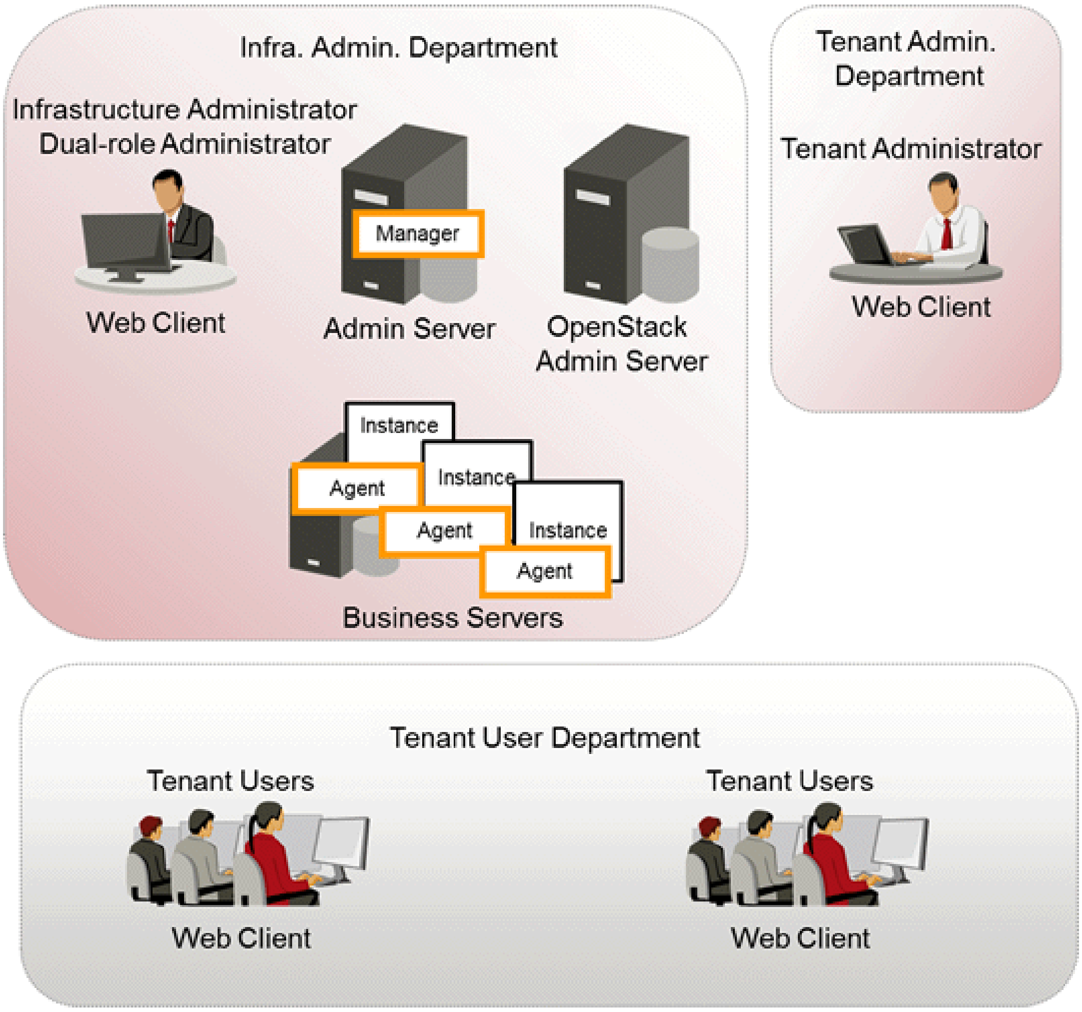
### Web client

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

## 1.4.4 System Configuration for Performing OpenStack Coordination

The system configuration for performing OpenStack coordination is as given below.

Figure 1.5 System Configuration for Performing OpenStack Coordination



### Admin server

Admin server is the server that operates Systemwalker Software Configuration Manager. The admin server collects the configuration information of the OpenStack virtual environments.

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.

### OpenStack Admin Server

A controller of OpenStack that manages OpenStack environments.

### Instance (business server)

An instance (virtual machine) managed by Systemwalker Software Configuration Manager.

### Web client

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

## 1.5 Benefits of Installation

Installing Systemwalker Software Configuration Manager provides the following benefits:

- Keep server patches up to date
- Centralized management of ICT resources, hardware, OS, and middleware configuration information

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

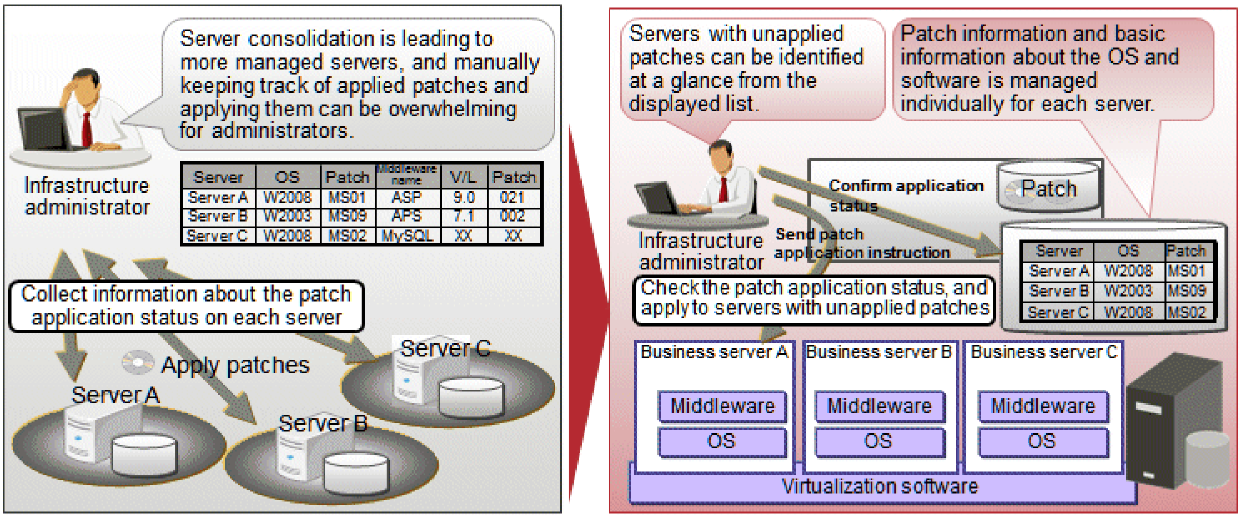
- Reduce system configuration time and human errors using software parameter management

### 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 1.6 Benefit 1 (Keeping server patches up to date)



Server consolidation is leading to more managed servers, and manually keeping track of applied patches and applying them can be overwhelming for administrators.
Infrastructure administrator
Collect information about the patch application status on each server
Apply patches
Server A
Server B
Server C
Servers with unapplied patches can be identified at a glance from the displayed list.
Patch information and basic information about the OS and software is managed individually for each server.
Confirm application status
Patch
Infrastructure administrator
Send patch application instruction
Check the patch application status, and apply to servers with unapplied patches
Business server A
Business server B
Business server C
Middleware
OS
Virtualization software

| Server | OS | Patch | Middleware name | V/L | Patch |
|---|---|---|---|---|---|
| Server A | W2008 | MS01 | ASP | 9.0 | 021 |
| Server B | W2003 | MS09 | APS | 7.1 | 002 |
| Server C | W2008 | MS02 | MySQL | XX | XX |

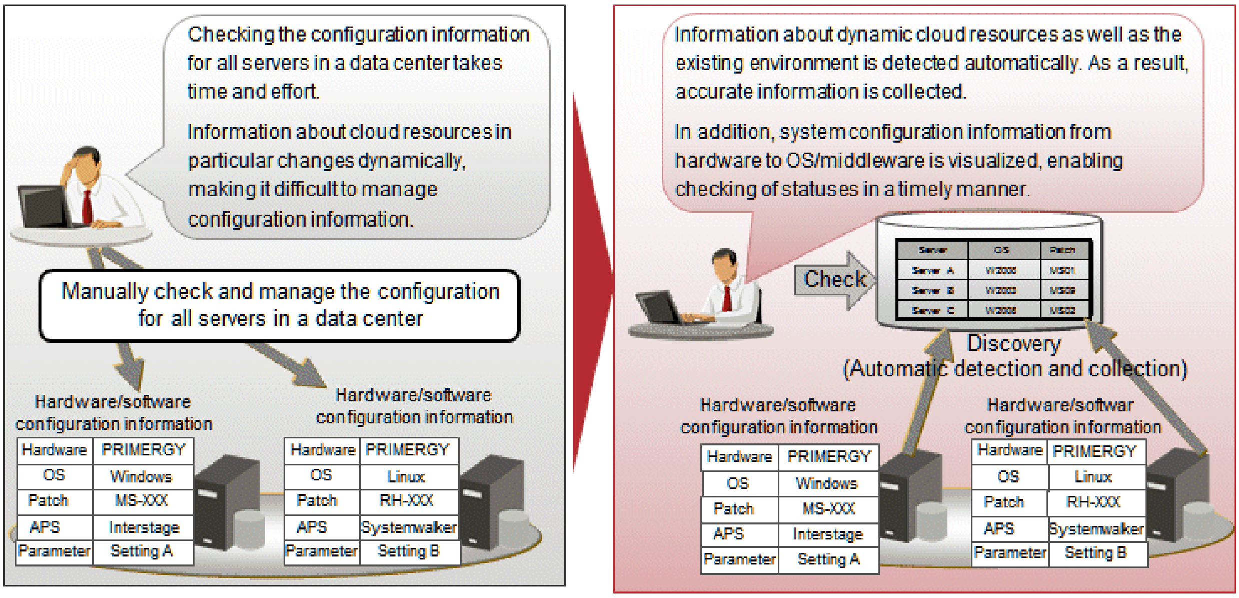
| Server | OS | Patch |
|---|---|---|
| Server A | W2008 | MS01 |
| Server B | W2003 | MS09 |
| Server C | W2008 | MS02 |

### Centralized management of ICT resources, hardware, OS, and middleware configuration information

For resources in a data center, especially the ones 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 centrally manage the configuration information of the servers, VM hosts, OS, and middleware in a data center, including the resources deployed using cloud environments, accurately and in a timely manner.

Figure 1.7 Benefit 2 (Centralized management of ICT resources, hardware, OS, and middleware configuration information)


Checking the configuration information for all servers in a data center takes time and effort.
Information about cloud resources in particular changes dynamically, making it difficult to manage configuration information.
Manually check and manage the configuration for all servers in a data center
Hardware/software configuration information
Hardware/software configuration information
Information about dynamic cloud resources as well as the existing environment is detected automatically. As a result, accurate information is collected.
In addition, system configuration information from hardware to OS/middleware is visualized, enabling checking of statuses in a timely manner.
Check
Discovery
(Automatic detection and collection)
Hardware/software configuration information
Hardware/softwar configuration information

| Hardware | PRIMERGY |
|---|---|
| OS | Windows |
| Patch | MS-XXX |
| APS | Interstage |
| Parameter | Setting A |

| Hardware | PRIMERGY |
|---|---|
| OS | Linux |
| Patch | RH-XXX |
| APS | Systemwalker |
| Parameter | Setting B |

| Server | OS | Patch |
|---|---|---|
| Server A | W2008 | MS01 |
| Server B | W2003 | MS09 |
| Server C | W2008 | MS02 |

| Hardware | PRIMERGY |
|---|---|
| OS | Windows |
| Patch | MS-XXX |
| APS | Interstage |
| Parameter | Setting A |

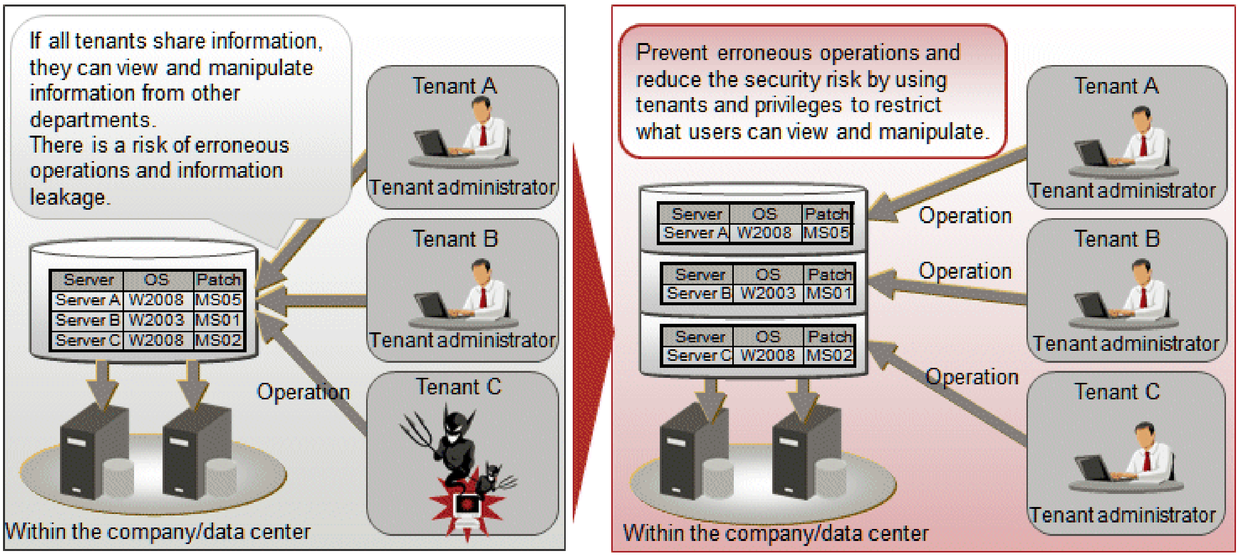
| Hardware | PRIMERGY |
|---|---|
| OS | Linux |
| Patch | RH-XXX |
| APS | Systemwalker |
| Parameter | Setting B |

### 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 1.8 Benefit 3 (Visualizing software configuration information based on tenant and administrator privileges)


If all tenants share information, they can view and manipulate information from other departments.
There is a risk of erroneous operations and information leakage.
Tenant A
Tenant administrator
Tenant B
Tenant administrator
Tenant C
Operation
Within the company/data center
Prevent erroneous operations and reduce the security risk by using tenants and privileges to restrict what users can view and manipulate.
Operation
Operation
Operation
Tenant A
Tenant administrator
Tenant B
Tenant administrator
Tenant C
Tenant administrator
Within the company/data center

| Server | OS | Patch |
|---|---|---|
| Server A | W2008 | MS05 |
| Server B | W2003 | MS01 |
| Server C | W2008 | MS02 |

| Server | OS | Patch |
|---|---|---|
| Server A | W2008 | MS05 |

| Server | OS | Patch |
|---|---|---|
| Server B | W2003 | MS01 |

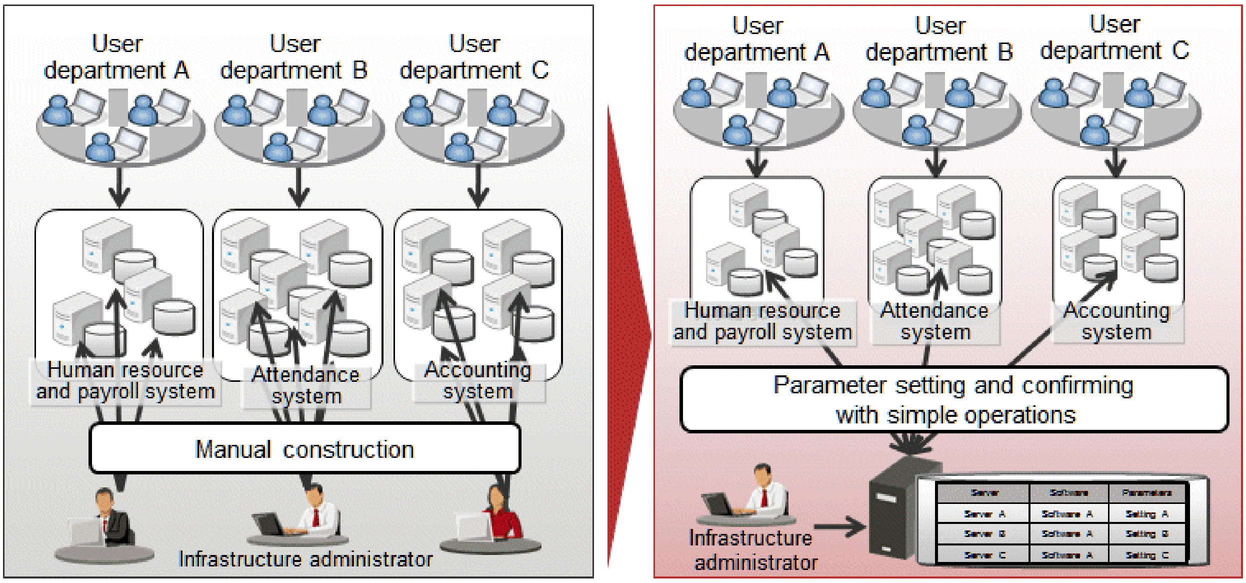
| Server | OS | Patch |
|---|---|---|
| Server C | W2008 | MS02 |

### Reducing system construction time and human errors using the software parameter management function

In systems where ICT resources have simply been consolidated in a data center, 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.

With Systemwalker Software Configuration Manager, software installation and parameter configuration can be performed remotely, in batches. In addition, the function that automatically collects (discovers) software parameter information eliminates human errors such as configuration/checking mistakes. As software parameter information is managed centrally, system configuration time can be significantly reduced.

Figure 1.9 Benefit 4 (Reduce system configuration time and human errors using software parameter management)



| Server | Software | Parameters |
|---|---|---|
| Server A | Software A | Setting A |
| Server B | Software A | Setting B |
| Server C | Software A | Setting C |

# Chapter 2 Function Explanation

This product provides the following functions:

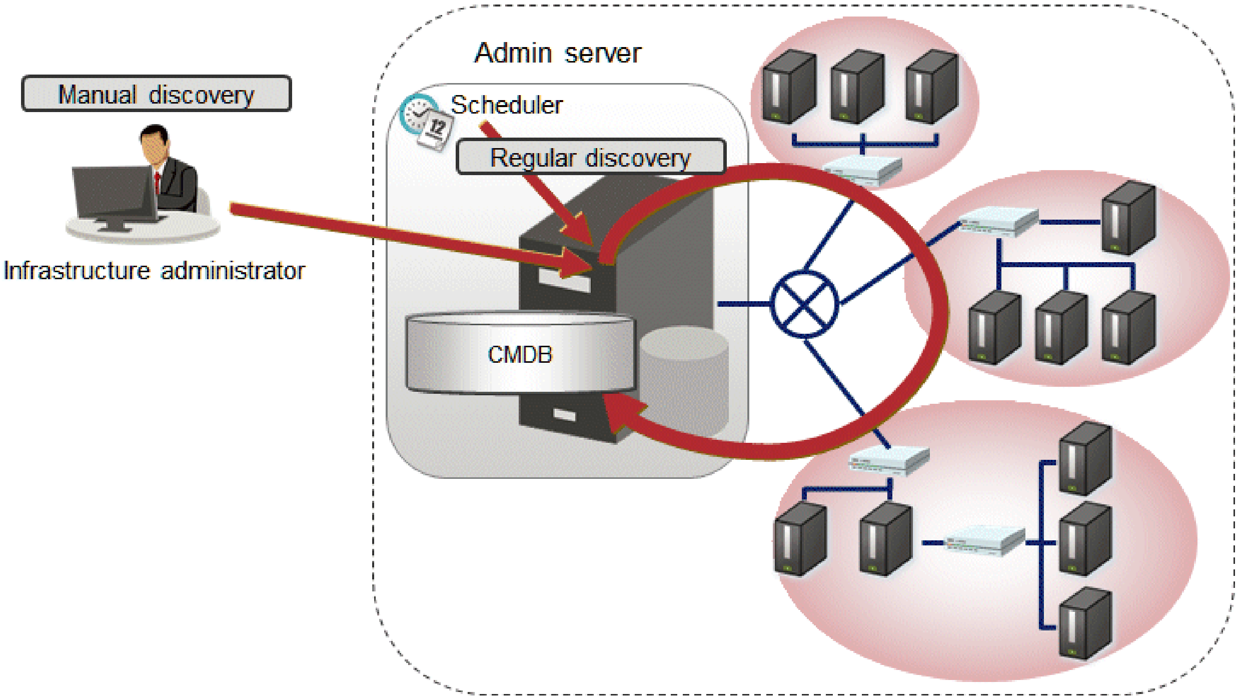
- Discovery
- Patch management
- Software installation
- Software parameter management
- Configuration management

## 2.1 Discovery

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

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

Figure 2.1 Overview of the discovery function



### Hardware/virtual environment configuration to be collected

The following hardware/virtual environment configuration information can be collected using the discovery function:

The configuration information of the virtual environments is collected from VMware vSphere ESXi or OpenStack.

Table 2.1 Hardware configuration information collected by the discovery function (chassis, blade servers)

| Device | Item | Example |
|---|---|---|
| Chassis body<br>Fujitsu PRIMERGY BX400 S1, BX600 S2/S3, BX900 S1/S2 | Product name | BX900 |
| | Serial number | AA1234567890 |
| | Firmware version(*1) | 5.32 |

| Device | Item | Example |
|---|---|---|
| Blade server<br>Fujitsu PRIMERGY BX620 S3 - S6, BX920 S1 - S4, BX922 S2, BX924 S2 - S4, BX960 S1 | Slot number | 1 |
| | Vendor name | FUJITSU |
| | Product name | PRIMERGY BX920 S1 |
| | Serial number | BB1234567890 |
| | CPU Type | Xeon |
| | Frequency | 1995 MHz |
| | Quantity | 2 |
| | Memory size | 4096 MB |
| | Firmware version(*2) | 551 |
| | BIOS version(*2) | 3D41 |
| | OS name(*3) | VMware ESXi 5.1.0 build-1157734 |

*1: On PRIMERGY BX400 S1 and BX600 S2/S3, the firmware version cannot be discovered.

*2: On PRIMERGY BX620 S3 - S6, the firmware version and BIOS version cannot be discovered.

*3: Only when the version of the mounted hypervisor is VMware vSphere ESXi 5.1 or later can discovery be performed.

Table 2.2 Hardware configuration information collected by the discovery function (rack mount servers)

| Device | Item | Example |
|---|---|---|
| Fujitsu PRIMERGY RX100/ RX200/RX300 S6 or later, RX1330/RX2520/RX2540 M1 or later<br>IBM System x3550 M4<br>HP ProLiant DL320e Gen8 v2 | Product name | PRIMERGY RX300 S7 |
| | Serial number | CC1234567890 |
| | CPU Type (*2) | Intel(R) Xeon(R) CPU E5-2609 v2 @ 2.50GHz |
| | Frequency(*3) | 2500 MHz |
| | Quantity | 2 |
| | Memory size | 4096 MB |
| | OS name(*1) | VMware ESXi 5.1.0 build-1157734 |

*1: Only when the version of the mounted hypervisor is VMware vSphere ESXi 5.1 or later can discovery be performed.

*2: On PRIMERGY RX100/RX200/RX300 S6 the CPU type cannot be discovered.

*3: On IBM servers and HP servers, the frequency cannot be discovered.

Table 2.3 Virtual environment configuration information collected by the discovery function (for VMware vSphere ESXi)

| Hypervisor | Type | Item | Example |
|---|---|---|---|
| VMware vSphere ESXi | VM host information | OS name | VMware ESXi 5.1.0 build-1021289 |
| | | CPU core count | 8 |
| | | MAC address | 60:EB:69:07:F3:xx |
| | | IP address | 192.168.1.12 |
| | VM guest information | Virtual machine name | VM001 |
| | | OS name | Microsoft Windows Server 2012 (64-bit) |
| | | CPU core count | 2 |
| | | Frequency (GHz) | 1.0 |

| Hypervisor | Type | Item | Example |
|---|---|---|---|
| | | Memory size (GB) | 2.0 |
| | | MAC address | 60:EB:69:07:D3:xx |
| | | IP address | 192.168.10.122 |

Table 2.4 Virtual environment configuration information collected by the discovery function (for OpenStack)

| Hypervisor | Type | Item | Example |
|---|---|---|---|
| KVM (QEMU) | VM host information | CPU core count | 8 |
| | | IP address | 192.168.1.12 |
| | VM guest information | Virtual machine name | VM001 |
| | | OS name | rhel 6.6 |
| | | CPU core count | 2 |
| | | Memory size (GB) | 2.0 |
| | | MAC address | 60:EB:69:07:D3:xx |
| | | IP address | 192.168.10.122 |
| | | | |

### Software configuration information collected

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

Table 2.5 Software configuration information collected by the discovery function

| Resource | | | | Linkage product/linkage function | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | ServerView Resource Orchestrator | Microsoft Windows Server Update Services (WSUS) | yum(Yellow dog Updater Modified) | UpdateAdvisor (middleware) | Solaris | Software |
| 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) | 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 | - | - | - | - |

| Resource | | | | Linkage product/linkage function | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | ServerView Resource Orchestrator | Microsoft Windows Server Update Services (WSUS) | yum(Yellow dog Updater Modified) | UpdateAdvisor (middleware) | Solaris | Software |
| | | 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 | - | - | - |
| | Solaris OS Patches | Solaris OS patch (SRU) information released on the Oracle or Fujitsu website | OS patch (SRU) information | - | - | - | - | - | - |
| | | | Applicable physical or virtual Solaris servers | - | - | - | - | - | - |
| | | Information about the OS patches (SRU) that have already been applied to the physical and virtual Solaris servers that comprise the system | | - | - | - | - | Y | - |
| | Software patches | Released software patches | Software patches | - | - | - | - (*2) | - | - |
| | | | Physical or virtual servers where the | - | - | - | - (*3) | - | - |

| Resource | | | | Linkage product/linkage function | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | ServerView Resource Orchestrator | Microsoft Windows Server Update Services (WSUS) | yum(Yellow dog Updater Modified) | UpdateAdvisor (middleware) | Solaris | Software |
| | | | patches can be applied | | | | | | |
| | | Information about the software patches that have already been applied to the physical or virtual servers that make up the system | | - | - | - | Y | - | - |
| Software information | | Information about the software products that have already been installed on the physical or virtual servers that make up the system | | - | - | - | Y | - | - |
| Parameter information | | Information on configured software parameters | | - | - | - | - | - | 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 swcfmg_fjmwpatch_update (Fujitsu Middleware Patch Registration command). Information about all other software patches is registered in the CMDB by executing swcfmg_patch_def (Patch Information Management command). For details on swcfmg_fjmwpatch_update (Fujitsu Middleware Patch Registration command), refer to the *Reference Guide*. For details on swcfmg_patch_def (Patch Information Management command), refer to the *Developer's Guide*.

*3: For Fujitsu middleware, information about patchable physical or virtual servers is registered in the CMDB by executing swcfmg_fjmwpatch_update (Fujitsu Middleware Patch Registration command). For all other software, information about patchable physical or virtual servers is registered in the CMDB by registering the patch information by executing swcfmg_patch_def (Patch Information Management command). For details on swcfmg_fjmwpatch_update (Fujitsu Middleware Patch Registration command), refer to the *Reference Guide*. For details on swcfmg_patch_def (Patch Information Management command), refer to the *Developer's Guide*.

### The timing of discovery

Discovery is performed at the following times:

- Regular discovery

  Discovery is executed periodically according to a schedule.

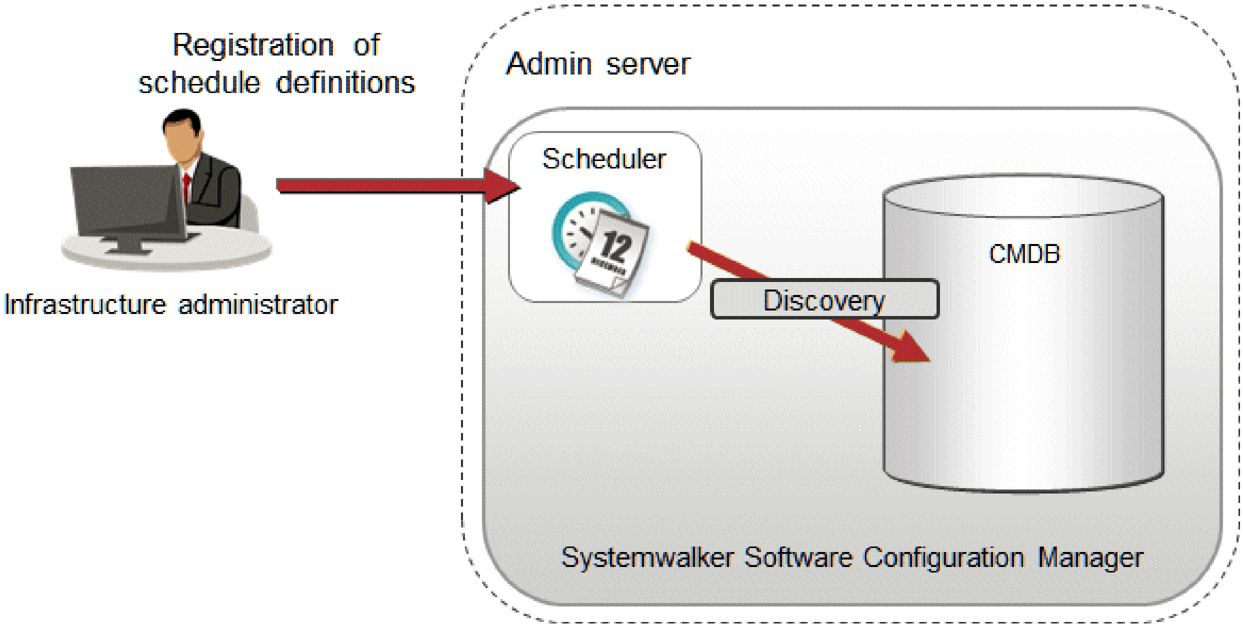
- Manual discovery

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

Regular discovery

With regular discovery, the latest configuration information is collected according to a schedule that the infrastructure administrator has defined in advance.

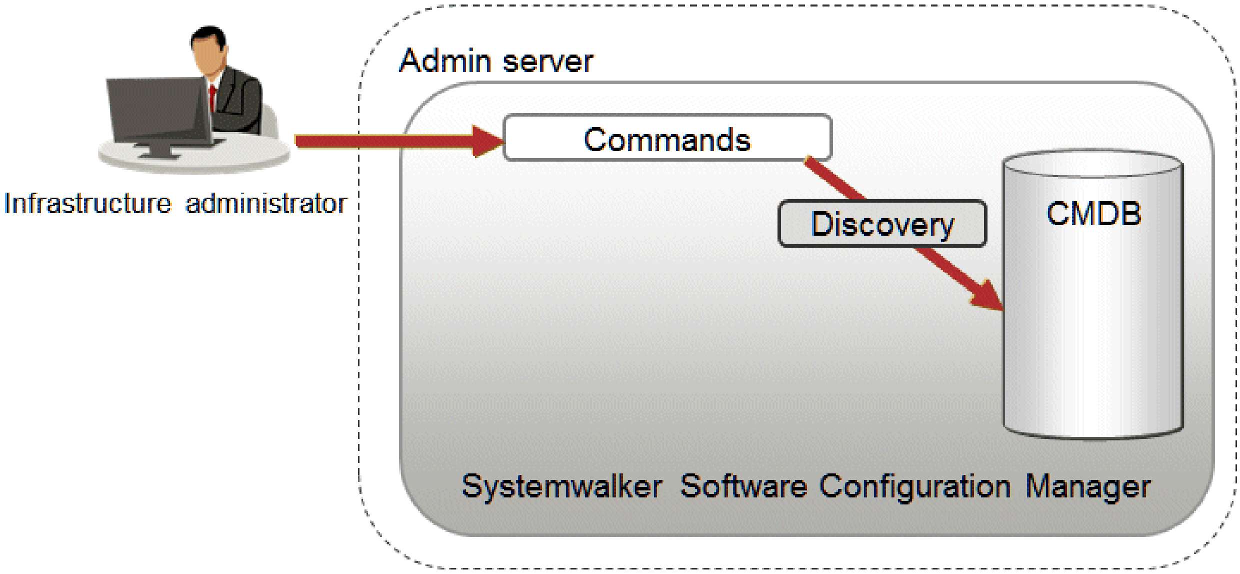
Figure 2.2 Regular discovery


Registration of schedule definitions
Infrastructure administrator
Admin server
Scheduler
12
Discovery
CMDB
Systemwalker Software Configuration Manager

Manual discovery

The infrastructure administrator collects the latest configuration information by executing the command to perform discovery.

Figure 2.3 Manual discovery


Infrastructure administrator
Admin server
Commands
Discovery
CMDB
Systemwalker Software Configuration Manager

## 2.2 Patch Management

Systemwalker Software Configuration Manager manages the following patches:

- Windows patches
- Linux patches
- Solaris OS 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 managed servers.

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

### Solaris OS patches

Patches for the Solaris OS are managed using the standard OS pkg command.

For Solaris 11, patches are applied as Support Repository Updates (SRU). Application of patches is performed by the infrastructure administrator of business servers. Systemwalker Software Configuration Manager collects and manages patch application status information from managed servers.

### Fujitsu middleware patches

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

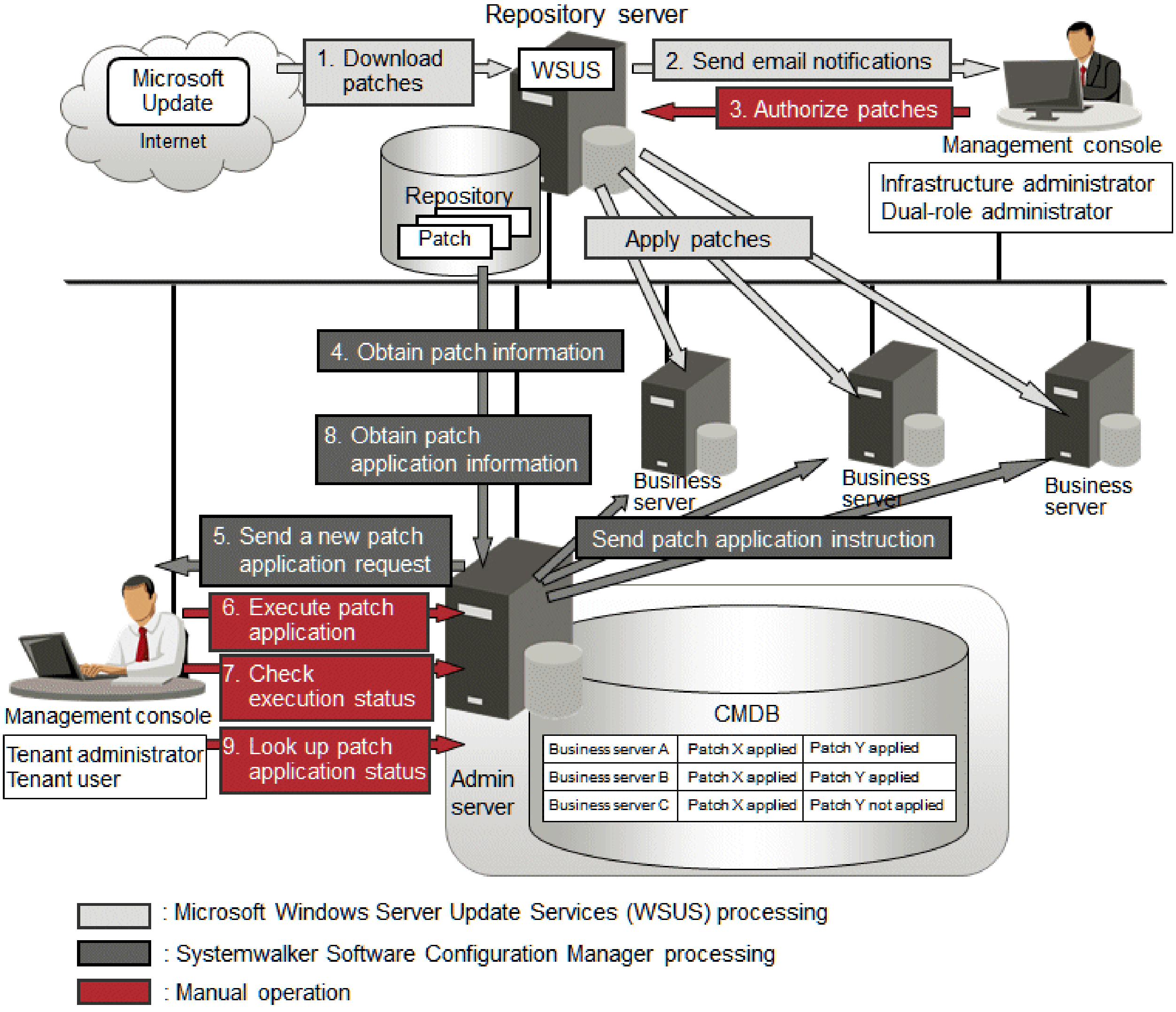
Acquisition of the latest patches from the UpdateSite and registration of the latest patches with Systemwalker Software Configuration Manager is performed by the infrastructure administrator, while Systemwalker Software Configuration Manager collects and manages patch application status information from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

It is also possible to distribute and apply update files to managed servers remotely from the management console for Systemwalker Software Configuration Manager. However, patch distribution and application to managed Solaris servers is not supported.

## 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


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

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

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

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

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

   By setting up the WSUS email notification function, 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.

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

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

   Infrastructure administrators can perform patch application using the command on the admin server.

   Point

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

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

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

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

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

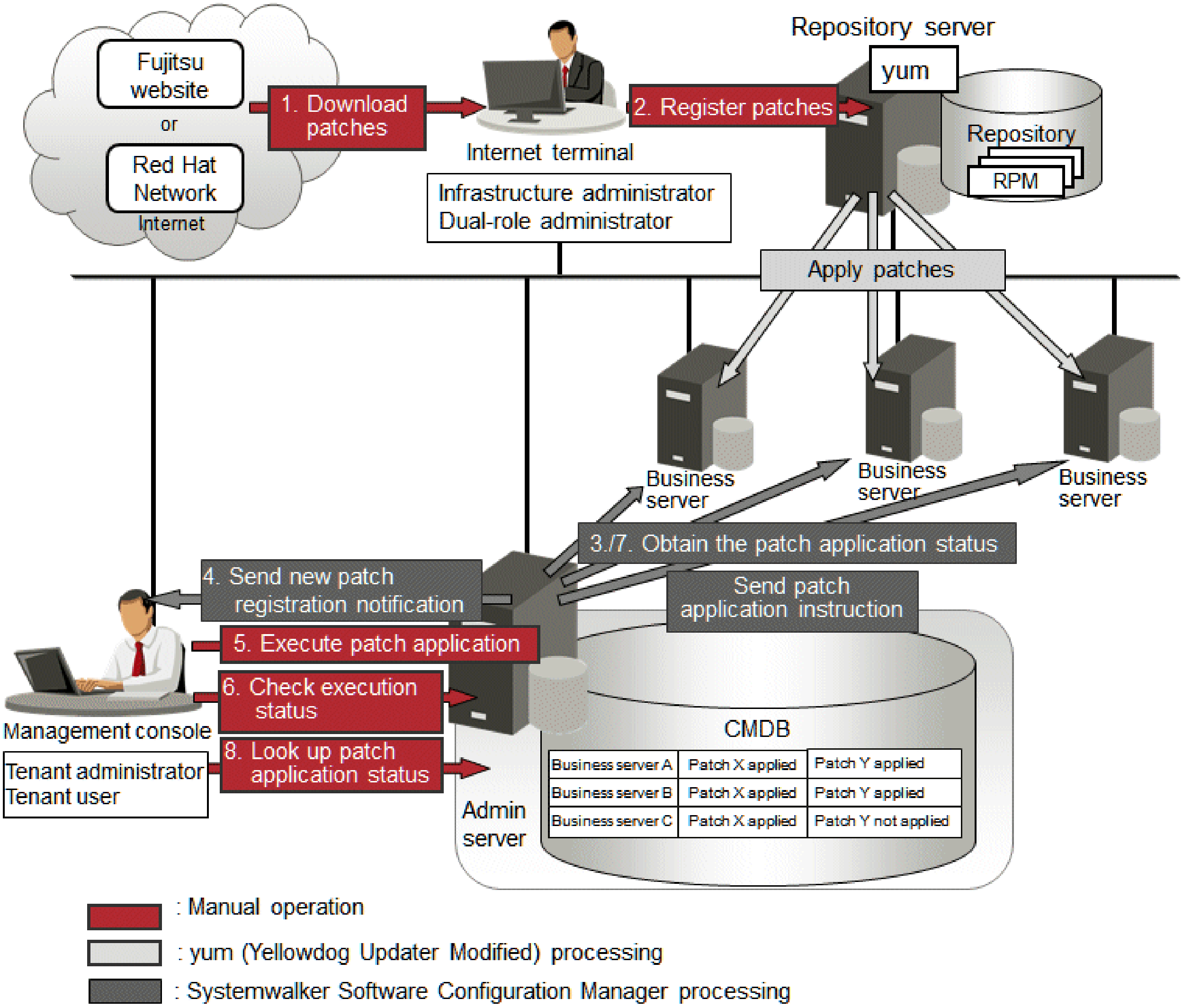
9. Look up patch application status

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

## 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


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

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

## Point

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

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

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

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

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

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

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

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

4. Send new patch registration 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 infrastructure administrator, the tenant user or the tenant administrator]**

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

   Infrastructure administrators can perform patch application using the command on the admin server.

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

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

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

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

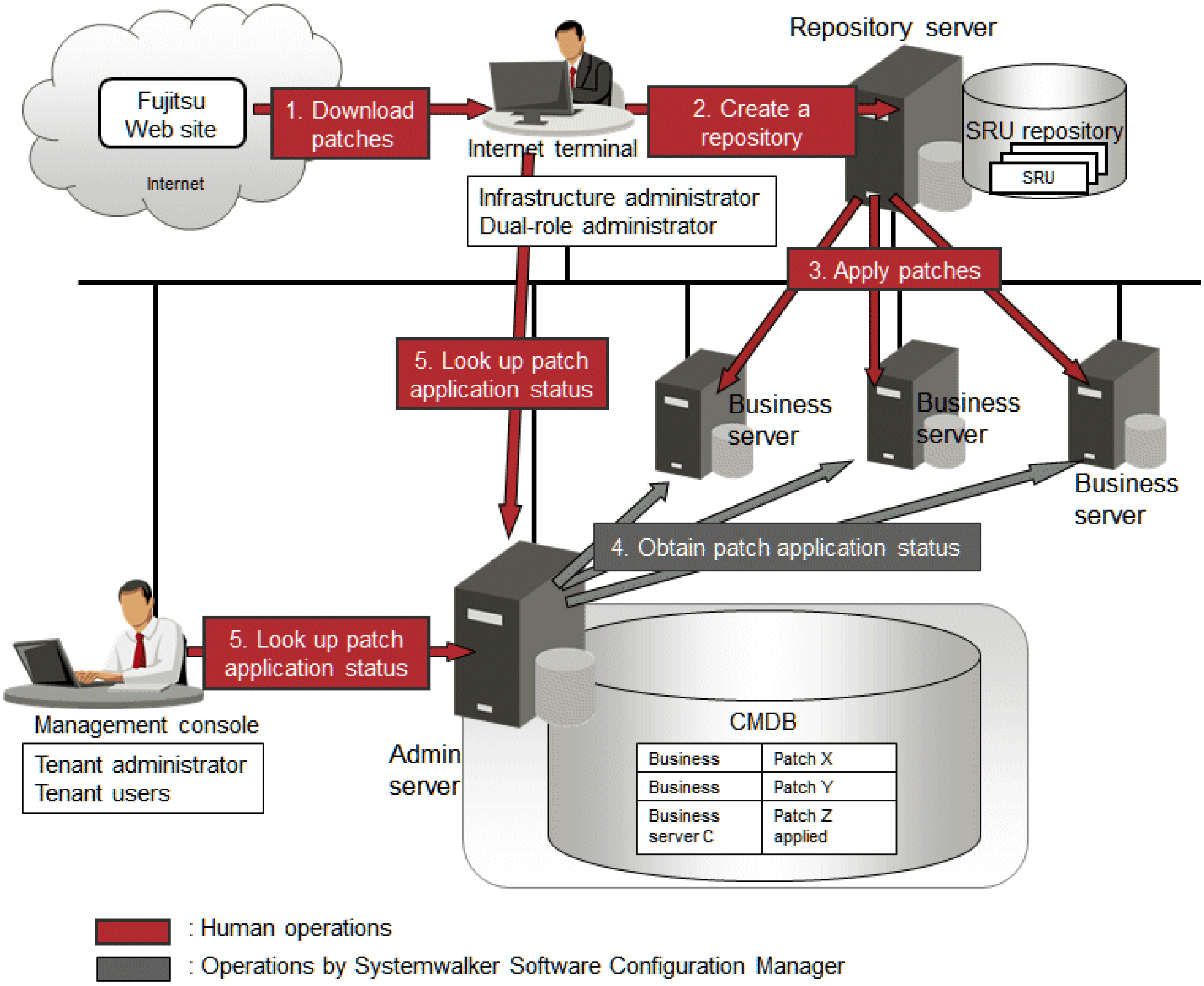
8. Look up patch application status

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

## 2.2.3 Solaris OS Patch Management

Patches for Solaris OS (Solaris 11) are managed using the standard OS pkg command. The following diagram shows the overall flow of Solaris OS patch management:

Figure 2.6 Overview of Solaris OS patch management



| | |
|---|---|
| Business | Patch X |
| Business | Patch Y |
| Business server C | Patch Z applied |

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

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

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

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

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

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

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

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

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

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

5. Look up patch application status

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

Information

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

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

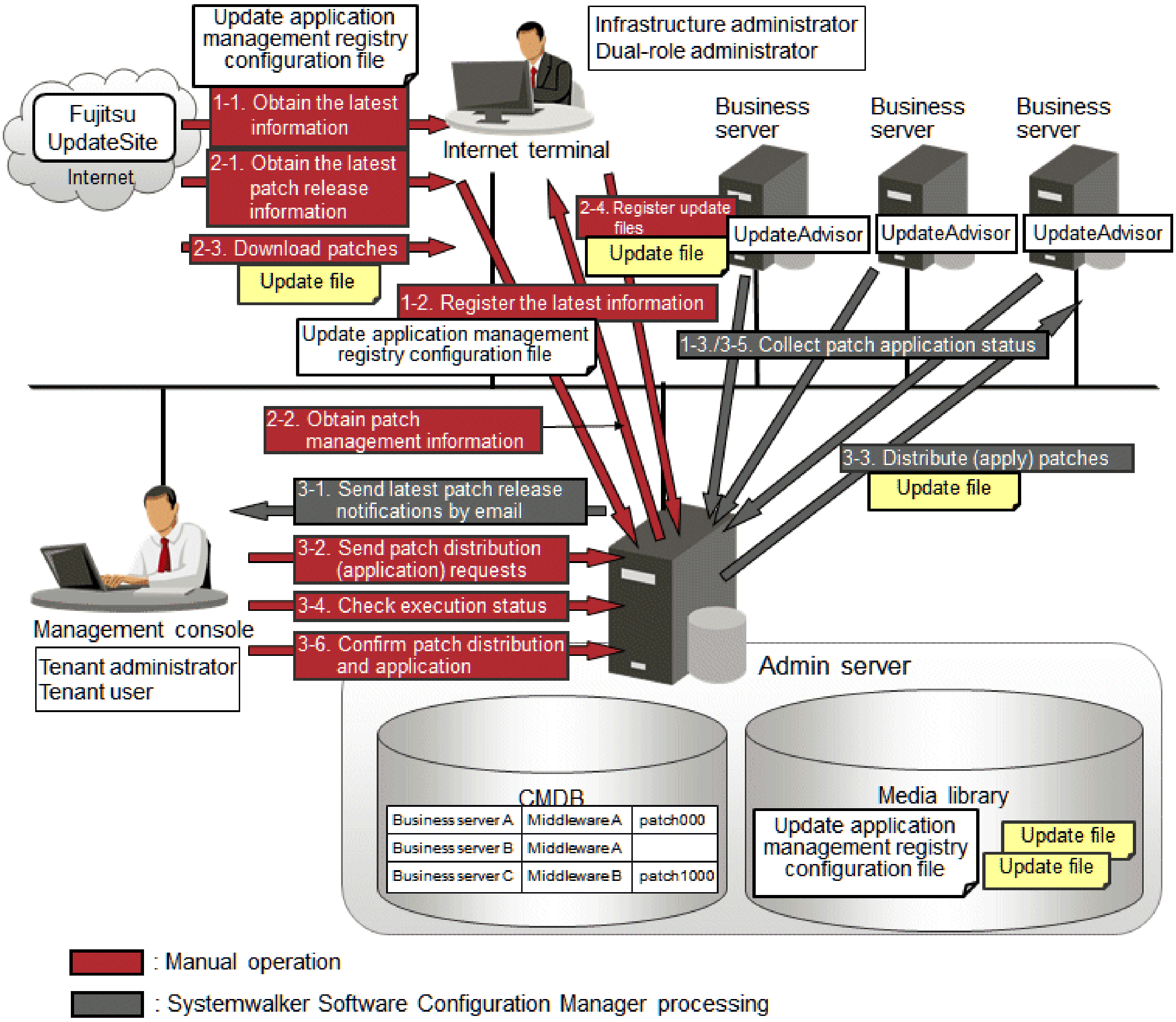
It is not possible to perform patch application, parameter setting, or script execution on Solaris servers.

### 2.2.4 Software Patch Management

Manage software patches. Software patch management is performed in coordination with the software (patch) management tools provided by the respective software vendors. In Systemwalker Software Configuration Manager, a coordinated software (patch) management tool is called an information collection source. For Fujitsu middleware, use UpdateAdvisor (middleware) as the information collection source. Patch management methods differ between Fujitsu middleware and other software. The following diagram shows the overall flow of Fujitsu middleware patch management:

### 2.2.4.1 Fujitsu Middleware Patch Management

Figure 2.7 Overview of Fujitsu middleware patch management


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

| | | |
|---|---|---|
| Business server A | Middleware A | patch000 |
| Business server B | Middleware A | |
| Business server C | Middleware B | patch1000 |

### Point

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

1. Obtain Fujitsu middleware information, and perform discovery

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

   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.

2. Obtain Fujitsu middleware patches

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

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

       The infrastructure administrator looks up email notifications from FSC-NEWS (SupportDesk customer notifications) and the UpdateSite (Fujitsu SupportDeskWeb) to obtain information about the latest patches.

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

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

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

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

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

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

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

3. Check the distribution and application of Fujitsu middleware patches

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

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

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

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

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

       Infrastructure administrators can perform patch application using the command on the admin server.

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

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

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

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

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

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

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

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

6. Confirm patch distribution/application

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

### 2.2.4.2 Patch Management for Software Other than Fujitsu Middleware

In order to manage patches for software other than Fujitsu middleware, obtain and register the latest software information and patch information as definitions. This enables comparison between the installed software information collected during discovery and the software definitions registered beforehand and comparison between applied patch information and patch definitions, making it possible to collect the software installation status and patch application status. Patch application can be performed using the configuration modification function.

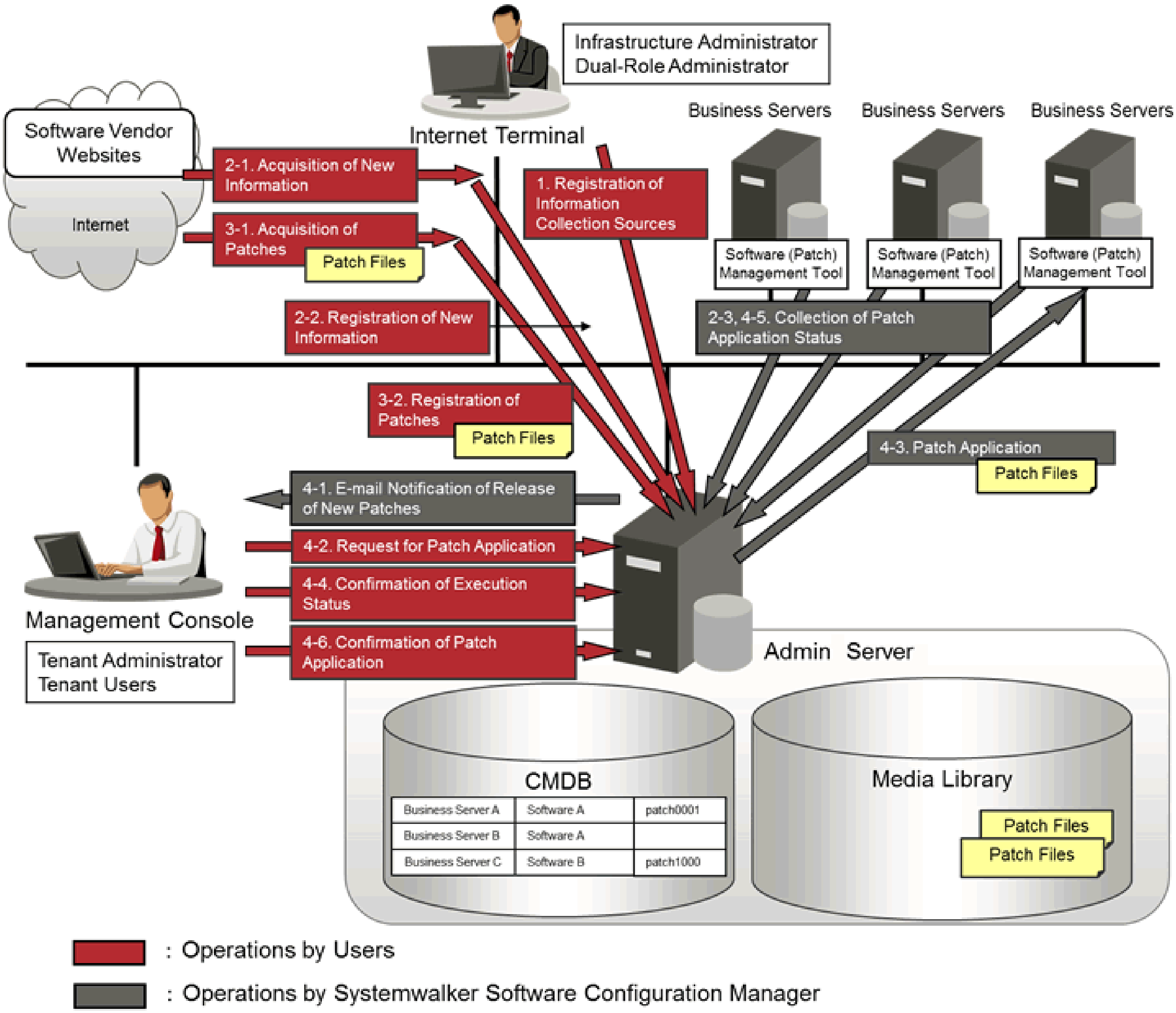
There are two ways to obtain the latest software information and patch information:

a. Obtain from the information released by the software vendor.

b. Use the installed software information and applied patch information that are collected from this server by the discovery function using a server with the latest patches already applied as a means of verification.

The overall flow of patch management is explained below for cases a and b, respectively.

Figure 2.8 Overview of Patch Management for Software Other than Fujitsu Middleware


Infrastructure Administrator
Dual-Role Administrator
Internet Terminal
Software Vendor Websites
Internet
2-1. Acquisition of New Information
3-1. Acquisition of Patches
Patch Files
1. Registration of Information Collection Sources
Business Servers
Business Servers
Business Servers
Software (Patch) Management Tool
Software (Patch) Management Tool
Software (Patch) Management Tool
2-2. Registration of New Information
2-3, 4-5. Collection of Patch Application Status
3-2. Registration of Patches
Patch Files
4-3. Patch Application
Patch Files
4-1. E-mail Notification of Release of New Patches
4-2. Request for Patch Application
4-4. Confirmation of Execution Status
4-6. Confirmation of Patch Application
Management Console
Tenant Administrator
Tenant Users
Admin Server
CMDB
Media Library
Patch Files
Patch Files

| | | |
|---|---|---|
| Business Server A | Software A | patch0001 |
| Business Server B | Software A | |
| Business Server C | Software B | patch1000 |

🟥 : Operations by Users

⬛ : Operations by Systemwalker Software Configuration Manager

1. Register information collection sources **[operation by the infrastructure administrator]**

   The infrastructure administrator defines coordinated software (patch) management tools as information collection sources. The definition of an information collection source includes scripts that collect installed software information and applied patch information from software (patch) management tools. Definitions of information collection sources can be registered using a command.

   This step is not necessary if using the information collection sources pre-registered in this product.

2. Obtain the latest software information and patch information

   Obtain the latest software information and patch information and collect the software installation status and patch application status. To collect the software installation status and patch application status, it is necessary to obtain the latest software information and patch information periodically during operation.

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

      a. The infrastructure administrator obtains the latest software and patch information from the information released by the respective software vendors.

      b. This step is not necessary.

   2. Register the latest information **[operation by the infrastructure administrator]**

      a. The infrastructure administrator registers the obtained software information and patch information using the command on the admin server.

b. This step is not necessary.

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

   Systemwalker Software Configuration Manager collects the software installation status and patch application status from each business server.

   For case b, when collecting patch application status information, include a server with the latest patches already applied in the target servers as a means of verification.

3. Download patches

   Obtain software patches through the information released by the respective software vendors and store them in the media library. Patches stored in the media library can be distributed and applied to the business servers.

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

      The infrastructure administrator obtains the latest software and patch information from the site or other information source published by the respective software vendors.

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

      The infrastructure administrator stores the obtained patches as assets in the media library by using the command on the admin server. In addition, the infrastructure administrator creates a configuration modification template by using the management console or the command on the admin server. In the configuration modification template, define the processes, parameters, and assets necessary for applying patches. Create the configuration modification template according to the manuals or other information provided by the software vendor.

4. Apply patches and confirm patch application

   Apply the patches that are stored in the media library.

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

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

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

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

      Infrastructure administrators can perform patch application using the command on the admin server.

   3. Apply patches **[processing by Systemwalker Software Configuration Manager]**

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

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

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

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

      Systemwalker Software Configuration Manager collects the software installation status and patch application status from each business server.

   6. Confirm patch application

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

## 2.3 Software Installation

Install software on managed servers. Software installation is performed using configuration modification. Only software that can be installed in silent mode can be installed. Collection of software installation statuses is performed in coordination with the software (patch) management tools provided by the respective software vendors. For details on software patch management, refer to "Software Patch Management" in the *Operation Guide*.

### Configuration Modification

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

- The Configuration Modification template that standardizes the processes necessary for changing software configuration information

- The media library that manages the files necessary for configuration modification as assets

The software installation flow is as shown below.

1. Collect the software installation status **[performed using Systemwalker Software Configuration Manager]**

   Systemwalker Software Configuration Manager collects the software installation status from each business server.

2. Register assets **[infrastructure administrator]**

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

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

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

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

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

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

5. Install the software **[process performed by Systemwalker Software Configuration Manager]**

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

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

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

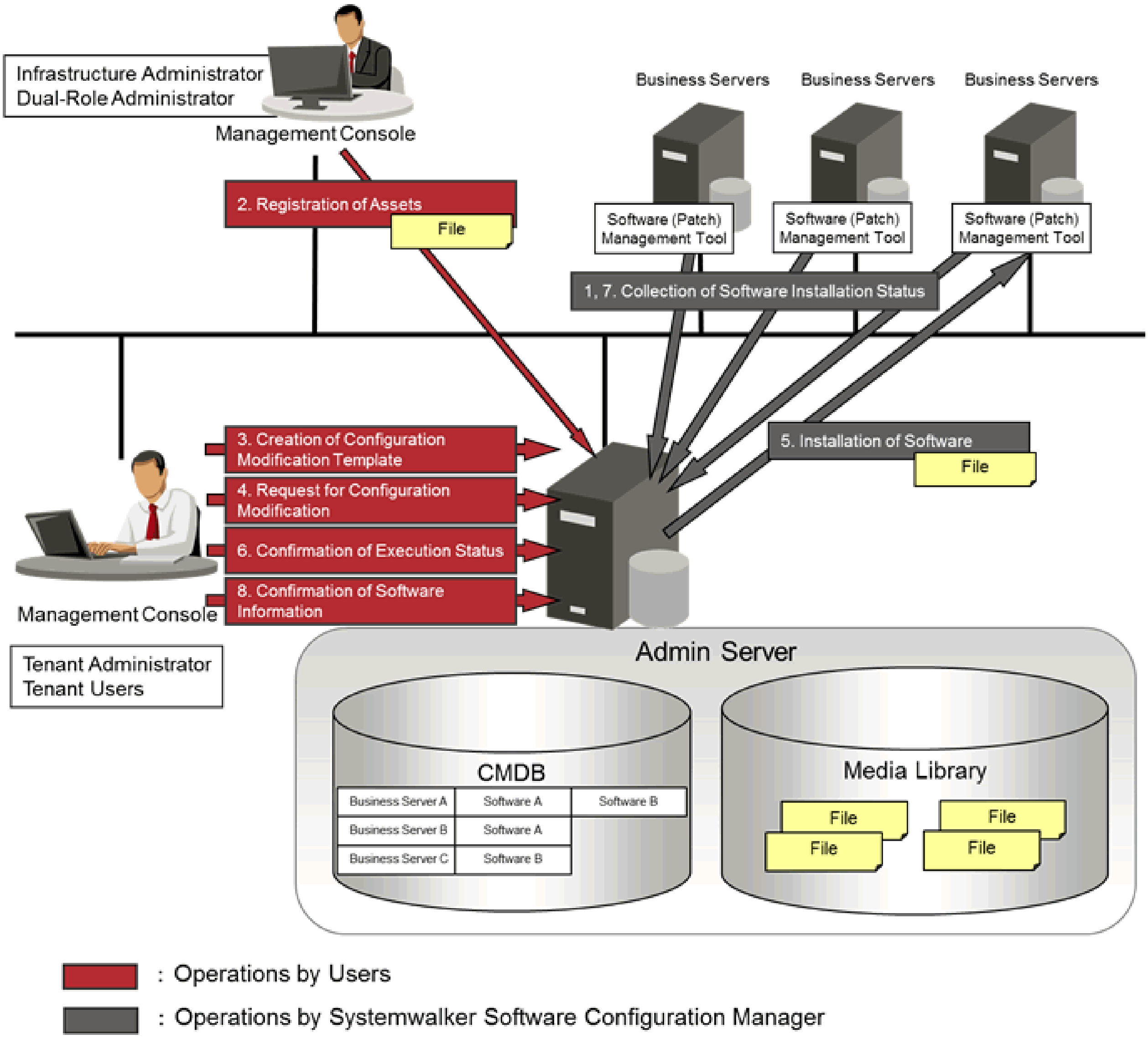
7. Collect the software installation status **[performed using Systemwalker Software Configuration Manager]**

   Systemwalker Software Configuration Manager collects the software installation status from each business server.

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

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

   Figure 2.9 Overview of software installation


Infrastructure Administrator
Dual-Role Administrator
Management Console
Business Servers
Business Servers
Business Servers
Software (Patch) Management Tool
Software (Patch) Management Tool
Software (Patch) Management Tool
2. Registration of Assets
File
1, 7. Collection of Software Installation Status
3. Creation of Configuration Modification Template
4. Request for Configuration Modification
6. Confirmation of Execution Status
8. Confirmation of Software Information
5. Installation of Software
File
Management Console
Tenant Administrator
Tenant Users
Admin Server
CMDB
Media Library
File
File
File
File

| | | |
|---|---|---|
| Business Server A | Software A | Software B |
| Business Server B | Software A | |
| Business Server C | Software B | |

🟥 : Operations by Users

⬛ : Operations by Systemwalker Software Configuration Manager

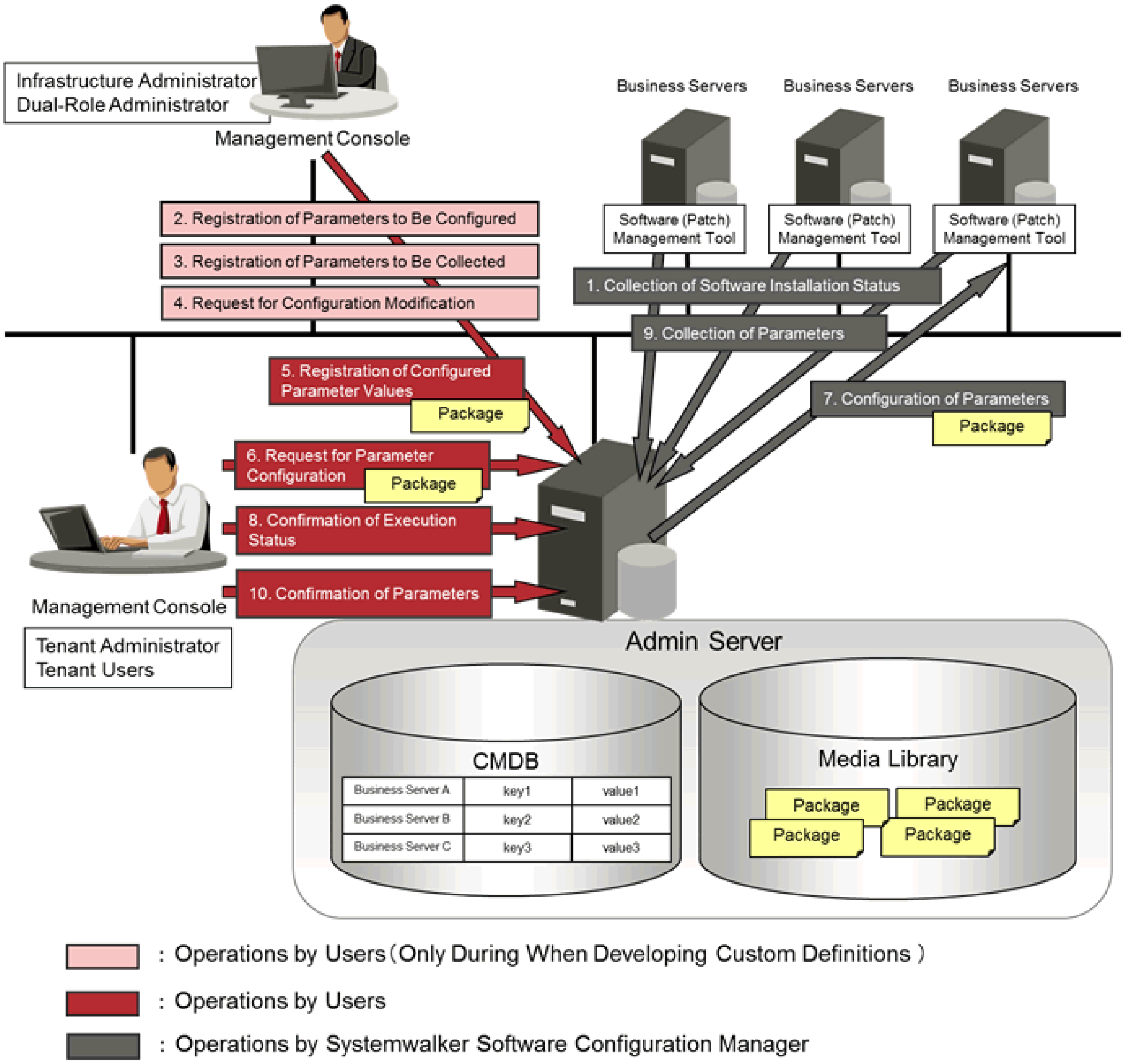
## 2.4 Software Parameter Management

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

Collection of software installation statuses is performed in coordination with the software (patch) management tools provided by the respective software vendors. For details on software patch management, refer to "Software Patch Management" in the *Operation Guide*.

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

Figure 2.10 Overview of Software Parameter Management


Infrastructure Administrator
Dual-Role Administrator
Management Console
Business Servers
Business Servers
Business Servers
Software (Patch) Management Tool
Software (Patch) Management Tool
Software (Patch) Management Tool
2. Registration of Parameters to Be Configured
3. Registration of Parameters to Be Collected
4. Request for Configuration Modification
1. Collection of Software Installation Status
9. Collection of Parameters
5. Registration of Configured Parameter Values
Package
7. Configuration of Parameters
Package
6. Request for Parameter Configuration
Package
8. Confirmation of Execution Status
10. Confirmation of Parameters
Management Console
Tenant Administrator
Tenant Users
Admin Server
CMDB
Business Server A
key1
value1
Business Server B
key2
value2
Business Server C
key3
value3
Media Library
Package
Package
Package
Package
🟥 : Operations by Users (Only During When Developing Custom Definitions )
🟥 : Operations by Users
⬛ : Operations by Systemwalker Software Configuration Manager

1. Collect the software installation status **[performed using Systemwalker Software Configuration Manager]**

   Systemwalker Software Configuration Manager collects the software installation status from each business server.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# 2.5 Configuration Management

## 2.5.1 Hardware/Virtual Environment Configuration Management

Discovery of hardware configuration information collects serial numbers of chassis, blade servers, rack mount servers, firmware versions, and CPU/memory information.

Discovery of virtual environment configuration information collects the host OS version, guest OS type, IP address, and CPU/memory information in VMware vSphere or OpenStack environments.

To manage hardware/virtual environment configuration management, perform the following operations.

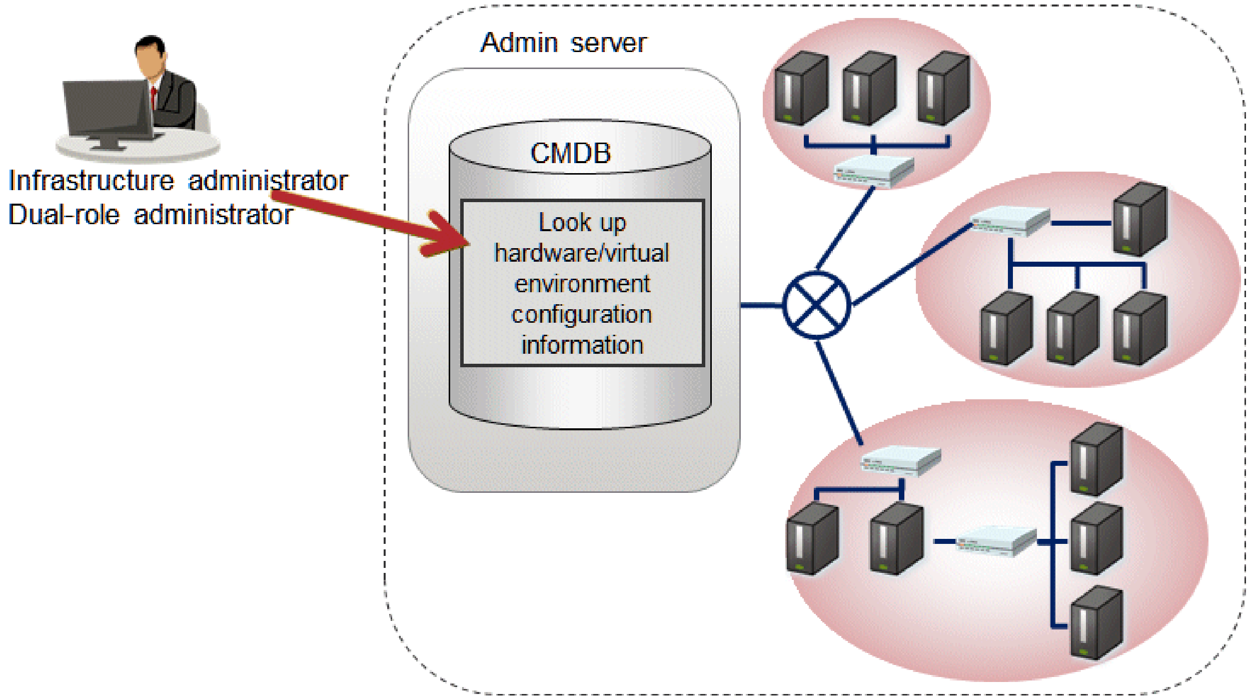
- Referencing the hardware/virtual configuration information

  The servers for which 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. It is also possible to display information that has been filtered by specifying particular conditions.

The following table shows the range within which each role can use hardware/virtual environment configuration management:

| Role | Usage range of hardware/virtual environment 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. |

Figure 2.11 Overview of hardware/virtual environment configuration management


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

## 2.5.2 Software Configuration Management

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

- Referencing 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.

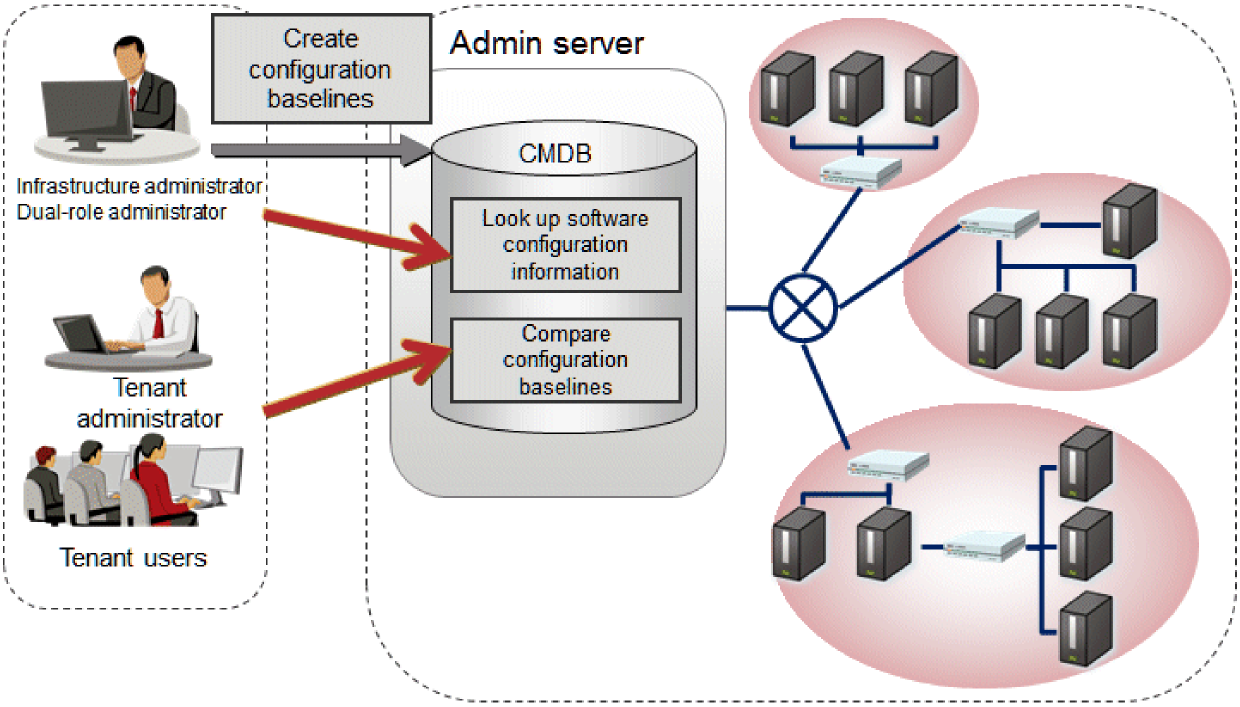
  If a problem occurs with a server, it is possible to check which patches have been applied since the server was last running correctly by comparing the current configuration baseline with the configuration baseline at the time when the server was running correctly.

  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 software 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 2.12 Overview of software configuration management


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

# Chapter 3 Operating Environment

This chapter explains the operating environment for this product.

## 3.1 Hardware Environments

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 1000/2000 series |
| CPU | Intel(R) Xeon(R) 3 GHz or higher |
| Number of CPUs | 2 or more |
| Memory capacity (excluding the operating system) | 8.0 GB or more |

See

Memory space for the CMDB manager

The size of the memory space for the CMDB manager increases as the number of managed business servers increases. Estimate the memory size based on the number of business servers. Refer to "Database and memory space for the CMDB manager" for details.

**Linkage server**

| Type of hardware | Requirements |
|---|---|
| CPU | Intel(R) Pentium 4 equivalent or higher |
| Memory capacity (excluding the operating system) | At least 1 GB |

**Business server**

| Type of hardware | Requirements |
|---|---|
| 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: 13.3 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

#### When linking to ServerView Resource Orchestrator

| 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

### Static disk capacity [Linux]

| Product name | Area used | Disk space required for installation |
|---|---|---|
| Systemwalker Software Configuration Manager | /opt | 3.2 GB or more |
| | /var | 9.2 GB or more |
| | /etc | 0.7 GB or more |

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

-/opt: 150 MB

### Dynamic disk capacity

#### Database and memory space for the CMDB manager

The amount of space for the database and memory for the CMDB manager increases as the number of managed business servers increases. Estimate the amount of space for the database and memory 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 |
| 1,000 | Approx. 2.6 GB (*1) | Approx. 3.6 GB |
| 1,500 | Approx. 3.7 GB (*1) | Approx. 4.8 GB |

*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.

#### Disk space for the media library

The following table indicates the recommended disk space for the media library:

| Area name | Disk space |
|---|---|
| Media library | Approximately 2.5 GB + Total asset size (*1) |

*1: Total size of all files managed as assets.

#### Database space for process management

A rough estimate of the database space required for process management can be calculated using the following formula:

| |
|---|
| Database space (rough estimate) = 1 MB x total number of automated operation processes (*1) |

*1: The total number of requests for patch application, patch distribution, parameter setting, script execution, or configuration modification. If this type of request is made to multiple servers at the same time, the number of servers is regarded as the number of requests.

**[Windows]**

Note

- Do not select **Compress drive to save disk space** on the drive where you will create the database space.

  This is because compressing the drive incurs higher performance overhead than normal I/O processing, leading to access errors, which are dependent on I/O capacity and are caused by insufficient operating system resources.

- Do not select the **Compress and Encrypt attributes** group box in the dialog box displayed when you click **Advanced** in the **General** tab for setting properties of the folder where you will create the database space.

  This is because, as with drive compression, setting the compression attribute incurs higher performance overhead than normal I/O processing, leading to access errors, which are dependent on I/O capacity and are caused by insufficient operating system resources.

  In addition, if the encryption attribute is set, encryption cannot be disabled and access errors occur because the user who controls the database space is different from users used with Systemwalker Software Configuration Manager.

### 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] [Solaris]**

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

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

-/opt: 150 MB

## 3.2 Software Environments

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

## 3.2.1 Operating Systems for Managing Patches and Software Configuration

This section lists the operating systems supported for managing patches and software configuration.

### Admin server

- Windows Server 2012 (for x64)
- Windows Server 2012 R2 (for x64)
- Red Hat Enterprise Linux 6 (for Intel64)
- Red Hat Enterprise Linux 7

### Linkage server (32-bit agent)

- Windows Server 2012 (for x64) (*1)
- Windows Server 2012 R2 (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 2012 R2 (for x64)
- Windows Server 2008 (for x64)
- Windows Server 2008 R2

### Business server (32-bit agent)

- Windows Server 2012 (for x64) (*1)
- Windows Server 2012 R2 (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 Intel64) (*2)
- Red Hat Enterprise Linux 6 (for x86)
- Red Hat Enterprise Linux 6 (for Intel64) (*2)

### Business server (64-bit agent)

- Windows Server 2012 (for x64)
- Windows Server 2012 R2 (for x64)
- Windows Server 2008 (for x64)

- Windows Server 2008 R2
- Red Hat Enterprise Linux 5 (for Intel64)
- Red Hat Enterprise Linux 6 (for Intel64)
- Red Hat Enterprise Linux 7

### Business server (Solaris agent)

- Oracle Solaris 11

*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 Software Installation and Software Parameter Management

This section lists the operating systems supported by this product for installing software and managing software parameters.

The supported operating systems may differ depending on the software. Refer to *Parameter Reference* for information on the supported operating systems for each software product.

### Admin server

- Windows Server 2012 (for x64)
- Windows Server 2012 R2 (for x64)
- Red Hat Enterprise Linux 6 (for Intel64)
- Red Hat Enterprise Linux 7

### Business server (32-bit agent)

- Windows Server 2012 (for x64) (*1)
- Windows Server 2012 R2 (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 Intel64) (*2)
- Red Hat Enterprise Linux 6 (for x86)
- Red Hat Enterprise Linux 6 (for Intel64) (*2)

### Business server (64-bit agent)

- Windows Server 2012 (for x64)
- Windows Server 2012 R2 (for x64)
- Windows Server 2008 (for x64)

- Windows Server 2008 R2
- Red Hat Enterprise Linux 5 (for Intel64)
- Red Hat Enterprise Linux 6 (for Intel64)
- Red Hat Enterprise Linux 7

#### Business server (Solaris agent)

- Oracle Solaris 11 (*3)

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

*2: Runs in the 32-bit compatible mode

*3: Software parameter management cannot be performed for Oracle Solaris 11.

### 3.2.3 Operating Systems for Managing Hardware/Virtual Environment Configuration

This section lists the operating systems supported for managing hardware and virtual environment configuration.

#### Admin server

- Windows Server 2012 (for x64)
- Windows Server 2012 R2 (for x64)
- Red Hat Enterprise Linux 6 (for Intel64)
- Red Hat Enterprise Linux 7

### 3.2.4 System Configuration for Performing OpenStack Coordination

This section lists the operating systems supported by this product for managing business servers deployed by OpenStack.

#### Admin server

- Red Hat Enterprise Linux 6 (for Intel64)
- Red Hat Enterprise Linux 7

#### Business server (32-bit agent)

- Red Hat Enterprise Linux 5 (for x86)
- Red Hat Enterprise Linux 5 (for Intel64) (*1)
- Red Hat Enterprise Linux 6 (for x86)
- Red Hat Enterprise Linux 6 (for Intel64) (*1)

*1: Runs in the 32-bit compatible mode

#### Business server (64-bit agent)

- Red Hat Enterprise Linux 5 (for Intel64)
- Red Hat Enterprise Linux 6 (for Intel64)
- Red Hat Enterprise Linux 7

## 3.2.5 Mandatory Software

This section lists mandatory software.

### Admin server

- ServerView Operations Manager V6.0 or later except following versions.

  **[Windows]**

  V7.11.04 to V7.11.06

  **[Linux]**

  V7.11.04 to V7.11.07

  This software is required for Single Sign-On.

### Web client

- Internet Explorer 9, 10, 11, or Microsoft Edge
- Adobe Reader XI or Adobe Acrobat Reader DC (required to view PDF manuals)

Note

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

### Business server

- VMware Tools must be installed on the guest OS on ESXi (required for managing hardware and virtual environment configurations)

### 3.2.5.1 Mandatory Software for Linux

### Admin server

For Red Hat Enterprise Linux 6.0 or later, the following software, which comes with the operating system, is required.

Red Hat Enterprise Linux 6.0 (for Intel64)

- alsa-lib package (64-bit version)
- apr package (32-bit version)
- apr-util package (32-bit version)
- cloog-ppl package (64-bit version)
- compat-expat1 package (32-bit version)
- compat-openldap package (32-bit version)
- cpp package (64-bit version)
- cyrus-sasl-lib package (32-bit version)
- db4 package (32-bit version)
- expat package (32-bit version)
- file package (64-bit version)
- gcc package (64-bit version)
- gcc-c++ package (64-bit version)
- gdb package (64-bit version)
- glibc package (32-bit version)

- glibc package (64-bit versions)
- glibc-devel package (64-bit version)
- glibc-headers package (64-bit version)
- kernel-headers package (64-bit version)
- keyutils-libs package (32-bit version)
- krb5-libs package (32-bit version)
- libICE package (64-bit version)
- libSM package (64-bit version)
- libX11 package (64-bit version)
- libX11-common package
- libXau package (64-bit version)
- libXext package (64-bit version)
- libXi package (64-bit version)
- libXp package (64-bit version)
- libXrender package (64-bit versions)
- libXt package (64-bit version)
- libXtst package (64-bit version)
- libattr package (32-bit version)
- libcap package (32-bit version)
- libgcc package (32-bit version)
- libgomp package (64-bit version)
- libselinux package (32-bit version)
- libstdc++ package (32-bit version)
- libstdc++-devel package (64-bit version)
- libtool-ltdl package (64-bit version)
- libuuid package (32-bit version)
- libxcb package (64-bit version)
- lksctp-tools package (64-bit versions)
- make package (64-bit version)
- mpfr package (64-bit version)
- ncurses-libs package (64-bit versions)
- net-snmp package (64-bit version)
- net-snmp-utils package (64-bit version)
- nss-softokn-freebl package (32-bit version)
- nss-softokn-freebl package (64-bit versions)
- openssl package (32-bit version)
- openssl098e package (32-bit versions)
- perl package (64-bit version)

- perl-Module-Pluggable package (64-bit version)
- perl-Pod-Escapes package (64-bit version)
- perl-Pod-Simple package (64-bit version)
- perl-libs package (64-bit version)
- perl-version package (64-bit version)
- ppl package (64-bit version)
- redhat-lsb package (64-bit version)
- strace package (64-bit version)
- sysstat package (64-bit version)
- tcsh package (64-bit version)
- unixODBC package (64-bit version)
- zlib package (32-bit version)
- zlib package (64-bit versions)

For Red Hat Enterprise Linux 7.0 or later, the following software, which comes with the operating system, is required.

Red Hat Enterprise Linux 7.0 or later

- apr package (32-bit version)
- apr-util package (32-bit version)
- compat-openldap package (32-bit version)
- cpp package (64-bit version)
- cyrus-sasl-lib package (32-bit version)
- expat package (32-bit version)
- gcc package (64-bit version)
- gcc-c++ package (64-bit version)
- glibc package (32-bit version)
- glibc package (64-bit version)
- glibc-devel package (64-bit version)
- glibc-headers package (64-bit version)
- kernel-headers package (64-bit version)
- keyutils-libs package (32-bit version)
- krb5-libs package (32-bit version)
- libICE package (64-bit version)
- libSM package (64-bit version)
- libX11 package (64-bit version)
- libX11-common package
- libXau package (64-bit version)
- libXext package (64-bit version)
- libXi package (64-bit version)

- libXp package (64-bit version)
- libXrender package (64-bit version)
- libXt package (64-bit version)
- libXtst package (64-bit version)
- libattr package (32-bit version)
- libcap package (32-bit version)
- libdb package (32-bit version)
- libgcc package (32-bit version)
- libselinux package (32-bit version)
- libstdc++ package (32-bit version)
- libstdc++-devel package (64-bit version)
- libtool-ltdl package (64-bit version)
- libuuid package (32-bit version)
- libxcb package (64-bit version)
- lksctp-tools package (64-bit version)
- mpfr package (64-bit version)
- ncurses-libs package (64-bit version)
- net-snmp package (64-bit version)
- net-snmp-utils package (64-bit version)
- nss-softokn-freebl package (32-bit version)
- nss-softokn-freebl package (64-bit version)
- openssl package (64-bit version)
- openssl-libs package (32-bit version)
- openssl098e package (32-bit version)
- perl package (64-bit version)
- perl-Module-Pluggable package (64-bit version)
- perl-Pod-Escapes package (64-bit version)
- perl-Pod-Simple package (64-bit version)
- perl-libs package (64-bit version)
- perl-version package (64-bit version)
- redhat-lsb package (64-bit version)
- strace package (64-bit version)
- sysstat package (64-bit version)
- tcsh package (64-bit version)
- unixODBC package (64-bit version)
- zlib package (32-bit version)
- zlib package (64-bit version)

### Business server

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

- redhat-lsb package
- unzip package

For installations in Red Hat Enterprise Linux 6 (for Intel64) or Red Hat Enterprise Linux 7 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

## 3.2.6 Related Software

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

### Admin server

- ServerView Resource Orchestrator V3.2 Cloud Edition

  This software is required to manage business servers deployed by ServerView Resource Orchestrator.

  Note

  If Systemwalker Software Configuration Manager is linked to ServerView Resource Orchestrator, uninstall Systemwalker Software Configuration Manager before performing the following tasks:

  - Upgrading ServerView Resource Orchestrator
  - Uninstalling ServerView Resource Orchestrator

  Note

  For the authentication method for ServerView Resource Orchestrator, use ServerView Single Sign-On (SSO). If the internal authentication system is used for authentication, ServerView Resource Orchestrator cannot coordinate with Systemwalker Configuration Manager.

### Linkage server

- Microsoft Windows Server Update Services (WSUS)

  This software is required to manage Windows patches.

  The following versions/levels of WSUS are supported:

  - Microsoft Windows Server Update Services (WSUS) 3.0 SP2
  - Microsoft Windows Server Update Services (WSUS) 4.0

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.

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 standard yum provided by RHEL5, RHEL6, and RHEL7 can be used.

  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)

- pkg command/entire package

  Required for Solaris OS patch management.

  pkg command/entire package is pre-installed on Solaris 11 by default.

  Obtain entire package information using the pkg command to obtain the SRU (Support Repository Updates) already applied to business servers.

- 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 software such as Fujitsu middleware and Linux operating systems, or to collect software information, prepare an "Internet terminal" (a terminal that can connect to the Internet).

Use Windows Vista, Windows 7, Windows 8.1, or Windows 10 as the operating system for an Internet terminal.

### OpenStack admin server

The following software is required to manage business servers deployed by OpenStack:

- Red Hat Enterprise Linux OpenStack Platform 6
- Red Hat Enterprise Linux OpenStack Platform 7
- Red Hat Enterprise Linux OpenStack Platform 8
- FUJITSU Integrated System PRIMEFLEX for Cloud K5 model

### Public cloud

Systemwalker Software Configuration Manager can manage servers on the following public cloud environment:

- FUJITSU Cloud Service K5

Note

**Notes on public cloud environments**

Take note of the following:

- This product does not support functions for configuration management of hardware and virtual environments.
- This product does not support the following operating systems:
    - Admin server
        - All OS types
    - Business servers
        - Red Hat Enterprise Linux 5 (for x86)
        - Red Hat Enterprise Linux 5 (for Intel64)
        - Oracle Solaris 11
- To manage business servers in a public cloud environment using an admin server in an on-premises or private cloud environment, a virtual private network (VPN) connection is required.

## 3.2.7 Conflicting Software

The following table lists software that conflicts with this product.

### Admin server

The Systemwalker Software Configuration Manager admin server cannot coexist with the following software:

**[Windows]**

| Product | V/L |
|---|---|
| Cloud Services Management | V1.0.0 |
| Systemwalker Runbook Automation (Management Server) | Cannot coexist with V15.1.3 or earlier |
| Systemwalker Runbook Automation (Linkage Server/Relay Server) | Cannot coexist with V15.1.3 or earlier |
| Systemwalker Runbook Automation (Business Server) | Cannot coexist with V15.1.3 or earlier |

| Product | V/L |
|---|---|
| Systemwalker Software Configuration Manager (linkage server) | Cannot coexist with any version |
| Systemwalker Software Configuration Manager (business server) | Cannot coexist with any version |
| Cloud infrastructure management software | Cannot coexist with any version |

**[Linux]**

| Product | V/L |
|---|---|
| Systemwalker Runbook Automation (Management Server) | Cannot coexist with V15.1.3 or earlier |
| Systemwalker Runbook Automation (Linkage Server/Relay Server) | Cannot coexist with V15.1.3 or earlier |
| Systemwalker Runbook Automation (Business Server) | Cannot coexist with V15.1.3 or earlier |
| Systemwalker Software Configuration Manager (linkage server) | Cannot coexist with any version |
| Systemwalker Software Configuration Manager (business server) | Cannot coexist with any version |
| Cloud infrastructure management software | Cannot coexist with any version |

## Linkage server

The Systemwalker Software Configuration Manager linkage server cannot coexist with the following software:

| Product | V/L |
|---|---|
| Cloud Services Management | V1.0.0 |
| Systemwalker Runbook Automation (Management Server) | Cannot coexist with V15.1.3 or earlier |
| Systemwalker Runbook Automation (Linkage Server/Relay Server) | Cannot coexist with V15.1.3 or earlier |
| Systemwalker Runbook Automation (Business Server) | Cannot coexist with V15.1.3 or earlier |
| Systemwalker Software Configuration Manager (admin server) | Cannot coexist with any version |
| Systemwalker Software Configuration Manager (business server) | Cannot coexist with any version |

## Business server

The Systemwalker Software Configuration Manager business server cannot coexist with the following software:

| Product | V/L |
|---|---|
| Cloud Services Management | V1.0.0 |
| Systemwalker Runbook Automation (Management Server) | Cannot coexist with V15.1.3 or earlier |
| Systemwalker Runbook Automation (Linked Server/Relay Server) | Cannot coexist with V15.1.3 or earlier |
| Systemwalker Runbook Automation (Business Server) | Cannot coexist with V15.1.3 or earlier |
| Systemwalker Software Configuration Manager (admin server) | Cannot coexist with any version |

| Product | V/L |
|---|---|
| Systemwalker Software Configuration Manager (linkage server) | Cannot coexist with any version |

# 3.3 Virtual Environments

This section explains the points to consider when operating this product in a virtual environment.

## Admin server

Operation of the admin server is supported in the following virtual environments:

- VMware vSphere 4 ESX 4.0/4.1 and ESXi 4.1
- VMware vSphere 5 ESXi 5.0/5.1/5.5
- VMware vSphere 6 ESXi 6.0
- Hyper-V
- Linux virtual machine function

Note

**Notes common for all virtual environments**

- When a problem occurs, support is provided under the condition that it is reproducible in a physical environment (outside of a virtual environment). For this reason, reproduction of the problem in a physical environment may be requested.
- Cloning cannot be used on the admin server.

**For VMware**

- VMware vMotion can be used only when communication processing (discovery, parameter setting, and deployment and application of patches) is not performed on managed servers.
- When switchover occurs using the HA function of VMware during an operation (discovery, parameter setting, and deployment and application of patches), the operation may need to be performed again after the switchover.
- When switchover occurs using the DR function of VMware, the states which were affected by operations (discovery, definitions, operation information) between the creation of the last backup and occurrence of the disaster are restored to the states at the time when the last backup was created. In addition, operations are not possible when the host name or IP address is not taken over.

**For Hyper-V**

- The Live Migration and Quick Migration functions of Hyper-V can be used only when communication processing (discovery, parameter setting, and deployment and application of patches) is not performed on managed servers.
- When switchover occurs using the replication function of Hyper-V, the states which were affected by operations (discovery, definitions, operation information) between the creation of the last backup and occurrence of the disaster are restored to the states at the time when the last backup was created. In addition, operations are not possible when the host name or IP address is not taken over.
- The import and export functions of Hyper-V do not work when the host name or IP address is not taken over.
- When switchover occurs using the failover function of VMware during an operation (discovery, parameter setting, and deployment and application of patches), the operation may need to be performed again after the switchover.

## Linkage servers and business servers

Operation of linkage servers and business servers are supported in the following environments:

- VMware vSphere 4 ESX 4.0/4.1 and ESXi 4.1

- VMware vSphere 5 ESXi 5.0/5.1/5.5
- VMware vSphere 6 ESXi 6.0
- Hyper-V
- Linux virtual machine function

Note

**Notes common for all virtual environments**

- When a problem occurs, support is provided under the condition that it is reproducible in a physical environment (outside of a virtual environment). For this reason, reproduction of the problem in a physical environment may be requested.

**For VMware**

- VMware vMotion can be used only when communication processing (discovery, parameter setting, and deployment and application of patches) is not performed on managed servers.
- When switchover occurs using the HA function of VMware during an operation (discovery, parameter setting, and deployment and application of patches), the operation may need to be performed again after the switchover.
- When switchover occurs using the DR function of VMware, the states which were affected by operations (discovery, definitions, operation information) between the creation of the last backup and occurrence of the disaster are restored to the states at the time when the last backup was created. In addition, operations are not possible when the host name or IP address is not taken over.

**For Hyper-V**

- The Live Migration and Quick Migration functions of Hyper-V can be used only when communication processing (discovery, parameter setting, and deployment and application of patches) is not performed on managed servers.
- When switchover occurs using the replication function of Hyper-V, the states which were affected by operations (discovery, definitions, operation information) between the creation of the last backup and occurrence of the disaster are restored to the states at the time when the last backup was created. In addition, operations are not possible when the host name or IP address is not taken over.
- When switchover occurs using the failover function of VMware during an operation (discovery, parameter setting, and deployment and application of patches), the operation may need to be performed again after the switchover.

## 3.4 Hardware and Hypervisor Supported for Configuration Management of Hardware/Virtual Environment

Hardware supported for hardware configuration management is as follows.

Table 3.1 Hardware supported for hardware configuration management (chassis, blade servers)

| Device | Attribute name | Management blade | | | Server blade | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | BX600 S2/S3 | BX900 S1/S2 | BX400 S1 | BX620 S3/S4 | BX620 S5/S6 | BX920 S1 - S4 | BX922 S2 | BX924 S2 - S4 | BX960 S1 |
| Chassis body | Product name | Y | Y | Y | - | - | - | - | - | - |
| | Serial number | Y | Y | Y | - | - | - | - | - | - |
| | Firmware version | - | Y | - | - | - | - | - | - | - |
| Blade server | Slot number | - | - | - | Y | Y | Y | Y | Y | Y |
| | Vendor name | - | - | - | Y | Y | Y | Y | Y | Y |
| | Product name | - | - | - | Y | Y | Y | Y | Y | Y |

| Device | Attribute name | Management blade | | | Server blade | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | BX600 S2/S3 | BX900 S1/S2 | BX400 S1 | BX620 S3/S4 | BX620 S5/S6 | BX920 S1 - S4 | BX922 S2 | BX924 S2 - S4 | BX960 S1 |
| | Serial number | - | - | - | Y | Y | Y | Y | Y | Y |
| | CPU Type | - | - | - | Y | Y | Y | Y | Y | Y |
| | Frequency | - | - | - | Y | Y | Y | Y | Y | Y |
| | Quantity | - | - | - | Y | Y | Y | Y | Y | Y |
| | Memory size | - | - | - | Y | Y | Y | Y | Y | Y |
| | Firmware version | - | - | - | - | - | Y | Y | Y | Y |
| | BIOS version | - | - | - | - | - | Y | Y | Y | Y |
| | OS name | - | - | - | Y (*1) | Y (*1) | Y (*1) | Y (*1) | Y (*1) | Y (*1) |

Y: Target of discovery.

-: Not target of discovery.

*1: When the version of the mounted hypervisor is VMware vSphere ESXi 5.1 or later, discovery can be performed.

Table 3.2 Hardware supported for hardware configuration management (rack mount servers)

| Device | Attribute name | Target of discovery |
|---|---|---|
| Fujitsu PRIMERGY RX100/ RX200/RX300 S6 or later,RX1330/RX2520/RX2540 M1 or later<br>IBM System x3550 M4<br>HP ProLiant DL320e Gen8 v2 | Vendor name | Y |
| | Product name | Y |
| | Serial number | Y |
| | CPU Type | Y(*1) |
| | Frequency | Y(*2) |
| | Quantity | Y |
| | Memory size | Y |
| | OS name | Y(*3) |

Y: Target of discovery.

*1: On PRIMERGY RX100/RX200/RX300 S6 the CPU type cannot be discovered.

*2: On IBM servers and HP servers, the frequency cannot be discovered.

*3: Discovery can only be performed when the version of the mounted hypervisor is VMware vSphere ESXi 5.1 or later.

The following diagram illustrates the hypervisors for which virtual environment configuration can be managed.

Table 3.3 Hypervisor supported for virtual environment configuration management

| Hypervisor | Type | Item | Target of discovery |
|---|---|---|---|
| VMware vSphere ESXi5.1 or later | VM host information | OS name | Y |
| | | CPU core count | Y |
| | | MAC address | Y |
| | | IP address | Y |
| | VM guest information | Virtual machine name | Y |

| Hypervisor | Type | Item | Target of discovery |
|---|---|---|---|
| | | OS name | Y |
| | | CPU core count | Y |
| | | Frequency | Y |
| | | Memory size | Y |
| | | MAC address | Y |
| | | IP address | Y |

Y: Target of discovery.

## 3.5 Advisory Notes

This section explains the points to consider regarding this product.

### Operations in IPv6 environments

IPv6 may be used when connecting to the management console from a web browser.

IPv4 must be used for management-related communications such as the discovery function.

### Character encoding

This product does not support JIS2004 (JIS X 0213:2004).